Referenz Und Support

Data Infrastructure Insights

NetApp
October 08, 2025

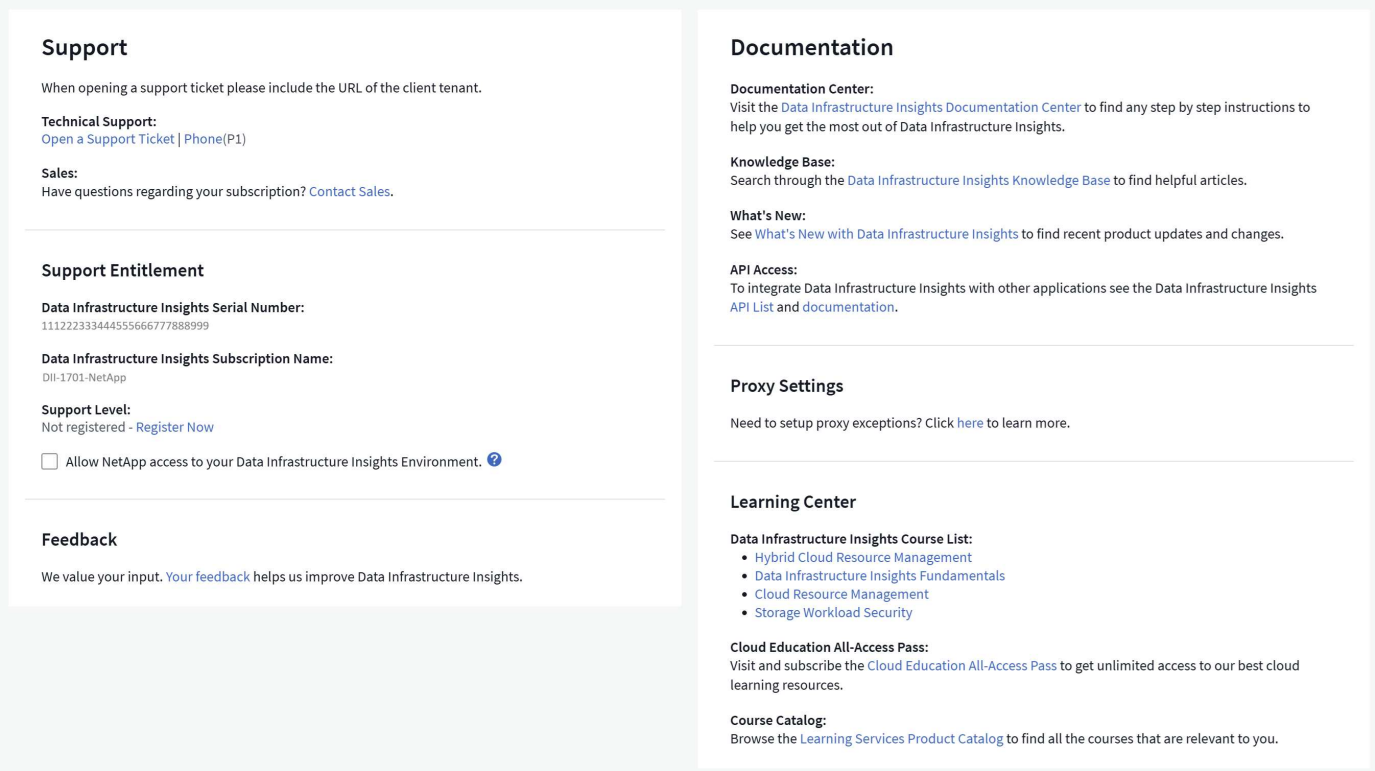
This PDF was generated from https://docs.netapp.com/de-de/data-infrastructure-insights/concept_requesting_support.html on October 08, 2025. Always check docs.netapp.com for the latest.

Inhalt

Referenz Und Support

Support Wird Angefordert

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



Aktivieren der Supportberechtigung

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. SehenDetails unten.

Während des ersten Abonnements generiert Ihre Data Infrastructure Insights Instanz eine 20-stellige NetApp-Seriennummer, die mit „950“ beginnt. Diese NetApp Seriennummer steht für das Abonnement von Data Infrastructure Insights, das Ihrem Konto zugeordnet ist. Sie müssen die NetApp Seriennummer registrieren, um die Support-Berechtigung zu aktivieren. Wir bieten zwei Optionen für die Support-Registrierung:

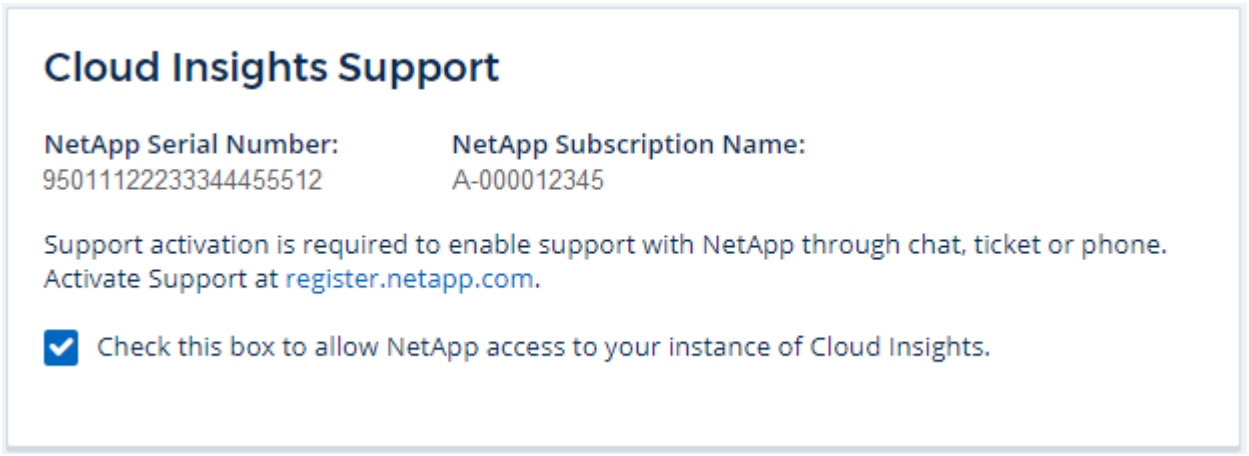
1. Benutzer mit vorvorhandenem NetApp Support Site (NSS) SSO-Konto (z. B. aktueller NetApp Kunde)
2. Neuer NetApp Kunde ohne vorbestehendes NSS SSO-Konto (NetApp Support Site

Option 1: Schritte für einen Benutzer mit einem zuvor bestehenden NSS SSO-Konto (NetApp Support Site

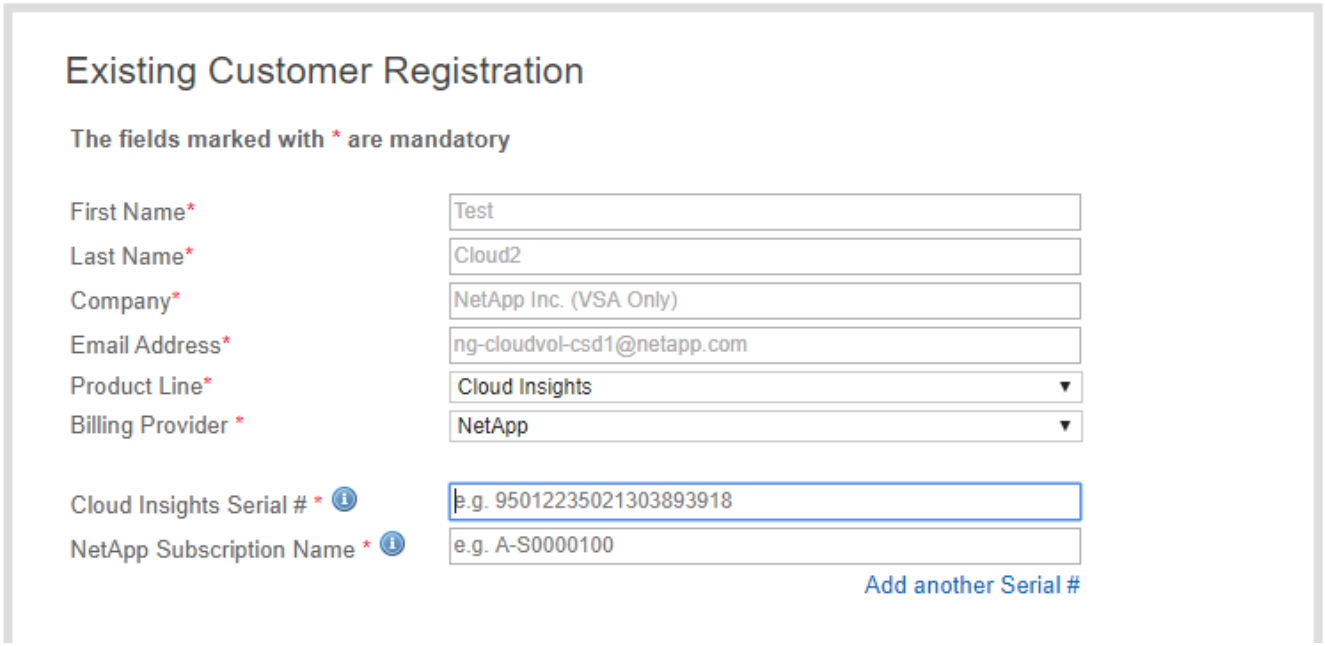
Schritte

1. Navigieren Sie zur NetApp Registrierungs-Website https://register.netapp.com

2. Wählen Sie „Ich bin bereits als NetApp-Kunde registriert“ und wählen Sie als Produktlinie „*Data Infrastructure Insights*“. Wählen Sie Ihren Abrechnungsanbieter (NetApp oder AWS) aus, und geben Sie Ihre Seriennummer und den Namen Ihres NetApp-Abonnements oder Ihre AWS Kunden-ID an. Verwenden Sie hierzu in der Insights Benutzeroberfläche der Dateninfrastruktur das Menü „Hilfe > Support“:



3. Füllen Sie das bestehende Registrierungsformular aus und klicken Sie auf **Absenden**.



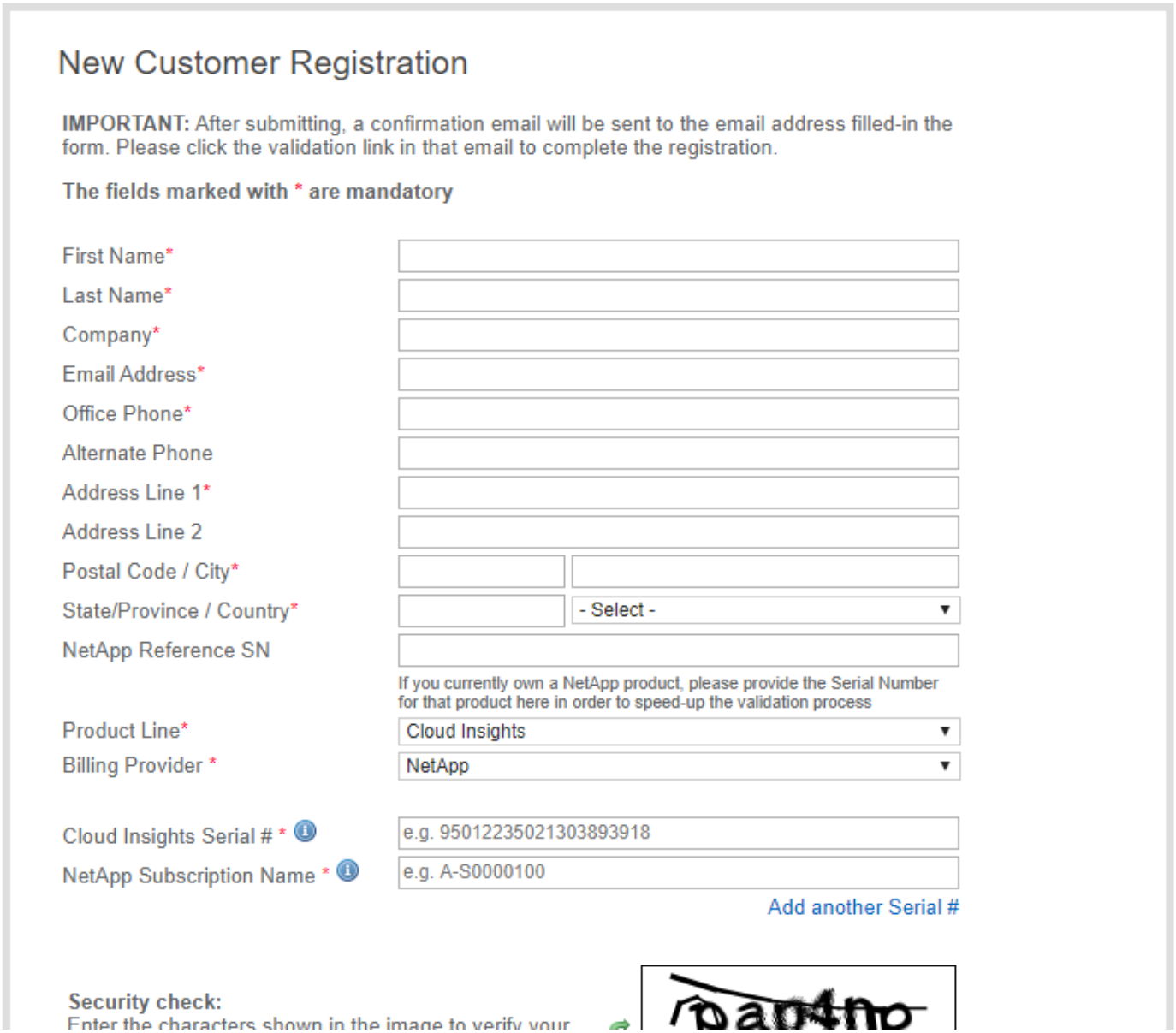
4. Wenn keine Fehler auftreten, wird der Benutzer auf eine Seite „Registrierung erfolgreich übermittelt“ weitergeleitet. Die E-Mail-Adresse, die mit dem NSS SSO-Benutzernamen verbunden ist, der für die Registrierung verwendet wird, erhält innerhalb von wenigen Minuten eine E-Mail mit der Angabe „Ihr Produkt ist jetzt für Support berechtigt“.
5. Dies ist eine einmalige Registrierung für die Seriennummer des Data Infrastructure Insights NetApp.

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

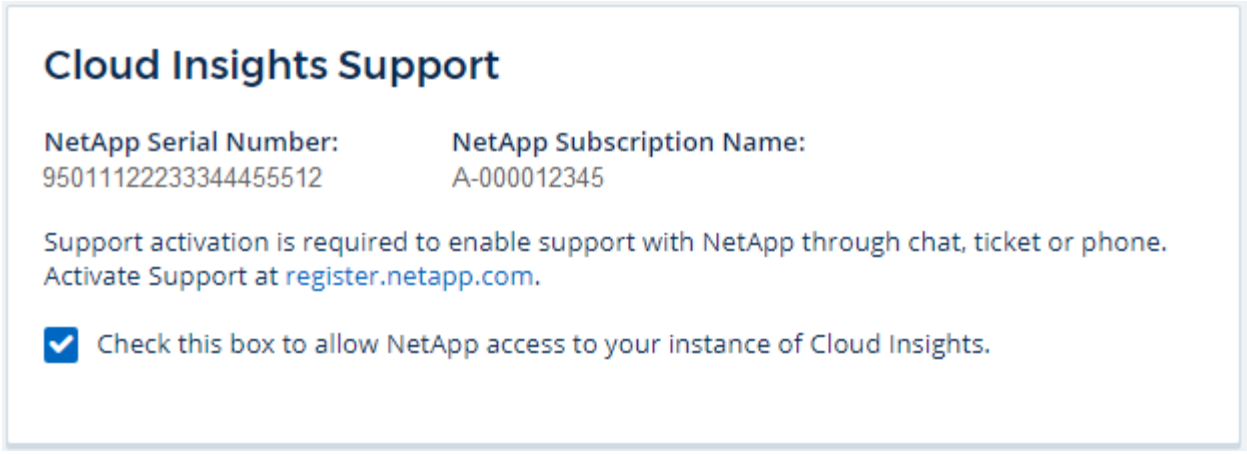
Schritte

1. Navigieren Sie zur NetApp Registrierungs-Website https://register.netapp.com
2. Wählen Sie „Ich bin kein registrierter NetApp Kunde“ und füllen Sie die erforderlichen Informationen im

folgenden Beispielformular aus:



1. Wählen Sie *Data Infrastructure Insights* als Produktlinie aus. Wählen Sie Ihren Abrechnungsanbieter (NetApp oder AWS) aus, und geben Sie Ihre Seriennummer und den Namen Ihres NetApp-Abonnements oder Ihre AWS Kunden-ID an. Verwenden Sie hierzu in der Insights Benutzeroberfläche der Dateninfrastruktur das Menü „Hilfe > Support“:



2. Wenn keine Fehler auftreten, wird der Benutzer auf eine Seite „Registrierung erfolgreich übermittelt“ weitergeleitet. Die E-Mail-Adresse, die mit dem NSS SSO-Benutzernamen verbunden ist, der für die Registrierung verwendet wird, erhält innerhalb weniger Stunden eine E-Mail mit der Angabe „Ihr Produkt ist jetzt für Support berechtigt“.
3. Als neuer NetApp Kunde müssen Sie außerdem ein 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 Seriennummer des Data Infrastructure Insights NetApp.

Abrufen Von Support-Informationen

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 Support-Optionen 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, in der Sie relevante Artikel und Anleitungen durchsuchen können.

- **"Dokumentation"**

  Durch Klicken auf den Link Dokumentation gelangen Sie zu diesem Dokumentationszentrum.

- **"Community"**

  Durch Klicken auf den Community-Link gelangen Sie zur NetApp Data Infrastructure Insights Community, in der Sie sich mit Kollegen und Experten austauschen können.

Außerdem gibt es einen Link**"Feedback"**, den Sie uns zur Verbesserung der Einblicke aus der Dateninfrastruktur zur Verfügung stellen können.

Abonnementunterstützung

Wenn Sie zusätzlich zu den oben aufgeführten Self-Support-Optionen ein Abonnement für Data Infrastructure Insights oder bezahlten Support für überwachte NetApp Produkte und Services haben, können Sie gemeinsam mit einem NetApp Support Engineer das Problem lösen.

Sie müssen sich für NetApp Cloud-Produkte registrierenAktivieren Sie den Support. Um sich zu registrieren, gehen Sie zu NetApp's "Support-Registrierung Für Cloud-Datenservices".

Es wird dringend empfohlen, das Kontrollkästchen zu aktivieren, damit NetApp-Support-Techniker während der Support-Sitzung auf den Mandanten Ihrer Dateninfrastruktur zugreifen können. So kann der Techniker das Problem beheben und es schnell beheben. Wenn Ihr Problem behoben ist oder Ihre Support-Sitzung beendet wurde, können Sie das Kontrollkästchen deaktivieren.

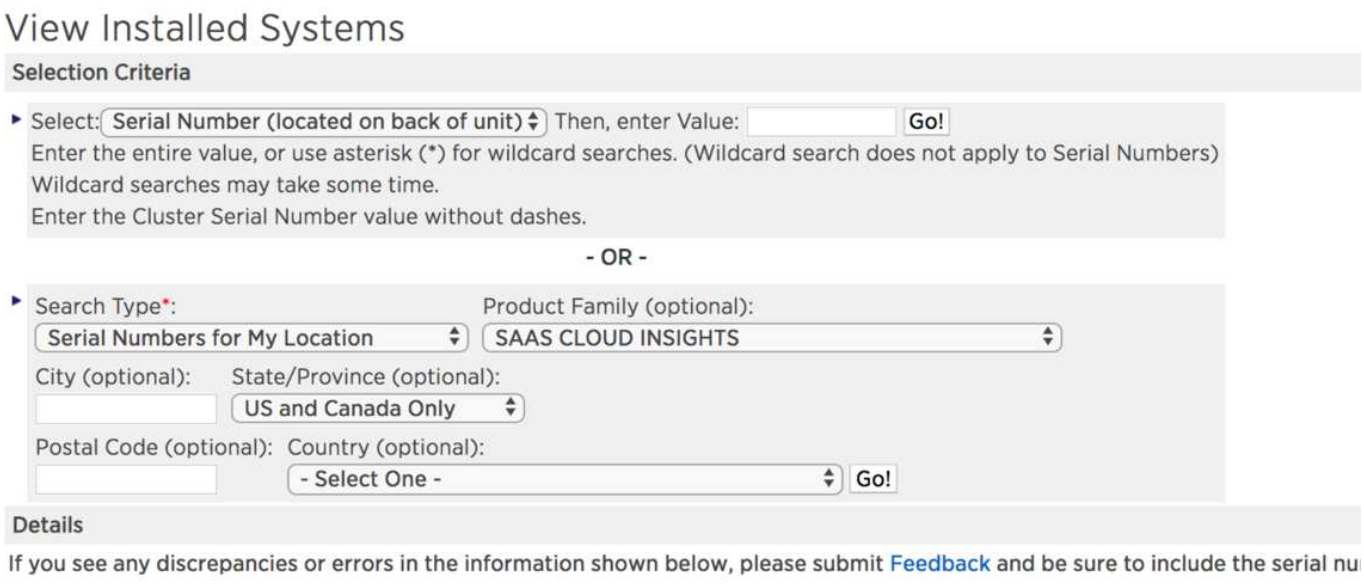
Sie können Unterstützung durch eine der folgenden Methoden anfordern. Um die folgenden Support-Optionen nutzen zu können, benötigen Sie ein aktives Abonnement von Data Infrastructure Insights:

- "* Telefon*"
- **"Support-Ticket"**

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

Ihre Data Infrastructure Insights Seriennummer wird im Service über das Menü **Hilfe > Support** angezeigt. Wenn beim Zugriff auf den Service Probleme auftreten und Sie zuvor eine Seriennummer bei NetApp registriert haben, können Sie sich wie folgt auf der NetApp Support-Website Ihre Liste mit Seriennummern von Data Infrastructure Insights anzeigen lassen:

- Melden Sie sich bei mysupport.netapp.com an
- Verwenden Sie auf der Menüregisterkarte Produkte > Meine Produkte die Produktfamilie „SaaS Data Infrastructure Insights“, um alle Ihre registrierten Seriennummern zu finden:



Data Infrastructure Insights Data Collector Support Matrix

Informationen und Details zu unterstützten Datensammlern können Sie im anzeigen oder herunterladen**Data Infrastructure Insights Data Collector Support Matrix**, Rolle=„extern“.

Learning Center

Unabhängig von Ihrem Abonnement führt **Hilfe > Support** Links zu verschiedenen Kursangeboten der NetApp University, damit Sie die Erkenntnisse über Ihre Dateninfrastruktur optimal nutzen können. Erfahren Sie mehr darüber!

Data Collector Reference - Infrastruktur

Anbieterspezifische Referenz

Die Themen in diesem Abschnitt enthalten anbieterspezifische Referenzinformationen. In den meisten Fällen ist die Konfiguration eines Datensammlers einfach. In einigen Fällen benötigen Sie möglicherweise zusätzliche Informationen oder Befehle, um den Datensammler richtig zu konfigurieren.

Klicken Sie im Menü links auf einen **Anbieter**, um Informationen zu ihren Datensammlern anzuzeigen.

Amazon EC2 Data Collector konfigurieren

Data Infrastructure Insights verwendet den Amazon EC2 Datensammler, um Bestands- und Performance-Daten von EC2-Instanzen zu erfassen.

Anforderungen

Um Daten von Amazon EC2 Geräten zu erfassen, müssen Sie folgende Informationen haben:

- Sie müssen eine der folgenden Optionen aufweisen:
  - Die **IAM-Rolle** für Ihr Amazon EC2 Cloud-Konto, wenn Sie IAM-Rollenauthentifizierung verwenden. Die IAM-Rolle gilt nur, wenn die Acquisition Unit auf einer AWS-Instanz installiert ist.
  - Die **IAM Access Key**-ID und der geheime Zugriffsschlüssel für Ihr Amazon EC2 Cloud-Konto bei Verwendung der IAM Access Key-Authentifizierung.
- Sie müssen über die Berechtigung „Listenorganisation“ verfügen
- Port 443 HTTPS
- EC2-Instanzen können als Virtual Machine oder (weniger natürlich) als Host gemeldet werden. EBS Volumes können sowohl von der VM als virtualisierte Festplatte genutzt werden als auch als Datenspeicher, die die Kapazität der virtuellen Festplatte bereitstellen.

Zugriffsschlüssel bestehen aus einer Zugriffsschlüssel-ID (z. B. AKIAIOSFODN7EXAMPLE) und einem geheimen Zugriffsschlüssel (z. B. wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Sie verwenden Zugriffsschlüssel, um programmatische Anfragen zu signieren, die Sie an EC2 vornehmen, wenn Sie die Amazon EC2 SDKs, REST oder Abfrage-API-Operationen verwenden. Diese Schlüssel werden mit Ihrem Vertrag von Amazon zur Verfügung gestellt.

Konfiguration

Geben Sie die Daten in die Felder des Datensammlers gemäß der folgenden Tabelle ein:

Feld	Beschreibung
AWS Region	Wählen Sie die Region AWS

Feld	Beschreibung
IAM-Rolle	Nur zur Verwendung bei Übernahme auf einer AU in AWS. Siehe unten für weitere Informationen über IAM-Rolle.
AWS IAM Access Key-ID	Geben Sie die AWS IAM-Zugriffsschlüssel-ID ein. Erforderlich, wenn Sie die IAM-Rolle nicht verwenden.
AWS IAM Secret Access Key	Geben Sie den AWS IAM-Schlüssel für den geheimen Zugriff ein. Erforderlich, wenn Sie die IAM-Rolle nicht verwenden.
Ich verstehe, dass mir AWS API-Anfragen nach	Überprüfen Sie dies, um zu überprüfen, ob AWS Sie für API-Anfragen abfragt, die durch die Data Infrastructure Insights Umfrage gemacht wurden.

Erweiterte Konfiguration

Feld	Beschreibung
Zusätzliche Regionen Einschließen	Geben Sie zusätzliche Bereiche an, die in die Abfrage einbezogen werden sollen.
Accountübergreifende Rolle	Rolle für den Zugriff auf Ressourcen in unterschiedlichen AWS Konten.
Abfrageintervall für Bestand (min)	Der Standardwert ist 60
Wählen Sie „exclude“ oder „include“, um VMs nach Tags zu filtern	Geben Sie an, ob VM's by Tags beim Sammeln von Daten einbezogen oder ausgeschlossen werden sollen. Wenn 'include' ausgewählt ist, kann das Feld Tag-Schlüssel nicht leer sein.
Markieren Sie Schlüssel und Werte, nach denen VMs gefiltert werden sollen	Klicken Sie auf **+ Filter Tag**, um die VMs (und die zugehörigen Festplatten) auszuwählen, die durch Filtern nach Schlüsseln und Werten, die Schlüssel und Werte von Tags auf der VM entsprechen, einzuschließen bzw. auszuschließen. Tag-Schlüssel erforderlich, Tag-Wert ist optional. Wenn der Tag-Wert leer ist, wird die VM solange gefiltert, wie sie dem Tag-Schlüssel entspricht.
Leistungsintervall (Sek.)	Der Standardwert ist 1800
CloudWatch Agent Metrics Namespace	Namespace in EC2/EBS zur Erfassung von Daten Wenn die Namen der Standardmetriken in diesem Namespace geändert werden, kann Data Infrastructure Insights diese umbenannten Daten möglicherweise nicht erfassen. Es wird empfohlen, die standardmäßigen metrischen Namen zu belassen.

IAM-Zugriffsschlüssel

Zugriffsschlüssel sind langfristige Anmeldedaten für einen IAM-Benutzer oder den Root-Benutzer des AWS-Kontos. Mit Zugriffsschlüsseln werden programmatische Anfragen an die AWS CLI oder die AWS API (direkt oder über das AWS SDK) signieren.

Zugriffsschlüssel bestehen aus zwei Teilen: Einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel. Wenn Sie die Authentifizierung *IAM Access Key* verwenden (im Gegensatz zur Authentifizierung von *IAM Role*), müssen Sie für die Authentifizierung von Anfragen sowohl den Zugriffsschlüssel-ID als auch den geheimen Zugriffsschlüssel gemeinsam verwenden. Weitere Informationen finden Sie in der Amazon-Dokumentation auf "Zugriffsschlüssel".

IAM-Rolle

Bei der Verwendung der Authentifizierung über *IAM-Rolle* (im Gegensatz zur IAM-Zugriffsschlüsselauthentifizierung) müssen Sie sicherstellen, dass die von Ihnen erstellte oder angegebene Rolle über die entsprechenden Berechtigungen verfügt, die für den Zugriff auf Ihre Ressourcen erforderlich sind.

Wenn Sie beispielsweise eine IAM-Rolle mit dem Namen *InstanceEc2ReadOnly* erstellen, müssen Sie die Richtlinie einrichten, um allen EC2-Ressourcen für diese IAM-Rolle schreibgeschützten Zugriff auf EC2-Listen zu gewähren. Außerdem müssen Sie STS (Security Token Service)-Zugriff gewähren, damit diese Rolle Rollenübergreifende Konten übernehmen kann.

Nachdem Sie eine IAM-Rolle erstellt haben, können Sie sie beim Erstellen einer neuen EC2-Instanz oder einer vorhandenen EC2-Instanz anhängen.

Nachdem Sie die IAM-Rolle *InstanceEc2ReadOnly* an eine EC2-Instanz angehängt haben, können Sie die temporären Anmeldedaten über die Metadaten der Instanz per IAM-Rollennamen abrufen und verwenden, um von jeder auf dieser EC2-Instanz ausgeführten Anwendung auf AWS-Ressourcen zuzugreifen.

Weitere Informationen finden Sie im Amazon-Dokument auf "IAM-Rollen".

Hinweis: Die IAM-Rolle kann nur verwendet werden, wenn die Acquisition Unit in einer AWS-Instanz ausgeführt wird.

Zuordnen von Amazon Tags zu Annotationen zu Data Infrastructure Insights

Der Amazon EC2 Datensammler enthält eine Option zum Ausfüllen von Anmerkungen zu Data Infrastructure Insights mit auf EC2 konfigurierten Tags. Die Anmerkungen müssen genau wie die EC2-Tags benannt werden. Data Infrastructure Insights füllt immer Anmerkungen vom gleichen Namen aus und versucht, Anmerkungen anderer Typen (Zahl, Boolescher Wert usw.) zu füllen. Wenn Ihre Anmerkung einen anderen Typ hat und der Datensammler sie nicht füllt, kann es erforderlich sein, die Anmerkung zu entfernen und sie als Texttyp neu zu erstellen.

Bei AWS muss die Groß-/Kleinschreibung nicht beachtet werden, während bei Data Infrastructure Insights die Groß-/Kleinschreibung nicht beachtet werden muss. Wenn Sie in Data Infrastructure Insights eine Annotation mit dem Namen „OWNER“, „OWNER“ und „OWNER“ in EC2 erstellen, werden alle EC2-Variationen von „Owner“ der „Owner“ in der Annotation von Cloud Insight mit der Bezeichnung „OWNER“ zusammengefasst.

Zusätzliche Regionen Einschließen

Im Abschnitt AWS Data Collector **Erweiterte Konfiguration** können Sie das Feld * zusätzliche Regionen* so einstellen, dass zusätzliche durch Komma oder Semikolon getrennte Bereiche einbezogen werden. Standardmäßig ist dieses Feld auf ***US-.**** gesetzt, das auf allen US AWS Regionen sammelt. Um in *all* Regionen zu sammeln, setzen Sie dieses Feld auf ***.**. Ist das Feld **zusätzliche Regionen** leer, sammelt der Datensammler die im Feld **AWS Region** angegebenen Werte, wie im Abschnitt **Konfiguration** angegeben.

Erfassung über AWS Child-Konten

Data Infrastructure Insights unterstützt die Erfassung von untergeordneten Konten für AWS innerhalb eines einzigen AWS-Datensammlers. Die Konfiguration dieser Sammlung erfolgt in der AWS-Umgebung:

- Sie müssen jedes untergeordnete Konto so konfigurieren, dass es über eine AWS-Rolle verfügt, die es der Hauptkonto-ID ermöglicht, über das untergeordnete Konto auf EC2-Details zuzugreifen.
- Für jedes untergeordnete Konto muss der Rollenname mit demselben String konfiguriert sein.
- Geben Sie diese Zeichenfolge für den Rollennamen im Abschnitt Data Infrastructure Insights AWS Data Collector **Advanced Configuration** im Feld **Cross Account role** ein.
- Das Konto, auf dem der Collector installiert ist, muss über *Delegate Access Administrator* Privileges verfügen. "AWS-Dokumentation"Weitere Informationen finden Sie im.

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

Im Folgenden finden Sie Informationen zur Konfiguration Ihrer Umgebung, damit Data Infrastructure Insights von untergeordneten AWS-Konten erfasst werden kann:

"Tutorial: Delegieren des Zugriffs über AWS Konten mithilfe von IAM-Rollen"

"AWS Setup: Zugriff auf einen IAM-Benutzer in einem anderen AWS-Konto bereitstellen, das Sie besitzen"

"Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer"

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Amazon FSX für NetApp ONTAP Datensammler

Dieser Datensammler erfasst Bestands- und Performance-Daten von Amazon FSX für NetApp ONTAP. Dieser Datensammler wird in den gesamten Serviceregionen von Data Infrastructure Insights inkrementell zur Verfügung gestellt. Wenden Sie sich an Ihren Vertriebsmitarbeiter, wenn das Symbol für diesen Collector in Ihrer Data Infrastructure Insights Environment nicht angezeigt wird.

> Für diesen Dateninfrastrukturüberblick ist ein ONTAP-Benutzer mit einer Rolle *Filesystem-scoped* erforderlich. In der AWS "Rollen und Regeln" Dokumentation finden Sie weitere Informationen zu verfügbaren Optionen. AWS unterstützt derzeit nur eine Art Benutzerrolle mit Filesystem Scope, nämlich *fsxadmin*. Dies ist die geeignete Rolle für den Data Infrastructure Insights Collector. Dem Benutzer sollten auch alle drei dieser Anwendungen zugewiesen sein: http, ontapi, ssh.

Terminologie

Data Infrastructure Insights erfasst Inventar- und Performance-Daten aus dem FSX-NetApp-Datensammler. Für jeden erworbenen Asset-Typ wird die am häufigsten für das Asset verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Cluster	Storage
LUN	Datenmenge
Datenmenge	Internes Volumen

FSX-NetApp – Terminologie

Die folgenden Begriffe gelten für Objekte oder Referenzen, die Sie auf den FSX-NetApp Storage Asset Landing Pages finden können. Viele dieser Bedingungen gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Komma getrennte Liste der eindeutigen, diskreten Modellnamen in diesem Cluster.
- Anbieter – AWS
- Seriennummer: Die Seriennummer des Arrays.
- IP: In der Regel werden die in der Datenquelle konfigurierten IP(s) oder Hostnamen(s) verwendet.
- Rohkapazität: Die Summe aus 2 des gesamten SSD-Speichers, der dem FSX-Dateisystem zugewiesen ist
- Latenz – eine Darstellung der Workloads, die sich auf dem Host auslasten, sowohl bei Lese- als auch bei Schreibzugriffen. Idealerweise bezieht Data Infrastructure Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Statt dieses Array in Betracht zu ziehen, führt Data Infrastructure Insights in der Regel eine IOPS-gewichtete Berechnung aus den Statistiken der einzelnen internen Volumes durch.
- Durchsatz: Aggregiert aus internen Volumes. Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert erstellt von der Datenquelle „Data Infrastructure Insights“ als Teil der Bestandsberichterstattung.

Storage-Pool

- Storage – auf welchem Storage-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibenden Wert aus einer Liste mit einer Aufzählung der Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ sein.
- Kapazität – die Werte hier sind die logische genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der dafür genutzte Prozentsatz.
- IOPS – die Summe der IOPS aller Volumes, die in diesem Storage-Pool zugewiesen sind.
- Durchsatz – der Gesamtdurchsatz aller Volumes, die in diesem Storage-Pool zugewiesen sind.

Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration und Verwendung dieses Datensammlers:

- Sie müssen Zugriff auf ein Konto mit der Rolle „fsxadmin“ haben, wobei drei Anwendungen zugewiesen sind - ssh, ontapi, http
- Zu den Kontodetails gehören Benutzername und Passwort.
- Anforderungen an den Hafen: 443

Konfiguration

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

Erweiterte Kennzahlen

Dieser Datensammler sammelt die folgenden erweiterten Metriken aus dem FSX für NetApp ONTAP Storage:

- fpolicy
- nfsv3
- nfsv3:Node
- nfsv4
- nfsv4_1
- nfsv4_1:Node
- nfsv4:Node
- Policy_Group
- Qtree
- Datenmenge
- Workload_Volume

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

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Erhalten Sie 401 HTTP-Antwort oder 13003 ZAPI-Fehlercode und ZAPI gibt „unzureichende Berechtigungen“ oder „nicht autorisiert für diesen Befehl“ zurück	Benutzernamen und Kennwort sowie Benutzerrechte/Berechtigungen überprüfen.
ZAPI gibt zurück „Cluster-Rolle ist keine Cluster_Mgmt LIF“	AU muss mit Cluster Management IP sprechen. Überprüfen Sie die IP und wechseln Sie ggf. auf eine andere IP

Problem:	Versuchen Sie dies:
ZAPI-Befehl schlägt nach dem erneuten Versuch fehl	AU hat ein Kommunikationsproblem mit dem Cluster. Überprüfen Sie Netzwerk, Port-Nummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl von der Befehlszeile aus dem AU-Rechner auszuführen.
AU konnte über HTTP keine Verbindung mit ZAPI herstellen	Prüfen Sie, ob der ZAPI-Port Klartext akzeptiert. Wenn AU versucht, Klartext an einen SSL-Socket zu senden, schlägt die Kommunikation fehl.
Die Kommunikation schlägt mit SSLException fehl	AU versucht, SSL an einen Klartext Port auf einem Filer zu senden. Überprüfen Sie, ob der ZAPI-Port SSL akzeptiert, oder verwenden Sie einen anderen Port.
Weitere Verbindungsfehler: ZAPI-Antwort hat Fehlercode 13001, „Datenbank ist nicht geöffnet“ ZAPI-Fehlercode ist 60 und die Antwort enthält „API hat nicht auf Zeit beendet“ ZAPI-Antwort enthält „initialize_Session() zurückgegebene Null-Umgebung“ ZAPI-Fehlercode ist 14007 und die Antwort enthält „Knoten ist nicht gesund“	Überprüfen Sie Netzwerk, Port-Nummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl von der Befehlszeile aus dem AU-Rechner auszuführen.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Konfigurieren des Azure Compute-Datensammlers

Data Infrastructure Insights verwendet den Compute-Datensammler Azure, um Inventar- und Performance-Daten aus Azure Computing-Instanzen zu erfassen.

Anforderungen

Sie benötigen die folgenden Informationen, um diesen Datensammler zu konfigurieren.

- Port-Anforderung: 443 HTTPS
- Azure OAuth 2.0 Redirect URI (login.microsoftonline.com)
- Azure Management Rest-IP (management.azure.com)
- Azure Resource Manager IP (management.core.windows.net)
- Azure Service Principal Application (Client)-ID (Reader-Rolle erforderlich)
- Azure Service Principal Authentifizierungsschlüssel (Benutzerkennwort)
- Sie müssen ein Azure-Konto für die Erkennung von Data Infrastructure Insights einrichten.

  Sobald das Konto ordnungsgemäß konfiguriert ist und Sie die Applikation in Azure registrieren, verfügen Sie über die erforderlichen Zugangsdaten, um die Azure-Instanz mit Data Infrastructure Insights zu ermitteln. Über den folgenden Link wird beschrieben, wie Sie das Konto für die Ermittlung einrichten. https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Konfiguration

Geben Sie die Daten in die Felder des Datensammlers gemäß der folgenden Tabelle ein:

Feld	Beschreibung
Azure Service Principal Application (Client)-ID (Reader-Rolle erforderlich)	Anmelde-ID bei Azure. Erfordert Zugriff auf die Leserrolle.
Azure-Mandanten-ID	Microsoft Mandanten-ID
Authentifizierungsschlüssel Des Azure Service Principal	Anmeldeauthentifizierungsschlüssel
Ich verstehe, dass Microsoft mir API-Anforderungen in Rechnung stellt	Überprüfen Sie dies, um zu überprüfen, ob Microsoft Ihnen die durch eine Insight-Umfrage gestellten API-Anforderungen abrechnungen aufstellt.

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60
Wählen Sie „exclude“ oder „include“, um VMs nach Tags zu filtern	Geben Sie an, ob VM's by Tags beim Sammeln von Daten einbezogen oder ausgeschlossen werden sollen. Wenn 'include' ausgewählt ist, kann das Feld Tag-Schlüssel nicht leer sein.
Markieren Sie Schlüssel und Werte, nach denen VMs gefiltert werden sollen	Klicken Sie auf **+ Filter Tag**, um die VMs (und die zugehörigen Festplatten) auszuwählen, die durch Filtern nach Schlüsseln und Werten, die Schlüssel und Werte von Tags auf der VM entsprechen, einzuschließen bzw. auszuschließen. Tag-Schlüssel erforderlich, Tag-Wert ist optional. Wenn der Tag-Wert leer ist, wird die VM solange gefiltert, wie sie dem Tag-Schlüssel entspricht.
Leistungsintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Broadcom

Datensammler Brocade Network Advisor

Dateninfrastrukturanalysen verwenden den Datensammler Brocade Netzwerkberater, um Bestands- und Performancedaten von Brocade-Switches zu erfassen.

Terminologie

Data Infrastructure Insights erfasst die folgenden Inventarinformationen aus dem Brocade Netzwerkberater-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese

Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Switch	Switch
Port	Port
Virtual Fabric, Physische Fabric	Fabric
Logischer Switch	Logischer Switch

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Die Data Infrastructure Insights Acquisition Unit führt Verbindungen zu TCP-Port 443 auf dem BNA-Server ein. BNA-Server muss Version 14.2.1 oder höher ausführen.
- IP-Adresse des Brocade Network Advisor Servers
- Benutzername und Kennwort für ein Administratorkonto
- Port-Anforderung: HTTP/HTTPS 443

Konfiguration

Feld	Beschreibung
Brocade Network Advisor Server IP	IP-Adresse des Network Advisor-Servers
Benutzername	Benutzername für den Switch
Benutzername	Administrator-Benutzername
Passwort	Administratorpasswort

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS (Standardport 443) oder HTTP (Standardport 80)
Verbindungs-Port Überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport im Feld Verbindungstyp. Andernfalls geben Sie den zu verwendenden Anschluss ein
Passwort	Passwort für den Switch
Abfrageintervall für Bestand (min)	Der Standardwert ist 40
Access Gateway Melden	Aktivieren Sie diese Option, um Geräte im Access Gateway-Modus einzubeziehen
Leistungsintervall (Sek.)	Der Standardwert ist 1800

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Sie erhalten eine Meldung, dass mehr als 1 Knoten am Access Gateway-Port angemeldet ist, oder Datensammler kann das Access Gateway-Gerät nicht erkennen.	Überprüfen Sie, ob das NPV-Gerät ordnungsgemäß funktioniert und dass alle verbundenen WWNs erwartet werden. Erwerben Sie das NPV-Gerät nicht direkt. Stattdessen erfasst die Akquisition des Core Fabric Switch die NPV Geräte-Daten.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Datensammler Brocade FC Switch

Dateninfrastruktur Insights verwendet die SSH-Datenquelle (Brocade FC Switch), um eine Bestandsaufnahme für Brocade- oder umbenannte Switch-Geräte zu erkennen, auf denen die Firmware des Factsored Operating System (FOS) 4.2 und höher ausgeführt wird. Geräte werden sowohl im FC-Switch- als auch im Access Gateway-Modus unterstützt.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Brocade FC Switch-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Switch	Switch
Port	Port
Virtual Fabric, Physische Fabric	Fabric
Zone	Zone
Logischer Switch	Logischer Switch
Virtual Volume	Datenmenge
LSAN-Zone zu erreichen	IVR-Zone zu erreichen

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Die Data Infrastructure Insights Acquisition Unit (AU) initiiert Verbindungen zu TCP-Port 22 auf Brocade-Switches, um Bestandsdaten zu sammeln. Die AU wird auch Verbindungen zu UDP Port 161 für die Sammlung von Leistungsdaten initiieren.

- Es muss eine IP-Verbindung zu allen Switches in der Fabric vorhanden sein. Wenn Sie das Kontrollkästchen Alle Switches in der Fabric ermitteln aktivieren, identifiziert Data Infrastructure Insights alle Switches in der Fabric, benötigt jedoch IP-Konnektivität zu diesen zusätzlichen Switches, um sie zu erkennen.
- Weltweit ist dasselbe Konto über alle Switches in der Fabric erforderlich. Sie können PuTTY (Open Source Terminal Emulator) verwenden, um den Zugriff zu bestätigen.
- Die Ports 161 und 162 müssen offen sein für alle Switches im Fabric für SNMP-Performance-Abfragen.
- SNMP Read-Only Community String

Konfiguration

Feld	Beschreibung
Switch-IP	IP-Adresse oder vollständig qualifizierter Domänenname des EFC-Servers
Benutzername	Benutzername für den Switch
Passwort	Passwort für den Switch
SNMP	SNMP-Version
SNMP-Community-Zeichenfolge	SNMP read-only Community String verwendet, um auf den Switch zugreifen
SNMP-Benutzername	SNMP-Benutzername
SNMP-Kennwort	SNMP-Passwort

Erweiterte Konfiguration

Feld	Beschreibung
Fabric-Name	Der Fabric-Name wird vom Data Collector gemeldet. Lassen Sie das Feld leer, um den Fabric-Namen als WWN zu melden.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 15.
Ausgeschlossene Geräte	Kommagetrennte Liste der Geräte-IDs, die von der Abfrage ausgeschlossen werden sollen
Admin-Domänen Aktiv	Wählen Sie, wenn Sie Admin-Domains verwenden
MPR-Daten abrufen	Wählen Sie diese Option aus, um Routing-Daten von Ihrem Multiprotokoll-Router zu erhalten.
Trapping Aktivieren	Wählen Sie diese Option aus, um die Erfassung beim Empfang eines SNMP-Trap vom Gerät zu aktivieren. Wenn Sie Trapping aktivieren auswählen, müssen Sie auch SNMP aktivieren.
Mindestzeit zwischen Traps (s)	Mindestzeit zwischen durch Traps ausgelösten Erfassungsversuchen. Der Standardwert ist 10.
Erkennung aller Switches in der Fabric	Wählen Sie diese Option, um alle Switches in der Fabric zu erkennen

Feld	Beschreibung
Wählen Sie „HBA vs. Zone Aliases bevorzugen“	Wählen Sie, ob HBA- oder Zonenaliasen bevorzugt werden sollen
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.
SNMP-Auth-Protokoll	SNMP-Authentifizierungsprotokoll (nur SNMP v3)
SNMP-Datenschutzkennwort	SNMP-Datenschutzkennwort (nur SNMP v3)
SNMP wird erneut verwendet	Anzahl der SNMP-Wiederholungsversuche

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Die Bestandsaufnahme der Brocade Datenquelle schlägt mit dem Fehler fehl: <date> <time> ERROR [com.onaro.sanscreen.acquisition.framework.datasource.BaseDataSource] Fehler 2 von 2: <datasource Name> [Interner Fehler] - das Modell für das Gerät konnte nicht generiert werden <IP>. Fehler beim Erkennen der Eingabeaufforderung ([Gerätename <Name>]: Fehler beim Generieren des Modells für Gerät <IP> nicht möglich. Fehler beim Erkennen der Eingabeaufforderung)	Das Problem kann verursacht werden, wenn der Brocade Switch mit einer Eingabeaufforderung zu lange zurückgibt und damit die Standardzeitüberschreitung von 5 Sekunden überschreitet. Versuchen Sie in den Einstellungen für die erweiterte Konfiguration des Datensammlers in Data Infrastructure Insights, das *SSH Banner Wait Timeout (sec)* auf einen höheren Wert zu erhöhen.
Fehler: „Data Infrastructure Insights received invalid Chassis role“	Vergewissern Sie sich, dass dem in dieser Datenquelle konfigurierten Benutzer die Berechtigung für die Gehäuserolle erteilt wurde.
Fehler: „IP-Adresse des Gehäuses nicht stimmt überein“	DII unterstützt grundsätzlich KEINE Netzwerkadressübersetzung oder Portadressübersetzung zwischen der Erfassungseinheit und den Geräten. DII erkennt möglicherweise, dass der Hostname/die IP-Adresse in der Collector-Konfiguration NICHT mit den Adressen übereinstimmt, die das Gerät zu haben glaubt.
Sie erhalten eine Meldung, dass mehr als 1 Knoten am Access Gateway-Port angemeldet ist	Überprüfen Sie, ob das NPV-Gerät ordnungsgemäß funktioniert und dass alle verbundenen WWNs erwartet werden. Erwerben Sie das NPV-Gerät nicht direkt. Stattdessen erfasst die Akquisition des Core Fabric Switch die NPV Geräte-Daten.

Problem:	Versuchen Sie dies:
Fehler: …Max. Remote-Sitzungen für die Anmeldung…	FOS hat unterschiedliche Limits für die Anzahl gleichzeitig unterstützter SSH-Sitzungen pro Benutzerrolle. Die SSH-Sitzung von DII zu diesem Gerät wird beim Login wegen Verstoßes gegen diese Limits abgelehnt. Dies kann ein Hinweis darauf sein, dass mehrere Collector-Instanzen dasselbe Asset entdecken. Dies sollte vermieden werden.

Performance

Problem:	Versuchen Sie dies:
Performance-Erfassung schlägt mit „Timeout 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 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“ konfiguriert, der keinem der SNMPv3-Benutzerslots zugeordnet ist. Das Anlegen eines Benutzers auf Brocade FOS führt NICHT zwangsläufig dazu, dass dieser als SNMPv3-Benutzer aktiviert wird. 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, allerdings 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 der Wert für „SNMP-Datenschutzkennwort“ ist leer, sodass DII keine verschlüsselten SNMPv3-Datenströme mit diesem Gerät aushandeln kann.
Die Leistungserfassung schlägt mit …..VF:nn fehl, Fehler: Kein Zugriff…	Sie haben Ihren DII-Collector für die Verwendung von SNMPv3 auf einem Gerät mit mehreren aktivierten virtuellen Fabrics konfiguriert, der SNMPv3-Benutzer verfügt jedoch NICHT über Rechte für VF NN. DII unterstützt keine partielle Erkennung eines physischen Assets. Sie sollten DII stets proaktiv Zugriff auf alle 128 möglichen VFs gewähren, da DII stets versucht, Leistungsdaten für alle vorhandenen VFs auf einem bestimmten physischen Gerät abzurufen.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Brocade FOS REST Data Collector

Data Infrastructure Insights verwendet den Brocade FOS REST Collector, um Bestand und Performance für Brocade-Switch-Geräte mit FabricOS (FOS) Firmware 8.2 und höher zu ermitteln. Bitte beachten Sie, 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: FOS' Standard "user"-Ebene ist nicht ausreichend leistungsfähig, damit Data Infrastructure Insights alle logischen Aspekte eines Geräts anzeigen kann - wir benötigen ein Benutzerkonto mit aktivierter "Chassis Role" sowie Berechtigungen für alle auf einem Switch konfigurierten virtuellen Fabrics.

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

UserConfig --add NetAppCIUser -r user -l 1-128 -c user -p Qwerty!

Dadurch wird ein User „NetAppCIUser“ mit einem Passwort von „Qwerty!“ eingerichtet. Dieser Benutzer hat die „user“-Rolle (-r) für alle 128 möglichen virtuellen Fabrics (-l). Dieser Benutzer verfügt zusätzlich über die erforderliche „Chassis“-Rolle (-c) mit zugewiesenem Zugriff auf Benutzerebene.

Standardmäßig versucht dieser Collector, alle FOS-Geräte zu ermitteln, die Teil aller Fabrics sind, zu denen der Switch gehört.

Bitte beachten Sie: FOS' Standard-schreibgeschützter Benutzer "user" hat KEINE Ansichtsberechtigungen auf allen virtuellen Fabrics, noch hat er "Chassis Role" Berechtigungen. Dies bedeutet, dass Sie mit „Benutzer“ mit Data Infrastructure Insights eine geringe Erfolgswahrscheinlichkeit haben, da diese sowohl die physische als auch die logische Konfiguration des FOS-Geräts verstehen müssen.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Brocade FOS REST Data Collector. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Switch	Switch
Port	Port
Virtual Fabric, Physische Fabric	Fabric
Zone	Zone
Logischer Switch	Logischer Switch
LSAN-Zone zu erreichen	IVR-Zone zu erreichen

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Es muss eine TCP-Verbindung zu allen Switches in der Fabric vorhanden sein. Dieser Datensammlertyp

versucht nahtlos sowohl HTTP als auch HTTPS für jedes Gerät in der Fabric. Wenn Sie das Kontrollkästchen *Discover all Switches in the Fabric* aktivieren, identifiziert Data Infrastructure Insights alle Switches in der Fabric; es benötigt jedoch TCP-Konnektivität zu diesen zusätzlichen Switches, um sie zu erkennen.

- Weltweit ist dasselbe Konto über alle Switches in der Fabric erforderlich. Sie können den Zugriff über die Webschnittstelle des Geräts bestätigen.

Konfiguration

Feld	Beschreibung
Switch-IP	IP-Adresse oder vollständig qualifizierter Domänenname des FOS-Switches
Benutzername	Benutzername für den Switch
Passwort	Passwort für den Switch

Erweiterte Konfiguration

Feld	Beschreibung
Ausgeschlossene Geräte	Kommagetrennte Liste der Geräte-IPv4-Adressen, die von der Abfrage ausgeschlossen werden sollen.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60.
Erkennung aller Switches in der Fabric	Wählen Sie diese Option aus, um alle Switches in der Fabric zu ermitteln.
Wählen Sie „HBA vs. Zone Aliases bevorzugen“	Wählen Sie aus, ob HBA- oder Zonenaliase bevorzugt werden sollen.
Verbindungstyp	HTTP oder HTTPS.
Beachten Sie, dass diese Einstellung nur ändert, welches Protokoll-CI zuerst pro Gerät verwendet. CI versucht automatisch, das andere Protokoll zu verwenden, wenn die Standardeinstellung fehlschlägt	TCP-Port überschreiben
Geben Sie einen Port an, wenn der Standardwert nicht verwendet wird.	Leistungsintervall (Sek.)

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Die Testfunktion warnt mich, dass ein Protokoll nicht zugänglich ist	Ein bestimmtes Brocade FOS 8.2+ Gerät will nur über HTTP oder HTTPS sprechen - wenn ein Switch ein digitales Zertifikat installiert hat, wirft der Switch HTTP-Fehler auf, wenn man versucht, mit unverschlüsseltem HTTP gegen HTTPS zu kommunizieren. Die Testfunktion versucht die Kommunikation mit HTTP und HTTPS - wenn der Test Ihnen mitteilt, dass ein Protokoll erfolgreich ist, können Sie den Collector sicher speichern und sich keine Sorgen machen, dass das andere Protokoll nicht erfolgreich war - der Collector versucht beide Protokolle während der Sammlung und schlägt nur fehl, wenn keines funktioniert.
Fehler: Inventarisierung schlägt mit 401 Nicht autorisiert 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 ordnungsgemäß unterstützen. Aktualisieren Sie auf eine spätere Version 8.2 oder 9.*
Fehler: „Data Infrastructure Insights received invalid Chassis role“	Vergewissern Sie sich, dass dem in dieser Datenquelle konfigurierten Benutzer die Berechtigung für die Gehäuserolle erteilt wurde.
Fehler: „IP-Adresse des Gehäuses nicht stimmt überein“	Ändern Sie die Konfiguration der Datenquelle, um die Gehäuse-IP-Adresse zu verwenden.
Die Inventur schlägt mit einer 403 Verbotenen fehl	Dies kann einfach schlechte Anmeldeinformationen sein, oder es kann bezeichnend sein, dass Sie versuchen, eine nicht ausreichend leistungsstarke Rolle zu verwenden - denken Sie daran, dass Benutzer auf Benutzerebene nicht über das erforderliche Recht auf „Gehäuserolle“ verfügen oder den Zugriff auf nicht standardmäßige virtuelle Fabrics anzeigen.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Cisco MDS Fabric Switches Datensammler

Data Infrastructure Insights verwendet den Data Collector der Cisco MDS-Fabric-Switches zur Bestandsaufnahme von Cisco MDS-Fabric-Switches sowie einer Vielzahl von Cisco Nexus FCoE-Switches, auf denen der FC-Service aktiviert ist.

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

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Cisco FC Switch-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Switch	Switch
Port	Port
VSAN	Fabric
Zone	Zone
Logischer Switch	Logischer Switch
Name Server-Eintrag	Name Server-Eintrag
Inter-VSAN Routing-Zone (IVR	IVR-Zone zu erreichen

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Eine IP-Adresse eines Switches in der Fabric oder den einzelnen Switches
- Chassis-Erkennung für die Fabric-Erkennung
- Bei Verwendung von SNMP V2, nur lesbare Community-String
- Port 161 wird für den Zugriff auf das Gerät verwendet

Konfiguration

Feld	Beschreibung
Cisco Switch IP	IP-Adresse oder vollqualifizierter Domain-Name des Switches
SNMP-Version	Wählen Sie V1, V2 oder V3 aus. Für Leistungserfassung ist V2 oder höher erforderlich.
SNMP-Community-Zeichenfolge	SNMP Read-Only-Community-String zum Zugriff auf den Switch (gilt nicht für SNMP v3)
Benutzername	Benutzername für den Switch (nur SNMP v3)
Passwort	Passwort für den Switch (nur SNMPv3)

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten)
SNMP-Auth-Protokoll	SNMP-Authentifizierungsprotokoll (nur SNMPv3)
SNMP-Datenschutzprotokoll	SNMP-Datenschutzprotokoll (nur SNMPv3)
SNMP-Datenschutzkennwort	SNMP-Datenschutzkennwort
SNMP wird erneut verwendet	Anzahl der SNMP-Wiederholungsversuche
SNMP-Timeout (ms)	SNMP-Timeout (Standard 5000 ms)

Feld	Beschreibung
Trapping Aktivieren	Wählen Sie, um das Überfüllen zu aktivieren. Wenn Sie Trapping aktivieren, müssen Sie auch SNMP-Benachrichtigungen aktivieren.
Mindestzeit zwischen Traps (s)	Mindestzeit zwischen den von Traps ausgelösten Erfassungsversuchen (Standard: 10 Sekunden)
Alle Fabric Switches Erkennen	Wählen Sie diese Option, um alle Switches in der Fabric zu erkennen
Ausgeschlossene Geräte	Kommagetrennte Liste der Geräte-IP-Adressen, die von der Abfrage ausgeschlossen werden sollen
Enthaltene Geräte	Kommagetrennte Liste der Geräte-IPs, die in Abfrage aufgenommen werden sollen
Überprüfen Sie Den Gerätetyp	Wählen Sie diese Option aus, um nur die Geräte zu akzeptieren, die sich explizit als Cisco-Geräte bewerben
Erster Alias-Typ	Geben Sie eine erste Präferenz für die Auflösung des Alias an. Wählen Sie aus folgenden Optionen: **Device Alais** Dies ist ein benutzerfreundlicher Name für einen Port WWN (PWWN), der bei Bedarf in allen Konfigurationsbefehlen verwendet werden kann. Alle Switches der Produktfamilie Cisco MDS 9000 unterstützen Distributed Device Alias Services (Geräte-Aliase). **Keine** meldet keinen Alias. **Port Description** Eine Beschreibung, um den Port in einer Liste von Ports zu identifizieren. **Zone Alias (all)** Ein benutzerfreundlicher Name für einen Port, der nur für die aktive Konfiguration verwendet werden kann. Dies ist die Standardeinstellung.
Typ Des Zweiten Alias	Geben Sie eine zweite Vorliebe für die Auflösung des Alias an
Dritter Aliastyp	Geben Sie eine dritte Präferenz für die Auflösung des Alias an
Aktivieren Sie die Unterstützung für den SANTAP-Proxy-Modus	Wählen Sie aus, ob Ihr Cisco Switch SANTAP im Proxy-Modus verwendet. Wenn Sie EMC RecoverPoint verwenden, verwenden Sie wahrscheinlich SANTAP.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abfragen (Standard: 300 Sekunden)

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: Gehäuse konnte nicht erkannt werden. Es wurden keine Switches gefunden	• Ping the device with the IP Configured • Melden Sie sich mit der Cisco Device Manager-GUI am Gerät an • Melden Sie sich über CLI beim Gerät an • Versuchen Sie, SNMP Walk auszuführen
Fehler: Gerät ist kein Cisco MDS Switch	• Vergewissern Sie sich, dass die für das Gerät konfigurierte IP-Adresse der Datenquelle richtig ist • Melden Sie sich über die Cisco Device Manager-GUI am Gerät an • Melden Sie sich über die CLI an
Fehler: Data Infrastructure Insights kann den WWN des Switches nicht abrufen.	Hierbei handelt es sich möglicherweise nicht um einen FC- oder FCoE-Switch, dessen Unterstützung möglicherweise nicht möglich ist. Stellen Sie sicher, dass der in der Datenquelle konfigurierte IP/FQDN wirklich ein FC/FCoE-Switch ist.
Fehler: Es wurden mehrere Knoten gefunden, die beim NPV Switch Port angemeldet sind	Deaktivieren Sie die direkte Akquisition des NPV-Schalters
Fehler: Verbindung zum Schalter konnte nicht hergestellt werden	• Stellen Sie sicher, dass das Gerät EINGESCHALTET ist • Überprüfen Sie die IP-Adresse und den Zuhörport • Ping the device • Melden Sie sich über die Cisco Device Manager-GUI beim Gerät an • Melden Sie sich über CLI beim Gerät an • Ausführen von SNMP Walk

Performance

Problem:	Versuchen Sie dies:
Fehler: Leistungsaufnahme wird von SNMP v1 nicht unterstützt	• Datenquelle bearbeiten und Switch-Performance deaktivieren • Datenquelle und Switch-Konfiguration ändern, um SNMP v2 oder höher zu verwenden

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Datensammler Cohesity SmartFiles

Dieser REST-API-basierte Collector erwirbt ein Cohesity-Cluster, das die „Ansichten“ (als interne Data Infrastructure Insights Volumes) und die verschiedenen Nodes erkennt und Performance-Metriken sammelt.

Konfiguration

Feld	Beschreibung
Cohesity Cluster-IP	IP-Adresse des Cohesity-Clusters
Benutzername	Benutzername für den Cohesity Cluster
Passwort	Passwort, das für den Cohesity Cluster verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Anschluss	Port, der für die TCP-Kommunikation mit dem Cohesity-Cluster verwendet wird
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 60 Minuten.
Leistungsintervall (min)	Intervall zwischen Performance-Abstimmungen Die Standardeinstellung ist 900 Sekunden.

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Dell

Datensammler der Dell EMC XC-Serie

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

Konfiguration

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

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Anschluss	Port, der für die TCP-Kommunikation mit dem XC-Server verwendet wird
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 60 Minuten.
Leistungsintervall (min)	Intervall zwischen Performance-Abstimmungen Die Standardeinstellung ist 300 Sekunden.

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Dell EMC

DELL EMC Data Domain-Datensammler

Dieser Datensammler erfasst Bestands- und Performance-Informationen von DELL EMC Data Domain Deduplizierungs-Storage-Systemen. Zur Konfiguration dieses Datensammlers sind spezifische Konfigurationsanweisungen und Nutzungsempfehlungen zu beachten.

Terminologie

Data Infrastructure Insights bezieht die folgenden Bestandsinformationen aus dem Data Domain-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Array Erledigen	Storage
FC-Anschluss	Port
File-System	Internes Volumen
Kontingente	Kontingente
NFS- und CIFS-Freigabe	Dateifreigabe

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. In diesem Datencolletor sind dies möglicherweise nicht alle Fälle.

Anforderungen

Sie benötigen die folgenden Informationen, um diesen Datensammler zu konfigurieren:

- IP-Adresse des Data Domain-Geräts
- Schreibgeschützter Benutzername und Kennwort für den Data Domain-Speicher
- SSH-Port 22

Konfiguration

Feld	Beschreibung
IP-Adresse	Die IP-Adresse oder der vollqualifizierte Domänenname des Data Domain-Speicherarrays
Benutzername	Der Benutzername für das Data Domain-Speicherarray
Passwort	Das Kennwort für das Data Domain-Speicherarray

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20.
SSH-Anschluss	SSH-Service-Port

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Konfigurieren des EMC ECS-Datensammlers

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

Dell EMC ECS wird mit einer anderen Rate von Raw TB zu Managed Units gemessen. Jede 40 TB unformatierte ECS-Kapazität wird als 1 berechnet"Verwaltete Einheit (ME)".

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem ECS-Datensammler. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Cluster	Storage
Mandant	Storage-Pool
Eimer	Internes Volumen
Festplatte	Festplatte

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

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

Konfiguration

Feld	Beschreibung
ECS Host	IP-Adresse oder vollqualifizierter Domain-Name des ECS-Systems

Feld	Beschreibung
ECS-Host-Port	Port, der für die Kommunikation mit ECS Host verwendet wird
ECS-Benutzer-ID	Benutzer-ID für ECS
Passwort	Passwort wird für ECS verwendet

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Die Standardeinstellung ist 360 Minuten.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

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

Performance

Problem:	Versuchen Sie dies:
Fehler: Es wurden nicht genügend Daten erfasst.	* Überprüfen Sie den Erfassungszeitstempel in der Protokolldatei und ändern Sie das Abfrageintervall entsprechend. * Warten Sie länger
Fehler: Das Abfrageintervall für die Performance ist zu groß.	Überprüfen Sie den Sammlungs-Zeitstempel in der Protokolldatei €{logfile} und ändern Sie das Abfrageintervall entsprechend

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Dell EMC PowerScale Datensammler

Data Infrastructure Insights verwendet den SSH-Datensammler Dell EMC PowerScale (ehemals Isilon), um Bestands- und Performance-Daten aus PowerScale-out-NAS-Speicher zu erfassen.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Laufwerk	Festplatte
Cluster	Storage
Knoten	Storage-Node
File-System	Internes Volumen

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Sie benötigen die folgenden Informationen, um diesen Datensammler zu konfigurieren:

- Administrator Berechtigungen für den PowerScale-Speicher
- IP-Adresse des PowerScale-Clusters
- SSH-Zugriff auf Port 22

Konfiguration

Feld	Beschreibung
IP-Adresse	Die IP-Adresse oder der vollqualifizierte Domänenname des PowerScale-Clusters
Benutzername	Benutzername für den PowerScale-Cluster
Passwort	Passwort, das für den PowerScale-Cluster verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.
SSH-Anschluss	SSH-Service-Port. Der Standardwert ist 22.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Ungültige Anmeldeinformationen“ mit Fehlermeldungen „Befehle, die für die rollenbasierte Administration nicht aktiviert sind, benötigen Root-Benutzerzugriff“	* Überprüfen Sie, dass der Benutzer über die Berechtigungen verfügt, um die folgenden Befehle auf dem Gerät auszuführen: > isi Version osselease > isi Status -q > isi Status -n > isi Devices -d %s > isi Lizenz * Überprüfen Sie, dass die im Assistenten verwendeten Anmeldeinformationen mit den Geräteanmeldeinformationen übereinstimmen
„Interner Fehler“ mit Fehlermeldungen “Befehl <Ihr Befehl> Ausführen fehlgeschlagen mit Berechtigung: <Ihre aktuelle Berechtigung>. Sudo Befehl ausführen Berechtigungsproblem“	Überprüfen Sie, ob der Benutzer über sudo-Berechtigungen verfügt, um den folgenden Befehl auf dem Gerät auszuführen

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Rest-Datensammler Dell EMC Isilon/PowerScale

Data Infrastructure Insights verwendet den REST-Datensammler Dell EMC Isilon/PowerScale, um Bestands- und Performance-Daten von Dell EMC Isilon- oder PowerScale-Speicher zu erfassen. Dieser Collector unterstützt Arrays, auf denen OneFS 8.0.0+ ausgeführt wird.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Laufwerk	Festplatte
Cluster	Storage
Knoten	Storage-Node
OneFS File System	Internes Volumen
OneFS File System	Storage-Pool
Qtree	Qtree

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Sie benötigen die folgenden Informationen, um diesen Datensammler zu konfigurieren:

- Ein Benutzerkonto und ein Passwort. Dieses Konto muss nicht Administrator/Root sein, aber Sie MÜSSEN Ihrem Servicekonto eine beträchtliche Anzahl an schreibgeschützten Berechtigungen gewähren - siehe Tabelle unten

- IP-Adresse / Fully Qualified Domain Name des Dell EMC Isilon / PowerScale Clusters
- HTTPS-Zugriff auf Port 8080
- Isilon/PowerScale-Cluster mit OneFS 8.0.0 oder höher

Berechtigungsname	Beschreibung	r(Lesen) oder rw (Lesen+Schreiben)
ISI_PRIV_LOGIN_PAPI	Plattform-API	r
ISI_PRIV_SYS_TIME	Zeit	r
ISI_PRIV_AUTH	Auth	r
ISI_PRIV_ROLE	Berechtigung	r
ISI_PRIV_DEVICES	Geräte	r
ISI_PRIV_EVENT	Ereignis	r
ISI_PRIV_HDFS	HDFS	r
ISI_PRIV_NDMP	NDMP	r
ISI_PRIV_NETWORK	Netzwerk	r
ISI_PRIV_NFS	NFS	r
ISI_PRIV_PAPI_CONFIG	Konfigurieren Sie die Plattform-API	r
ISI_PRIV_QUOTA	Kontingente	r
ISI_PRIV_SMARTPOOLS	SmartPools	r
ISI_PRIV_SMB	SMB	r
ISI_PRIV_STATISTICS	Statistiken	r
ISI_PRIV_SWIFT	Swift	r
ISI_PRIV_JOB_ENGINE	Job-Engine	r

Konfiguration

Feld	Beschreibung
Isilon IP-Adresse	Die IP-Adresse oder der vollqualifizierte Domain-Name des Isilon-Speichers
Benutzername	Benutzername für Isilon
Passwort	Passwort, das für Isilon verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
HTTPS-Anschluss	Der Standardwert ist 8080.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20.

Feld	Beschreibung
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Ungültige Anmeldeinformationen“ mit Fehlermeldungen „Befehle, die für die rollenbasierte Administration nicht aktiviert sind, benötigen Root-Benutzerzugriff“	* Überprüfen Sie, dass der Benutzer über die Berechtigungen verfügt, um die folgenden Befehle auf dem Gerät auszuführen: > isi Version osselease > isi Status -q > isi Status -n > isi Devices -d %s > isi Lizenz * Überprüfen Sie, dass die im Assistenten verwendeten Anmeldeinformationen mit den Geräteanmeldeinformationen übereinstimmen
„Interner Fehler“ mit Fehlermeldungen “Befehl <Ihr Befehl> Ausführen fehlgeschlagen mit Berechtigung: <Ihre aktuelle Berechtigung>. Sudo Befehl ausführen Berechtigungsproblem“	Überprüfen Sie, ob der Benutzer über sudo-Berechtigungen verfügt, um den folgenden Befehl auf dem Gerät auszuführen

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Dell EMC PowerStore-Datensammler

Der EMC PowerStore Data Collector sammelt Bestandsdaten aus dem EMC PowerStore-Speicher. Zur Konfiguration benötigt der Datensammler die IP-Adresse der Speicherprozessoren sowie einen schreibgeschützten Benutzernamen und ein Kennwort.

Der EMC PowerStore Datensammler erfasst die Replikationsbeziehungen zwischen Volume und Volume, die PowerStore über andere Speicher-Arrays hinweg koordiniert. Data Infrastructure Insights zeigt ein Speicher-Array für jeden PowerStore-Cluster und sammelt Bestandsdaten für Knoten und Speicherports auf diesem Cluster. Es werden keine Storage-Pool- oder Volume-Daten erfasst.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Host	Host
Host_Volume_Zuordnung	Host_Volume_Zuordnung
Hardware (es hat Laufwerke unter „extra_Details“-Objekt): Laufwerke	Festplatte

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Appliance	Storage Pool
Cluster	Storage Array Durchführt
Knoten	StorageNode
fc_Port	Port
Datenmenge	Datenmenge
InternalVolume	File_System

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Informationen erforderlich:

- IP-Adresse oder vollqualifizierter Domain-Name des Speicherprozessors
- Schreibgeschützter Benutzername und Kennwort

Konfiguration

Feld	Beschreibung
PowerStore Gateway(s)	IP-Adressen oder vollqualifizierte Domain-Namen des PowerStore-Speichers
Benutzername	Benutzername für PowerStore
Passwort	Passwort, das für PowerStore verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
HTTPS-Anschluss	Der Standardwert ist 443
Abfrageintervall für Bestand (Minuten)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 60 Minuten.

Die PowerStore Performance-Sammlung von Cloud Insight nutzt die 5-minütigen Granularitätsquelldaten von PowerStore. Daher fragt Data Infrastructure Insights diese Daten alle fünf Minuten ab. Dies ist nicht konfigurierbar.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Dell EMC RecoverPoint Data Collector

Der primäre Anwendungsfall des EMC RecoverPoint Data Collector ist die Ermittlung von Replikationsbeziehungen zwischen Volumes, die von der RecoverPoint-Speicher-

Appliance unterstützt werden. Dieser Sammler entdeckt auch das RecoverPoint-Gerät selbst. Bitte beachten Sie, dass Dell/EMC eine VMware Backup-Lösung für VMs--„RecoverPoint for VMs“ verkauft, die von diesem Collector nicht unterstützt wird

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

Der EMC RecoverPoint Data Collector sammelt die Replikationsbeziehungen zwischen Volume und Volume, die RecoverPoint über andere Speicher-Arrays hinweg koordiniert. Data Infrastructure Insights zeigt ein Speicher-Array für jeden RecoverPoint-Cluster an und sammelt Bestandsdaten für Knoten und Speicherports auf diesem Cluster. Es werden keine Storage-Pool- oder Volume-Daten erfasst.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Informationen erforderlich:

- IP-Adresse oder vollqualifizierter Domain-Name des Speicherprozessors
- Schreibgeschützter Benutzername und Kennwort
- REST-API-Zugriff über Port 443

Konfiguration

Feld	Beschreibung
Adresse von RecoverPoint	IP-Adresse oder vollqualifizierter Domain-Name des RecoverPoint-Clusters
Benutzername	Benutzername für das RecoverPoint-Cluster
Passwort	Passwort, das für den RecoverPoint-Cluster verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Anschluss	TCP-Port für die Verbindung mit dem RecoverPoint-Cluster
Abfrageintervall für Bestand (Minuten)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 20 Minuten.
Ausgeschlossene Cluster	Kommagetrennte Liste von Cluster-IDs oder Namen, die beim Abfragen ausgeschlossen werden sollen.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

DELL EMC ScaleIO/PowerFlex-Datensammler

Der Datensammler ScaleIO/PowerFlex erfasst Bestandsdaten aus ScaleIO und PowerFlex-Speicher. Für die Konfiguration benötigt dieser Datensammler die

ScaleIO/PowerFlex-Gateway-Adresse sowie einen Admin-Benutzernamen und ein Passwort.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Datensammler ScaleIO/PowerFlex. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
MDM-Cluster (Meta Data Manager	Storage
SDS (ScaleIO/PowerFlex Data Server)	Storage-Node
Storage-Pool	Storage-Pool
Datenmenge	Datenmenge
Gerät	Festplatte

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Schreibgeschützter Zugriff auf das Admin-Benutzerkonto
- Port-Anforderung: HTTPS-Port 443

Konfiguration

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

Erweiterte Konfiguration

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

Feld	Beschreibung
HTTPS-Port	443
Abfrageintervall für Bestand (min)	Der Standardwert ist 60.
Verbindungs-Timeout (s)	Der Standardwert ist 60.

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Konfigurieren des EMC Unity Data Collector

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

Anforderungen

- Der Unity Data Collector ist CLI-basiert. Sie müssen Unisphere for Unity CLI (uemcli.exe) auf der Erfassungseinheit installieren, in der sich Ihr VNXe Data Collector befindet.
- uemcli.exe verwendet HTTPS als Transportprotokoll, sodass die Erfassungseinheit in der Lage sein muss, HTTPS-Verbindungen zur Unity zu initiieren.
- IP-Adresse oder vollqualifizierter Domänenname des Unity-Geräts
- Sie müssen mindestens einen schreibgeschützten Benutzer zur Verwendung durch den Datensammler haben.
- HTTPS am Port 443 ist erforderlich
- Der EMC Unity Data Collector bietet NAS- und iSCSI-Unterstützung für die Bestandsaufnahme. Fibre-Channel-Volumes werden erkannt, Data Infrastructure Insights jedoch keine Berichte zu FC-Mapping, -Masking oder -Speicherports.

Terminologie

Data Infrastructure Insights bezieht die folgenden Inventarinformationen aus dem Unity-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Storage Array Durchführt	Storage
Prozessor	Storage-Node
Storage-Pool	Storage-Pool
Allgemeine Informationen zu iSCSI Block, VMware VMFS	Share
Remote-Replikationssystem	Synchronisierung
ISCSI-Node	ISCSI-Ziel-Node
ISCSI-Initiator	ISCSI-Target-Initiator

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. In dieser Datenquelle fallen möglicherweise nicht alle Fälle an.

Konfiguration

Feld	Beschreibung
Unity Storage	IP-Adresse oder vollqualifizierter Domänenname des Unity-Geräts
Benutzername	Benutzername für das Unity-Gerät
Passwort	Kennwort für das Unity-Gerät
Vollständiger Pfad zur ausführbaren UEMCLI	Vollständiger Pfad zum Ordner mit der ausführbaren Datei *uemcli.exe*

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40 Minuten
Unity-CLI-Port	Port, der für die Unity-CLI verwendet wird
Leistungsintervall (Sek.)	Der Standardwert ist 300.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Externes Dienstprogramm konnte nicht ausgeführt werden“ mit Fehlermeldungen „Unisphere executable uemcli konnte nicht gefunden werden“	* Korrekte IP-Adresse, Benutzername und Kennwort überprüfen * Bestätigen Sie, dass Unisphere CLI auf der Data Infrastructure Insights Acquisition Unit installiert ist * Bestätigen Sie, dass das Unisphere CLI-Installationsverzeichnis in der Datenquelle korrekt ist * Bestätigen Sie, dass die IP-Adresse der VNXe in der Konfiguration der Datenquelle korrekt ist. Öffnen Sie in der Data Infrastructure Insights Acquisition Unit eine CMD und wechseln Sie in das konfigurierte Installationsverzeichnis: €{INSTALLDIR. Versuchen Sie, eine Verbindung zum VNXe-Gerät herzustellen, indem Sie Folgendes eingeben: Uemcli -d <Ihre IP> -U <Ihre ID> /sys/General show

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Datensammler der Dell EMC VMAX- und PowerMax-Gerätefamilie

Data Infrastructure Insights erkennt EMC VMAX- und PowerMax-Speicher-Arrays mithilfe der symcli-Befehle von Solutions Enabler in Verbindung mit einem vorhandenen Solutions Enabler-Server in Ihrer Umgebung. Der vorhandene Solutions Enabler-Server verfügt über eine Verbindung zum VMAX/PowerMax-Speicher-Array über den Zugriff auf

Gatekeeper-Volumes.

Anforderungen

Bevor Sie diesen Datensammler konfigurieren, sollten Sie sicherstellen, dass Data Infrastructure Insights über TCP-Verbindungen zu Port 2707 auf dem vorhandenen Solutions Enabler-Server verfügt. Data Infrastructure Insights ermittelt alle Symmetrix-Arrays, die auf diesem Server „lokal“ sind, wie in der Ausgabe „symcfg list“ dieses Servers dargestellt.

- Die Anwendung EMC Solutions Enabler (CLI) mit SMI-S Provider muss auf dem Acquisition Unit-Server installiert sein. Die Version muss mit der Version übereinstimmen oder niedriger als die auf dem Solutions Enabler Server ausgeführte Version sein.
- Eine ordnungsgemäß konfigurierte Datei {installdir}\EMC\SYMAPI\config\netcnfg ist erforderlich. Diese Datei definiert Dienstnamen für Solutions Enabler-Server sowie die Zugriffsmethode (SECURE / NOSECURE /ANY).
- Wenn Sie eine Lese-/Schreiblatenz auf Speicherknotenebene benötigen, muss der SMI-S-Provider mit einer laufenden Instanz der UNISPHERE for VMAX-Anwendung kommunizieren.
- IP-Adresse des Management Solutions Enabler Servers
- Administratorberechtigungen auf dem Solutions Enabler (SE)-Server
- Schreibgeschützter Benutzername und Kennwort für die SE-Software
- DIE UNISPHERE for VMAX-Anwendung muss ausgeführt werden und Statistiken für die EMC VMAX- und PowerMax-Speicher-Arrays sammeln, die von der SMI-S Provider-Installation gemanagt werden
- Zugriffsprüfung für Leistung: Gehen Sie in einem Webbrowser auf Ihrer Akquisitionseinheit zu *https://<SMI-S-Hostname oder IP>:5989/ecomconfig* wobei "SMI-S-Hostname oder IP" die IP-Adresse oder den Hostnamen Ihres SMI-S-Servers ist. Diese URL ist für ein Verwaltungsportal für den Service EMC SMI-S (auch bekannt als „ECOM“) vorgesehen. Sie erhalten ein Login-Popup.
- Berechtigungen müssen in der Daemon-Konfigurationsdatei des Solutions Enabler Servers deklariert werden, die üblicherweise hier zu finden ist: */var/symapi/config/daemon_Users*

  Hier ist eine Beispieldatei mit den richtigen Cisys Berechtigungen.

```
root@cernciaukc101:/root
14:11:25 # tail /var/symapi/config/daemon_users
###
###     Refer to the storrdfd(3) man page for additional details.
###
###     As noted above, only authorized users can perform stordaemon
control
###     operations (e.g., shutdown).
#############################################################################
########
# smith         storrdfd
cisys storapid <all>
```

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus der EMC VMAX/PowerMax-Datenquelle. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Festplattengruppe	Festplattengruppe
Storage	Array-Storage
Direktor	Storage-Node
Geräte-Pool, Storage-Ressourcen-Pool (SRP)	Storage-Pool
Gerät TDEV	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Konfiguration

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

Feld	Beschreibung
Name Des Service	Dienstname wie in der Datei *netcnfg* angegeben
Vollständiger Pfad zur CLI	Vollständiger Pfad zu dem Ordner, der die Symmetrix CLI enthält
SMI-S-Host-IP-Adresse	IP-Adresse des SMI-S-Hosts

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 40 Minuten.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten aufgeführte Array-Liste beim Sammeln von Daten aufgenommen oder ausgeschlossen werden soll.
Bestandsfilter Geräteliste	Kommagetrennte Liste der Geräte-IDs, die einbezogen oder ausgeschlossen werden sollen

Feld	Beschreibung
Verbindungs-Caching	Wählen Sie die Methode zum Zwischenspeichern von Verbindungen: * LOCAL bedeutet, dass der Cloud Insights Acquisition-Dienst auf dem Solutions Enabler-Server ausgeführt wird, der über eine Fibre-Channel-Verbindung zu den Symmetrix-Arrays verfügt, die Sie ermitteln möchten, und Zugriff auf Gatekeeper-Volumes hat. Dies ist möglicherweise in einigen Konfigurationen der Remote Acquisition Unit (rau) zu sehen. * REMOTE_CACHED ist der Standard und sollte in den meisten Fällen verwendet werden. Hierbei werden die NETCNFG-Dateieinstellungen verwendet, um eine Verbindung über IP mit dem Solutions Enabler-Server herzustellen. Dieser muss über eine Fibre-Channel-Verbindung zu den Symmetrix-Arrays verfügen, die Sie ermitteln möchten, und hat Zugriff auf Gatekeeper-Volumes. * Wenn DIE OPTIONEN REMOTE_CACHED CLI-Befehle fehlschlagen, verwenden Sie DIE REMOTE-Option. Denken Sie daran, dass es den Erfassungsprozess verlangsamen wird (möglicherweise auf Stunden oder sogar Tage in extremen Fällen). Die NETCNFG-Dateieinstellungen werden weiterhin für eine IP-Verbindung zum Solutions Enabler-Server verwendet, der über Fibre Channel-Verbindungen zu den erkannten Symmetrix-Arrays verfügt. **Hinweis:** Diese Einstellung ändert nicht das Verhalten von Data Infrastructure Insights in Bezug auf die Arrays, die von der Ausgabe „symcfg list“ als REMOTE aufgeführt werden. Data Infrastructure Insights sammelt nur Daten zu Geräten, die mit diesem Befehl als LOKAL angezeigt werden.
SMI-S-Protokoll	Protokoll für die Verbindung mit dem SMI-S-Provider. Zeigt auch den verwendeten Standardport an.
SMIS-Port überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport im Feld Verbindungstyp. Andernfalls geben Sie den zu verwendenden Anschluss ein
SMI-S-Benutzername	Benutzername für den SMI-S Provider Host
SMI-S-Passwort	Benutzername für den SMI-S Provider Host
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abfragen (Standard: 1000 Sekunden)
hoose 'exclude' oder 'include', um eine Liste anzugeben	Geben Sie an, ob die unten aufgeführte Array-Liste beim Erfassen von Performancedaten einbezogen oder ausgeschlossen werden soll
Geräteliste Für Leistungsfilter	Kommagetrennte Liste der Geräte-IDs, die einbezogen oder ausgeschlossen werden sollen

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Problem:	Versuchen Sie dies:
Fehler: Die angeforderte Funktion ist derzeit nicht lizenziert	Installieren Sie die SYMAPI-Serverlizenz.
Fehler: Es wurden keine Geräte gefunden	Stellen Sie sicher, dass Symmetrix-Geräte vom Solutions Enabler-Server verwaltet werden: - Führen Sie die symcfg-Liste -V aus, um die Liste der konfigurierten Symmetrix-Geräte anzuzeigen.
Fehler: Ein angeforderter Netzwerkdienst wurde in der Servicedatei nicht gefunden	Stellen Sie sicher, dass der Solutions Enabler Service Name die netcnfg-Datei für Solutions Enabler definiert hat. Diese Datei befindet sich in der Regel unter SYMAPI\config\ in der Installation des Solutions Enabler-Clients.
Fehler: Die Handshake des Remote-Clients/Servers ist fehlgeschlagen	Überprüfen Sie die letzten speichersrvd.log*-Dateien auf dem Solutions Enabler-Host, den wir zu entdecken versuchen.
Fehler: Allgemeiner Name im Clientzertifikat ungültig	Bearbeiten Sie die Datei *Hosts* auf dem Solutions Enabler-Server, damit der Hostname der Acquisition Unit wie in der storsrvd.log auf dem Solutions Enabler-Server angegeben auf der IP-Adresse auflöst.
Fehler: Die Funktion konnte keinen Speicher abrufen	Stellen Sie sicher, dass genügend freier Speicherplatz im System vorhanden ist, um Solutions Enabler auszuführen
Fehler: Solutions Enabler konnte nicht alle erforderlichen Daten bereitstellen.	Untersuchen Sie den Integritätsstatus und das Lastprofil von Solutions Enabler
Fehler: • Der CLI-Befehl "symcfg list -tdev" gibt bei der Erfassung mit Solutions Enabler 7.x von einem Solutions Enabler Server 8.x. möglicherweise falsche Daten zurück • Der CLI-Befehl „symcfg list -srp“ kann bei der Erfassung mit Solutions Enabler 8.1.0 oder früher von einem Solutions Enabler Server 8.3 oder höher falsche Daten zurückgeben.	Vergewissern Sie sich, dass Sie die gleiche Solutions Enabler-Hauptversion verwenden

Problem:	Versuchen Sie dies:
Ich sehe Datenerhebungsfehler mit der Meldung "unbekannter Code"	Diese Meldung wird möglicherweise angezeigt, wenn Berechtigungen nicht in der Daemon-Konfigurationsdatei des Solutions Enabler Servers deklariert werden (siehe Anforderungenoben). Dabei wird davon ausgegangen, dass Ihre SE-Clientversion mit Ihrer SE-Serverversion übereinstimmt. Dieser Fehler kann auch auftreten, wenn der Benutzer *cisys* (der Solutions Enabler-Befehle ausführt) nicht mit den erforderlichen Daemon-Berechtigungen in der Konfigurationsdatei /var/symapi/config/daemon_users konfiguriert wurde. Um dies zu beheben, bearbeiten Sie die Datei /var/symapi/config/daemon_users und stellen Sie sicher, dass der cisys-Benutzer über die für den storapid-Daemon angegebene <all>-Berechtigung verfügt. Beispiel: 14:11:25 # tail /var/symapi/config/daemon_users … Cisys storapid <all>

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Datensammler Dell EMC VNX Block Storage (NaviCLI

Data Infrastructure Insights verwendet den Dell EMC VNX Block Storage (NaviSec) Data Collector (ehemals CLARiiON) zur Erfassung von Bestands- und Performance-Daten.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem EMC VNX Block Storage Data Collector. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Storage	Storage
Storage Processor	Storage-Node
Dieser Pool, RAID-Gruppe	Storage-Pool
LUN	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. In dieser Datenquelle fallen möglicherweise nicht alle Fälle an.

Anforderungen

Zur Datenerfassung müssen die folgenden Anforderungen erfüllt sein:

- Eine IP-Adresse jedes VNX-Blockspeicherprozessors
- Schreibgeschützter Navisphere-Benutzername und Kennwort für die VNX-Block-Speicher-Arrays

- Naviseccli muss auf der Data Infrastructure Insights AU installiert sein
- Zugriffsvalidierung: Führen Sie NaviSecCLI von der Data Infrastructure Insights AU zu jedem Array mit dem Benutzernamen und Passwort aus.
- Port-Anforderungen: 80, 443
- Naviseccli Version sollte mit dem neuesten FLARE-Code auf Ihrem Array entsprechen
- Zur Performance muss die Statistik-Protokollierung aktiviert sein.

Syntax der Navisphere Befehlszeilenschnittstelle

NaviSECCLI.exe -h <IP-Adresse> -user <user> -password <password> -scope <scope,use 0 for global Scope> -Port <use 443 by default> Command

Konfiguration

Feld	Beschreibung
VNX Block Storage-IP-Adresse	IP-Adresse oder vollqualifizierter Domain-Name des VNX-Blockspeichers
Benutzername	Name, der für die Anmeldung beim VNX-Block-Speichergerät verwendet wird.
Passwort	Passwort zur Anmeldung beim VNX-Block-Speichergerät.
CLI-Pfad zu NaviSECCLI.exe	Vollständiger Pfad zum Ordner mit der ausführbaren Datei *naviseccli.exe*

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40 Minuten.
Umfang	Der Umfang des sicheren Clients. Die Standardeinstellung ist Global.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Die Standardeinstellung ist 300 Sekunden.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: • Agent Wird Nicht Ausgeführt • Naviseccli konnte nicht gefunden werden • Fehler beim Ausführen eines Befehls	• Vergewissern Sie sich, dass Navisphere CLI auf der Cloud Insight Acquisition Unit installiert ist • Sie haben die Option „Secure Client verwenden“ im Assistenten für die Konfiguration des Datensammlers nicht ausgewählt und haben keine nicht sichere Version der Navisphere CLI installiert. • Vergewissern Sie sich, dass das Navisphere CLI-Installationsverzeichnis in der Data Collector-Konfiguration korrekt ist • Vergewissern Sie sich, dass die IP-Adresse des VNX-Blockspeichers in der Data Collector-Konfiguration korrekt ist: • Aus der Abteilung Data Infrastructure Insights Acquisition: ◦ Öffnen Sie eine CMD. ◦ Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis ◦ Versuchen Sie, eine Verbindung mit dem VNX-Blockspeichergerät herzustellen, indem Sie „navicli -h} ip {getagent“ eingeben (ersetzen Sie die {ip} durch die tatsächliche IP).
Fehler: 4.29 emc235848 emc241018 getall konnte keine Host-Alias-Info analysieren	Dies wird wahrscheinlich durch eine FLARE 29-Fehlerproblematik der Host-Initiator-Datenbank auf dem Array selbst verursacht. Siehe EMC Knowledge Base Artikel: Emc235848, emc241018. Sie können auch überprüfen https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128
Fehler: Die Meta-LUNs können nicht abgerufen werden. Fehler beim Ausführen von java -jar navicli.jar	• Ändern der Datensammlerkonfiguration zur Verwendung des sicheren Clients (empfohlen) • Installieren Sie navicli.jar im CLI-Pfad zu navicli.exe ODER NaviSECCLI.exe • Hinweis: navicli.jar ist ab EMC Navisphere Version 6.26 veraltet • Das navicli.jar steht möglicherweise auf http://powerlink.emc.com zur Verfügung
Fehler: Speicherpools melden keine Festplatten auf dem Serviceprozessor bei der konfigurierten IP-Adresse	Konfigurieren Sie den Datensammler mit beiden Service-Prozessor-IPs, getrennt durch Komma

Problem:	Versuchen Sie dies:
Fehler: Fehler bei nicht übereinstimmender Revision	• Dies wird normalerweise durch die Aktualisierung der Firmware auf dem VNX-Blockspeichergerät verursacht, aber nicht durch die Aktualisierung der Installation von NaviCLI.exe. Dies kann auch dadurch verursacht werden, dass verschiedene Geräte mit unterschiedlichen Firmwares installiert sind, aber nur eine CLI (mit einer anderen Firmware-Version). • Vergewissern Sie sich, dass sowohl das Gerät als auch der Host identische Versionen der Software ausführen: ◦ Öffnen Sie in der Data Infrastructure Insights Acquisition Unit ein Befehlszeilenfenster ◦ Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis ◦ Stellen Sie eine Verbindung mit dem CLARiiON-Gerät her, indem Sie „navicli -h <ip> getagent“ eingeben. ◦ Achten Sie auf die Versionsnummer auf den ersten Zeilen. Beispiel: „Agent Rev: 6.16.2 (0.1)“ ◦ Suchen und vergleichen Sie die Version in der ersten Zeile. Beispiel: „Navisphere CLI Revision 6.07.00.04.07“
Fehler: Nicht Unterstützte Konfiguration - Keine Fibre-Channel-Ports	Das Gerät ist nicht mit Fibre-Channel-Ports konfiguriert. Aktuell werden nur FC-Konfigurationen unterstützt. Überprüfen Sie, ob diese Version/Firmware unterstützt wird.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

DATENSAMMLUNG FÜR DELL EMC VNX File (ehemals Celerra Unified Storage System

Dieser Datensammler erfasst Bestandsinformationen vom VNX File Storage System. Für die Konfiguration benötigt dieser Datensammler die IP-Adresse der Speicherprozessoren sowie einen schreibgeschützten Benutzernamen und ein Kennwort.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem VNX File Data Collector. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Celerra Network Server/Celerra Storage-Pool	Storage-Pool
File-System	Internes Volumen
Data Mover	Controller
Auf einem Data Mover gemountet	Dateifreigabe
CIFS- und NFS-Exporte	Share
Festplatten-Volume	Back-End LUN

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Sie benötigen Folgendes, um diesen Datensammler zu konfigurieren:

- Die IP-Adresse des Speicherprozessors
- Schreibgeschützter Benutzername und Kennwort
- SSH-Port 22

Konfiguration

Feld	Beschreibung
VNX-Datei-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des VNX-Dateigeräts
Benutzername	Name, der zum Anmelden am VNX-Speichergerät verwendet wird
Passwort	Passwort zur Anmeldung beim VNX-Speichergerät

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (Minuten)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 20 Minuten.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: Fortfahren nicht möglich, während die DART-Aktualisierung ausgeführt wird	Mögliche Lösung: Unterbrechen Sie den Datensammler, und warten Sie, bis die DART-Aktualisierung abgeschlossen ist, bevor Sie eine andere Erfassungsanforderung versuchen.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Konfigurieren des Dell EMC VNX Unified Data Collectors

Für die Konfiguration benötigt der Dell EMC VNX Unified (SSH)-Datensammler die IP-Adresse der Control Station sowie einen schreibgeschützten Benutzernamen und ein Kennwort.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Festplattenordner	Festplattengruppe
File-System	Internes Volumen
Storage	Storage
Storage Processor	Storage-Node
Speicherpool, RAID-Gruppe	Storage-Pool
LUN	Datenmenge
Data Mover	Controller
Auf einem Data Mover gemountet	Dateifreigabe
CIFS- und NFS-Exporte	Share
Festplatten-Volume	Back-End LUN

Anforderungen

Sie benötigen Folgendes, um den VNX (SSH) Data Collector zu konfigurieren:

- VNX-IP-Adresse und Anmeldeinformationen an der Celerra Control Station.
- Nur-Lese-Benutzername und Kennwort.
- Der Datensammler kann NaviCLI/NaviSecCLI Befehle gegen das Backend-Array ausführen, das die DART OS NAS Heads verwendet

Konfiguration

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

Erweiterte Konfigiration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 40 Minuten.
Leistungsintervall (Sek.).	Intervall zwischen Performance-Abstimmungen Die Standardeinstellung ist 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Konfigurieren des EMC VPLEX-Datensammlers

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

> Die Performance-Erfassung von Data Infrastructure Insights aus VPLEX-Clustern erfordert, dass der Performance-Archivierungsservice betriebsbereit ist, um die CSV-Dateien und Protokolle zu füllen, die Data Infrastructure Insights über SCP-basierte Dateikopien abruft. NetApp hat beobachtet, dass viele Updates der VPLEX-Firmware-Upgrades/Management Station diese Funktionen nicht mehr betriebsbereit machen werden. Kunden, die ein solches Upgrade planen, fragen Dell/EMC möglicherweise proaktiv, ob ihr geplantes Upgrade diese Funktion nicht mehr funktionsfähig bleibt. Wenn ja, wie kann sie die IT neu aktivieren, um Lücken bei der Performance-Sichtbarkeit zu minimieren? Der VPLEX-Performance-Code von Cloud Insight bewertet bei jeder Umfrage, ob alle erwarteten Dateien vorhanden sind und ob sie ordnungsgemäß aktualisiert werden. Fehlen oder sind sie veraltet, protokolliert Data Infrastructure Insights Fehler bei der Performance-Erfassung.

Terminologie

Data Infrastructure Insightst erfasst die folgenden Bestandsinformationen aus dem VPLEX-Datensammler. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Cluster	Storage
Motor	Storage-Node
Gerät, Systemumfang	Back-End Storage-Pool
Virtual Volume	Datenmenge
Front-End-Port, Back-End-Port	Port
Verteiltes Gerät	Storage-Synchronisierung
Übersicht Storage	Volume Map, Volume Mask
Storage Volume	Back-End LUN

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
ITLS	Back-End-Pfad

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Eine IP-Adresse der VPLEX Management Console
- Domänenkonto auf Administratorebene für den VPLEX-Server
- Port 443 (HTTPS). Erfordert eine ausgehende Verbindung zum TCP-Port 443 auf der VPLEX-Managementstation.
- Für die Leistung können Sie den schreibgeschützten Benutzernamen und das Kennwort für den ssh/scp-Zugriff verwenden.
- Für die Leistung ist Port 22 erforderlich.

Konfiguration

Feld	Beschreibung
IP-Adresse der VPLEX Management Console	IP-Adresse oder vollqualifizierter Domänenname der VPLEX Management Console
Benutzername	Benutzername für VPLEX-CLI
Passwort	Passwort, das für die VPLEX-CLI verwendet wird
Remote-IP-Adresse für die Performance	Performance Remote IP-Adresse der VPLEX Management Console
Performance Remote User Name	Performance Remote-Benutzername der VPLEX Management Console
Kennwort Für Das Remote-Netzwerk Der Performance	Remote-Kennwort für die Performance der VPLEX Management Console

Erweiterte Konfiguration

Feld	Beschreibung
Kommunikations-Port	Für VPLEX-CLI verwendeter Port. Der Standardwert ist 443.
Abfrageintervall für Bestand (min)	Die Standardeinstellung ist 20 Minuten.
Anzahl der Verbindungsversuche	Der Standardwert ist 3.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Die Standardeinstellung ist 600 Sekunden.
Anzahl Wiederholungen	Der Standardwert ist 2.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

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

Performance

Problem:	Versuchen Sie dies:
Fehler: VPLEX-Performance für Version unter 5.3 wird nicht unterstützt.	Aktualisieren Sie VPLEX auf 5.3 oder höher
Fehler: Es wurden nicht genügend Daten erfasst.	• Prüfen Sie den Zeitstempel der Sammlung in der Protokolldatei und ändern Sie das Abfrageintervall entsprechend • Warten Sie länger
Fehler: Unbefristete Log-Dateien werden nicht aktualisiert.	Wenden Sie sich an den EMC Support, um die Aktualisierung der unbefristeten Protokolldateien zu aktivieren
Fehler: Das Abfrageintervall für die Performance ist zu groß.	Überprüfen Sie den Sammlungs-Zeitstempel in der Protokolldatei €{logfile} und ändern Sie das Abfrageintervall entsprechend
Fehler: Performance Remote IP-Adresse der VPLEX Management Console ist nicht konfiguriert.	Bearbeiten Sie die Datenquelle, um die Performance Remote IP-Adresse der VPLEX Management Console festzulegen.
Fehler: Keine Leistungsdaten vom Director gemeldet	• Überprüfen Sie, ob die System-Performance-Monitore ordnungsgemäß ausgeführt werden • Bitte wenden Sie sich an den EMC Support, um die Aktualisierung der Protokolldateien des Systems Performance Monitor zu ermöglichen

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Dell EMC XtremeIO-Datensammler

Der EMC XtremIO Data Collector erwirbt Bestands- und Performance-Daten vom EMC XtremIO Storage-System.

Anforderungen

Zum Konfigurieren des EMC XtremIO (HTTP) Datensammlers sind folgende Funktionen erforderlich:

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

Terminologie

Data Infrastructure Insights bezieht die folgenden Inventarinformationen aus dem EMC XtremIO Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese

Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte (SSD)	Festplatte
Cluster	Storage
Controller	Storage-Node
Datenmenge	Datenmenge
LUN-Zuordnung	Volume-Zuordnung
Ziel-FC-Initiator	Volume-Maske

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. In dieser Datenquelle fallen möglicherweise nicht alle Fälle an.

Anforderungen

- Die XMS-Host-IP-Adresse des XtremIO Management Servers (XMS)
- Administratorbenutzername und -Passwort für den XtremIO

Konfiguration

Feld	Beschreibung
XMS Host	IP-Adresse oder vollqualifizierter Domain-Name des XtremIO Management Servers
Benutzername	Benutzername für den XtremIO Management Server
Passwort	Passwort für den XtremIO Management Server

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port für die Verbindung mit dem XtremIO Management Server. Der Standardwert ist 443.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 60 Minuten.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Die Standardeinstellung ist 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Fujitsu ETERNUS Datensammler

Der Fujitsu ETERNUS-Datensammler erfasst Bestandsdaten über administrativen Zugriff

auf das Speichersystem.

Terminologie

Data Infrastructure Insights bezieht die folgenden Bestandsinformationen aus dem Fujitsu ETERNUS Storage. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Storage	Storage
Thin Pool, Flexible Tier Pool, Raid-Gruppe	Storage-Pool
Standard-Volume, Snap Data Volume (SDV), Snap Data Pool Volume (SDPV), Thin Provisioning Volume (TPV), Flexible Tier Volume (FTV), Wide Striping Volume (WSV)	Datenmenge
Channel-Adapter	Controller

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diese Datensammlung möglicherweise nicht alle Fälle dar.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Eine IP-Adresse des ETERNUS-Speichers, die nicht durch Komma getrennt werden kann
- Benutzername und Passwort der SSH-Administration
- Anschluss 22
- Stellen Sie sicher, dass die Seitenscrollen deaktiviert ist (clienv-show-more-Scroll deaktiviert)

Konfiguration

Feld	Beschreibung
IP-Adresse des ETERNUS-Speichers	IP-Adresse des ETERNUS-Speichers
Benutzername	Benutzername für ETERNUS-Speicher
Passwort	Passwort für den ETERNUS-Speicher

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Die Standardeinstellung ist 20 Minuten.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Fehler beim Abrufen von Daten“ mit Fehlermeldungen „Error Finding prompt CLI“ oder „Error Finding prompt at the end of Shell results“	Wahrscheinlich verursacht durch: Speichersystem hat Seite Scrollen aktiviert. Mögliche Lösung: * Versuchen Sie, den Bildlauf zu deaktivieren, indem Sie den folgenden Befehl ausführen: Clienv-show-more -scroll disable
„Verbindungsfehler“ mit Fehlermeldungen „konnte eine SSH-Verbindung zum Storage nicht instanziieren“ oder „Verbindung zum VirtualCenter konnte nicht hergestellt werden“	Wahrscheinliche Ursachen: * Falsche Anmeldeinformationen. * Falsche IP-Adresse. * Netzwerkproblem. * Storage kann ausgefallen oder nicht mehr reagiert werden. Mögliche Lösungen: * Überprüfen Sie die eingegebenen Anmeldeinformationen und die eingegebene IP-Adresse. * Versuchen Sie, mit dem Speicher über SSH Client zu kommunizieren.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

NetApp Google Compute Data Collector

Dieser Datensammler unterstützt Inventar- und Performance-Erfassung aus Google Compute Cloud-Plattformkonfigurationen. Dieser Sammler wird versuchen, alle Computing-Ressourcen in allen Projekten innerhalb einer Google-Organisation zu entdecken. Wenn Sie über mehrere Google-Unternehmen verfügen, die Sie mit Data Infrastructure Insights ermitteln möchten, möchten Sie pro Unternehmen einen Data Infrastructure Insights Collector implementieren.

Anforderungen Für Servicekonten

- Sie müssen ein Service-Konto erstellen, indem Sie die Anweisungen in befolgen"Erstellen/Verwalten Von Servicekonten". Ein solches Dienstkonto wird durch eine eindeutige ID identifiziert, die als *ClientID* bezeichnet wird und als Benutzername verwendet wird.
- Erstellen Sie außerdem einen Servicekontoschlüssel, indem Sie die Anweisungen in befolgen"Erstellen/Verwalten Von Servicekontoschlüsseln". Dieser Schlüssel kann als json-Datei heruntergeladen werden, deren Inhalt als Passwort verwendet wird.
- Das Servicekonto muss für *Compute.Readonly*, *Monitoring.read* und *Cloud-Platform* berücksichtigt werden.

Konfiguration

Feld	Beschreibung
Organisation-ID	Die Organisations-ID, die Sie mit diesem Sammler entdecken möchten. Dieses Feld ist erforderlich, wenn Ihr Servicekonto mehr als eine Organisation sehen kann
Wählen Sie „Ausschließen“ oder „Einschließen“, um GCP-Projekte nach IDs zu filtern	Wenn Sie einschränken möchten, welche Projektressourcen in Data Infrastructure Insights einfließen.

Feld	Beschreibung
Projekt-IDs	Die Liste der Projekt-IDs, die Sie in oder aus der Erkennung filtern möchten, hängt vom Wert des Werts "Ausschließen"… ab. Die Standardliste ist leer
Client-ID	Client-ID für die Konfiguration der Google Cloud Platform
Kopieren Sie den Inhalt Ihrer Google Credential-Datei hier	Kopieren Sie Ihre Google-Anmeldedaten für das Cloud-Plattform-Konto in dieses Feld

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten
Wählen Sie „Exclude“ oder „include“, um VMs nach Etiketten filtern zu können	Geben Sie an, ob VM’s by Labels beim Sammeln von Daten einbezogen oder ausgeschlossen werden sollen. Wenn ‘include’ ausgewählt ist, kann das Feld Label Key nicht leer sein.
Bezeichnungsschlüssel und Werte, auf denen VMs gefiltert werden sollen	Klicken Sie auf **+ Filter Label**, um die VMs (und zugehörigen Festplatten) auszuwählen, die durch Filtern nach Schlüsseln und Werten, die Schlüssel und Werte der Labels auf der VM entsprechen, einzuschließen bzw. auszuschließen. Etikettenschlüssel ist erforderlich, Etikettenwert ist optional. Wenn der Etikettenwert leer ist, wird die VM solange gefiltert, wie sie dem Etikettenschlüssel entspricht.
Leistungsintervall (Sek.)	Der Standardwert ist 1800 Sekunden

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Google Cloud NetApp Volumes Datensammler

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

Anforderungen Für Servicekonten

- Sie müssen ein Service-Konto erstellen, indem Sie die Anweisungen in befolgen"Erstellen/Verwalten Von Servicekonten". Dieses Dienstkonto wird durch eine eindeutige ID identifiziert, die als *clientId* bezeichnet wird und als Benutzername verwendet wird.
- Erstellen Sie außerdem einen Servicekontoschlüssel, indem Sie die Anweisungen in

befolgen"Erstellen/Verwalten Von Servicekontoschlüsseln". Dieser Schlüssel kann als json-Datei heruntergeladen werden, deren Inhalt als Passwort verwendet wird.

- Das Servicekonto muss für *Compute.Readonly*, *Monitoring.read* und *Cloud-Platform* berücksichtigt werden.

Konfiguration

Feld	Beschreibung
Organisation-ID	Die Organisations-ID, die Sie mit diesem Sammler entdecken möchten. Dieses Feld ist erforderlich, wenn Ihr Servicekonto mehr als eine Organisation sehen kann
Wählen Sie „Ausschließen“ oder „Einschließen“, um GCNV-Assets nach Standort zu filtern	Dies wird standardmäßig ausgeschlossen, da dieser Collector standardmäßig beabsichtigt, alle GCNV-Volumes weltweit in Ihrem Unternehmen zu ermitteln.
GCNV Exclude/Include Locations	Dies ist standardmäßig leer und wird in Verbindung mit der Option „Wählen Sie ‚Ausschließen‘ oder ‚Einschließen‘“ verwendet. Wenn Sie Assets nur in bestimmten Regionen ermitteln möchten, verwenden Sie diese beiden Optionen, um den Umfang dieses Collectors einzuschränken.
Projekt-IDs	Die Liste der Projekt-IDs, die Sie in oder aus der Erkennung filtern möchten, hängt vom Wert des Werts "Ausschließen"… ab. Die Standardliste ist leer
Client-ID	Client-ID für die Konfiguration der Google Cloud Platform
Kopieren Sie den Inhalt Ihrer Google Credential-Datei hier	Kopieren Sie Ihre Google-Anmeldedaten für das Cloud-Plattform-Konto in dieses Feld

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten
Verwenden Sie AU-Proxy für REST-API-Aufrufe	Wählen Sie diese Option, damit der Collector denselben Proxy verwendet wie die Acquisition Unit, auf der er sich befindet. Standardmäßig ist diese Option deaktiviert. Der Collector versucht daher, HTTPS-API-Aufrufe direkt an Google zu senden.
Bezeichnungsschlüssel und Werte, auf denen VMs gefiltert werden sollen	Klicken Sie auf **+ Filter Label**, um die VMs (und zugehörigen Festplatten) auszuwählen, die durch Filtern nach Schlüsseln und Werten, die Schlüssel und Werte der Labels auf der VM entsprechen, einzuschließen bzw. auszuschließen. Etikettenschlüssel ist erforderlich, Etikettenwert ist optional. Wenn der Etikettenwert leer ist, wird die VM solange gefiltert, wie sie dem Etikettenschlüssel entspricht.

Feld	Beschreibung
Leistungsintervall (Sek.)	Der Standardwert ist 300 Sekunden

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

HP Enterprise

HP Enterprise Alletra 9000 / Primera Storage Datensammler

Data Infrastructure Insights verwendet den Datensammler HP Enterprise Alletra 9000 / HP Enterprise Primera (ehemals 3PAR) zur Ermittlung von Bestand und Leistung.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Feld	Beschreibung
Physisches Laufwerk	Festplatte
Storage-System	Storage
Controller-Node	Storage-Node
Gemeinsame Bereitstellungsgruppe	Storage-Pool
Virtual Volume	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- IP-Adresse oder FQDN des InServ-Clusters
- Für den Bestand können Sie den schreibgeschützten Benutzernamen und das Kennwort für den StoreServ Server verwenden
- Für eine bessere Leistung können Sie den Benutzernamen und das Kennwort für Lese- und Schreibvorgänge auf dem StoreServ Server verwenden
- Port-Anforderungen: 22 (Bestandsaufnahme), 5988 oder 5989 (Performance-Sammlung) [Hinweis: Leistung wird für StoreServ OS 3.x+ unterstützt]
- Bei der Erfassung der Performance bestätigen Sie, dass SMI-S durch Anmeldung am Array über SSH aktiviert ist.

Konfiguration

Feld	Beschreibung
Storage-IP-Adresse	Speicher-IP-Adresse oder vollqualifizierter Domain-Name des StoreServ-Clusters
Benutzername	Benutzername für den StoreServ Server
Passwort	Passwort, das für den StoreServ Server verwendet wird
SMI-S-Benutzername	Benutzername für den SMI-S Provider Host
SMI-S-Passwort	Passwort, das für den SMI-S Provider-Host verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 40 Minuten.
SMI-S-Konnektivität	Protokoll für die Verbindung mit dem SMI-S-Provider
SMI-S-Standardport überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport von SMI-S Connectivity. Andernfalls geben Sie den zu verwendenden Verbindungsport ein
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Die Standardeinstellung ist 300 Sekunden.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

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

Performance

Problem:	Versuchen Sie dies:
Verbindung oder Anmeldung fehlgeschlagen. Fehler bei der Initialisierung des Providers.	Ein Name eines rein numerischen Arrays kann Probleme mit dem SMI-S-Server verursachen. Versuchen Sie, den Namen des Arrays zu ändern.
Der konfigurierte SMI-S-Benutzer verfügt über keine Domäne	Gewähren Sie dem konfigurierten SMI-S-Benutzer entsprechende Domänenberechtigungen

Problem:	Versuchen Sie dies:
Data Infrastructure Insights gibt an, dass keine Verbindung zum SMI-S-Service hergestellt bzw. angemeldet werden kann.	Vergewissern Sie sich, dass es keine Firewall zwischen der CI AU und dem Array gibt, die die CI AU daran versperren würde, TCP-Verbindungen zu 5988 oder 5989 zu machen. Sobald das geschehen ist, und wenn Sie bestätigt haben, dass es keine Firewall gibt, sollten Sie SSH auf das Array, und verwenden Sie den "showcim" Befehl zu bestätigen. Überprüfen Sie, dass: * Dienst aktiviert ist * HTTPS-Port sollte 5989 sein. Wenn alle diese sind, können Sie versuchen, „stopcim“ und dann ein „startcim“, um den CIM neu zu starten (d.h. SMI-S-Service).

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

HP Enterprise Command View-Datensammler

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

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem HP Enterprise Command View-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
PDEV	Festplatte
Journalpool	Festplattengruppe
Storage Array Durchführt	Storage
Port Controller	Storage-Node
Array-Gruppe, DP-Pool	Storage-Pool
Logische Einheit, LDEV	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Inventaranforderungen

Zur Erfassung von Bestandsdaten müssen Sie Folgendes haben:

- IP-Adresse des CVAE-Servers
- Schreibgeschützter Benutzername und Kennwort für die CVAE-Software und die Peer-Rechte
- Port-Anforderung: 2001

Performance-Anforderungen erfüllt

Zur Erfassung von Leistungsdaten müssen die folgenden Anforderungen erfüllt sein:

- HDS USP, USP V und VSP Performance
  - Performance Monitor muss lizenziert sein.
  - Überwachungsschalter muss aktiviert sein.
  - Das Export-Tool (Export.exe) muss in die Data Infrastructure Insights AU kopiert und an einen Speicherort extrahiert werden. Stellen Sie unter CI Linux aus sicher, dass „cisys“ Berechtigungen gelesen und ausgeführt hat.
  - Die Version des Exportwerkzeugs muss mit der Microcode-Version des Ziel-Arrays übereinstimmen.
- AMS-Leistung:
  - Performance Monitor muss lizenziert sein.
  - Das CLI-Dienstprogramm Storage Navigator Modular 2 (SNM2) wird auf der Data Infrastructure Insights AU installiert.
- Netzwerkanforderungen
  - Die Exportwerkzeuge sind Java-basiert und verwenden RMI, um mit dem Array zu sprechen. Diese Tools sind möglicherweise nicht für die Firewall geeignet, da sie auf jedem Aufruf dynamisch die Quell- und Ziel-TCP-Ports aushandeln können. Außerdem verhalten sich die Export-Tools der verschiedenen Modell-Arrays im Netzwerk möglicherweise unterschiedlich - Fragen Sie HPE nach den Anforderungen Ihres Modells

Konfiguration

Feld	Beschreibung
Command View Server	IP-Adresse oder vollqualifizierter Domain-Name des Command View Servers
Benutzername	Benutzername für den Command View Server.
Passwort	Passwort, das für den Command View-Server verwendet wird.
GERÄTE – VSP G1000 (R800), VSP (R700), HUS VM (HM700) UND USP-SPEICHER	Geräteliste für VSP G1000 (R800), VSP (R700), HUS VM (HM700) und USP-Speicher. Jeder Speicher benötigt: * Array IP: IP-Adresse des Speichers * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher * Ordner mit Export Utility JAR-Dateien
SNM2Geräte - WMS/SMS/AMS-Speicher	Geräteliste für WMS/SMS/AMS-Speicher. Jeder Speicher benötigt: * Array’s IP: IP address of the Storage * Storage Navigator CLI Pfad: SNM2 CLI Pfad * Konto Authentifizierung gültig: Wählen Sie gültige Konto Authentifizierung * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher
Wählen Sie Tuning Manager für Leistung	Andere Leistungsoptionen überschreiben
Tuning Manager Host	IP-Adresse oder vollqualifizierter Domain-Name des Tuning Managers

Feld	Beschreibung
Tuning-Manager-Port	Port, der für Tuning Manager verwendet wird
Benutzername Für Tuning Manager	Benutzername für Tuning Manager
Kennwort Für Tuning-Manager	Passwort für Tuning Manager

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

Erweiterte Konfiguration

Feld	Beschreibung
Command View Server Port	Port, der für den Command View Server verwendet wird
HTTPS aktiviert	Wählen Sie diese Option aus, um HTTPS zu aktivieren
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten aufgeführte Array-Liste beim Sammeln von Daten aufgenommen oder ausgeschlossen werden soll.
Schließen Sie Geräte aus oder schließen Sie sie ein	Kommagetrennte Liste der Geräte-IDs oder Array-Namen, die einbezogen oder ausgeschlossen werden sollen
Abfrage-Host-Manager	Wählen Sie diese Option aus, um den Hostmanager abzufragen
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: Benutzer hat nicht genügend Berechtigung	Verwenden Sie ein anderes Benutzerkonto, das über mehr Berechtigungen verfügt oder die Berechtigung des Benutzerkontos, das im Datensammler konfiguriert ist, erhöht
Fehler: Speicherliste ist leer. Entweder sind Geräte nicht konfiguriert oder der Benutzer verfügt nicht über ausreichende Berechtigungen	* Verwenden Sie DeviceManager, um zu überprüfen, ob die Geräte konfiguriert sind. * Verwenden Sie ein anderes Benutzerkonto, das mehr Berechtigungen hat, oder erhöhen Sie die Berechtigung des Benutzerkontos
Fehler: HDS Speicher-Array wurde einige Tage lang nicht aktualisiert	Untersuchen Sie, warum dieses Array in HP CommandView AE nicht aktualisiert wird.

Performance

Problem:	Versuchen Sie dies:
Fehler: * Fehler beim Ausführen des Exportdienstprogramms * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass das Exportdienstprogramm auf der Data Infrastructure Insights Acquisition Unit installiert ist * Bestätigen Sie, dass der Speicherort des Exportdienstprogramms in der Data Collector-Konfiguration korrekt ist * Bestätigen Sie, dass die IP des USP/R600-Arrays in der Konfiguration des Data Collectors korrekt ist * Öffnen Sie einen CMD und das Kennwort in der Konfiguration des Data Collectors * Bestätigen Sie, dass die Export Utility-Version mit der Speicher-Microcode-Version kompatibel ist * aus der Data Infrastructure Insights Acquisition Unit, öffnen Sie eine CMD - Aufforderung zur Installation mit dem folgenden Ordner konfigurieren: runWin.bat
Fehler: Export Tool-Anmeldung für Ziel-IP fehlgeschlagen	* Bestätigen Sie, dass Benutzername/Passwort korrekt ist * Erstellen Sie eine Benutzer-ID hauptsächlich für diesen HDS-Datensammler * Bestätigen Sie, dass keine anderen Datensammler für die Erfassung dieses Arrays konfiguriert sind
Fehler: Exportwerkzeuge protokolliert "Zeitbereich für Überwachung nicht abrufen".	* Bestätigung der Leistungsüberwachung auf dem Array ist aktiviert. * Versuchen Sie, die Exportwerkzeuge außerhalb von Data Infrastructure Insights aufzurufen, um zu bestätigen, dass das Problem außerhalb von Data Infrastructure Insights liegt.
Fehler: * Konfigurationsfehler: Speicher-Array wird vom Exportdienstprogramm nicht unterstützt * Konfigurationsfehler: Speicher-Array wird nicht von Speicher-Navigator Modular CLI unterstützt	* Nur unterstützte Storage-Arrays konfigurieren. * Verwenden Sie „Filter Device List“, um nicht unterstützte Speicher-Arrays auszuschließen.
Fehler: * Fehler beim Ausführen des externen Befehls * Konfigurationsfehler: Speicher-Array nicht gemeldet von Inventory * Konfigurationsfehler:Exportordner enthält keine JAR-Dateien	* Überprüfen Sie den Speicherort des Exportdienstprogramms. * Prüfen Sie, ob Speicher-Array in Frage in Command View Server konfiguriert ist * Festlegen des Performance-Abfrageintervalls als mehrere 60 Sekunden.
Fehler: * Fehler Storage Navigator CLI * Fehler beim Ausführen von auPerform Befehl * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass Storage Navigator Modular CLI auf der Data Infrastructure Insights Acquisition Unit installiert ist * Bestätigen Sie, dass Storage Navigator Modular CLI-Speicherort in der Data Collector-Konfiguration korrekt ist * Bestätigen Sie, dass die IP des WMS/SMS/SMS-Arrays in der Konfiguration des Data Collectors korrekt ist * Bestätigen Sie, dass Storage Navigator Modular CLI-Version kompatibel ist mit Microcode-Version des Speicher-Arrays konfiguriert im Data Collector * von der Data Infrastructure Insights Acquisition Unit, öffnen Sie eine CMD-Eingabeaufforderung und führen Sie den folgenden Befehl aus:

Problem:	Versuchen Sie dies:
Fehler: Konfigurationsfehler: Speicher-Array wird vom Inventory nicht gemeldet	Überprüfen Sie, ob Speicher-Array in Frage im Command View-Server konfiguriert ist
Fehler: * Kein Array ist beim Speicher Navigator Modular 2 CLI registriert * Array ist nicht bei der Speicher Navigator Modular 2 CLI registriert * Konfigurationsfehler: Speicher-Array nicht bei StorageNavigator Modular CLI registriert	* Öffnen Sie die Eingabeaufforderung und ändern Sie das Verzeichnis in den konfigurierten Pfad * führen Sie den Befehl „set=STONAVM_HOME=“ aus. * Führen Sie den Befehl „auunitref“ aus * Bestätigen Sie, dass die Befehlsausgabe Details des Arrays mit IP enthält * Wenn die Ausgabe keine Array-Details enthält, registrieren Sie das Array mit Storage Navigator CLI: - Öffnen Sie die Eingabeaufforderung und ändern Sie das Verzeichnis auf den konfigurierten Pfad - führen Sie den Befehl „set=STONAVM_HOME=“ aus. - Führen Sie den Befehl „auunitaddauto -ip{ip}“ aus. Ersetzen Sie{ip} durch echtes IP

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

HPE Alletra 6000 Datensammler

Der HP Enterprise Alletra 6000 (vormals Nimble) Datensammler unterstützt Bestands- und Performancedaten von Alletra 6000 Storage Arrays.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dieser Sammlung. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Array Erledigen	Storage
Festplatte	Festplatte
Datenmenge	Datenmenge
Pool	Storage-Pool
Initiator	Storage-Host-Alias
Controller	Storage-Node
Fibre Channel-Schnittstelle	Controller

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Zum Erfassen von Bestands- und Konfigurationsdaten aus dem Speicher-Array müssen Sie Folgendes haben:

- Das Array muss installiert und konfiguriert sein und über den Client über seinen vollständig qualifizierten

Domänennamen (FQDN) oder die Array-Management-IP-Adresse erreichbar sein.

- Auf dem Array muss NimbleOS 2.3.x oder höher ausgeführt werden.
- Sie müssen einen gültigen Benutzernamen und ein Kennwort für das Array mit der Rolle „Operator“ besitzen. Die „Gast“-Rolle verfügt nicht über ausreichenden Zugriff, um Initiator-Konfigurationen zu verstehen.
- Port 5392 muss auf dem Array geöffnet sein.

Zum Erfassen von Performance-Daten aus dem Speicher-Array müssen Sie Folgendes haben:

- Auf dem Array muss NimbleOS 4.0.0 oder höher ausgeführt werden
- Für das Array müssen Volumes konfiguriert sein. Die einzige Performance-API, die NimbleOS bietet, gilt für Volumes. Alle Statistiken zu Data Infrastructure Insights Berichten werden aus den Statistiken zu Volumes abgeleitet

Konfiguration

Feld	Beschreibung
Array-Management-IP-Adresse	Vollständig qualifizierter Domain-Name (FQDN) oder Array-Management-IP-Adresse.
Benutzername	Benutzername für das Array
Passwort	Kennwort für das Array

Erweiterte Konfiguration

Feld	Beschreibung
Port	Der von Nimble REST API verwendete Port. Der Standardwert ist 5392.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 60 Minuten.

Hinweis: Das Standard-Performance-Abfrageintervall beträgt 300 Sekunden und kann nicht geändert werden. Dies ist das einzige von HPE Alletra 6000 unterstützte Intervall.

Hitachi Data Systems (Hds)

Datensammler der Hitachi Vantara Command Suite

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

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Datensammler der Hitachi Vantara Command Suite. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
PDEV	Festplatte
Journalpool	Festplattengruppe
Storage Array Durchführt	Storage
Port Controller	Storage-Node
Array-Gruppe, HDS-Pool	Storage-Pool
Logische Einheit, LDEV	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Storage

Die folgenden Begriffe beziehen sich auf Objekte oder Referenzen, die auf HDS Storage Asset Landing Pages zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Name – kommt direkt aus dem Attribut „Name“ des HDS HiCommand Device Managers über den GetStorageArray XML API-Aufruf
- Modell - kommt direkt aus dem „arrayType“-Attribut des HDS HiCommand Device Managers über den GetStorageArray XML API-Aufruf
- Anbieter – HDS
- Family - kommt direkt aus dem Attribut „arrayFamily“ des HDS HiCommand Device Managers über den GetStorageArray XML API-Aufruf
- IP – hierbei handelt es sich um die Management-IP-Adresse des Arrays, keine vollständige Liste aller IP-Adressen im Array
- Rohkapazität: Ein base2-Wert, der die Summe der Gesamtkapazität aller Festplatten in diesem System darstellt, unabhängig von der Festplattenrolle.

Storage-Pool

Die folgenden Begriffe beziehen sich auf Objekte oder Referenzen, die auf HDS Storage Pool Asset Landing Pages zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Typ: Der Wert hier ist einer von:
  - RESERVIERT – Wenn dieser Pool für andere Zwecke als Datenvolumes, i.e, Journaling, Snapshots bestimmt ist
  - Thin Provisioning – wenn es sich um einen HDP-Pool handelt
  - RAID-Gruppe – aus ein paar Gründen werden Sie diese wahrscheinlich nicht sehen:

    Data Infrastructure Insights ist ein starker Standpunkt, um zu vermeiden, dass bei allen Kosten eine doppelte Kapazität gezählt wird. Auf HDS muss man normalerweise RAID-Gruppen von Festplatten erstellen, Pool-Volumes auf diesen RAID-Gruppen erstellen und Pools (oft HDP, könnte aber besonderer Zweck sein) aus diesen Pool Volumes erstellen. Wenn Data Infrastructure Insights sowohl die zugrunde liegenden RAID-Gruppen wie auch die Pools meldet, würde die Summe ihrer Rohkapazität die Summe der Festplatten erheblich übersteigen.

Stattdessen verkleinert der Datensammler HDS Command Suite von Data Infrastructure Insights die Größe von RAID-Gruppen willkürlich nach der Kapazität von Pool Volumes. Dies kann dazu führen, dass Data Infrastructure Insights die RAID-Gruppe überhaupt nicht meldet. Darüber hinaus werden alle resultierenden RAID-Gruppen so gekennzeichnet, dass sie in der Data Infrastructure Insights WebUI nicht sichtbar sind, aber sie fließen in das Data Warehouse (DWH) von Data Infrastructure Insights ein. Der Zweck dieser Entscheidungen ist es, UI-Gerinnung für Dinge zu vermeiden, die den meisten Benutzern egal sind – wenn Ihr HDS-Array RAID-Gruppen mit 50 MB frei hat, können Sie diesen freien Speicherplatz wahrscheinlich nicht für ein sinnvolles Ergebnis nutzen.

- Node – k. A., da HDS Pools nicht an einen bestimmten Node gebunden sind
- Redundanz: Der RAID-Level des Pools. Möglicherweise mehrere Werte für einen HDP-Pool, die aus mehreren RAID-Typen bestehen
- Kapazität % - der Prozentsatz, der für die Datenverwendung des Pools verwendet wird, wobei die verwendete GB und die gesamte logische GB-Größe des Pools verwendet werden
- Überzuviel Kapazität - ein abgeleiteter Wert, der angibt, „die logische Kapazität dieses Pools wird durch diesen Prozentsatz überzeichnet, aufgrund der Summe der logischen Volumes, die die logische Kapazität des Pools um diesen Prozentsatz überschreiten“
- Snapshot - zeigt die Kapazität an, die für die Snapshot-Nutzung in diesem Pool reserviert ist

Storage-Node

Die folgenden Begriffe beziehen sich auf Objekte oder Referenzen, die auf den HDS Storage Node Asset Landing Pages zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Name: Der Name des Front-End-Director (FED) oder Channel-Adapters auf monolithischen Arrays oder der Name des Controllers auf einem modularen Array. Ein bestimmtes HDS-Array verfügt über zwei oder mehr Storage-Nodes
- Volumes – die Volume-Tabelle zeigt jedes Volume an, das einem beliebigen Port dieses Speicherknoten zugeordnet ist

Inventaranforderungen

Zur Erfassung von Bestandsdaten müssen Sie Folgendes haben:

- IP-Adresse des HiCommand Device Manager-Servers
- Schreibgeschützter Benutzername und Kennwort für die HiCommand Device Manager-Software und Peer-Berechtigungen
- Port-Anforderungen: 2001 (http) oder 2443 (https)
- Melden Sie sich mit Benutzernamen und Kennwort bei der HiCommand Device Manager-Software an
- Überprüfen Sie den Zugriff auf HiCommand Device Manager http://<HiCommand_Device_Manager_IP>:2001/Service/StorageManager

Performance-Anforderungen erfüllt

Zur Erfassung von Leistungsdaten müssen die folgenden Anforderungen erfüllt sein:

- HDS USP, USP V und VSP Performance
  - Performance Monitor muss lizenziert sein.
  - Überwachungsschalter muss aktiviert sein.

- Das Export-Tool (Export.exe) muss in die Data Infrastructure Insights AU kopiert werden.
- Die Version des Exportwerkzeugs muss mit der Microcode-Version des Ziel-Arrays übereinstimmen.

- AMS-Leistung:
  - NetApp empfiehlt dringend, ein dediziertes Dienstkonto auf AMS-Arrays zu erstellen, damit Dateninfrastrukturdaten zum Abrufen von Leistungsdaten verwendet werden können. Storage Navigator ermöglicht nur ein Benutzerkonto, das gleichzeitig mit dem Array angemeldet ist. Wenn Data Infrastructure Insights dasselbe Benutzerkonto wie Verwaltungsskripte oder HiCommand verwendet, kann es dazu kommen, dass Data Infrastructure Insights, Verwaltungsskripte oder HiCommand aufgrund der Beschränkung der gleichzeitigen Anmeldung eines Benutzerkontos nicht mit dem Array kommunizieren kann
  - Performance Monitor muss lizenziert sein.
  - Das CLI-Dienstprogramm Storage Navigator Modular 2 (SNM2) muss auf der Data Infrastructure Insights AU installiert werden.

Konfiguration

Feld	Beschreibung
HiCommand Server	IP-Adresse oder vollqualifizierter Domänenname des HiCommand Device Manager-Servers
Benutzername	Benutzername für den HiCommand Device Manager-Server.
Passwort	Passwort, das für den HiCommand Device Manager-Server verwendet wird.
GERÄTE – VSP G1000 (R800), VSP (R700), HUS VM (HM700) UND USP-SPEICHER	Geräteliste für VSP G1000 (R800), VSP (R700), HUS VM (HM700) und USP-Speicher. Jeder Speicher benötigt: * Array IP: IP-Adresse des Speichers * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher * Ordner mit Export Utility JAR-Dateien
SNM2Geräte - WMS/SMS/AMS-Speicher	Geräteliste für WMS/SMS/AMS-Speicher. Jeder Speicher benötigt: * Array's IP: IP address of the Storage * Storage Navigator CLI Pfad: SNM2 CLI Pfad * Konto Authentifizierung gültig: Wählen Sie gültige Konto Authentifizierung * Benutzername: Benutzername für den Speicher * Passwort: Passwort für den Speicher
Wählen Sie Tuning Manager für Leistung	Andere Leistungsoptionen überschreiben
Tuning Manager Host	IP-Adresse oder vollqualifizierter Domain-Name des Tuning Managers
Tuning Manager-Port Überschreiben	Wenn leer, verwenden Sie den Standardport im Feld Tuning Manager für Performance auswählen. Geben Sie andernfalls den zu verwendenden Port ein
Benutzername Für Tuning Manager	Benutzername für Tuning Manager
Kennwort Für Tuning-Manager	Passwort für Tuning Manager

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

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS oder HTTP: Zeigt auch den Standardport an
HiCommand Server-Port	Port, der für den HiCommand Device Manager verwendet wird
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten aufgeführte Array-Liste beim Sammeln von Daten aufgenommen oder ausgeschlossen werden soll.
Geräteliste filtern	Kommagetrennte Liste der einzuschließenden oder auszuschließenden Geräteseriennummer
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.
Ausfuhrzeitlimit in Sekunden	Zeitüberschreitung beim Exportieren der Dienstprogrammfunktion. Der Standardwert ist 300.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	**Versuchen Sie dies:**
Fehler: Benutzer hat nicht genügend Berechtigung	Verwenden Sie ein anderes Benutzerkonto, das über mehr Berechtigungen verfügt oder die Berechtigung des Benutzerkontos, das im Datensammler konfiguriert ist, erhöht
Fehler: Speicherliste ist leer. Entweder sind Geräte nicht konfiguriert oder der Benutzer verfügt nicht über ausreichende Berechtigungen	* Verwenden Sie DeviceManager, um zu überprüfen, ob die Geräte konfiguriert sind. * Verwenden Sie ein anderes Benutzerkonto, das mehr Berechtigungen hat, oder erhöhen Sie die Berechtigung des Benutzerkontos
Fehler: HDS Speicher-Array wurde einige Tage lang nicht aktualisiert	Untersuchen Sie, warum dieses Array nicht in HDS HiCommand aktualisiert wird.

Performance

Problem:	Versuchen Sie dies:
Fehler: * Fehler beim Ausführen des Exportdienstprogramms * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass das Exportdienstprogramm auf der Data Infrastructure Insights Acquisition Unit installiert ist * Bestätigen Sie, dass der Speicherort des Exportdienstprogramms in der Data Collector-Konfiguration korrekt ist * Bestätigen Sie, dass die IP des USP/R600-Arrays in der Konfiguration des Data Collectors korrekt ist * Öffnen Sie einen CMD und das Kennwort in der Konfiguration des Data Collectors * Bestätigen Sie, dass die Export Utility-Version mit der Speicher-Microcode-Version kompatibel ist * aus der Data Infrastructure Insights Acquisition Unit, öffnen Sie eine CMD - Aufforderung zur Installation mit dem folgenden Ordner konfigurieren: runWin.bat
Fehler: Export Tool-Anmeldung für Ziel-IP fehlgeschlagen	* Bestätigen Sie, dass Benutzername/Passwort korrekt ist * Erstellen Sie eine Benutzer-ID hauptsächlich für diesen HDS-Datensammler * Bestätigen Sie, dass keine anderen Datensammler für die Erfassung dieses Arrays konfiguriert sind
Fehler: Exportwerkzeuge protokolliert "Zeitbereich für Überwachung nicht abrufen".	* Bestätigung der Leistungsüberwachung auf dem Array ist aktiviert. * Versuchen Sie, die Exportwerkzeuge außerhalb von Data Infrastructure Insights aufzurufen, um zu bestätigen, dass das Problem außerhalb von Data Infrastructure Insights liegt.
Fehler: * Konfigurationsfehler: Speicher-Array wird vom Exportdienstprogramm nicht unterstützt * Konfigurationsfehler: Speicher-Array wird nicht von Speicher-Navigator Modular CLI unterstützt	* Nur unterstützte Storage-Arrays konfigurieren. * Verwenden Sie „Filter Device List“, um nicht unterstützte Speicher-Arrays auszuschließen.
Fehler: * Fehler beim Ausführen des externen Befehls * Konfigurationsfehler: Speicher-Array nicht gemeldet von Inventory * Konfigurationsfehler:Exportordner enthält keine JAR-Dateien	* Überprüfen Sie den Speicherort des Exportdienstprogramms. * Prüfen Sie, ob Speicher-Array in Frage in HiCommand Server konfiguriert ist * Festlegen des Performance-Abfrageintervalls als mehrere 60 Sekunden.
Fehler: * Fehler Storage Navigator CLI * Fehler beim Ausführen von auPerform Befehl * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass Storage Navigator Modular CLI auf der Data Infrastructure Insights Acquisition Unit installiert ist * Bestätigen Sie, dass Storage Navigator Modular CLI-Speicherort in der Data Collector-Konfiguration korrekt ist * Bestätigen Sie, dass die IP des WMS/SMS/SMS-Arrays in der Konfiguration des Data Collectors korrekt ist * Bestätigen Sie, dass Storage Navigator Modular CLI-Version kompatibel ist mit Microcode-Version des Speicher-Arrays konfiguriert im Data Collector * von der Data Infrastructure Insights Acquisition Unit, öffnen Sie eine CMD-Eingabeaufforderung und führen Sie den folgenden Befehl aus:
Fehler: Konfigurationsfehler: Speicher-Array wird vom Inventory nicht gemeldet	Überprüfen Sie, ob Speicher-Array in Frage im HiCommand-Server konfiguriert ist

Problem:	Versuchen Sie dies:
Fehler: * Kein Array ist beim Speicher Navigator Modular 2 CLI registriert * Array ist nicht bei der Speicher Navigator Modular 2 CLI registriert * Konfigurationsfehler: Speicher-Array nicht bei StorageNavigator Modular CLI registriert	* Öffnen Sie die Eingabeaufforderung und ändern Sie das Verzeichnis in den konfigurierten Pfad * führen Sie den Befehl „set=STONAVM_HOME=“ aus. * Führen Sie den Befehl „auunitref“ aus * Bestätigen Sie, dass die Befehlsausgabe Details des Arrays mit IP enthält * Wenn die Ausgabe keine Array-Details enthält, registrieren Sie das Array mit Storage Navigator CLI: - Öffnen Sie die Eingabeaufforderung und ändern Sie das Verzeichnis auf den konfigurierten Pfad - führen Sie den Befehl „set=STONAVM_HOME=“ aus. - Führen Sie den Befehl „auunitaddauto -ip <ip>“ aus. Ersetzen Sie <ip> durch die richtige IP.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Konfiguration des Hitachi Vantara NAS Data Collector

Der Hitachi Vantara NAS Data Collector ist ein Bestands- und Konfigurationsdatensammler, der die Erkennung von HDS NAS-Clustern unterstützt. Data Infrastructure Insights unterstützt die Erkennung von NFS- und CIFS-Freigaben, Filesystemen (interne Volumes) und Spanns (Storage-Pools).

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem HNAS-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Ebene	Festplattengruppe
Cluster	Storage
Knoten	Storage-Node
Span	Storage-Pool
Systemlaufwerk	Back-End Lun
File System	Internes Volumen

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- IP-Adresse des Geräts
- Port 22, SSH-Protokoll
- Benutzername und Passwort - Berechtigungsebene: Supervisor

- Hinweis: Dieser Datensammler ist SSH-basiert, also muss die AU, die auf dem HNAS selbst SSH-Sitzungen auf TCP 22 oder auf der Systemverwaltungseinheit (SMU) initiieren können, mit der das Cluster verbunden ist.

Konfiguration

Feld	Beschreibung
HNAS Host	IP-Adresse oder vollqualifizierter Domain-Name des HNAS Management Host
Benutzername	Benutzername für HNAS-CLI
Passwort	Passwort, das für die HNAS-CLI verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 30 Minuten.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Fehler beim Verbinden“ mit Fehlermeldungen „Fehler beim Einrichten des Shell-Kanals:“ oder „Fehler beim Öffnen des Shell-Kanals“	Wahrscheinlich verursacht durch Probleme mit der Netzwerkverbindung oder SSH ist falsch konfiguriert. Bestätigen Sie die Verbindung mit dem alternativen SSH-Client
„Timeout“ oder „Fehler beim Abrufen von Daten“ mit Fehlermeldungen „Befehl: XXX hat Timeout.“	* Versuchen Sie den Befehl mit dem alternativen SSH-Client * Erhöhen Sie die Zeitüberschreitung
„Fehler beim Verbindungsaufbau“ oder „Ungültige Anmeldeinformationen“ mit Fehlermeldungen „konnte nicht mit dem Gerät kommunizieren:“	* IP-Adresse prüfen * Benutzername und Passwort überprüfen * Verbindung mit alternativem SSH-Client bestätigen

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Datensammler Hitachi Ops Center

Dieser Datensammler verwendet die integrierte Anwendungssuite von Hitachi Ops Center, um auf Bestands- und Performancedaten mehrerer Speichergeräte zuzugreifen. Eine Bestandsaufnahme und Kapazitätserkennung muss in Ihrer Ops Center-Installation sowohl die Komponenten „Common Services“ als auch „Administrator“ enthalten. Zur Performance-Erfassung muss zusätzlich „Analyzer“ implementiert sein.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Storage-Systeme	Storage
Datenmenge	Datenmenge
Paritätsgruppen	Speicherpool (RAID), Festplattengruppen
Festplatte	Festplatte
Storage-Pool	Speicherpool (Thin, SNAP)
Externe Paritätsgruppen	Speicherpool (Backend), Festplattengruppen
Port	Storage-Node → Controller-Node →-Port
Host-Gruppen	Volume-Zuordnung und -Maskierung
Volume-Paare	Storage-Synchronisierung

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Inventaranforderungen

Zur Erfassung von Bestandsdaten müssen Sie Folgendes haben:

- IP-Adresse oder Hostname des Ops Center-Servers, der die „Common Services“-Komponente hostet
- Root/sysadmin Benutzerkonto und Passwort, die auf allen Servern vorhanden sind, auf denen Ops Center Komponenten gehostet werden. HDS hat KEINE REST-API-Unterstützung für LDAP/SSO-Benutzer bis Ops Center 10.8+ implementiert

Performance-Anforderungen erfüllt

Zur Erfassung von Leistungsdaten müssen die folgenden Anforderungen erfüllt sein:

Das HDS Ops Center „Analyzer“-Modul muss installiert sein Storage Arrays müssen das Ops Center-Modul „Analyzer“ speisen

Konfiguration

Feld	Beschreibung
Hitachi Ops Center-IP-Adresse	IP-Adresse oder vollqualifizierter Domänenname des Ops Center-Servers, der die Komponente „Allgemeine Dienste“ hostet
Benutzername	Benutzername für den Ops-Center-Server.
Passwort	Passwort, das für den Ops-Center-Server verwendet wird.

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS (Port 443) ist der Standard
TCP-Port überschreiben	Geben Sie den zu verwendenden Port an, wenn nicht der Standardport
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten aufgeführte Array-Liste beim Sammeln von Daten aufgenommen oder ausgeschlossen werden soll.
Geräteliste filtern	Kommagetrennte Liste der einzuschließenden oder auszuschließenden Geräteseriennummer
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Infiniat InfiniBox Datensammler

Der Datensammler Infinibei InfiniBox (HTTP) wird verwendet, um Inventarinformationen vom Infiniat InfiniBox-Speichersystem zu sammeln.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Infinidat Infinibox Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	**Einblicke Aus Der Dateninfrastruktur**
Storage-Pool	Storage-Pool
Knoten	Controller
Dateisystem	Internes Volumen
Dateisystem	Dateifreigabe
Dateisystem-Exporte	Share

Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration dieses Datensammlers.

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

Konfiguration

Feld	Beschreibung
InfiniBox Host	IP-Adresse oder vollqualifizierter Domainname des InfiniBox Management Node
Benutzername	Benutzername für InfiniBox Management Node
Passwort	Passwort für den InfiniBox Management-Knoten

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Anschluss	TCP-Port zur Verbindung mit InfiniBox-Server. Der Standardwert ist 443.
Abfrageintervall Für Bestand	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 60 Minuten.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Huawei OceanStor Datensammler

Data Infrastructure Insights nutzt den Huawei OceanStor (REST/HTTPS) Datensammler zur Ermittlung von Inventar und Leistung für Huawei OceanStor und OceanStor Dorado Speicher.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestands- und Leistungsinformationen vom Huawei OceanStor. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Storage-Pool	Storage-Pool
File-System	Internes Volumen
Controller	Storage-Node
FC-Port (zugeordnet)	Volume-Zuordnung
Host FC Initiator (zugeordnet)	Volume-Maske
NFS/CIFS-Freigabe	Share
ISCSI-Link-Ziel	ISCSI-Ziel-Node
ISCSI-Link-Initiator	ISCSI-Initiator-Node
Festplatte	Festplatte

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
LUN	Datenmenge

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Anforderungen erforderlich:

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

Konfiguration

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

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Anschluss	TCP-Port zur Verbindung mit dem OceanStor Device Manager. Der Standardwert ist 8088.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 60 Minuten.
Leistungsintervall (Sek.).	Die Standardeinstellung ist 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

IBM

IBM Cleversafe Datensammler

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

IBM Cleversafe wird mit einer anderen Raw TB zu Managed Unit Rate gemessen. Jede 40 TB unformatierte IBM Cleversafe Kapazität wird als 1 berechnet"Verwaltete Einheit (ME)".

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem IBM Cleversafe Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Storage-Pool	Storage-Pool
Container	Internes Volumen
Container	Dateifreigabe
NFS-Share	Share

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Die IP-Adresse für externe Datendienste für den Cluster
- Administrator-Benutzername und -Passwort
- Anschluss 9440

Konfiguration

Feld	Beschreibung
Manager-IP oder Host-Name	IP-Adresse oder Hostname des Management-Node
Benutzername	Benutzername für das Benutzerkonto mit Superuser- oder Systemadministrator-Rolle
Passwort	Kennwort für das Benutzerkonto mit Superuser- oder Systemadministrator-Rolle

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen
HTTP-Verbindungszeitlimit (Sek.)	HTTP-Zeitüberschreitung in Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

IBM CS Datensammler

Data Infrastructure Insights nutzt diesen Datensammler zur Ermittlung von Bestands- und Leistungsdaten für IBM CS-Speichersysteme.

Terminologie

Data Infrastructure Insights erfasst die folgenden Inventarinformationen aus dem IBM CS-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Storage-Pool	Storage-Pool
Container	Internes Volumen
Container	Dateifreigabe
NFS-Share	Share

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Die IP-Adresse für externe Datendienste für den Cluster
- Administrator-Benutzername und -Passwort
- Anschluss 9440

Konfiguration

Feld	Beschreibung
Externe IP-Adresse des Prism	Die IP-Adresse für externe Datendienste für den Cluster
Benutzername	Benutzername für das Administratorkonto
Passwort	Kennwort für das Administratorkonto

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port, der für die Verbindung mit dem IBM CS-Array verwendet wird. Der Standardwert ist 9440.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 60 Minuten.
Abfrageintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Die Standardeinstellung ist 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Datensammler der IBM System Storage DS8000-Serie

Der IBM DS (CLI) Datensammler unterstützt die Erfassung von Bestands- und Performancedaten für DS6xxx- und DS8xxx-Geräte.

DS3xxx-, DS4xxx- und DS5xxx-Geräte werden vom unterstützt"NetApp E-Series Datensammler". Unterstützte Modelle und Firmware-Versionen finden Sie in der Data Infrastructure Insights Supportmatrix.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem IBM DS-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplattenmodul	Festplatte
Storage-Bild	Storage
Extent-Pool	Storage-Node
Festes Block-Volume	Datenmenge
Host FC Initiator (zugeordnet)	Volume-Maske

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen möglicherweise nicht alle Fälle für diese Datensammlung dar.

Anforderungen

Sie benötigen Folgendes, um diesen Datensammler zu konfigurieren:

- IP-Adresse jedes DS-Arrays
- Schreibgeschützter Benutzername und Kennwort auf jedem DS-Array
- Software von Drittanbietern, die auf der Data Infrastructure Insights AU installiert ist: IBM *dscli*
- Zugriffsvalidierung: Führen Sie die Befehle *dscli* mit dem Benutzernamen und Passwort aus
- Port-Anforderungen: 80, 443 und 1750

Konfiguration

Feld	Beschreibung
DS-Speicher	IP-Adresse oder vollqualifizierter Domain-Name des DS-Geräts
Benutzername	Benutzername für die DS-CLI
Passwort	Passwort für die DS-CLI
Dscli ausführbare Datei-Pfad	Vollständiger Pfad zur ausführbaren Datei *dscli*

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen (min). Der Standardwert ist 40.
Anzeigename Für Speicher	Name des IBM DS-Speicherarrays
Inventory Exclude Devices	Kommagetrennte Liste von Geräteseriennummer, die von der Bestandserfassung ausgeschlossen werden sollen
Leistungsintervall (Sek.)	Der Standardwert ist 300.
Typ Des Leistungsfilters	Enthalten: Daten, die nur von Geräten in der Liste erfasst werden. Ausschließen: Es werden keine Daten von diesen Geräten erfasst
Geräteliste Für Leistungsfilter	Kommagetrennte Liste der Geräte-IDs, die die Leistungssammlung einschließen oder ausschließen sollen

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler mit CMUC00192E, CMUC00191E oder CMUC00190E	* Eingabe von Anmeldeinformationen und IP-Adresse überprüfen. * Versuchen Sie, mit dem Array über die Web-Management-Konsole https://<ip>:8452/DS8000/Console zu kommunizieren. Ersetzen Sie <ip> durch konfigurierte IP-Adresse für den Data Collector.
Fehler: * Programm kann nicht ausgeführt werden * Fehler beim Ausführen des Befehls	* Aus Data Infrastructure Insights Acquisition Unit Öffnen Sie eine CMD * Open CLI.CFG-Datei in CLI's Home dir/lib und überprüfen Sie die Eigenschaft Java_INSTALL, bearbeiten Sie den Wert, der Ihrer Umgebung entspricht * Java-Version auf diesem Rechner anzeigen, indem Sie "java -Version" eingeben * Ping die IP-Adresse des IBM-Speichergeräts, das im CLI-Befehl ausgegeben wurde. * Wenn alle oben genannten gut funktioniert haben, dann führen Sie manuell einen CLI-Befehl aus

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Konfigurieren des IBM PowerVM-Datensammlers

Der IBM PowerVM (SSH) Datensammler wird verwendet, um Informationen über virtuelle Partitionen zu sammeln, die auf IBM POWER Hardware-Instanzen ausgeführt werden, die von einer Hardware Management Console (HMC) verwaltet werden.

Terminologie

Data Infrastructure Insights erfasst Bestandsinformationen von den virtuellen Partitionen, die auf IBM POWER Hardware-Instanzen ausgeführt werden. Für jeden erworbenen Asset-Typ wird die am häufigsten für das Asset verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Hdisk	Virtuelles Laufwerk
Managed System	Host
LPAR, VIO Server	Virtual Machine
Volume-Gruppe	Datastore
Physisches Volume	LUN

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Zur Konfiguration und Nutzung dieses Datensammlers müssen die folgenden Anforderungen erfüllt sein:

- IP-Adresse der Hardware Management Console (HMC)
- Benutzername und Passwort, die Zugriff auf die Hardware Management Console (HMC) über SSH ermöglichen
- Port-Anforderung SSH-22
- Zeigen Sie Berechtigungen auf allen Verwaltungssystemen und Sicherheitsdomänen logischer Partitionen an

  Der Benutzer muss darüber hinaus über die Berechtigung View für HMC-Konfigurationen und die Möglichkeit verfügen, VPD-Informationen für die Sicherheitsgruppierung der HMC-Konsole zu sammeln. Der Benutzer muss außerdem den Zugriff auf den virtuellen IO-Server-Befehl unter der Sicherheitsgruppierung der logischen Partition zulassen. Es ist eine bewährte Vorgehensweise, von einer Rolle eines Bedieners zu beginnen und dann alle Rollen zu entfernen. Schreibgeschützte Benutzer auf dem HMC haben keine Berechtigungen zum Ausführen von Proxed-Befehlen auf AIX-Hosts.

- Die Best Practice von IBM besteht darin, dass die Geräte von zwei oder mehr HMCs überwacht werden. Beachten Sie, dass dies dazu führen kann, dass OnCommand Insight doppelte Geräte meldet. Daher wird dringend empfohlen, redundante Geräte zur Liste „Geräte ausschließen“ in der erweiterten Konfiguration für diesen Datensammler hinzuzufügen.

Konfiguration

Feld	Beschreibung
IP-Adresse für Hardware Management Console (HMC)	IP-Adresse oder vollqualifizierter Domänenname der PowerVM Hardware Management Console
HMC-Benutzer	Benutzername für die Hardware Management Console

Feld	Beschreibung
Passwort	Kennwort, das für die Hardware-Verwaltungskonsole verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 20 Minuten.
SSH-Anschluss	Port, der für SSH zu PowerVM verwendet wird
Passwort	Kennwort, das für die Hardware-Verwaltungskonsole verwendet wird
Anzahl Wiederholungen	Anzahl der Versuche für einen erneuten Versuch in der Bestandsaufnahme
Geräte Ausschließen	Kommagetrennte Liste von Geräte-IDs oder zu schließenden Anzeigenamen

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Konfigurieren des IBM SAN Volume Controller-Datensammlers

Der IBM SAN Volume Controller (SVC)-Datensammler sammelt Bestands- und Performancedaten mithilfe von SSH und unterstützt eine Vielzahl von Geräten, auf denen das SVC-Betriebssystem ausgeführt wird.

Die Liste der unterstützten Geräte umfasst Modelle wie SVC, v7000, v5000 und v3700. Unterstützte Modelle und Firmware-Versionen finden Sie in der Data Infrastructure Insights Supportmatrix.

Terminologie

Data Infrastructure Insights erfasst die folgenden Inventarinformationen aus dem IBM SVC-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Laufwerk	Festplatte
Cluster	Storage
Knoten	Storage-Node
Mdisk-Gruppe	Storage-Pool
Vdisk	Datenmenge
Mdisk	Back-End-LUNs und -Pfade

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Inventaranforderungen

- IP-Adresse jedes SVC-Clusters
- Port 22 verfügbar
- Schreibgeschützter Benutzername und Kennwort

Performance-Anforderungen Erfüllt

- SVC-Konsole, die für jeden SVC-Cluster obligatorisch und für das Foundation-Paket für die SVC-Erkennung erforderlich ist
- Mit den Anmeldedaten ist nur Administratorzugriff erforderlich, um Performance-Dateien von Cluster-Nodes auf den Konfigurations-Node zu kopieren.
- Aktivieren Sie die Datensammlung, indem Sie über SSH eine Verbindung zum SVC-Cluster herstellen und ausführen: *Svctask startstats -Interval 1*

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

Konfiguration

Feld	Beschreibung
Cluster-IP-Adressen	IP-Adressen oder vollqualifizierte Domain-Namen des SVC-Speichers
Benutzername Des Inventurbenutzers	Benutzername für die SVC-CLI
Inventurpasswort	Passwort für die SVC-CLI

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 40 Minuten.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Die Standardeinstellung ist 300 Sekunden.
Um dumpte Statistikdateien zu bereinigen	Aktivieren Sie dieses Kontrollkästchen, um heruntergelegte Statistikdateien zu bereinigen

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

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

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

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

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Konfiguration des IBM XIV/A9000 Datensammlers

Der Datensammler IBM XIV und A9000 (CLI) verwendet die XIV-Befehlszeilenschnittstelle, um Bestandsdaten zu sammeln, während die Performance erfasst wird, indem SMI-S-Aufrufe zum XIV/A9000 Array ausführt, auf dem ein SMI-S-Provider über Port 7778 ausgeführt wird.

Terminologie

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Storage-System	Storage
Storage-Pool	Storage-Pool
Datenmenge	Datenmenge

Anforderungen

Zur Konfiguration und Nutzung dieses Datensammlers müssen die folgenden Anforderungen erfüllt sein:

- Port-Anforderung: TCP-Port 7778
- Schreibgeschützter Benutzername und Kennwort
- Das XIV CLI muss auf der AU installiert sein

Performance-Anforderungen erfüllt

Im Folgenden sind Anforderungen für die Performance-Erfassung aufgeführt:

- SMI-S Agent 1.4 oder höher
- SMI-S-kompatibler CIMService auf Array. Bei den meisten XIV Arrays ist standardmäßig ein Cimserver installiert.
- Für den Cimserver muss eine Benutzeranmeldung bereitgestellt werden. Die Anmeldung muss vollständigen Lesezugriff auf die Arraykonfiguration und -Eigenschaften haben.
- SMI-S-Namespace. Der Standardwert ist root/ibm. Dies ist im Cimserver konfigurierbar.
- Port-Anforderungen: 5988 für HTTP, 5989 für HTTPS.
- Informationen zum Erstellen eines Kontos für die SMI-S Performance Collection finden Sie unter dem folgenden Link: https://www.ibm.com/docs/en/products?topic=/com.ibm.tpc_V41.doc/fqz0_t_adding_cim_agent.html

Konfiguration

Feld	Beschreibung
XIV-IP-Adresse	IP-Adresse oder vollqualifizierter Domain-Name des XIV Storage
Benutzername	Benutzername für den XIV Storage
Passwort	Passwort für den XIV-Speicher
Vollständiger Pfad zu XIV CLI Directory	Vollständiger Pfad zum Ordner mit der XIV CLI
SMI-S-Host-IP-Adresse	IP-Adresse des SMI-S-Hosts

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 40 Minuten.
SMI-S-Protokoll	Protokoll für die Verbindung mit dem SMI-S-Provider. Zeigt auch den Standardport an.
SMI-S-Port überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport im Feld Verbindungstyp. Andernfalls geben Sie den zu verwendenden Anschluss ein
Benutzername	Benutzername für den SMI-S Provider Host
Passwort	Kennwort für den SMI-S Provider-Host
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Die Standardeinstellung ist 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Lenovo Datensammler

Data Infrastructure Insights verwendet den Lenovo Datensammler zur Ermittlung von Bestands- und Leistungsdaten für Lenovo HX-Speichersysteme.

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

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

Konfiguration

Feld	Beschreibung
Externe IP-Adresse des Prism	Die IP-Adresse für externe Datendienste für den Cluster
Benutzername	Benutzername für das Administratorkonto
Passwort	Kennwort für das Administratorkonto

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port für die Verbindung zum Array. Der Standardwert ist 9440.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 60 Minuten.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Die Standardeinstellung ist 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Microsoft

Konfigurieren des Azure NetApp Files-Datensammlers

Data Infrastructure Insights verwendet den Azure NetApp Files Datensammler zur Erfassung von Bestands- und Performance-Daten.

Anforderungen

Sie benötigen die folgenden Informationen, um diesen Datensammler zu konfigurieren.

- Port-Anforderung: 443 HTTPS
- Azure Management Rest-IP (management.azure.com)
- Principal Client-ID für den Azure-Service (Benutzerkonto)
- Azure Service Principal Authentifizierungsschlüssel (Benutzerkennwort)
- Sie müssen ein Azure-Konto für die Erkennung von Data Infrastructure Insights einrichten.

  Sobald das Konto ordnungsgemäß konfiguriert ist und Sie die Applikation in Azure registrieren, verfügen Sie über die erforderlichen Zugangsdaten, um die Azure-Instanz mit Data Infrastructure Insights zu ermitteln. Über den folgenden Link wird beschrieben, wie Sie das Konto für die Ermittlung einrichten:

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Konfiguration

Geben Sie die Daten in die Felder des Datensammlers gemäß der folgenden Tabelle ein:

Feld	Beschreibung
Azure Service Principal Client-ID	Anmelde-ID bei Azure
Azure Mandanten-ID	Azure Mandanten-ID
Authentifizierungsschlüssel Des Azure Service Principal	Anmeldeauthentifizierungsschlüssel
Ich verstehe, dass Microsoft mir API-Anforderungen in Rechnung stellt	Überprüfen Sie dies, um zu überprüfen, ob Microsoft Ihnen die durch eine Insight-Umfrage gestellten API-Anforderungen abrechnungen aufstellt.

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60

Fehlerbehebung

- Die von Ihrem ANF-Datensammler verwendeten Zugangsdaten müssen auf alle Azure-Abonnements zugreifen können, die ANF-Volumes enthalten.
- Wenn der Zugang zum Reader dazu führt, dass die Leistensammlung fehlschlägt, versuchen Sie, den Zugriff auf Mitarbeiter auf Ressourcengruppenebene zu gewähren.

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Microsoft Hyper-V Datensammler

Der Microsoft Hyper-V Datensammler erfasst Bestands- und Performancedaten aus der virtualisierten Server Computing-Umgebung. Dieser Datensammler kann einen eigenständigen Hyper-V-Host oder einen gesamten Cluster erkennen und einen Collector pro eigenständigen Host oder Cluster erstellen.

Terminologie

Data Infrastructure Insights erfasst die folgenden Inventarinformationen aus dem Microsoft Hyper-V (WMI). Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Virtuelle Festplatte	Virtuelles Laufwerk
Host	Host
Virtual Machine	Virtual Machine
Cluster Shared Volumes (CSV), Partition Volume	Datastore

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Internet SCSI-Gerät, Multi Path SCSI LUN	LUN
Fibre Channel-Port	Port

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Für die Hyper-V muss Port 5985 geöffnet sein, damit Daten erfasst und Remote-Zugriff/-Management erfolgen können.
- IP-Adresse oder FQDN des Clusters oder Standalone-Hypervisors. Die Verwendung des unverankerten Cluster-Hostnamens oder der IP ist wahrscheinlich der zuverlässigste Ansatz im Vergleich dazu, den Collector nur auf einen bestimmten Knoten in einem Cluster zu verweisen.
- Benutzerkonto auf administrativer Ebene, das für alle Hypervisoren im Cluster funktioniert.
- WinRM muss aktiviert sein und alle Hypervisoren abhören
- Port-Anforderungen: Port 135 über WMI & Dynamic TCP Ports zugewiesen 1024-65535 für Windows 2003 und älter und 49152-65535 für Windows 2008.
- DNS-Auflösung muss erfolgreich sein, auch wenn der Datensammler nur auf eine IP-Adresse verweist
- Für jeden Hyper-V Hypervisor muss für jede VM, auf jedem Host, „Resource Metering“ aktiviert sein. Dadurch kann jeder Hypervisor bei jedem Gast mehr Daten für Data Infrastructure Insights zur Verfügung haben. Wenn diese Einstellung nicht festgelegt ist, werden für jeden Gast weniger Performance-Metriken erfasst. Weitere Informationen zur Ressourcenmessung finden Sie in der Microsoft-Dokumentation:

  "Hyper-V Übersicht zur Ressourcenmessung"

  "Aktivieren-VMressourcenMetering"

Für den Hyper-V-Datensammler ist eine Windows Acquisition Unit erforderlich.

Konfiguration

Feld	Beschreibung
Cluster-IP-Adresse oder fließender Cluster-FQDN	Die IP-Adresse oder der vollständig qualifizierte Domänenname für das Cluster oder ein eigenständiger Hypervisor ohne Cluster
Benutzername	Administrator-Benutzername für den Hypervisor
Passwort	Kennwort für den Hypervisor
DNS-Domain-Suffix	Das Hostnamen-Suffix, das mit dem einfachen Hostnamen kombiniert wird, um den FQDN eines Hypervisors zu rendern

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Die Standardeinstellung ist 20 Minuten.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

NetApp

NetApp Cloud Volumes ONTAP Datensammler

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

Konfiguration

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

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS empfohlen. Zeigt außerdem den Standardport an.
Kommunikations-Port Überschreiben	Port zu verwenden, wenn nicht standardmäßig.
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten.
Inventurzählung Der Threads	Anzahl der gleichzeitigen Threads.
Erzwingen von TLS für HTTPS	TLS über HTTPS erzwingen
Netzgruppen Automatisch Suchen	Netzgruppen Automatisch Suchen
Netzgruppenerweiterung	Wählen Sie Shell oder Datei aus
HTTP-Lesezeit Sekunden	Der Standardwert ist 30 Sekunden
Antworten als UTF-8 erzwingen	Antworten als UTF-8 erzwingen
Leistungsintervall (min)	Der Standardwert ist 900 Sekunden.
Performance-Threads Anzahl	Anzahl der gleichzeitigen Threads.
Erweiterte Zähldatensammlung	Aktivieren Sie diese Option, damit Data Infrastructure Insights die erweiterten Metriken aus der folgenden Liste erfasst.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

NetApp Cloud Volumes Services für AWS Data Collector

Dieser Datensammler unterstützt die Bestandserfassung von NetApp Cloud Volumes Services für AWS Konfigurationen.

Konfiguration

Feld	Beschreibung
Region Von Cloud Volumes	Region der NetApp Cloud Volumes Services für AWS
API-Schlüssel	API-Schlüssel für Cloud Volumes
Geheimer Schlüssel	Geheimen Schlüssel von Cloud Volumes

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Problem:	Versuchen Sie dies:
Ich habe einen Fehler wie diesen erhalten: 'Anfrage konnte nicht ausgeführt werden: Verbindung zu <AWS Region Endpunkt>:8080 [<AWS Region Endpunkt>/AWS Region Endpunkt IP>] fehlgeschlagen: Verbindung abgelaufen: https://<AWS Region Endpunkt FQDN ABRUFEN>:8080/v1/Speicher/IPRanges HTTP/1.1'	Der"Proxy" Wird von Data Infrastructure Insights zur Kommunikation mit der Erfassungseinheit verwendet, erfolgt keine Kommunikation zwischen Data Infrastructure Insights und dem Datensammler selbst. Hier sind einige Dinge, die Sie versuchen können: Stellen Sie sicher, dass die Erfassungseinheit den FQDN auflösen und den erforderlichen Port erreichen kann. Bestätigen Sie, dass kein Proxy erforderlich ist, um den in der Fehlermeldung angegebenen Endpunkt zu erreichen. Mit Curl kann die Kommunikation zwischen der Erfassungseinheit und dem Endpunkt getestet werden. Stellen Sie sicher, dass Sie für diesen Test **keinen** Proxy verwenden. Beispiel: root@acquisitionunit# curl -s -H accept:application/json -H "Content-type: application/json" -H api-key:<in den Anmeldeinformationen des Datensammlers verwendeter API-Schlüssel -H secret-key:<in den Anmeldeinformationen des Datensammlers verwendeter geheimer Schlüssel> -X GET https://<Regionaler AWS-Endpunkt>:8080/v1/Storage/IPRanges

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

NetApp ONTAP ASA r2 (All-SAN Array) Datenkollektor

Dieser Datensammler erfasst mithilfe von REST-API-Aufrufen Bestände, EMS-Protokolle und Performance-Daten von Speichersystemen mit ONTAP 9.16.0 und höher.

Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration und Verwendung dieses Datensammlers:

- Sie müssen Zugriff auf ein Benutzerkonto mit der erforderlichen Zugriffsebene haben. Beachten Sie, dass Administratorberechtigungen erforderlich sind, wenn Sie einen neuen REST-Benutzer/eine neue REST-Rolle erstellen.
  - Zu ihren Funktionen gehören in erster Linie Leseanforderungen. Für die Registrierung im ONTAP Array sind jedoch einige Schreibberechtigungen erforderlich, damit sich Dateninfrastruktur Insights registrieren kann. Siehe *Hinweis zu Berechtigungen* direkt unten.
- ONTAP Version 9.16.0 oder höher.
- Anforderungen an den Hafen: 443

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

Für alle ASA-Systeme der vorherigen Generation verwenden Sie bitte den "ONTAP REST" Collector.

Ein Hinweis zu Berechtigungen

Da eine Reihe von ONTAP-Dashboards von Data Infrastructure Insights auf erweiterten ONTAP-Zählern basieren, sollten Sie **Enable Advanced Counter Data Collection** im Abschnitt Data Collector Advanced Configuration aktivieren.

Um ein lokales Konto für Dateninfrastrukturanalysen auf Cluster-Ebene zu erstellen, melden Sie sich mit dem Benutzernamen/Kennwort des Clusterverwaltungsadministrators bei ONTAP an, und führen Sie die folgenden Befehle auf dem ONTAP-Server aus:

1. Bevor Sie beginnen, müssen Sie mit einem *Administrator*-Konto bei ONTAP angemeldet sein und die Befehle *diagnoseebene* müssen aktiviert sein.
2. Rufen Sie den Namen des vservers vom Typ *admin* ab. Sie werden diesen Namen in nachfolgenden Befehlen verwenden.

```
 vserver show -type admin
. Erstellen Sie eine Rolle mit den folgenden Befehlen:
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
security login create -user-or-group-name {username} -application http
-authentication-method password -role {role name}
```

3. Erstellen Sie den schreibgeschützten Benutzer mit dem folgenden Befehl. Sobald Sie den Befehl create ausgeführt haben, werden Sie aufgefordert, ein Passwort für diesen Benutzer einzugeben.

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

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

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
Die daraus resultierende Rolle und Benutzeranmeldung sieht folgendermaßen
aus: Die tatsächliche Ausgabe kann variieren:
```

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

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   --------------------    ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                  Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

Migration

Gehen Sie wie folgt vor, um von einem früheren ONTAP (ontapi)-Datensammler zum neueren ONTAP-REST-Collector zu migrieren:

1. Fügen Sie den REST Collector hinzu. Es wird empfohlen, Informationen für einen anderen Benutzer einzugeben als für den vorherigen Collector konfiguriert. Verwenden Sie zum Beispiel den Benutzer, der im Abschnitt Berechtigungen oben angegeben ist.
2. Unterbrechen Sie den vorherigen Collector, damit er nicht weiter Daten sammelt.
3. Lassen Sie den neuen REST-Collector Daten für mindestens 30 Minuten erfassen. Ignorieren Sie während dieser Zeit alle Daten, die nicht „normal“ angezeigt werden.
4. Nach der Ruhezeit sollten Sie Ihre Daten stabilisieren sehen, während der REST-Collector weiterhin zu erfassen.

Sie können diesen Vorgang verwenden, um zum vorherigen Collector zurückzukehren, wenn Sie möchten.

Konfiguration

Feld	Beschreibung
ONTAP-Management-IP-Adresse	Die IP-Adresse oder der vollständig qualifizierte Domänenname des NetApp-Clusters. Muss Cluster-Management-IP/FQDN sein.
ONTAP REST-Benutzername	Benutzername für NetApp Cluster
ONTAP REST-Kennwort	Passwort für NetApp Cluster

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten.
Leistungsintervall (Sek.)	Der Standardwert ist 60 Sekunden.
Erweiterte Zähldatensammlung	Wählen Sie diese Option aus, um ONTAP Advanced Counter-Daten in Umfragen einzubeziehen. Standardmäßig aktiviert.
Aktivieren Sie die EMS-Ereigniserfassung	Wählen Sie diese Option aus, um die Ereignisdaten des ONTAP-EMS-Protokolls einzuschließen. Standardmäßig aktiviert.
EMS-Abfrageintervall (s)	Der Standardwert ist 60 Sekunden.

Terminologie

Data Infrastructure Insights erfasst Inventar-, Protokoll- und Performance-Daten aus dem ONTAP Datensammler. Für jeden erworbenen Asset-Typ wird die am häufigsten für das Asset verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Raid-Gruppe	Festplattengruppe
Cluster	Storage
Knoten	Storage-Node
Aggregat	Storage-Pool
LUN	Datenmenge
Datenmenge	Internes Volumen
Storage Virtual Machine/Vserver	Storage Virtual Machine

Terminologie für ONTAP Datenmanagement

Die folgenden Begriffe gelten für Objekte oder Referenzen, die Sie auf den Landing Pages für ONTAP Storage-Assets finden können. Viele dieser Bedingungen gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Komma getrennte Liste der eindeutigen Node-Modellnamen in diesem Cluster. Wenn alle Nodes in den Clustern denselben Modelltyp aufweisen, wird nur ein Modellname angezeigt.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden.
- Seriennummer – die Array-UUID
- IP: In der Regel werden die in der Datenquelle konfigurierten IP(s) oder Hostnamen(s) verwendet.
- Microcode-Version – Firmware.
- Rohkapazität – Basis-2-Zusammenfassung aller physischen Laufwerke im System, unabhängig von ihrer Rolle.
- Latenz – eine Darstellung der Workloads, die sich auf dem Host auslasten, sowohl bei Lese- als auch bei Schreibzugriffen. Idealerweise bezieht Data Infrastructure Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Statt dieses Array in Betracht zu ziehen, führt Data Infrastructure Insights in der Regel eine IOPS-gewichtete Berechnung aus den Statistiken der einzelnen internen Volumes durch.
- Durchsatz: Aggregiert aus internen Volumes. Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert erstellt von der Datenquelle „Data Infrastructure Insights“ als Teil der Bestandsberichterstattung.

Storage-Pool

- Storage – auf welchem Storage-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibenden Wert aus einer Liste mit einer Aufzählung der Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ sein.
- Node – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Landing Page angezeigt.
- Verwendet Flash Pool – Ja/kein Wert: Verfügen in diesem SATA/SAS-basierten Pool über SSDs zur Caching-Beschleunigung?
- Redundanz: RAID-Level oder Schutzschema. RAID_DP ist Dual-Parity, RAID_TP ist die dreifache Parität.
- Kapazität – die Werte hier sind die logische genutzte, nutzbare Kapazität und die logische

Gesamtkapazität sowie der dafür genutzte Prozentsatz.

- Überprovisionierung der Kapazität – Wenn Sie durch den Einsatz von Effizienztechnologien eine Summe der Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer sind als die logische Kapazität des Speicherpools, wird der Prozentwert hier größer als 0 % sein.
- Snapshot – verwendete und insgesamt Snapshot-Kapazitäten, wenn Ihre Storage Pool-Architektur einem Teil ihrer Kapazität dedizierte Bereiche für Snapshots widmet. ONTAP in MetroCluster Konfigurationen zeigen dies wahrscheinlich, während andere ONTAP Konfigurationen weniger sind.
- Auslastung – ein Prozentwert, der den höchsten ausgelastet anteil der Festplatte anzeigt, die zur Kapazität dieses Speicherpools beiträgt. Die Festplattenauslastung ist nicht unbedingt mit der Array-Performance korreliert – die Auslastung kann aufgrund von Festplattenwiederherstellungen, Deduplizierungsaktivitäten usw. bei Abwesenheit von Host-gestützten Workloads sehr hoch sein. Auch viele Arrays Replikationsimplementierungen können die Festplattenauslastung steigern, während sie nicht als internes Volume oder Volume-Workload angezeigt werden.
- IOPS – die Summe der IOPS aller Festplatten, die Kapazität in diesem Storage-Pool beitragen. Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen.

Storage-Node

- Storage – welches Storage-Array gehört zu diesem Node? Obligatorisch.
- HA-Partner: Auf Plattformen, auf denen ein Node auf einen und nur einen anderen Node Failover ausgeführt wird, ist er allgemein zu sehen.
- Status: Systemzustand des Node. Nur verfügbar, wenn das Array ordnungsgemäß genug ist, um von einer Datenquelle inventarisiert zu werden.
- Modell: Modellname des Knotens
- Version – Versionsname des Geräts.
- Seriennummer: Die Seriennummer des Node.
- Speicher: Sockel 2 Speicher, falls verfügbar.
- Auslastung – bei ONTAP handelt es sich um einen Controller-Stressindex aus einem proprietären Algorithmus. Bei jeder Performance-Umfrage wird anhand einer Zahl zwischen 0 und 100 % angegeben, die der höhere Wert bei WAFL-Festplattenkonflikten oder der durchschnittlichen CPU-Auslastung ist. Wenn Sie nachhaltige Werte > 50 % beobachten, deutet dies auf eine Unterdimensionierung hin – möglicherweise ist ein Controller/Node nicht groß genug oder nicht genug rotierende Festplatten, um den Schreib-Workload abzufangen.
- IOPS – direkt von ONTAP-REST-Aufrufen des Node-Objekts abgeleitet.
- Latenz – wird direkt von ONTAP-REST-Aufrufen des Node-Objekts abgeleitet.
- Durchsatz – wird direkt von ONTAP-REST-Aufrufen des Node-Objekts abgeleitet.
- Prozessoren: Anzahl der CPUs

ONTAP-Leistungskennzahlen

Mehrere ONTAP Modelle bieten Stromkennzahlen für Einblicke in die Dateninfrastruktur, die für Monitoring oder Warnmeldungen genutzt werden können. Die unten aufgeführten Listen unterstützter und nicht unterstützter Modelle sind nicht umfassend, sollten jedoch einige Hinweise enthalten. Wenn ein Modell in der gleichen Familie wie ein Modell auf der Liste ist, sollte der Support identisch sein.

Unterstützte Modelle:

A200 A220 A250 A300 A320 A400 A700 A700S 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

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Problem:	Versuchen Sie dies:
Beim Versuch, einen ONTAP REST Data Collector zu erstellen, wird ein Fehler wie der folgende angezeigt: Konfiguration: 10.193.70.14: ONTAP Rest API at 10.193.70.14 ist nicht verfügbar: 10.193.70.14 Fehler beim ABRUFEN VON /API/Cluster: 400 Bad Request	Dies liegt wahrscheinlich an einem Oldeer ONTAP-Array), z. B. ONTAP 9.6), das keine REST-API-Funktionen hat. ONTAP 9.14.1 ist die minimale ONTAP-Version, die vom ONTAP REST Collector unterstützt wird. Bei den ONTAP-Versionen vor dem REST sind die Antworten auf „400 schlechte Anfragen“ zu erwarten. Für ONTAP-Versionen, die REST unterstützen, aber nicht 9.14.1 oder höher sind, können Sie die folgende ähnliche Nachricht sehen: Konfiguration: 10.193.98.84: ONTAP Rest API bei 10.193.98.84 ist nicht verfügbar: 10.193.98.84: ONTAP Rest API bei 10.193.98.84 ist verfügbar: Cheryl5-Cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 ist aber nicht von der Mindestversion 9.14.1.
Ich sehe leere oder „0“ Metriken, wo der ONTAP ontapi Collector Daten anzeigt.	ONTAP REST enthält keine Kennzahlen, die nur intern auf dem ONTAP System verwendet werden. Systemaggregate werden beispielsweise nicht von ONTAP REST erfasst, sondern nur SVM vom Typ „Daten“. Weitere Beispiele für ONTAP-REST-Metriken, die null oder leere Daten melden können: InternalVolumes: REST meldet nicht mehr vol0. Aggregate: REST meldet nicht mehr aggr0. Storage: Die meisten Metriken sind eine Auflutung der Kennzahlen für das interne Volume und werden von den oben genannten Auswirkungen beeinflusst. Storage Virtual Machines: REST meldet keine anderen SVM-Typen als „Daten“ (z. B. „Cluster“, „gmt“, „Node“). Sie können auch eine Änderung in der Darstellung von Diagrammen bemerken, die Daten enthalten, aufgrund der Änderung des standardmäßigen Performance-Abfragezeitraums von 15 Minuten auf 5 Minuten. Häufigere Abfragen bedeuten mehr Datenpunkte zum Plotten.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Datensammler der NetApp ONTAP Datenmanagement-Software

Diese Datensammlung erfasst Bestands- und Performancedaten von Storage-Systemen mit ONTAP unter Verwendung von schreibgeschützten API-Aufrufen eines ONTAP-

Kontos. Dieser Datensammler erstellt auch einen Datensatz in der Cluster-Anwendungsregistrierung, um den Support zu beschleunigen.

Terminologie

Data Infrastructure Insights erfasst Inventar- und Performance-Daten aus dem ONTAP Datensammler. Für jeden erworbenen Asset-Typ wird die am häufigsten für das Asset verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Raid-Gruppe	Festplattengruppe
Cluster	Storage
Knoten	Storage-Node
Aggregat	Storage-Pool
LUN	Datenmenge
Datenmenge	Internes Volumen

Terminologie für ONTAP Datenmanagement

Die folgenden Begriffe gelten für Objekte oder Referenzen, die Sie auf den Landing Pages für ONTAP Storage-Assets finden können. Viele dieser Bedingungen gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Komma getrennte Liste der eindeutigen Node-Modellnamen in diesem Cluster. Wenn alle Nodes in den Clustern denselben Modelltyp aufweisen, wird nur ein Modellname angezeigt.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden.
- Seriennummer: Die Seriennummer des Arrays. Bei Cluster-Architektur Storage-Systemen wie ONTAP Datenmanagement, ist diese Seriennummer möglicherweise weniger nützlich als die einzelnen Seriennummern der Storage-Nodes.
- IP: In der Regel werden die in der Datenquelle konfigurierten IP(s) oder Hostnamen(s) verwendet.
- Microcode-Version – Firmware.
- Rohkapazität – Basis-2-Zusammenfassung aller physischen Laufwerke im System, unabhängig von ihrer Rolle.
- Latenz – eine Darstellung der Workloads, die sich auf dem Host auslasten, sowohl bei Lese- als auch bei Schreibzugriffen. Idealerweise bezieht Data Infrastructure Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Statt dieses Array in Betracht zu ziehen, führt Data Infrastructure Insights in der Regel eine IOPS-gewichtete Berechnung aus den Statistiken der einzelnen internen Volumes durch.
- Durchsatz: Aggregiert aus internen Volumes. Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert erstellt von der Datenquelle „Data Infrastructure Insights“ als Teil der Bestandsberichterstattung.

Storage-Pool

- Storage – auf welchem Storage-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibenden Wert aus einer Liste mit einer Aufzählung der Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ sein.
- Node – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Landing Page angezeigt.
- Verwendet Flash Pool – Ja/kein Wert: Verfügen in diesem SATA/SAS-basierten Pool über SSDs zur Caching-Beschleunigung?
- Redundanz: RAID-Level oder Schutzschema. RAID_DP ist Dual-Parity, RAID_TP ist die dreifache Parität.
- Kapazität – die Werte hier sind die logische genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der dafür genutzte Prozentsatz.
- Überprovisionierung der Kapazität – Wenn Sie durch den Einsatz von Effizienztechnologien eine Summe der Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer sind als die logische Kapazität des Speicherpools, wird der Prozentwert hier größer als 0 % sein.
- Snapshot – verwendete und insgesamt Snapshot-Kapazitäten, wenn Ihre Storage Pool-Architektur einem Teil ihrer Kapazität dedizierte Bereiche für Snapshots widmet. ONTAP in MetroCluster Konfigurationen zeigen dies wahrscheinlich, während andere ONTAP Konfigurationen weniger sind.
- Auslastung – ein Prozentwert, der den höchsten ausgelastet anteil der Festplatte anzeigt, die zur Kapazität dieses Speicherpools beiträgt. Die Festplattenauslastung ist nicht unbedingt mit der Array-Performance korreliert – die Auslastung kann aufgrund von Festplattenwiederherstellungen, Deduplizierungsaktivitäten usw. bei Abwesenheit von Host-gestützten Workloads sehr hoch sein. Auch viele Arrays Replikationsimplementierungen können die Festplattenauslastung steigern, während sie nicht als internes Volume oder Volume-Workload angezeigt werden.
- IOPS – die Summe der IOPS aller Festplatten, die Kapazität in diesem Storage-Pool beitragen. Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen.

Storage-Node

- Storage – welches Storage-Array gehört zu diesem Node? Obligatorisch.
- HA-Partner: Auf Plattformen, auf denen ein Node auf einen und nur einen anderen Node Failover ausgeführt wird, ist er allgemein zu sehen.
- Status: Systemzustand des Node. Nur verfügbar, wenn das Array ordnungsgemäß genug ist, um von einer Datenquelle inventarisiert zu werden.
- Modell: Modellname des Knotens
- Version – Versionsname des Geräts.
- Seriennummer: Die Seriennummer des Node.
- Speicher: Sockel 2 Speicher, falls verfügbar.
- Auslastung – bei ONTAP handelt es sich um einen Controller-Stressindex aus einem proprietären Algorithmus. Bei jeder Performance-Umfrage wird anhand einer Zahl zwischen 0 und 100 % angegeben, die der höhere Wert bei WAFL-Festplattenkonflikten oder der durchschnittlichen CPU-Auslastung ist. Wenn Sie nachhaltige Werte > 50 % beobachten, deutet dies auf eine Unterdimensionierung hin – möglicherweise ist ein Controller/Node nicht groß genug oder nicht genug rotierende Festplatten, um den Schreib-Workload abzufangen.
- IOPS – direkt von ONTAP-ZAPI-Aufrufen des Node-Objekts abgeleitet.
- Latenz – wird direkt von ONTAP-ZAPI-Aufrufen des Node-Objekts abgeleitet.

- Durchsatz – wird direkt von ONTAP-ZAPI-Aufrufen des Node-Objekts abgeleitet.
- Prozessoren: Anzahl der CPUs

Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration und Verwendung dieses Datensammlers:

- Sie müssen Zugriff auf ein Administratorkonto haben, das für schreibgeschützte API-Aufrufe konfiguriert ist.
- Zu den Kontodetails gehören Benutzername und Passwort.
- Port-Anforderungen: 80 oder 443
- Kontoberechtigungen:
  - Nur den Rollennamen in der ontapi-Anwendung auf den Standard-Vserver lesen
  - Möglicherweise benötigen Sie zusätzliche optionale Schreibberechtigungen. Siehe Hinweis über Berechtigungen unten.
- ONTAP Lizenzanforderungen:
  - FCP-Lizenz und zugeordnete/maskierte Volumes sind für die Fibre-Channel-Erkennung erforderlich

Berechtigungsanforderungen für das Sammeln von ONTAP-Switch-Metriken

Data Infrastructure Insights bietet die Möglichkeit, ONTAP-Cluster-Switch-Daten als Option in den Collector-Erweiterte KonfigurationEinstellungen zu erfassen. Zusätzlich zur Aktivierung dieser Funktion im Data Infrastructure Insights Collector müssen Sie das ONTAP-System* selbst so konfigurieren, dass "Switch-Informationen"die korrekten BerechtigungenEinstellungen vorgenommen werden, damit die Switch-Daten an Data Infrastructure Insights gesendet werden können.

Konfiguration

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

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	Wählen Sie HTTP (Standardport 80) oder HTTPS (Standardport 443). Die Standardeinstellung ist HTTPS
Kommunikations-Port Überschreiben	Geben Sie einen anderen Port an, wenn Sie den Standardwert nicht verwenden möchten
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten.
Für TLS für HTTPS	TLS nur als Protokoll bei Verwendung von HTTPS zulassen

Feld	Beschreibung
Netzgruppen Automatisch Suchen	Aktivieren Sie die automatische Suche der Netzgruppe nach den Regeln für die Exportrichtlinie
Netzgruppenerweiterung	Erweiterungsstrategie Für Netzgruppen: Wählen Sie_file_ oder_Shell_. Der Standardwert ist *shell*.
HTTP-Lesezeit Sekunden	Der Standardwert ist 30
Antworten als UTF-8 erzwingen	Erzwingt den Datensammler-Code, um Antworten aus der CLI als in UTF-8 zu interpretieren
Leistungsintervall (Sek.)	Der Standardwert ist 900 Sekunden.
Erweiterte Zähldatensammlung	ONTAP Integration aktivieren. Wählen Sie diese Option aus, um ONTAP Advanced Counter-Daten in Umfragen einzubeziehen. Wählen Sie die gewünschten Zähler aus der Liste aus.
Kennzahlen Für Cluster-Switch	Erfassung von Cluster-Switch-Daten durch Data Infrastructure Insights Beachten Sie, dass Sie zusätzlich zur Aktivierung dieser Funktion auf der Seite Dateninfrastruktureinblicke auch das ONTAP-System so konfigurieren müssen"Switch-Informationen", dass die korrekten BerechtigungenEinstellungen vorgenommen werden, damit die Switch-Daten an Dateninfrastruktureinblicke gesendet werden können. Siehe „Ein Hinweis zu Berechtigungen“ weiter unten.

ONTAP-Leistungskennzahlen

Mehrere ONTAP Modelle bieten Stromkennzahlen für Einblicke in die Dateninfrastruktur, die für Monitoring oder Warnmeldungen genutzt werden können.

> Diese Listen sind nicht vollständig und können sich ändern. Wenn ein Modell zur gleichen Familie gehört wie ein in der Liste aufgeführtes, sollte die Unterstützung grundsätzlich gleich sein, dies kann jedoch nicht garantiert werden. Wenn Sie sich 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 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 **Advanced Counter Data Collection** aktivieren.

Sie sollten außerdem sicherstellen, dass die Schreibberechtigung für die ONTAP-API aktiviert ist. Dafür ist in

der Regel ein Konto auf Cluster-Ebene mit den erforderlichen Berechtigungen erforderlich.

Um ein lokales Konto für Dateninfrastrukturanalysen auf Cluster-Ebene zu erstellen, melden Sie sich mit dem Benutzernamen/Kennwort des Clusterverwaltungsadministrators bei ONTAP an, und führen Sie die folgenden Befehle auf dem ONTAP-Server aus:

1. Bevor Sie beginnen, müssen Sie mit einem *Administrator*-Konto bei ONTAP angemeldet sein und die Befehle *diagnoseebene* müssen aktiviert sein.
2. Erstellen Sie mit den folgenden Befehlen eine schreibgeschützte Rolle.

```
security login role create -role ci_readonly -cmddirname DEFAULT -access
readonly
security login role create -role ci_readonly -cmddirname security
-access readonly
security login role create -role ci_readonly -access all -cmddirname
{cluster application-record create}
```

3. Erstellen Sie den schreibgeschützten Benutzer mit dem folgenden Befehl. Sobald Sie den Befehl create ausgeführt haben, werden Sie aufgefordert, ein Passwort für diesen Benutzer einzugeben.

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

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

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application ontapi -authentication-method domain -role ci_readonly
Wenn Sie Cluster-Switch-Daten erfassen:
```

```
security login rest-role create -role ci_readonly_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 daraus resultierende Rolle und Benutzeranmeldung sieht folgendermaßen aus: Die tatsächliche Ausgabe kann variieren:

```
Role Command/ Access
Vserver Name Directory Query Level
---------- ------------- --------- ------------------ --------
cluster1 ci_readonly DEFAULT read only
cluster1 ci_readonly security readonly
```

```
cluster1:security login> show
Vserver: cluster1
Authentication Acct
UserName    Application   Method      Role Name      Locked
---------   -------      ----------- -------------- --------
ci_user     ontapi      password    ci_readonly   no
```

Wenn die ONTAP-Zugriffssteuerung nicht korrekt eingestellt ist, können die REST-Aufrufe von Data Infrastructure Insights fehlschlagen, was zu Datenlücken für das Gerät führt. Wenn Sie sie beispielsweise auf dem Dateninfrastruktursammler aktiviert haben, aber die Berechtigungen auf dem ONTAP nicht konfiguriert haben, schlägt die Erfassung fehl. Wenn die Rolle zuvor auf der ONTAP definiert ist und Sie die Rest-API-Fähigkeiten hinzufügen, stellen Sie außerdem sicher, dass *http* der Rolle hinzugefügt wird.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Erhalten Sie 401 HTTP-Antwort oder 13003 ZAPI-Fehlercode und ZAPI gibt „unzureichende Berechtigungen“ oder „nicht autorisiert für diesen Befehl“ zurück	Benutzernamen und Kennwort sowie Benutzerrechte/Berechtigungen überprüfen.
Cluster-Version ist < 8.1	Die unterstützte Version für das Cluster-Minimum ist 8.1. Upgrade auf die unterstützte Mindestversion.
ZAPI gibt zurück „Cluster-Rolle ist keine Cluster_Mgmt LIF“	AU muss mit Cluster Management IP sprechen. Überprüfen Sie die IP und wechseln Sie ggf. auf eine andere IP
Fehler: „7 Modus Filer werden nicht unterstützt“	Dies kann passieren, wenn Sie diese Datensammler benutzen, um 7 Modus Filer zu entdecken. Ändern Sie die IP, um stattdessen auf cdot Cluster zu verweisen.
ZAPI-Befehl schlägt nach dem erneuten Versuch fehl	AU hat ein Kommunikationsproblem mit dem Cluster. Überprüfen Sie Netzwerk, Port-Nummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl von der Befehlszeile aus dem AU-Rechner auszuführen.
AU konnte über HTTP keine Verbindung mit ZAPI herstellen	Prüfen Sie, ob der ZAPI-Port Klartext akzeptiert. Wenn AU versucht, Klartext an einen SSL-Socket zu senden, schlägt die Kommunikation fehl.
Die Kommunikation schlägt mit SSLException fehl	AU versucht, SSL an einen Klartext Port auf einem Filer zu senden. Überprüfen Sie, ob der ZAPI-Port SSL akzeptiert, oder verwenden Sie einen anderen Port.

Problem:	Versuchen Sie dies:
Weitere Verbindungsfehler: ZAPI-Antwort hat Fehlercode 13001, „Datenbank ist nicht geöffnet“ ZAPI-Fehlercode ist 60 und die Antwort enthält „API hat nicht auf Zeit beendet“ ZAPI-Antwort enthält „initialize_Session() zurückgegebene Null-Umgebung“ ZAPI-Fehlercode ist 14007 und die Antwort enthält „Knoten ist nicht gesund“	Überprüfen Sie Netzwerk, Port-Nummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl von der Befehlszeile aus dem AU-Rechner auszuführen.

Performance

Problem:	Versuchen Sie dies:
„Fehler beim Sammeln der Leistung aus ZAPI“ Fehler	Dies liegt normalerweise daran, dass perfstat nicht ausgeführt wird. Versuchen Sie auf jedem Knoten den folgenden Befehl: > *System Node systemshell -Node * -command „spmctl -h cmd -stop; spmctl -h cmd -exec“*

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

NetApp ONTAP REST-Datensammler

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 früheren ONTAPI-basierten Collector verwendet werden. Daher kann es bei den gesammelten oder berichteten Metriken zu Unterschieden kommen. Weitere Informationen zu den Unterschieden zwischen ONTAPI und REST finden Sie in der "ONTAP 9.14.1 ONTAPI-to-REST-Zuordnung" Dokumentation.

Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration und Verwendung dieses Datensammlers:

- Sie müssen Zugriff auf ein Benutzerkonto mit der erforderlichen Zugriffsebene haben. Beachten Sie, dass Administratorberechtigungen erforderlich sind, wenn Sie einen neuen REST-Benutzer/eine neue REST-Rolle erstellen.
  - Zu ihren Funktionen gehören in erster Linie Leseanforderungen. Für die Registrierung im ONTAP Array sind jedoch einige Schreibberechtigungen erforderlich, damit sich Dateninfrastruktur Insights registrieren kann. Siehe *Hinweis zu Berechtigungen* direkt unten.
- ONTAP Version 9.14.1 oder höher.
- Anforderungen an den Hafen: 443

Ein Hinweis zu Berechtigungen

Da eine Reihe von ONTAP-Dashboards von Data Infrastructure Insights auf erweiterten ONTAP-Zählern basieren, sollten Sie **Enable Advanced Counter Data Collection** im Abschnitt Data Collector Advanced

Configuration aktivieren.

Um ein lokales Konto für Dateninfrastrukturanalysen auf Cluster-Ebene zu erstellen, melden Sie sich mit dem Benutzernamen/Kennwort des Clusterverwaltungsadministrators bei ONTAP an, und führen Sie die folgenden Befehle auf dem ONTAP-Server aus:

1. Bevor Sie beginnen, müssen Sie mit einem *Administrator*-Konto bei ONTAP angemeldet sein und die Befehle *diagnoseebene* müssen aktiviert sein.
2. Rufen Sie den Namen des vservers vom Typ *admin* ab. Sie werden diesen Namen in nachfolgenden Befehlen verwenden.

```
 vserver show -type admin
. Erstellen Sie eine Rolle mit den folgenden Befehlen:
```

```
security login rest-role create -role {role name} -api /api -access
readonly
security login rest-role create -role {role name} -api
/api/cluster/agents -access all
vserver services web access create -name spi -role {role name} -vserver
{vserver name as retrieved above}
```

3. Erstellen Sie den schreibgeschützten Benutzer mit dem folgenden Befehl. Sobald Sie den Befehl create ausgeführt haben, werden Sie aufgefordert, ein Passwort für diesen Benutzer einzugeben. Beachten Sie, dass im folgenden Befehl die Rolle auf *CI_readonly* gesetzt wird. 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 AD/LDAP-Konto verwendet wird, sollte der Befehl sein
```

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
Die daraus resultierende Rolle und Benutzeranmeldung sieht
folgendermaßen aus: Die tatsächliche Ausgabe kann variieren:
```

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

               Role                                    Access
Vserver        Name            API                     Level
----------     -------------   -------------------     ------
<vserver name> restRole        /api                    readonly
                               /api/cluster/agents     all
2 entries were displayed.

security login show -vserver <vserver name> -user-or-group-name restUser

Vserver: <vserver name>
                                                                  Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------
--------------
restUser       http        password      restRole         no     none
```

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

Gehen Sie wie folgt vor, um von einem früheren ONTAP (ontapi)-Datensammler zum neueren ONTAP-REST-Collector zu migrieren:

1. Fügen Sie den REST Collector hinzu. Es wird empfohlen, Informationen für einen anderen Benutzer einzugeben als für den vorherigen Collector konfiguriert. Verwenden Sie zum Beispiel den Benutzer, der im Abschnitt Berechtigungen oben angegeben ist.
2. Unterbrechen Sie den vorherigen Collector, damit er nicht weiter Daten sammelt.
3. Lassen Sie den neuen REST-Collector Daten für mindestens 30 Minuten erfassen. Ignorieren Sie während dieser Zeit alle Daten, die nicht „normal“ angezeigt werden.
4. Nach der Ruhezeit sollten Sie Ihre Daten stabilisieren sehen, während der REST-Collector weiterhin zu erfassen.

Sie können diesen Vorgang verwenden, um zum vorherigen Collector zurückzukehren, wenn Sie möchten.

Konfiguration

Feld	Beschreibung
ONTAP-Management-IP-Adresse	Die IP-Adresse oder der vollständig qualifizierte Domänenname des NetApp-Clusters. Muss Cluster-Management-IP/FQDN sein.
ONTAP REST-Benutzername	Benutzername für NetApp Cluster
ONTAP REST-Kennwort	Passwort für NetApp Cluster

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten.
Leistungsintervall (Sek.)	Der Standardwert ist 60 Sekunden.
Erweiterte Zähldatensammlung	Wählen Sie diese Option aus, um ONTAP Advanced Counter-Daten in Umfragen einzubeziehen. Standardmäßig aktiviert.
Aktivieren Sie die EMS-Ereigniserfassung	Wählen Sie diese Option aus, um die Ereignisdaten des ONTAP-EMS-Protokolls einzuschließen. Standardmäßig aktiviert.
EMS-Abfrageintervall (s)	Der Standardwert ist 60 Sekunden.

Terminologie

Data Infrastructure Insights erfasst Inventar-, Protokoll- und Performance-Daten aus dem ONTAP Datensammler. Für jeden erworbenen Asset-Typ wird die am häufigsten für das Asset verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Raid-Gruppe	Festplattengruppe
Cluster	Storage
Knoten	Storage-Node
Aggregat	Storage-Pool
LUN	Datenmenge
Datenmenge	Internes Volumen
Storage Virtual Machine/Vserver	Storage Virtual Machine

Terminologie für ONTAP Datenmanagement

Die folgenden Begriffe gelten für Objekte oder Referenzen, die Sie auf den Landing Pages für ONTAP Storage-Assets finden können. Viele dieser Bedingungen gelten auch für andere Datensammler.

Storage

- Modell – Eine durch Komma getrennte Liste der eindeutigen Node-Modellnamen in diesem Cluster. Wenn alle Nodes in den Clustern denselben Modelltyp aufweisen, wird nur ein Modellname angezeigt.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden.
- Seriennummer – die Array-UUID
- IP: In der Regel werden die in der Datenquelle konfigurierten IP(s) oder Hostnamen(s) verwendet.
- Microcode-Version – Firmware.
- Rohkapazität – Basis-2-Zusammenfassung aller physischen Laufwerke im System, unabhängig von ihrer Rolle.
- Latenz – eine Darstellung der Workloads, die sich auf dem Host auslasten, sowohl bei Lese- als auch bei Schreibzugriffen. Idealerweise bezieht Data Infrastructure Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Statt dieses Array in Betracht zu ziehen, führt Data Infrastructure Insights in der Regel eine IOPS-gewichtete Berechnung aus den Statistiken der einzelnen internen Volumes durch.
- Durchsatz: Aggregiert aus internen Volumes. Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert erstellt von der Datenquelle „Data Infrastructure Insights“ als Teil der Bestandsberichterstattung.

Storage-Pool

- Storage – auf welchem Storage-Array dieser Pool lebt. Obligatorisch.
- Typ – ein beschreibenden Wert aus einer Liste mit einer Aufzählung der Möglichkeiten. Am häufigsten wird „Aggregat“ oder „RAID-Gruppe“ sein.
- Node – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Landing Page angezeigt.
- Verwendet Flash Pool – Ja/kein Wert: Verfügen in diesem SATA/SAS-basierten Pool über SSDs zur Caching-Beschleunigung?
- Redundanz: RAID-Level oder Schutzschema. RAID_DP ist Dual-Parity, RAID_TP ist die dreifache Parität.
- Kapazität – die Werte hier sind die logische genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der dafür genutzte Prozentsatz.
- Überprovisionierung der Kapazität – Wenn Sie durch den Einsatz von Effizienztechnologien eine Summe der Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer sind als die logische Kapazität des Speicherpools, wird der Prozentwert hier größer als 0 % sein.
- Snapshot – verwendete und insgesamt Snapshot-Kapazitäten, wenn Ihre Storage Pool-Architektur einem Teil ihrer Kapazität dedizierte Bereiche für Snapshots widmet. ONTAP in MetroCluster Konfigurationen zeigen dies wahrscheinlich, während andere ONTAP Konfigurationen weniger sind.
- Auslastung – ein Prozentwert, der den höchsten ausgelastet anteil der Festplatte anzeigt, die zur Kapazität dieses Speicherpools beiträgt. Die Festplattenauslastung ist nicht unbedingt mit der Array-Performance korreliert – die Auslastung kann aufgrund von Festplattenwiederherstellungen, Deduplizierungsaktivitäten usw. bei Abwesenheit von Host-gestützten Workloads sehr hoch sein. Auch viele Arrays Replikationsimplementierungen können die Festplattenauslastung steigern, während sie nicht als internes Volume oder Volume-Workload angezeigt werden.
- IOPS – die Summe der IOPS aller Festplatten, die Kapazität in diesem Storage-Pool beitragen. Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen.

Storage-Node

- Storage – welches Storage-Array gehört zu diesem Node? Obligatorisch.
- HA-Partner: Auf Plattformen, auf denen ein Node auf einen und nur einen anderen Node Failover ausgeführt wird, ist er allgemein zu sehen.
- Status: Systemzustand des Node. Nur verfügbar, wenn das Array ordnungsgemäß genug ist, um von einer Datenquelle inventarisiert zu werden.
- Modell: Modellname des Knotens
- Version – Versionsname des Geräts.
- Seriennummer: Die Seriennummer des Node.
- Speicher: Sockel 2 Speicher, falls verfügbar.
- Auslastung – bei ONTAP handelt es sich um einen Controller-Stressindex aus einem proprietären Algorithmus. Bei jeder Performance-Umfrage wird anhand einer Zahl zwischen 0 und 100 % angegeben, die der höhere Wert bei WAFL-Festplattenkonflikten oder der durchschnittlichen CPU-Auslastung ist. Wenn Sie nachhaltige Werte > 50 % beobachten, deutet dies auf eine Unterdimensionierung hin – möglicherweise ist ein Controller/Node nicht groß genug oder nicht genug rotierende Festplatten, um den Schreib-Workload abzufangen.
- IOPS – direkt von ONTAP-REST-Aufrufen des Node-Objekts abgeleitet.
- Latenz – wird direkt von ONTAP-REST-Aufrufen des Node-Objekts abgeleitet.
- Durchsatz – wird direkt von ONTAP-REST-Aufrufen des Node-Objekts abgeleitet.
- Prozessoren: Anzahl der CPUs

ONTAP-Leistungskennzahlen

Mehrere ONTAP Modelle bieten Stromkennzahlen für Einblicke in die Dateninfrastruktur, die für Monitoring oder Warnmeldungen genutzt werden können. Die unten aufgeführten Listen unterstützter und nicht unterstützter Modelle sind nicht umfassend, sollten jedoch einige Hinweise enthalten. Wenn ein Modell in der gleichen Familie wie ein Modell auf der Liste ist, sollte der Support identisch sein.

Unterstützte Modelle:

A200 A220 A250 A300 A320 A400 A700 A700S 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

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Problem:	Versuchen Sie dies:
Beim Versuch, einen ONTAP REST Data Collector zu erstellen, wird ein Fehler wie der folgende angezeigt: Konfiguration: 10.193.70.14: ONTAP Rest API at 10.193.70.14 ist nicht verfügbar: 10.193.70.14 Fehler beim ABRUFEN VON /API/Cluster: 400 Bad Request	Dies liegt wahrscheinlich an einem Oldeer ONTAP-Array), z. B. ONTAP 9.6), das keine REST-API-Funktionen hat. ONTAP 9.14.1 ist die minimale ONTAP-Version, die vom ONTAP REST Collector unterstützt wird. Bei den ONTAP-Versionen vor dem REST sind die Antworten auf „400 schlechte Anfragen“ zu erwarten. Für ONTAP-Versionen, die REST unterstützen, aber nicht 9.14.1 oder höher sind, können Sie die folgende ähnliche Nachricht sehen: Konfiguration: 10.193.98.84: ONTAP Rest API bei 10.193.98.84 ist nicht verfügbar: 10.193.98.84: ONTAP Rest API bei 10.193.98.84 ist verfügbar: Cheryl5-Cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7 ist aber nicht von der Mindestversion 9.14.1.
Ich sehe leere oder „0“ Metriken, wo der ONTAP ontapi Collector Daten anzeigt.	ONTAP REST enthält keine Kennzahlen, die nur intern auf dem ONTAP System verwendet werden. Systemaggregate werden beispielsweise nicht von ONTAP REST erfasst, sondern nur SVM vom Typ „Daten“. Weitere Beispiele für ONTAP-REST-Metriken, die null oder leere Daten melden können: InternalVolumes: REST meldet nicht mehr vol0. Aggregate: REST meldet nicht mehr aggr0. Storage: Die meisten Metriken sind eine Auflutung der Kennzahlen für das interne Volume und werden von den oben genannten Auswirkungen beeinflusst. Storage Virtual Machines: REST meldet keine anderen SVM-Typen als „Daten“ (z. B. „Cluster“, „gmt“, „Node“). Sie können auch eine Änderung in der Darstellung von Diagrammen bemerken, die Daten enthalten, aufgrund der Änderung des standardmäßigen Performance-Abfragezeitraums von 15 Minuten auf 5 Minuten. Häufigere Abfragen bedeuten mehr Datenpunkte zum Plotten.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

NetApp Data ONTAP mit 7-Mode Datensammler

Bei Storage-Systemen mit Data ONTAP Software im 7-Mode verwenden Sie den 7-Mode Datensammler, der mit der CLI Kapazitäts- und Performance-Daten bezieht.

Terminologie

Data Infrastructure Insights erfasst die folgenden Inventarinformationen aus dem Data Collector von NetApp 7-Mode. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Dieser Datensammler ist "Veraltet".

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Raid-Gruppe	Festplattengruppe
Filer	Storage
Filer	Storage-Node
Aggregat	Storage-Pool
LUN	Datenmenge
Datenmenge	Internes Volumen

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Sie benötigen Folgendes, um diesen Datensammler zu konfigurieren und zu verwenden:

- IP-Adressen des FAS Storage Controllers und des Partners.
- Anschluss 443
- Ein benutzerdefinierter Benutzername und Passwort für den Admin-Level für den Controller und den Partner-Controller mit den folgenden Rollenfunktionen für 7-Mode:
  - „api-*“: Nutzen Sie diese, um OnCommand Insight die Ausführung aller NetApp Storage-API-Befehle zu ermöglichen.
  - „login-http-admin“: Hiermit kann OnCommand Insight über HTTP eine Verbindung mit dem NetApp Storage herstellen.
  - „Security-API-vfiler“: Nutzen Sie dies, um OnCommand Insight zu ermöglichen, NetApp Storage API Befehle auszuführen, um vFiler Einheitsinformationen abzurufen.
  - „cli-Optionen“: Hier können Sie Storage-Systemoptionen lesen.
  - „cli-lun“: Greifen Sie auf diese Befehle zum Verwalten von LUNs zu. Zeigt den Status (LUN-Pfad, Größe, Online/Offline-Zustand und Shared-Zustand) der angegebenen LUN oder Klasse von LUNs an.
  - „cli-df“: Verwenden Sie dies, um freien Speicherplatz anzuzeigen.
  - „cli-ifconfig“: Verwenden Sie diese, um Schnittstellen und IP-Adressen anzuzeigen.

Konfiguration

Feld	Beschreibung
Adresse des Storage-Systems	IP-Adresse oder vollqualifizierter Domain-Name für das NetApp Storage-System
Benutzername	Benutzername für das NetApp Storage-System
Passwort	Passwort für das NetApp Storage-System
Adresse des HA-Partners im Cluster	IP-Adresse oder vollqualifizierter Domain-Name für den HA-Partner
Benutzername des HA-Partners in Cluster	Benutzername für den HA-Partner

Feld	Beschreibung
Passwort des HA Partner Filer in Cluster	Passwort für den HA-Partner

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 20 Minuten.
Verbindungstyp	HTTPS oder HTTP: Zeigt auch den Standardport an
Verbindungs-Port Überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport im Feld Verbindungstyp. Andernfalls geben Sie den zu verwendenden Anschluss ein
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Die Standardeinstellung ist 300 Sekunden.

Storage-Systemverbindung

Als Alternative zur Nutzung des Standard-Administrationsbenutzers für diesen Datensammler können Sie einen Benutzer mit Administratorrechten direkt auf den NetApp Storage-Systemen konfigurieren, sodass dieser Datensammler Daten von NetApp Storage-Systemen erfassen kann.

Für die Verbindung zu NetApp Storage-Systemen muss der Benutzer, der beim Erwerb der Haupt-pfiler angegeben ist (auf dem das Speichersystem vorhanden ist), die folgenden Bedingungen erfüllen:

- Der Benutzer muss auf vfiler0 (root Filer/pfiler) sein.

  Storage-Systeme werden beim Erwerb der Haupt-Filer erworben.

- Mit den folgenden Befehlen werden die Fähigkeiten der Benutzerrolle definiert:
  - „api-*“: Damit kann Dateninfrastruktur Insights alle NetApp Storage API-Befehle ausführen.

    Dieser Befehl ist erforderlich, um das ZAPI zu verwenden.

  - „login-http-admin“: Hiermit können Dateninfrastruktureinblicke über HTTP eine Verbindung zum NetApp-Speicher herstellen. Dieser Befehl ist erforderlich, um das ZAPI zu verwenden.
  - Security-API-vfiler: Verwenden Sie diese, damit Dateninfrastruktur Insights NetApp Storage API-Befehle ausführen kann, um Informationen über die vFiler Einheit abzurufen.
  - „cli-Opes“: Zum Befehl „Opes“, der für Partner-IP und aktivierte Lizenzen verwendet wird.
  - „cli-lun“: Greifen Sie auf diesen Befehl zum Verwalten von LUNs zu. Zeigt den Status (LUN-Pfad, Größe, Online/Offline-Zustand und Shared-Zustand) der angegebenen LUN oder Klasse von LUNs an.
  - „cli-df“: Für „df -s“, „df -r“, „df -A -r“ und für die Anzeige des freien Speicherplatzes
  - „cli-ifconfig“: Für „ifconfig -a“ Befehl und verwendet für das Abrufen von Filer IP Adresse.
  - "cli-rdfile": Für den Befehl "rdfile /etc/netgroup" und für das Abrufen von Netzgruppen verwendet.
  - „cli-Datum“: Für den Befehl „Datum“ und mit dem vollständigen Datum für das Abrufen von Snapshot Kopien.
  - „cli-Snap“: Für den Befehl „Snap list“ und zum Abrufen von Snapshot Kopien verwendet.

Wenn cli-Datum oder cli-Snap Berechtigungen nicht bereitgestellt werden, kann die Erfassung abgeschlossen werden. Snapshot Kopien werden jedoch nicht gemeldet.

Um eine 7-Mode Datenquelle erfolgreich zu erhalten und keine Warnungen auf dem Speichersystem zu generieren, sollten Sie eine der folgenden Befehlstrings verwenden, um Ihre Benutzerrollen zu definieren. Der zweite hier aufgeführte String ist eine optimierte Version des ersten:

- login-http-admin,API-*,Security-API-vfile,cli-rdfile,cli-options,cli-df,cli-lun,cli-ifconfig,cli-date,cli-Snap,_
- login-http-admin,API-*,Security-API-vfile,cli-

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Erhalten Sie 401 HTTP-Antwort oder 13003 ZAPI-Fehlercode und ZAPI gibt „unzureichende Berechtigungen“ oder „nicht autorisiert für diesen Befehl“ zurück	Benutzernamen und Kennwort sowie Benutzerrechte/Berechtigungen überprüfen.
Fehler „Befehl konnte nicht ausgeführt werden“	Prüfen Sie, ob der Benutzer auf dem Gerät über die folgenden Berechtigungen verfügt: • API-* • cli-date • cli-df • cli-ifconfig • cli-lun • cli-Operations • cli-rdfile • cli-Snap • Login-http-admin • Security-API-vfiler überprüfen Sie auch, ob die ONTAP-Version von Data Infrastructure Insights unterstützt wird, und überprüfen Sie, ob die verwendeten Anmeldeinformationen mit den Geräteanmeldeinformationen übereinstimmen
Cluster-Version ist < 8.1	Die unterstützte Version für das Cluster-Minimum ist 8.1. Upgrade auf die unterstützte Mindestversion.
ZAPI gibt zurück „Cluster-Rolle ist keine Cluster_Mgmt LIF“	AU muss mit Cluster Management IP sprechen. Überprüfen Sie die IP und wechseln Sie ggf. auf eine andere IP
Fehler: „7 Modus Filer werden nicht unterstützt“	Dies kann passieren, wenn Sie diese Datensammler benutzen, um 7 Modus Filer zu entdecken. Ändern Sie IP, um stattdessen auf cdot Filer zu verweisen.
ZAPI-Befehl schlägt nach dem erneuten Versuch fehl	AU hat ein Kommunikationsproblem mit dem Cluster. Überprüfen Sie Netzwerk, Port-Nummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl von der Befehlszeile aus dem AU-Rechner auszuführen.
AU konnte Verbindung zum ZAPI nicht herstellen	IP/Port-Konnektivität prüfen und ZAPI-Konfiguration bestätigen.
AU konnte über HTTP keine Verbindung mit ZAPI herstellen	Prüfen Sie, ob der ZAPI-Port Klartext akzeptiert. Wenn AU versucht, Klartext an einen SSL-Socket zu senden, schlägt die Kommunikation fehl.

Problem:	Versuchen Sie dies:
Die Kommunikation schlägt mit SSLException fehl	AU versucht, SSL an einen Klartext Port auf einem Filer zu senden. Überprüfen Sie, ob der ZAPI-Port SSL akzeptiert, oder verwenden Sie einen anderen Port.
Weitere Verbindungsfehler: ZAPI-Antwort hat Fehlercode 13001, „Datenbank ist nicht geöffnet“ ZAPI-Fehlercode ist 60 und die Antwort enthält „API hat nicht auf Zeit beendet“ ZAPI-Antwort enthält „initialize_Session() zurückgegebene Null-Umgebung“ ZAPI-Fehlercode ist 14007 und die Antwort enthält „Knoten ist nicht gesund“	Überprüfen Sie Netzwerk, Port-Nummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl von der Befehlszeile aus dem AU-Rechner auszuführen.
Socket-Zeitüberschreitungsfehler mit ZAPI	Prüfen Sie die Filer-Konnektivität und/oder erhöhen Sie die Zeitüberschreitung.
„C-Modus-Cluster werden nicht durch den 7-Mode-Datenquelle unterstützt“-Fehler	Überprüfen Sie die IP und ändern Sie die IP in ein 7-Mode-Cluster.
Fehler „Verbindung zum vFiler konnte nicht hergestellt werden“	Überprüfen Sie, ob die Fähigkeiten des Erwerbs von Benutzern mindestens folgende Fähigkeiten enthalten: api-* Security-API-vfiler Login-http-admin Bestätigen Sie, dass Filer mindestens ONTAPI Version 1.7 läuft.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Datensammler für die NetApp E-Series ältere SANtricity API

Der Datensammler für die ältere SANtricity-API der NetApp E-Series erfasst Inventar- und Performance-Daten. Der Collector unterstützt die Firmware 7.x+ unter Verwendung derselben Konfigurationen und meldet dieselben Daten.

Terminologie

Cloud Insight erfasst die folgenden Bestandsinformationen aus dem NetApp E-Series Data Collector. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Volume-Gruppe	Festplattengruppe
Storage Array Durchführt	Storage
Controller	Storage-Node
Volume-Gruppe	Storage-Pool
Datenmenge	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Terminologie der E-Series (Landing Page)

Die folgenden Begriffe gelten für Objekte oder Referenzen, die Sie auf den Asset-Landing-Pages der NetApp E-Series finden können. Viele dieser Bedingungen gelten auch für andere Datensammler.

Storage

- Modell – Modellname des Geräts.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden
- Seriennummer: Die Seriennummer des Arrays. Bei Storage-Systemen der Cluster-Architektur wie NetApp Clustered Data ONTAP ist diese Seriennummer möglicherweise weniger nützlich als die einzelnen Seriennummern der Storage-Nodes
- IP: In der Regel werden die in der Datenquelle konfigurierten IP(s) oder Hostnamen(s) verwendet
- Microcode-Version – Firmware
- Rohkapazität – Basis-2-Zusammenfassung aller physischen Laufwerke im System, unabhängig von ihrer Rolle
- Latenz – eine Darstellung der Workloads, die sich auf dem Host auslasten, sowohl bei Lese- als auch bei Schreibzugriffen. Idealerweise bezieht Data Infrastructure Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Statt dieses Array in Betracht zu ziehen, führt Data Infrastructure Insights in der Regel eine IOPS-gewichtete Berechnung aus den Statistiken der einzelnen Volumes durch.
- Durchsatz – der Gesamthost des Arrays mit Blick auf den Durchsatz. Data Infrastructure Insights wird im Idealfall direkt aus dem Array bezogen, falls nicht verfügbar, und fasst den Durchsatz der Volumes zusammen, um diesen Wert abzuleiten
- Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert erstellt von der Data Infrastructure Insights Datenquelle als Teil der Bestandsberichterstattung

Storage-Pool

- Storage – auf welchem Storage-Array dieser Pool lebt. Obligatorisch
- Typ – ein beschreibenden Wert aus einer Liste mit einer Aufzählung der Möglichkeiten. Am häufigsten wird „Thin Provisioning“ oder „RAID-Gruppe“ sein
- Node – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Landing Page angezeigt
- Verwendet Flash Pool – Ja/Nein-Wert
- Redundanz: RAID-Level oder Schutzschema. E-Series berichtet „RAID 7“ für DDP Pools
- Kapazität – die Werte hier sind die logische genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der dafür genutzte Prozentsatz. Zu diesen beiden Werten zählen die „Erhaltung“ der Kapazität der E-Series, was sowohl in Zahlen als auch in Prozent höher ist als die der E-Series eigenen Benutzeroberfläche angezeigt werden kann
- Überprovisionierung der Kapazität: Wenn Sie mithilfe von Effizienztechnologien eine Summe der Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer sind als die logische Kapazität des Speicherpools, wird der prozentuale Wert hier größer als 0 % sein.
- Snapshot – verwendete und insgesamt Snapshot-Kapazitäten, wenn Ihre Storage Pool-Architektur einem Teil ihrer Kapazität dedizierte Bereiche für Snapshots widmet
- Auslastung – ein Prozentwert, der den höchsten ausgelastet anteil der Festplatte anzeigt, die zur Kapazität

dieses Speicherpools beiträgt. Die Festplattenauslastung ist nicht unbedingt mit der Array-Performance korreliert – die Auslastung kann aufgrund von Festplattenwiederherstellungen, Deduplizierungsaktivitäten usw. bei Abwesenheit von Host-gestützten Workloads sehr hoch sein. Außerdem können viele Arrays Replikationsimplementierungen die Festplattenauslastung steigern, während sie nicht als Volume-Workload angezeigt werden.

- IOPS – die Summe der IOPS aller Festplatten, die Kapazität in diesem Storage-Pool beitragen. Wenn Festplatten-IOPS auf einer bestimmten Plattform nicht verfügbar sind, wird dieser Wert aus der Summe der Volume-IOPS für alle Volumes in diesem Speicherpool bezogen
- Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Wenn der Festplattendurchsatz auf einer bestimmten Plattform nicht verfügbar ist, wird dieser Wert für alle Volumes in diesem Speicherpool aus der Summe des Volumes abgerufen

Storage-Node

- Storage – welches Storage-Array gehört zu diesem Node? Obligatorisch
- HA-Partner: Auf Plattformen, auf denen ein Node auf einen und nur einen anderen Node Failover ausgeführt wird, ist er allgemein zu sehen
- Status: Systemzustand des Node. Nur verfügbar, wenn das Array ordnungsgemäß genug ist, um von einer Datenquelle inventarisiert zu werden
- Modell: Modellname des Knotens
- Version – Versionsname des Geräts.
- Seriennummer: Die Seriennummer des Node
- Speicher: Sockel 2 Speicher, falls verfügbar
- Auslastung – im Allgemeinen eine CPU-Auslastungsnummer, oder im Fall von NetApp ONTAP, ein Controller-Stressindex. Die Auslastung ist derzeit für die NetApp E-Series nicht verfügbar
- IOPS: Eine Zahl, die die Host-gestützten IOPS auf diesem Controller repräsentiert. Idealerweise direkt aus dem Array bezogen. Wenn nicht verfügbar, wird der Wert berechnet, indem alle IOPS für Volumes zusammengefasst werden, die ausschließlich zu diesem Node gehören.
- Latenz – eine Zahl, die die typische Host-Latenz oder Antwortzeit auf diesem Controller repräsentiert. Wenn nicht verfügbar, wird er idealerweise direkt aus dem Array bezogen. Wird das System dann berechnet, wenn die gewichtete IOPS-Berechnung aus den Volumes durchgeführt wird, die ausschließlich zu diesem Node gehören.
- Durchsatz: Eine Zahl, die den Host-basierten Durchsatz auf diesem Controller repräsentiert. Falls nicht verfügbar, wird der gesamte Durchsatz aus dem Array bezogen, wenn er nicht verfügbar ist, wird er berechnet, indem der gesamte Durchsatz für Volumes zusammengefasst wird, die ausschließlich zu diesem Node gehören.
- Prozessoren: Anzahl der CPUs

Anforderungen

- Die IP-Adresse jedes Controllers im Array
- Port-Anforderung 2463

Konfiguration

Feld	Beschreibung
Kommagetrennte Liste der Array-SANtricity-Controller-IPs	IP-Adressen und/oder vollqualifizierte Domain-Namen für die Array Controller

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 30 Minuten
Leistungsintervall bis zu 3600 Sekunden	Der Standardwert ist 300 Sekunden

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

NetApp E-Series REST-Datensammler

Der REST-Datensammler der NetApp E-Series erfasst Inventar- und Performance-Daten. Der Collector unterstützt die Firmware 7.x+ unter Verwendung derselben Konfigurationen und meldet dieselben Daten. Der REST Collector überwacht den Verschlüsselungsstatus von Speicherpools sowie den Verschlüsselungsstatus zugehöriger Festplatten und Volumes und bietet CPU-Auslastung von Speicherknoten als Performance-Zähler - Funktionalität, die nicht im älteren Collector der SANtricity E-Series bereitgestellt wird.

Terminologie

Cloud Insight erfasst mithilfe von REST die folgenden Inventarinformationen der NetApp E-Series: Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Festplatte
Volume-Gruppe	Festplattengruppe
Storage Array Durchführt	Storage
Controller	Storage-Node
Volume-Gruppe	Storage-Pool
Datenmenge	Datenmenge

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Die IP-Adresse jedes Controllers im Array
- Dieser Collector unterstützt nur Arrays mit E-Series-Modellen mit **nativen REST-API-Funktionen**. Die E-Series Organisation liefert eine Array-externe, installierbare REST API-Distribution für ältere E-Series

Arrays, die dieses Szenario nicht unterstützt. Benutzer mit älteren Arrays sollten weiterhin den "E-Series SANtricity API"Collector von Data Infrastructure Insights verwenden.

- Das Feld „E-Series Controller IP-Adressen“ unterstützt eine durch Kommas getrennte Zeichenfolge von 2 IP/Hostnamen. Der Collector versucht intelligent, den zweiten IP/Hostnamen zu verwenden, wenn der erste nicht zugänglich ist.
- HTTPS-Port: Der Standardwert ist 8443.

Konfiguration

Feld	Beschreibung
IP-Adressen der E-Series Controller	Kommagetrennte IP-Adressen und/oder vollständig qualifizierte Domänennamen für die Array-Controller

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 30 Minuten
Leistungsintervall bis zu 3600 Sekunden	Der Standardwert ist 300 Sekunden

Terminologie der E-Series (Landing Page)

Die folgenden Begriffe gelten für Objekte oder Referenzen, die Sie auf den Asset-Landing-Pages der NetApp E-Series finden können. Viele dieser Bedingungen gelten auch für andere Datensammler.

Storage

- Modell – Modellname des Geräts.
- Anbieter – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden
- Seriennummer: Die Seriennummer des Arrays. Bei Storage-Systemen der Cluster-Architektur wie NetApp Clustered Data ONTAP ist diese Seriennummer möglicherweise weniger nützlich als die einzelnen Seriennummern der Storage-Nodes
- IP: In der Regel werden die in der Datenquelle konfigurierten IP(s) oder Hostnamen(s) verwendet
- Microcode-Version – Firmware
- Rohkapazität – Basis-2-Zusammenfassung aller physischen Laufwerke im System, unabhängig von ihrer Rolle
- Latenz – eine Darstellung der Workloads, die sich auf dem Host auslasten, sowohl bei Lese- als auch bei Schreibzugriffen. Idealerweise bezieht Data Infrastructure Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Statt dieses Array in Betracht zu ziehen, führt Data Infrastructure Insights in der Regel eine IOPS-gewichtete Berechnung aus den Statistiken der einzelnen Volumes durch.
- Durchsatz – der Gesamthost des Arrays mit Blick auf den Durchsatz. Data Infrastructure Insights wird im Idealfall direkt aus dem Array bezogen, falls nicht verfügbar, und fasst den Durchsatz der Volumes zusammen, um diesen Wert abzuleiten
- Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Programmgesteuert erstellt von der Data Infrastructure Insights Datenquelle als Teil der Bestandsberichterstattung

Storage-Pool

- Storage – auf welchem Storage-Array dieser Pool lebt. Obligatorisch
- Typ – ein beschreibenden Wert aus einer Liste mit einer Aufzählung der Möglichkeiten. Am häufigsten wird „Thin Provisioning“ oder „RAID-Gruppe“ sein
- Node – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicherknoten gehören, wird sein Name hier als Hyperlink zu seiner eigenen Landing Page angezeigt
- Verwendet Flash Pool – Ja/Nein-Wert
- Redundanz: RAID-Level oder Schutzschema. E-Series berichtet „RAID 7“ für DDP Pools
- Kapazität – die Werte hier sind die logische genutzte, nutzbare Kapazität und die logische Gesamtkapazität sowie der dafür genutzte Prozentsatz. Zu diesen beiden Werten zählen die „Erhaltung“ der Kapazität der E-Series, was sowohl in Zahlen als auch in Prozent höher ist als die der E-Series eigenen Benutzeroberfläche angezeigt werden kann
- Überprovisionierung der Kapazität: Wenn Sie mithilfe von Effizienztechnologien eine Summe der Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer sind als die logische Kapazität des Speicherpools, wird der prozentuale Wert hier größer als 0 % sein.
- Snapshot – verwendete und insgesamt Snapshot-Kapazitäten, wenn Ihre Storage Pool-Architektur einem Teil ihrer Kapazität dedizierte Bereiche für Snapshots widmet
- Auslastung – ein Prozentwert, der den höchsten ausgelastet anteil der Festplatte anzeigt, die zur Kapazität dieses Speicherpools beiträgt. Die Festplattenauslastung ist nicht unbedingt mit der Array-Performance korreliert – die Auslastung kann aufgrund von Festplattenwiederherstellungen, Deduplizierungsaktivitäten usw. bei Abwesenheit von Host-gestützten Workloads sehr hoch sein. Außerdem können viele Arrays Replikationsimplementierungen die Festplattenauslastung steigern, während sie nicht als Volume-Workload angezeigt werden.
- IOPS – die Summe der IOPS aller Festplatten, die Kapazität in diesem Storage-Pool beitragen. Wenn Festplatten-IOPS auf einer bestimmten Plattform nicht verfügbar sind, wird dieser Wert aus der Summe der Volume-IOPS für alle Volumes in diesem Speicherpool bezogen
- Durchsatz – der Gesamtdurchsatz aller Festplatten, die Kapazität zu diesem Speicherpool beitragen. Wenn der Festplattendurchsatz auf einer bestimmten Plattform nicht verfügbar ist, wird dieser Wert für alle Volumes in diesem Speicherpool aus der Summe des Volumes abgerufen

Storage-Node

- Storage – welches Storage-Array gehört zu diesem Node? Obligatorisch
- HA-Partner: Auf Plattformen, auf denen ein Node auf einen und nur einen anderen Node Failover ausgeführt wird, ist er allgemein zu sehen
- Status: Systemzustand des Node. Nur verfügbar, wenn das Array ordnungsgemäß genug ist, um von einer Datenquelle inventarisiert zu werden
- Modell: Modellname des Knotens
- Version – Versionsname des Geräts.
- Seriennummer: Die Seriennummer des Node
- Speicher: Sockel 2 Speicher, falls verfügbar
- Auslastung – im Allgemeinen eine CPU-Auslastungsnummer, oder im Fall von NetApp ONTAP, ein Controller-Stressindex. Die Auslastung ist derzeit für die NetApp E-Series nicht verfügbar
- IOPS: Eine Zahl, die die Host-gestützten IOPS auf diesem Controller repräsentiert. Idealerweise direkt aus dem Array bezogen. Wenn nicht verfügbar, wird der Wert berechnet, indem alle IOPS für Volumes

zusammengefasst werden, die ausschließlich zu diesem Node gehören.

- Latenz – eine Zahl, die die typische Host-Latenz oder Antwortzeit auf diesem Controller repräsentiert. Wenn nicht verfügbar, wird er idealerweise direkt aus dem Array bezogen. Wird das System dann berechnet, wenn die gewichtete IOPS-Berechnung aus den Volumes durchgeführt wird, die ausschließlich zu diesem Node gehören.
- Durchsatz: Eine Zahl, die den Host-basierten Durchsatz auf diesem Controller repräsentiert. Falls nicht verfügbar, wird der gesamte Durchsatz aus dem Array bezogen, wenn er nicht verfügbar ist, wird er berechnet, indem der gesamte Durchsatz für Volumes zusammengefasst wird, die ausschließlich zu diesem Node gehören.
- Prozessoren: Anzahl der CPUs

Fehlerbehebung

Weitere Informationen zu diesem Datensammler finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Konfigurieren des Datensammlers des NetApp HCI-Verwaltungsservers

Der Datensammler des NetApp HCI-Verwaltungsservers sammelt Informationen zum NetApp HCI-Host und benötigt schreibgeschützte Berechtigungen auf allen Objekten innerhalb des Verwaltungsservers.

Dieser Datensammler erwirbt nur vom **NetApp HCI Management Server**. Um Daten vom Speichersystem zu erfassen, müssen Sie auch den Data Collector konfigurieren"NetApp SolidFire".

Terminologie

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

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Virtuelle Festplatte	Festplatte
Host	Host
Virtual Machine	Virtual Machine
Datastore	Datastore
LUN	Datenmenge
Fibre-Channel-Port	Port

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

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Informationen erforderlich:

- IP-Adresse des NetApp HCI-Verwaltungsservers
- Schreibgeschützter Benutzername und Kennwort für den NetApp HCI-Verwaltungsserver

- Schreibgeschützte Berechtigungen für alle Objekte im NetApp HCI-Verwaltungsserver.
- SDK-Zugriff auf den NetApp HCI-Verwaltungsserver – in der Regel bereits eingerichtet.
- Port-Anforderungen: http-80 HTTPS-443
- Zugriff validieren:
  - Melden Sie sich mit dem oben genannten Benutzernamen und Kennwort beim NetApp HCI-Verwaltungsserver an
  - Überprüfen Sie, ob das SDK aktiviert ist: telnet <vc_ip> 443

Einrichtung und Verbindung

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

Konfiguration

Feld	Beschreibung
NetApp HCI Storage Cluster MVIP	Management Virtual IP-Adresse
SolidFire-Management-Node (mNode)	Management-Node-IP-Adresse
Benutzername	Benutzername für den Zugriff auf den NetApp HCI-Verwaltungsserver
Passwort	Passwort für den Zugriff auf den NetApp HCI-Verwaltungsserver
VCenter-Benutzername	Benutzername für vCenter
VCenter Passwort	Passwort für vCenter

Erweiterte Konfiguration

Aktivieren Sie im Bildschirm Erweiterte Konfiguration die Option **VM Performance**, um Leistungsdaten zu sammeln. Bestandserfassung ist standardmäßig aktiviert. Die folgenden Felder können konfiguriert werden:

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Deafult ist 20
Filtern von VMs nach	Wählen Sie EINEN CLUSTER-, DATACENTER- oder ESX-HOST aus
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob VMs ein- oder ausgeschlossen werden sollen
Geräteliste Filtern	Liste der zu filternden VMs (durch Komma getrennt oder durch Semikolon getrennt, wenn Komma im Wert verwendet wird) für die Filterung nur nach ESX_HOST, CLUSTER und DATACENTER
Leistungsintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: Liste einschließen, um VMs zu filtern, darf nicht leer sein	Wenn Liste einschließen ausgewählt ist, geben Sie gültige DataCenter-, Cluster- oder Hostnamen an, um VMs zu filtern
Fehler: Es konnte keine Verbindung zu VirtualCenter bei IP hergestellt werden	Mögliche Lösungen: * Überprüfen Sie die eingegebenen Anmeldeinformationen und die eingegebene IP-Adresse. * Versuchen Sie, mit Virtual Center über Infrastructure Client zu kommunizieren. * Versuchen Sie, mit Virtual Center über Managed Object Browser (z. B. MOB) zu kommunizieren.
Fehler: VirtualCenter at IP verfügt über kein von JVM einkonformes Zertifikat	Mögliche Lösungen: * Empfohlen: Zertifikat für Virtual Center durch Verwendung von Stronger (z.B. neu generieren 1024-Bit) RSA-Schlüssel * Nicht empfohlen: Ändern Sie die JVM java.security-Konfiguration, um die Einschränkung jdk.certpath.diabledAlgorithms zu nutzen, um einen 512-Bit-RSA-Schlüssel zu ermöglichen. Siehe JDK 7 Update 40 Release Notes unter "http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

NetApp SolidFire All-Flash Array Datensammler

Der NetApp SolidFire All-Flash Array Data Collector unterstützt die Bestandsaufnahme und Performance der iSCSI- und Fibre Channel SolidFire-Konfigurationen.

Der SolidFire Datensammler nutzt die SolidFire REST API. Die Erfassungseinheit, in der sich der Datensammler befindet, muss in der Lage sein, HTTPS-Verbindungen zum TCP-Port 443 an der SolidFire-Cluster-Management-IP-Adresse zu initiieren. Der Datensammler benötigt Zugangsdaten, die in der Lage sind, REST-API-Abfragen auf dem SolidFire Cluster zu erstellen.

Terminologie

Data Infrastructure Insights bezieht die folgenden Inventarinformationen aus dem Datensammler für rein Flash-basierte NetApp SolidFire Arrays: Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Laufwerk	Festplatte

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Cluster	Storage
Knoten	Storage-Node
Datenmenge	Datenmenge
Fibre-Channel-Port	Port
Volume Access Group, LUN-Zuweisung	Volume-Zuordnung
ISCSI-Sitzung	Volume-Maske

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration dieses Datensammlers:

- Management Virtual IP-Adresse
- Schreibgeschützter Benutzername und Anmeldeinformationen
- Anschluss 443

Konfiguration

Feld	Beschreibung
Management Virtual IP-Adresse (MVIP)	Management-virtuelle IP-Adresse des SolidFire-Clusters
Benutzername	Name, der zur Anmeldung im SolidFire Cluster verwendet wird
Passwort	Passwort, das zur Anmeldung beim SolidFire Cluster verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	Wählen Sie den Verbindungstyp
Kommunikations-Port	Für NetApp API verwendeter Port
Abfrageintervall für Bestand (min)	Der Standardwert ist 20 Minuten
Leistungsintervall (Sek.)	Der Standardwert ist 300 Sekunden

Fehlerbehebung

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

Beim Versuch, Daten abzurufen, wurde eine Fehlermeldung von einem SolidFire-Gerät empfangen. Der Aufruf war <method> (<parameterString>). Die Fehlermeldung vom Gerät war (überprüfen Sie die Bedienungsanleitung des Geräts): <message>

Wo?

- Die ←Methode> ist eine HTTP-Methode, z. B. GET oder PUT.
- Der <parameterString> ist eine kommagetrennte Liste von Parametern, die im REST-Aufruf enthalten waren.
- Die Meldung <message> ist das Gerät, das als Fehlermeldung zurückgegeben wurde.

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

NetApp StorageGRID Datensammler

Der NetApp StorageGRID Datensammler unterstützt Inventar- und Performance-Sammlung aus 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 erfasst die folgenden Bestandsinformationen aus dem NetApp StorageGRID-Collector. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
StorageGRID	Storage
Knoten	Knoten
Mandant	Storage-Pool
Eimer	Internes Volumen

Anforderungen

Für die Konfiguration dieser Datenquelle gelten folgende Anforderungen:

- StorageGRID-Host-IP-Adresse
- Ein Benutzername und ein Passwort für einen Benutzer, dem die Rollen Metric Query und Tenant Access zugewiesen sind
- Anschluss 443

Konfiguration

Feld	Beschreibung
StorageGRID-Host-IP-Adresse	Management der virtuellen IP-Adresse der StorageGRID Appliance
Benutzername	Name, der zur Anmeldung bei der StorageGRID Appliance verwendet wird
Passwort	Passwort, das zur Anmeldung bei der StorageGRID Appliance verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten
Leistungsintervall (Sek.)	Der Standardwert ist 900 Sekunden

Single Sign On (SSO)

Die "StorageGRID" Firmware-Versionen verfügen über entsprechende API-Versionen; 3.0 API und neuere Versionen unterstützen Single Sign-On (SSO)-Anmeldung.

Die Firmware-Version	API-Version	Unterstützung von Single Sign On (SSO)
11,1	2	Nein
11,2	3,0	Ja.
11,5	3,3	Ja.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Nutanix NX-Datensammler

Data Infrastructure Insights nutzt den Nutanix Datensammler zur Erkennung von Bestands- und Performancedaten für Nutanix NX-Speichersysteme.

Terminologie

Data Infrastructure Insights erfasst die folgenden Bestandsinformationen aus dem Nutanix Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Storage-Pool	Storage-Pool

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Nutanix Container	Internes Volumen
Nutanix Container	Dateifreigabe
NFS-Share	Share

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- Die IP-Adresse für externe Datendienste für den Cluster
- Schreibgeschützter Benutzername und Kennwort, sofern keine Volume_groups verwendet werden, sind in diesem Fall Administratorbenutzername und Passwort erforderlich
- Port-Anforderung: HTTPS 443

Konfiguration

Feld	Beschreibung
Externe IP-Adresse des Prism	Die IP-Adresse für externe Datendienste für den Cluster
Benutzername	Benutzername für das Administratorkonto
Passwort	Kennwort für das Administratorkonto

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP Port für die Verbindung mit dem Nutanix Array. Der Standardwert ist 9440.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Die Standardeinstellung ist 60 Minuten.
Abfrageintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Die Standardeinstellung ist 300 Sekunden.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Datensammler der Oracle ZFS Storage Appliance

Data Infrastructure Insights verwendet den Datensammler der Oracle ZFS Storage Appliance zur Erfassung von Bestands- und Leistungsdaten.

Terminologie

Data Infrastructure Insights erfasst Bestandsinformationen mit dem Oracle ZFS-Datensammler. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte (SSD)	Festplatte
Cluster	Storage
Controller	Storage-Node
LUN	Datenmenge
LUN-Zuordnung	Volume-Zuordnung
Initiator, Ziel	Volume-Maske
Share	Internes Volumen

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. In dieser Datenquelle fallen möglicherweise nicht alle Fälle an.

Anforderungen

- Host-Namen für den ZFS-Controller-1 und den ZFS-Controller-2
- Administrator-Benutzername und -Passwort
- Port-Anforderung: 215 HTTP/HTTPS

Erforderliche Performance-Metriken

Oracle ZFS Appliances stellen Storage-Verwaltungen große Flexibilität zur Erfassung von Performance-Statistiken zur Verfügung. Data Infrastructure Insights erwartet, dass Sie in einem Hochverfügbarkeitspaar *each* Controller konfiguriert haben, um die folgenden Kennzahlen zu erfassen:

- smb2.OPS[Freigabe]
- nfs3.OPS[Freigabe]
- nfs4.OPS[Share]
- nfs4-1.OPS[Share]

Wird ein Controller diese oder alle Funktionen nicht erfassen, führt dies wahrscheinlich dazu, dass Data Infrastructure Insights den Workload auf den „internen Volumes“ nicht oder nur unzureichend meldet.

Konfiguration

Feld	Beschreibung
ZFS Controller-1-Hostname	Host-Name für Storage Controller 1
ZFS Controller-2-Hostname	Host-Name für Storage Controller 2

Feld	Beschreibung
Benutzername	Benutzername für das Benutzerkonto des Speichersystemadministrators
Passwort	Kennwort für das Administratorbenutzerkonto

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	HTTPS oder HTTP: Zeigt auch den Standardport an
Verbindungs-Port Überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport im Feld Verbindungstyp. Andernfalls geben Sie den zu verwendenden Anschluss ein
Abfrageintervall für den Bestand	Der Standardwert beträgt 60 Sekunden
Leistungsintervall (Sek.)	Der Standardwert ist 300.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Ungültige Anmeldeinformationen“	ZFS-Benutzerkonto und -Passwort validieren
„Anfrage mit Status 404 https://…..:215/api/access/v1" fehlgeschlagen	Ihr ZFS-Array ist möglicherweise zu alt, um REST-API-Unterstützung zu erhalten. AK 2013.1.3.0 war die erste REST API-fähige ZFS OS-Version, und nicht alle ZFS-Appliances können darauf aktualisiert werden.
„Konfigurationsfehler“ mit Fehlermeldung „REST Service ist deaktiviert“	Vergewissern Sie sich, dass DER REST-Dienst auf diesem Gerät aktiviert ist.

Problem:	Versuchen Sie dies:
„Konfigurationsfehler“ mit Fehlermeldung „Benutzer nicht autorisiert für Befehl“	Dieser Fehler ist wahrscheinlich darauf zurückzuführen, dass bestimmte Rollen (z. B. „Advanced_Analytics“) für den konfigurierten Benutzer nicht enthalten sind. Durch die Anwendung des Analysebereichs für den Benutzer mit schreibgeschützter Rolle kann der Fehler behoben werden. Führen Sie hierzu folgende Schritte aus: 1. Bewegen Sie auf dem ZFS-System im Bildschirm Konfiguration → Benutzer die Maus über die Rolle und doppelklicken Sie, um die Bearbeitung zu ermöglichen 2. Wählen Sie im Dropdown-Menü „Bereich“ die Option „Analyse“ aus. Eine Liste der möglichen Eigenschaften wird angezeigt. 3. Klicken Sie auf das Kontrollkästchen am oberen Ende, um alle drei Eigenschaften auszuwählen. 4. Klicken Sie auf der rechten Seite auf die Schaltfläche Hinzufügen. 5. Klicken Sie oben rechts im Popup-Fenster auf die Schaltfläche Übernehmen. Das Popup-Fenster wird geschlossen.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Datensammler Pure Storage FlashArray

Data Infrastructure Insights verwendet den Pure Storage FlashArray Datensammler zur Erfassung von Bestands- und Performance-Daten.

Terminologie

Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die gängigste Terminologie für die Ressource angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Laufwerk (SSD)	Festplatte
Array Erledigen	Storage
Controller	Storage-Node
Datenmenge	Datenmenge
LUN-Zuordnung	Volume-Zuordnung
Initiator, Ziel	Volume-Maske

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

- IP-Adresse des Storage-Systems
- Benutzername und Kennwort für das Administratorkonto des Pure Storage-Systems.
- Port-Anforderung: HTTP/HTTPS 80/443

Konfiguration

Feld	Beschreibung
FlashArray Host-IP-Adresse	IP-Adresse des Storage-Systems
Benutzername	Benutzername mit Administratorrechten
Passwort für das Administratorkonto	Passwort

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	Wählen Sie HTTP oder HTTPS. Zeigt auch den Standardport an.
TCP-Port überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport im Feld Verbindungstyp. Andernfalls geben Sie den zu verwendenden Anschluss ein
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten
Leistungsintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
„Ungültige Anmeldeinformationen“ mit Fehlermeldungen „Richtlinie lässt nicht zu“ oder „Sie sind nicht autorisiert“	Validierung des Pure Benutzerkontos und Passworts über die Pure http Schnittstelle

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Datensammler Red hat Virtualization

Data Infrastructure Insights verwendet den Datensammler Red hat Virtualization zur Erfassung von Bestandsdaten aus virtualisierten Linux- und Microsoft Windows-Workloads.

Terminologie

Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die gängigste Terminologie für die Ressource angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Festplatte	Virtuelles Laufwerk
Host	Host
Virtual Machine	Virtual Machine
Storage Domain	Datastore
Logische Einheit	LUN

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

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

Konfiguration

Feld	Beschreibung
IP-Adresse des RHEV-Servers	IP-Adresse des Storage-Systems
Benutzername	Benutzername mit Administratorrechten
Passwort für das Administratorkonto	Passwort

Erweiterte Konfiguration

Feld	Beschreibung
HTTPS-Kommunikationsschnittstelle	Port, der für die HTTPS-Kommunikation mit RHEV verwendet wird
Abfrageintervall für Bestand (min)	Die Standardeinstellung ist 20 Minuten.

Fehlerbehebung

Weitere Informationen zu diesem Data Collector finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Rubrik CDM Data Collector

Data Infrastructure Insights erfasst mithilfe des Rubrik Datensammlers Inventar- und Performance-Daten von Rubrik Storage Appliances.

Terminologie

Data Infrastructure Insights erfasst die folgenden Inventarinformationen aus dem Datensammler Rubrik. Für jeden Asset-Typ, der von Data Infrastructure Insights erworben wurde, wird die für diese Ressource am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Cluster	Storage, Storage-Pool
Knoten	Storage-Node
Festplatte	Festplatte

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. In dieser Datenquelle fallen möglicherweise nicht alle Fälle an.

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Die Data Infrastructure Insights Acquisition Unit initiiert Verbindungen zum TCP-Port 443 zum Cluster Rubrik. Ein Collector pro Cluster.
- IP-Adresse des Rubrik Clusters.
- Benutzername und Passwort für das Cluster.
- Rubrik Cluster IP-Adresse oder Hostname.
- Für die Basisauthentifizierung müssen ein Benutzername und ein Passwort für das Cluster eingegeben werden. Wenn Sie die Service Account-basierte Authentifizierung bevorzugen, benötigen Sie ein Dienstkonto, einen geheimen Schlüssel und eine Unternehmens-ID
- Port-Anforderung: HTTPS 443

Konfiguration

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

Erweiterte Konfiguration

Abfrageintervall für Bestand (min)	Der Standardwert ist 60
Leistungsintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Ich erhielt die Nachricht, dass mehr als ein Speicher erstellt wird.	Überprüfen Sie, ob das Cluster ordnungsgemäß konfiguriert ist und der Collector auf ein einzelnes Cluster verweist.
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 verweist, dass es sich um eine „ManagedId“ handelt.

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

VMware vSphere Data Collector konfigurieren

Der Datensammler für VMware vSphere erfasst Performance- und Konfigurationsinformationen für die VM-Gast- und ESXi Hosts und erfordert schreibgeschützte Privileges für alle Objekte in vSphere. Ab August 2024 werden bei vSphere Collector zusätzlich Protokollmeldungen aus vSphere-Umgebungen und einige VMware-spezifische Kennzahlen integriert. Beachten Sie bitte, dass Data Infrastructure Insights nur Informationen zu VMware-Protokollen aus Umgebungen mit vSphere 8.0.1 oder höher abrufen kann. Ebenso werden die anbieterspezifischen Metriken nur für vSphere 7+-Umgebungen unterstützt. Daher können Sie das Kontrollkästchen Protokolle und/oder anbieterspezifische Metriken für einen bestimmten Collector deaktivieren, wenn auf eine ältere vSphere-Instanz verwiesen wird.

Terminologie

Data Infrastructure Insights bezieht die folgenden Inventarinformationen aus dem VMware vSphere-Datensammler. Für jeden erworbenen Asset-Typ wird die am häufigsten für das Asset verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Einblicke Aus Der Dateninfrastruktur
Virtuelle Festplatte	Festplatte
Host	Host
Virtual Machine	Virtual Machine
Datastore	Datastore
LUN	Datenmenge
Fibre-Channel-Port	Port

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

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Informationen erforderlich:

- IP-Adresse des Virtual Center-Servers
- Schreibgeschützter Benutzername und Kennwort in Virtual Center
- Für alle Objekte im Virtual Center benötigen wir schreibgeschützte Berechtigungen.
- SDK-Zugriff auf dem Virtual Center-Server – in der Regel bereits eingerichtet.
- Port-Anforderungen: http-80 HTTPS-443
- Zugriff validieren:
  - Melden Sie sich mit dem oben genannten Benutzernamen und Kennwort beim Virtual Center Client an
  - Überprüfen Sie, ob das SDK aktiviert ist: telnet <vc_ip> 443

Einrichtung und Verbindung

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

Konfiguration

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

Erweiterte Konfiguration

Aktivieren Sie im Bildschirm Erweiterte Konfiguration die Option **VM Performance**, um Leistungsdaten zu sammeln. Bestandserfassung ist standardmäßig aktiviert. Die folgenden Felder können konfiguriert werden:

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 20
Filtern von VMs	Wählen Sie EINEN CLUSTER-, DATACENTER- oder ESX-HOST aus
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Filterliste erstellen (CLUSTER, DATACENTER und/oder ESX_HOST)
Anzahl der Wiederholungen	Der Standardwert ist 3
Kommunikations-Port	Der Standardwert ist 443

Geräteliste Filtern…	Diese Liste muss aus exakten String-Übereinstimmungen bestehen. Wenn Sie nach ESX_HOST filtern möchten, müssen Sie eine kommagetrennte Liste mit den genauen „Namen“ Ihrer ESX-Hosts erstellen, wie in Data Infrastructure Insights und vSphere gemeldet. Bei diesen „Namen“ handelt es sich entweder um IP-Adressen, einfache Hostnamen oder vollqualifizierte Domain-Namen (FQDNs) – dies wird durch den Namen dieser Hosts bestimmt, als sie ursprünglich zu vSphere hinzugefügt wurden. Verwenden Sie bei der Filterung nach CLUSTER die von CI auf Hypervisoren gemeldeten Cluster-Namen im Stil von Data Infrastructure Insights – Data Infrastructure Insights setzt den vSphere-Cluster-Namen mit dem vSphere-Datacenter-Namen und einem Schrägstrich voraus – „DC1/clusterA“ ist der Cluster-Name Data Infrastructure Insights würde über einen Hypervisor in ClusterA im Rechenzentrum DC1 berichten.
Leistungsintervall (Sek.)	Der Standardwert ist 300

Zuordnen von VMware Tags zu Annotationen zu Data Infrastructure Insights

Der VMware Datensammler ermöglicht das Befüllen von Data Infrastructure Insights Annotationen mit Tags, die auf VMware konfiguriert sind. Der DII-Anmerkungsname muss identisch mit dem VMware **category** -Namen sein; das Tag wird dann als Anmerkungswert einer DII-Anmerkung mit dem gleichen Namen wie die Kategorie angewendet. Data Infrastructure Insights füllt immer Anmerkungen vom gleichen Namen aus und versucht, Anmerkungen anderer Typen (Zahl, Boolescher Wert usw.) zu füllen. Wenn Ihre Anmerkung einen anderen Typ hat und der Datensammler sie nicht füllt, kann es erforderlich sein, die Anmerkung zu entfernen und sie als Texttyp neu zu erstellen.

Achten Sie darauf, dass bei VMware Tags die Groß-/Kleinschreibung beachtet wird, während bei Data Infrastructure Insights die Tags nicht beachtet werden müssen. Wenn Sie in Data Infrastructure Insights eine Annotation mit dem Namen „BESITZER“ und Tags mit den Namen „EIGENTÜMER“, „Eigentümer“ und „Eigentümer“ in VMware erstellen, würden alle diese Variationen von „Eigentümer“ auch der Annotation von Cloud Insight zugeordnet.

Beachten Sie Folgendes:

- Data Infrastructure Insights veröffentlicht derzeit nur automatisch Supportinformationen für NetApp-Geräte.
- Da diese Support-Informationen in Anmerkungsform gespeichert sind, können Sie sie abfragen oder in Dashboards verwenden.
- Wenn ein Benutzer den Anmerkungswert überschreibt oder leert, wird der Wert erneut automatisch gefräst, wenn Data Infrastructure Insights die Anmerkungen aktualisiert, die er einmal täglich tut.

Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

Inventar

Problem:	Versuchen Sie dies:
Fehler: Liste einschließen, um VMs zu filtern, darf nicht leer sein	Wenn Liste einschließen ausgewählt ist, geben Sie gültige DataCenter-, Cluster- oder Hostnamen an, um VMs zu filtern
Fehler: Es konnte keine Verbindung zu VirtualCenter bei IP hergestellt werden	Mögliche Lösungen: * Überprüfen Sie die eingegebenen Anmeldeinformationen und die eingegebene IP-Adresse. * Versuchen Sie, mit Virtual Center über den VMware Infrastructure Client zu kommunizieren. * Versuchen Sie, mit Virtual Center über Managed Object Browser (z. B. MOB) zu kommunizieren.
Fehler: VirtualCenter at IP verfügt über kein von JVM einkonformes Zertifikat	Mögliche Lösungen: * Empfohlen: Zertifikat für Virtual Center durch Verwendung von Stronger (z.B. neu generieren 1024-Bit) RSA-Schlüssel * Nicht empfohlen: Ändern Sie die JVM java.security-Konfiguration, um die Einschränkung jdk.certpath.diabledAlgorithms zu nutzen, um einen 512-Bit-RSA-Schlüssel zu ermöglichen. Siehe "JDK 7 Update 40 Versionshinweise".
Ich sehe die Meldung: „VMware Logs-Paket wird nicht auf VMware unterstützt, unter Version 8.0.1“	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 auf der "Support" Seite oder im "Data Collector Supportmatrix".

Data Collector Reference - Dienste

Erfassung Von Node-Daten

Data Infrastructure Insights sammelt Kennzahlen aus dem Knoten, auf dem Sie einen Agenten installieren.

Installation

1. Wählen Sie unter **Observability > Collectors** ein Betriebssystem/eine Plattform aus. Beachten Sie, dass durch die Installation eines Datensammlers für die Integration (Kubernetes, Docker, Apache usw.) auch die Erfassung von Node-Daten konfiguriert wird.
2. Befolgen Sie die Anweisungen, um den Agenten zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

Objekte und Zähler

Die folgenden Objekte und ihre Zähler werden als Node-Kennzahlen erfasst:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Knoten Dateisystem	Node-UUID-Gerätetyp	Node-IP Node-Name Node OS-Modus	Freie Inodes Free Inodes Total Inodes Used Total Used Total Used Total Used
Node-Festplatte	Node-UUID-Festplatte	Node-IP Node-Name Node OS	I/O-Zeit insgesamt IOPS in Bearbeitung Lesen von Bytes (pro s) Lesezeit insgesamt Lesevorgänge (pro s) gewichtete I/O-Zeit insgesamt Schreibbyte (pro s) Schreibzeit Gesamtzahl Schreibvorgänge (pro s) Aktuelle Festplattenwarteschlange Länge Schreibzeit I/O-Zeit
Node-CPU	Node-UUID-CPU	Node-IP Node-Name Node OS	System CPU Usage User CPU Usage Idle CPU Usage Prozessor CPU Usage Interrupt CPU Usage DPC CPU Usage

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Knoten	Node-UUID	Node-IP Node-Name Node OS	Kernel Boot Time Kernel Context Switches (per sec) Kernel Entropy Available Kernel Interrupts (per sec) Kernel processes Forked (per sec) Arbeitsspeicher Aktiver Speicher Verfügbar Gesamter Verfügbarer Speicher Gepufferter Speicher Im Cache Speicherlimit Speicher Speicher Bereitgestellt Als Speicher Schmutziger Speicher Freier Speicher Hoher Freier Speicher Hoher Gesamtspeicher Riesige Seitengröße Speicher Riesige Seiten Freier Speicher Riesige Seiten Gesamt Speicher Niedriger Freier Speicher Niedriger Speicher Gemappter Speicher Seitentabellen Speicher Gemeinsam Genutzter Speicher Slab Speicher Austausch Gecachten Speicher Austausch Freier Speicher Austausch Gesamt Speicher Verwendeter Gesamt-Speicher Verwendeter Speicher Vmalloc Chunk Speicher Vmalloc Gesamt-Speicher Vmalloc Verwendeter Speicher Wired Memory Writeback Total Memory Writeback Tmp Speicher Cache Fehler Speicheranforderung Null Fehler Speicherseiten Fehler Speicherseiten Fehler Speicherseiten-Speicher-Seiten-Speicher Nicht Gepageter Speicher Paged Memory Cache Core Memory Standby Cache Normaler Speicher Standby Cache Reserve Memory Transition Fehler Prozesse Blockierte Prozesse Dead Processes

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Node-Netzwerk	UUID der Netzwerkschnittstelle-Node	Node Name Node-IP-Node-OS	Bytes Empfangene Bytes Gesendete Pakete Ausgehende Pakete Ausgehende Pakete Ausgehende Pakete Ausgehende Pakete Paketfehler Empfangen Pakete Empfangene Fehler Pakete Empfangene Pakete Empfangene Pakete Empfangen Pakete

Einrichtung

Informationen zur Einrichtung und Fehlerbehebung finden Sie auf der "Konfigurieren eines Agenten" Seite.

ActiveMQ Data Collector

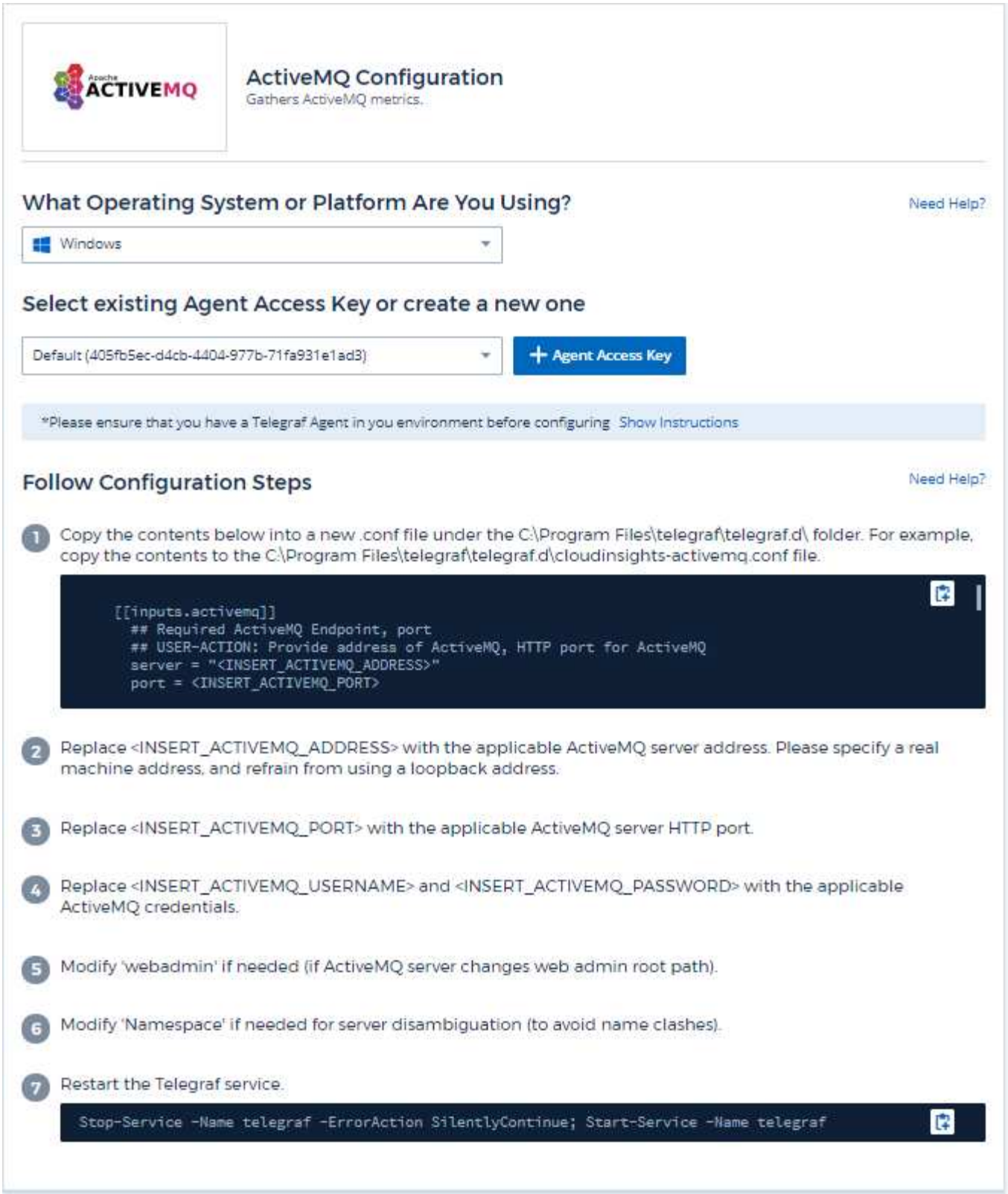
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen aus ActiveMQ zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie ActiveMQ.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie im "ActiveMQ-Dokumentation"

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
ActiveMQ-Warteschlange	Namespace Queue Port Server	Node Name Node-IP-Node-UUID	Anzahl Der Warteschlange Anzahl Der Kunden Anzahl Der Ausgleiche Anzahl Warteschlange Größe
ActiveMQ-Abonnenten	Namespace für Client-ID-Verbindungs-ID-Port-Server	Ist Active Destination Node Name Node IP Node UUID Node OS Selector Subscription	Anzahl Der Entsandten Absendete Warteschlange Anzahl Der Abgesandten Warteschlange Größe Anzahl Der Warteschlange Anzahl Der Ausstehenden Warteschlange Größe
ActiveMQ-Thema	Thema Port Server Namespace	Node Name Node-IP-Node-UUID-Node-OS	Anzahl Der Ausgleichen Anzahl Der Verbraucher Größe Der Anzahl Der Warteschlangen

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

Apache Data Collector

Dieser Datensammler ermöglicht die Erfassung von Daten von Apache-Servern auf Ihrem Mandanten.

Voraussetzungen

- Sie müssen Ihren Apache HTTP Server einrichten und ordnungsgemäß ausführen lassen
- Sie müssen über sudo- oder Administratorberechtigungen auf Ihrem Agent-Host/VM verfügen
- In der Regel ist das Apache *mod_Status*-Modul so konfiguriert, dass eine Seite am Speicherort '/Server-Status?Auto' des Apache-Servers angezeigt wird. Die Option *ExtendedStatus* muss aktiviert sein, um alle verfügbaren Felder zu erfassen. Informationen zur Konfiguration Ihres Servers finden Sie in der Dokumentation zum Apache-Modul: https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

Installation

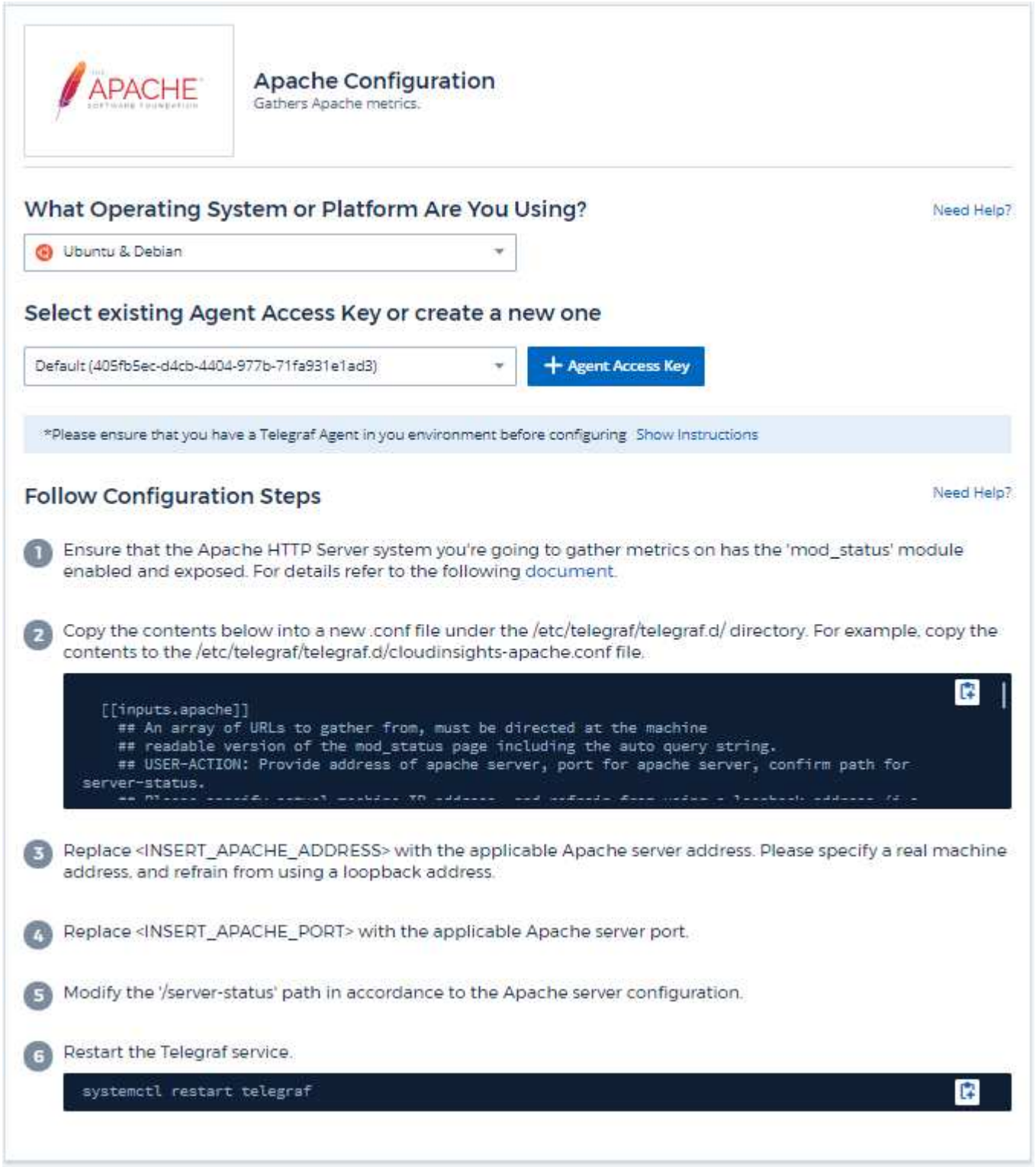
1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Apache.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-

Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.

4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Das Telegraf-Plugin für Apache's HTTP Server setzt auf das 'mod_Status'-Modul, um aktiviert zu werden. Wenn diese Option aktiviert ist, wird Apache HTTP Server einen HTML-Endpunkt anzeigen, der in Ihrem Browser angezeigt oder für die Extraktion des Status aller Apache HTTP Server-Konfigurationen gepatzt werden kann.

Kompatibilität:

Die Konfiguration wurde gegen Apache HTTP Server Version 2.4.38 entwickelt.

Aktivieren von mod_Status:

Das Aktivieren und Bereitstellen der 'mod_Status'-Module umfasst zwei Schritte:

- Modul wird aktivieren
- Legen Sie Statistiken aus dem Modul fest

Modul aktivieren:

Das Laden von Modulen wird durch die Konfigurationsdatei unter '/usr/local/apache/conf/httpd.conf' gesteuert. Bearbeiten Sie die config-Datei und heben Sie die folgenden Zeilen aus:

```
LoadModule status_module modules/mod_status.so
Include conf/extra/httpd-info.conf
```

Statistiken aus dem Modul offenlegen:

Die Offenlegung von 'mod_Status' wird durch die Konfigurationsdatei unter '/usr/local/apache2/conf/extra/httpd-info.conf' gesteuert. Stellen Sie sicher, dass Sie in dieser Konfigurationsdatei Folgendes haben (mindestens sind weitere Richtlinien vorhanden):

```
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
<Location /server-status>
    SetHandler server-status
</Location>

#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information
(ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
ExtendedStatus On
```

Ausführliche Anweisungen zum Modul 'mod_Status' finden Sie im "Apache-Dokumentation"

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Apache	Namespace-Server	Node-IP-Knotenname-Port-Parent Server-Konfiguration der übergeordnete Server-Generation der MPM-Generation wird angehalten	Beschäftigte Arbeiter Bytes pro Anfrage Bytes pro Sekunde CPU Kinder System CPU Kinder Benutzer CPU Last CPU System CPU System CPU Benutzer asynchrone Verbindungen Schließen Asynchronous Connections am Leben Asynchronous Connections Writing connections Total Duration per Request Idle Workers Load Average (Last 1m) Load Average (Last 15m) Load Average (Last Average (Last 5m) Prozesse Anfragen pro Sekunde Gesamtzugriff Gesamtdauer Gesamtdauer KBytes Scoreboard schließen Scoreboard DNS Lookups Scoreboard abschließen Scoreboard-Idle Cleanup Scoreboard halten am Leben Scoreboard Logging Scoreboard öffnen Scoreboard lesen Scoreboard senden Scoreboard Starting Scoreboard warten

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

Consul Data Collector

Data Infrastructure Insights verwendet diesen Datensammler, um Metriken von Consul zu erfassen.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Konsul.

   Wenn Sie keinen Agenten für die Sammlung konfiguriert haben, werden Sie auf Ihrem Mandanten zu

aufgefordert"Installieren Sie einen Agenten".

Wenn Sie bereits einen Agenten konfiguriert haben, wählen Sie das entsprechende Betriebssystem oder die entsprechende Plattform aus, und klicken Sie auf **Weiter**.

2. Befolgen Sie die Anweisungen auf dem Bildschirm Consul Configuration, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

Einrichtung

Informationen finden Sie im "Dokumentation für Konsul".

Objekte und Zähler für Konsul

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Konsul	Namespace-ID-Service-Node prüfen	Node-IP Node OS Node UUID Node Name Service Name Check Name Service Service ID Status	Warnung Bei Kritischem Durchgang

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

Couchbase Data Collector

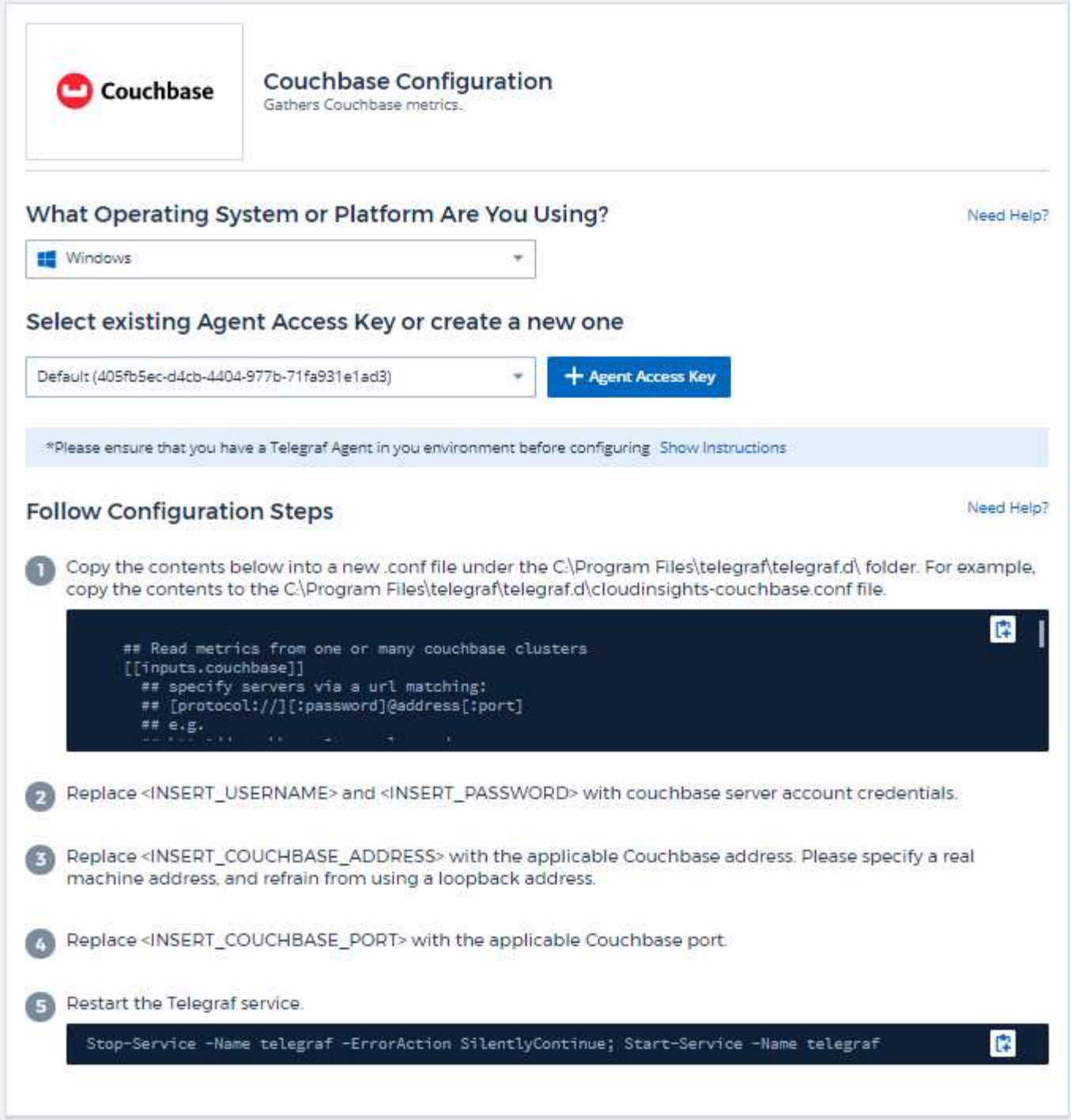
Data Infrastructure Insights nutzt diesen Datensammler zur Erfassung von Kennzahlen aus Couchbase.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Couchbase.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie im "Couchbase Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Couchbase Node	Namespace Cluster Couchbase Node-Hostname	Node Name Node-IP	Speicher Insgesamt
Couchbase Bucket	Namespace-Bucket-Cluster	Node Name Node-IP	Daten Verwendete Daten Abrufen Verwendete Elemente Anzahl Verwendete Elemente Speicher Verwendete Operationen Pro Sekunde Kontingent Verwendet

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

CouchDB Data Collector

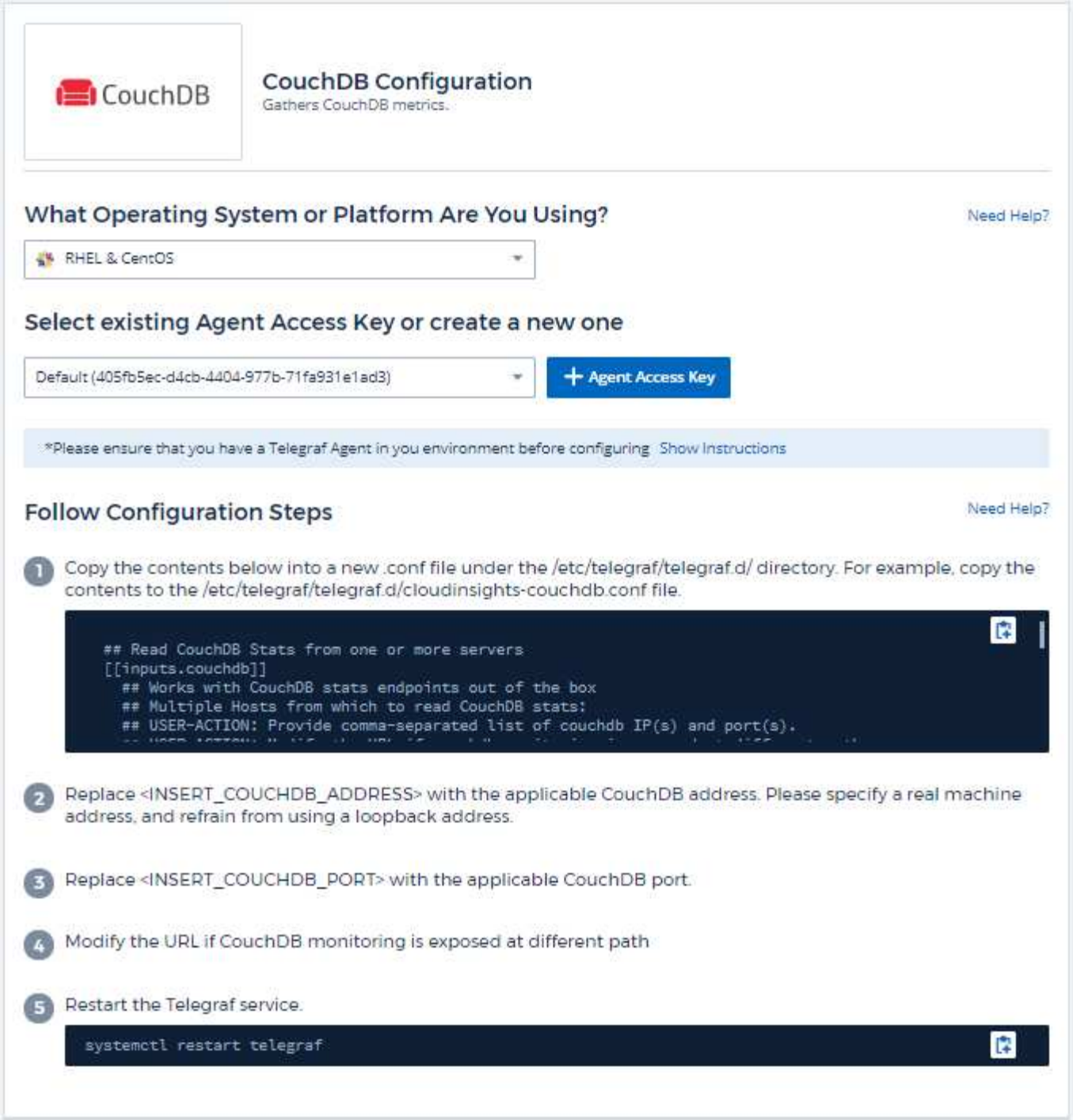
Data Infrastructure Insights nutzt diesen Datensammler, um Metriken von CouchDB zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie CouchDB.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie im "CouchDB-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
CouchDB	Namespace-Server	Node Name Node-IP	Authentifizierung Cache Treffer Authentifizierung Cache Fräulein Datenbank liest Datenbank schreibt Datenbanken Open OS Files Max Anfragenzeit Min Anfragestzeit httpd Request Methoden httpd Request Methoden httpd Request löschen httpd Request Methods Get httpd Request Methods Head httpd Request Methods Post httpd Request Methods Put Status Codes 200 Status Codes 201 Statuscodes 202 Statuscodes 301 Statuscodes 304 Statuscodes 400 Statuscodes 401 Statuscodes 403 Statuscodes 404 Statuscodes 405 Statuscodes 409 Statuscodes 412 Statuscodes 500

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

Docker Data Collector

Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen aus Docker zu sammeln.

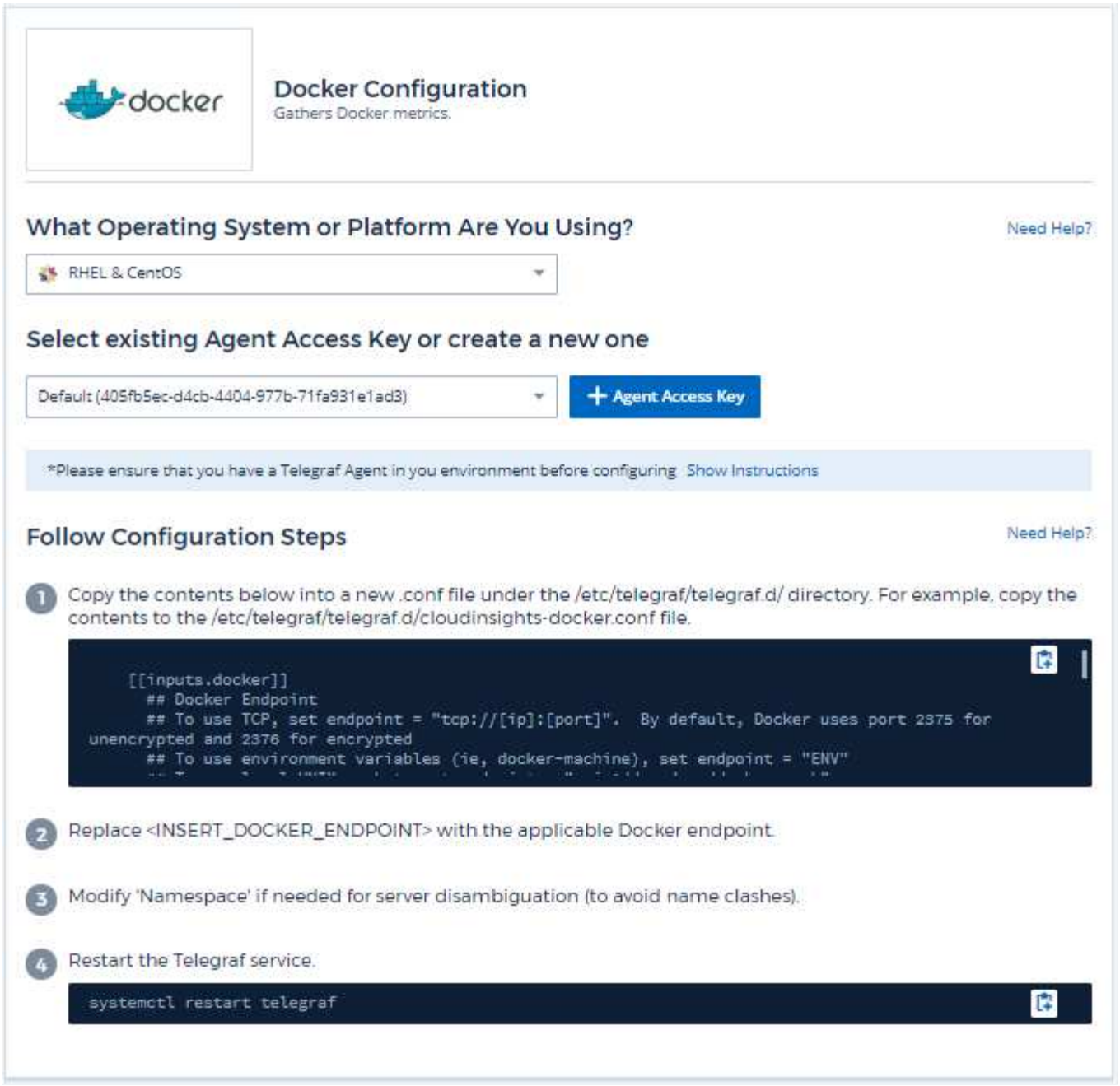
Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Für Docker:

   Wenn Sie keinen Agenten für die Sammlung konfiguriert haben, werden Sie auf Ihrem Mandanten zu aufgefordert"Installieren Sie einen Agenten".

   Wenn Sie bereits einen Agenten konfiguriert haben, wählen Sie das entsprechende Betriebssystem oder die entsprechende Plattform aus, und klicken Sie auf **Weiter**.

2. Befolgen Sie die Anweisungen im Bildschirm Docker-Konfiguration, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Das Telegraf-Input-Plug-in für Docker erfasst Kennzahlen über einen bestimmten UNIX-Socket oder einen TCP-Endpunkt.

Kompatibilität

Die Konfiguration wurde mit Docker Version 1.12.6 entwickelt.

Einrichtung

Zugriff auf Docker über einen UNIX-Socket

Wenn der Telegraf-Agent auf bareMetal läuft, fügen Sie den telegraf Unix-Benutzer zur Docker Unix-Gruppe hinzu, indem Sie Folgendes ausführen:

```
 sudo usermod -aG docker telegraf
Wenn der Telegraf-Agent in einem Kubernetes Pod ausgeführt wird, legen Sie
den Docker Unix-Socket offen, indem Sie den Socket als Volume in den POD
einbilden und das Volume dann in /var/run/docker.sock mounten. Fügen Sie
zum Beispiel der PodSpec Folgendes hinzu:
```

```
volumes:
...
- name: docker-sock
hostPath:
path: /var/run/docker.sock
type: File
```

Fügen Sie dann dem Container Folgendes hinzu:

```
volumeMounts:
...
- name: docker-sock
mountPath: /var/run/docker.sock
```

Beachten Sie, dass das Installationsprogramm von Data Infrastructure Insights für die Kubernetes-Plattform diese Zuordnung automatisch übernimmt.

Zugriff auf Docker über einen TCP-Endpunkt

Docker verwendet standardmäßig Port 2375 für unverschlüsselte Zugriffe und Port 2376 für verschlüsselten Zugriff.

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Engine	Docker Engine Für Namespace	Node Name Node-IP-Node-UUID Node OS Kubernetes Cluster Docker-Versionseinheit	Speichercontainer Container verwendete Container ausgeführt Container gestoppt CPUs Gehroutinen Bilder Listener Ereignisse verwendete Datei Deskriptoren Daten verfügbar Daten insgesamt verwendete Metadaten Verfügbare Metadaten insgesamt verwendete Pool Blocksize

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Container	Namespace Container-Name Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Kubernetes-Container Restart Anzahl Kubernetes-Container-Ende Meldungspfad Kubernetes Container-Beendigung Meldungsrichtlinie Kubernetes Pod Kulanzzeit Container-Image Container-Status Container-Version Node-Name Kubernetes Container-Log-Pfad Kubernetes Container-Name Kubernetes Docker-Typ Kubernetes Pod Name Kubernetes Namespace Kubernetes Pod UID Kubernetes Sandbox ID Node IP Node UUID Docker Version Kubernetes IO Config Kubernetes IO-Konfiguration gesehen Kubernetes IO-Konfiguration Quelle OpenShift IO SCC Kubernetes Beschreibung Kubernetes Anzeigename OpenShift Tags Kompose Service Pod Vorlage Hash Controller Revision Hash Pod Vorlage Erstellung Lizenz Schema Build Date Schema Lizenz Schema Name Schema URL Schema VCS URL Schema Vendor Schema Version Schema Schema Schema Version Maintainer Customer Pod Kubernetes StatefulSet Pod Name Tenant WebConsole Architektur autoritäre Quelle URL Build Datum RH Build Host RH Component Distribution Scope Installation Release Run Zusammenfassung Uninstall Ref Type Vendor Version Health Status	Speicher Aktiv Anonymer Speicher Aktiv Speicher Cache Hierarchischer Grenzwert Speicher Inaktiver Anonymer Speicher Inaktiver Speicher Speicherlimit Arbeitsspeicher Gemappter Speicher Max Nutzung Speicherseitenfehler Speicherseite Hauptfehler Speicher Im Speicher Ausgepeitet Speicher Resident Set Größe Speicher Resident Set Größe Riesige Speicher Gesamt Aktiv Anonymer Speicher Gesamt Active File Memory Gesamt Cache Speicher Inaktiver Anonymer Speicher Gesamt Inaktiver Speicher Gesamt Mapped File Memory Total Page Fault Memory Total Page Major Fehler Memory Total Paged In Memory Total Paged Out Memory Total Resident Set Größe Speicher Gesamt Resident Set Größe Riesige Speicher Gesamt Nicht entfernen Speicher nicht entfernen Speichernutzung Speichernutzung Prozent Exit Code OOM tötete PID bei fehlender Streak gestartet

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Container Block IO	Namespace Container Name Device Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Kubernetes-Container Restart Anzahl Kubernetes-Container-Ende Meldungspfad Kubernetes Container-Beendigung Meldungsrichtlinie Kubernetes Pod Kulanzzeit Container-Image Container-Status Container-Version Node-Name Kubernetes Container-Log-Pfad Kubernetes Container-Name Kubernetes Docker-Typ Kubernetes Pod Name Kubernetes Namespace Kubernetes Pod UID Kubernetes Sandbox ID Node IP Node UUID Docker Version Kubernetes Config Kubernetes Config gesehen Kubernetes Config Quelle OpenShift SCC Kubernetes Beschreibung Kubernetes Anzeigename OpenShift Tags Schema Schema Version Pod Template Hash Controller Revision Hash Pod Template Generation Kompose Service Schema Build Date Schema Lizenz Schema Name Schema Vendor Customer Pod Kubernetes StatprofSet Pod Name Tenant WebConsole Build Date License Vendor Architecture authorited Source URL RH Build Host RH Component Distribution Scope Install Maintainer Release Run Summary Uninstall VCS Ref VCS Typ Version Schema URL Schema VCS Schema Version Container ID	IO Service Bytes rekursiv Async IO Service Bytes rekursiv IO lesen Service Bytes rekursiv Sync IO Service Bytes rekursiv IO Service Bytes rekursiv Schreib IO Serviced rekursive Async E/A Serviced rekursive Read IO Serviced rekursive Sync IO Serviced rekursive Total IO Serviced rekursive Write

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Container Network	Namespace Container Name Network Docker Engine	Container Image Container Status Container Version Node Name Node IP Node UUID Node OS K8s Cluster Docker Version Container ID	RX-reduzierte RX-Bytes RX-Fehler RX-Pakete TX reduzierte TX-Bytes TX-Fehler TX-Pakete

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Docker Container-CPU	Namespace Container Name CPU Docker Engine	Kubernetes-Container-Hash Kubernetes-Container-Ports Kubernetes-Container Restart Anzahl Kubernetes-Container-Ende Meldungspfad Kubernetes Container-Beendigung Meldungsrichtlinie Kubernetes Pod Kulanzzeit Kubernetes-Konfiguration Kubernetes-Konfiguration Kubernetes-KonfigurationSCC-Container-Image Container-Status Container-Version Node-Name Kubernetes Container-Log-Pfad Kubernetes-Container-Name Kubernetes Docker Typ Kubernetes Pod Name Kubernetes Pod Namespace Kubernetes Pod UID Kubernetes Sandbox ID Node IP Node UUID Node OS Kubernetes Cluster Docker Version Kubernetes Beschreibung Kubernetes Anzeigename OpenShift Tags Schema Version Pod Template Hash Controller Revision Hash Pod Template Generation Kompose Service Schema Build Date Schema License Schema Name Schema Hersteller-Pod Kubernetes StatprofSet Pod Name Tenant WebConsole Build Date License Vendor Architecture authorited Source URL RH Build Host RH Component Distribution Scope Install Maintainer Release Run Summary Uninstall VCS Ref VCS Typ Version Schema URL Schema VCS Schema VCS URL Schema Version Container ID	Drosselungszeiträume Drosselung Gedrosselte Perioden Drosselung Gedrosselte Zeitnutzung Im Kernel-Modus Nutzung Im Benutzermodus Auslastung Prozent Nutzung Des Systems Gesamt

Fehlerbehebung

Problem:	Versuchen Sie dies:
Ich sehe meine Docker-Kennzahlen in Data Infrastructure Insights nicht, nachdem ich die Anweisungen auf der Konfigurationsseite befolgt habe.	Prüfen Sie die Telegraf-Agentenprotokolle, um zu sehen, ob es folgenden Fehler meldet: E! Fehler im Plugin [inputs.docker]: Berechtigung verweigert beim Versuch, eine Verbindung zum Docker Daemon-Socket herzustellen.Falls dies der Fall ist, ergreifen Sie die erforderlichen Schritte, um den Telegraf-Agent-Zugriff auf den Docker Unix-Sockel wie oben angegeben zu ermöglichen.

Weitere Informationen finden Sie auf der "Support" Seite.

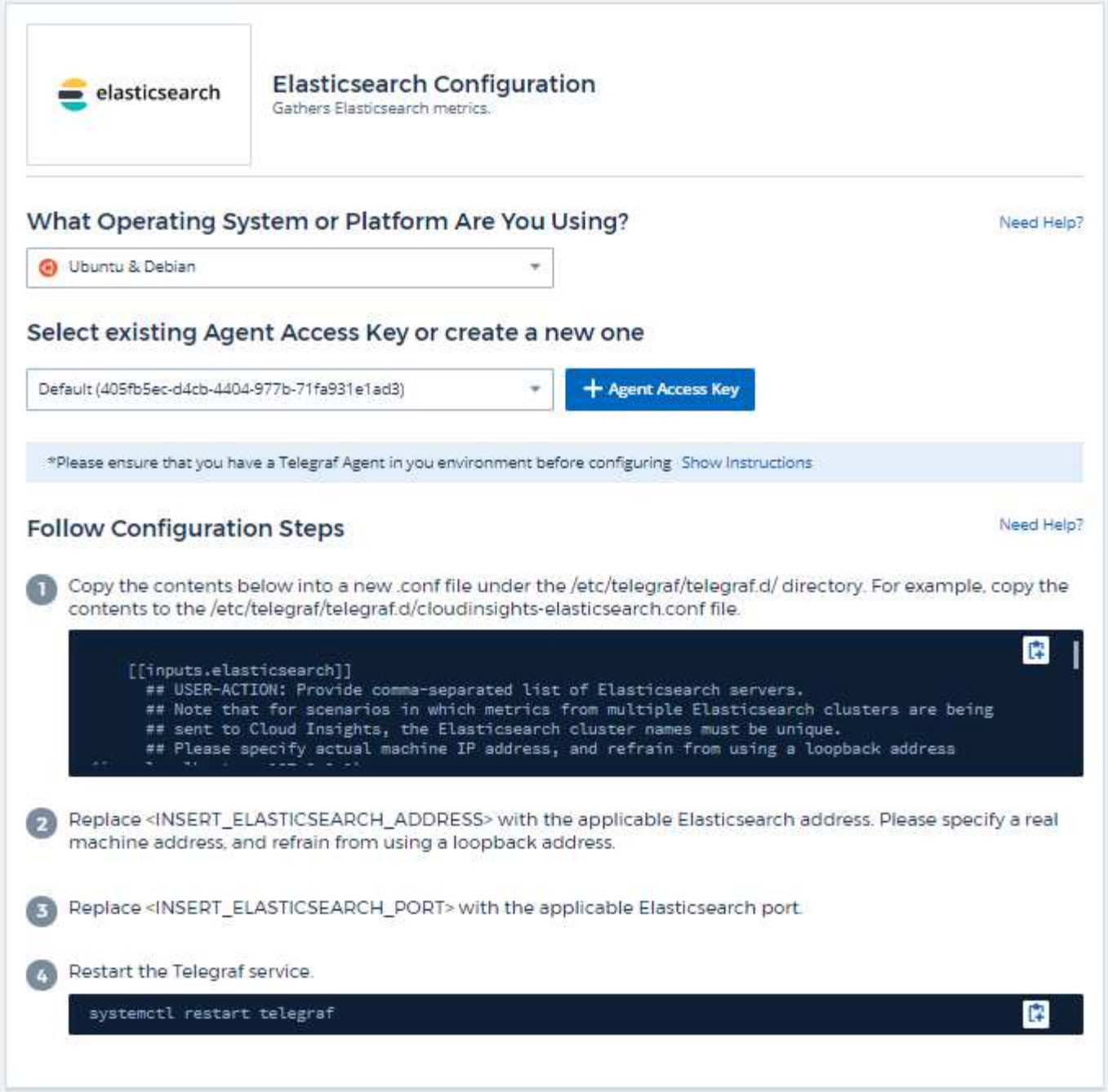
Elasticsearch Data Collector

Data Infrastructure Insights verwendet diesen Datensammler zum Erfassen von Kennzahlen aus Elasticsearch.

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Elasticsearch.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie im "Elasticsearch-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:
Elasticsearch-Cluster	Namespace-Cluster	Node-IP Node-Name Cluster-Status
Elasticsearch-Node	Namespace Cluster es Node ID es Node IP es Node	Zone-ID

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

Flik Data Collector

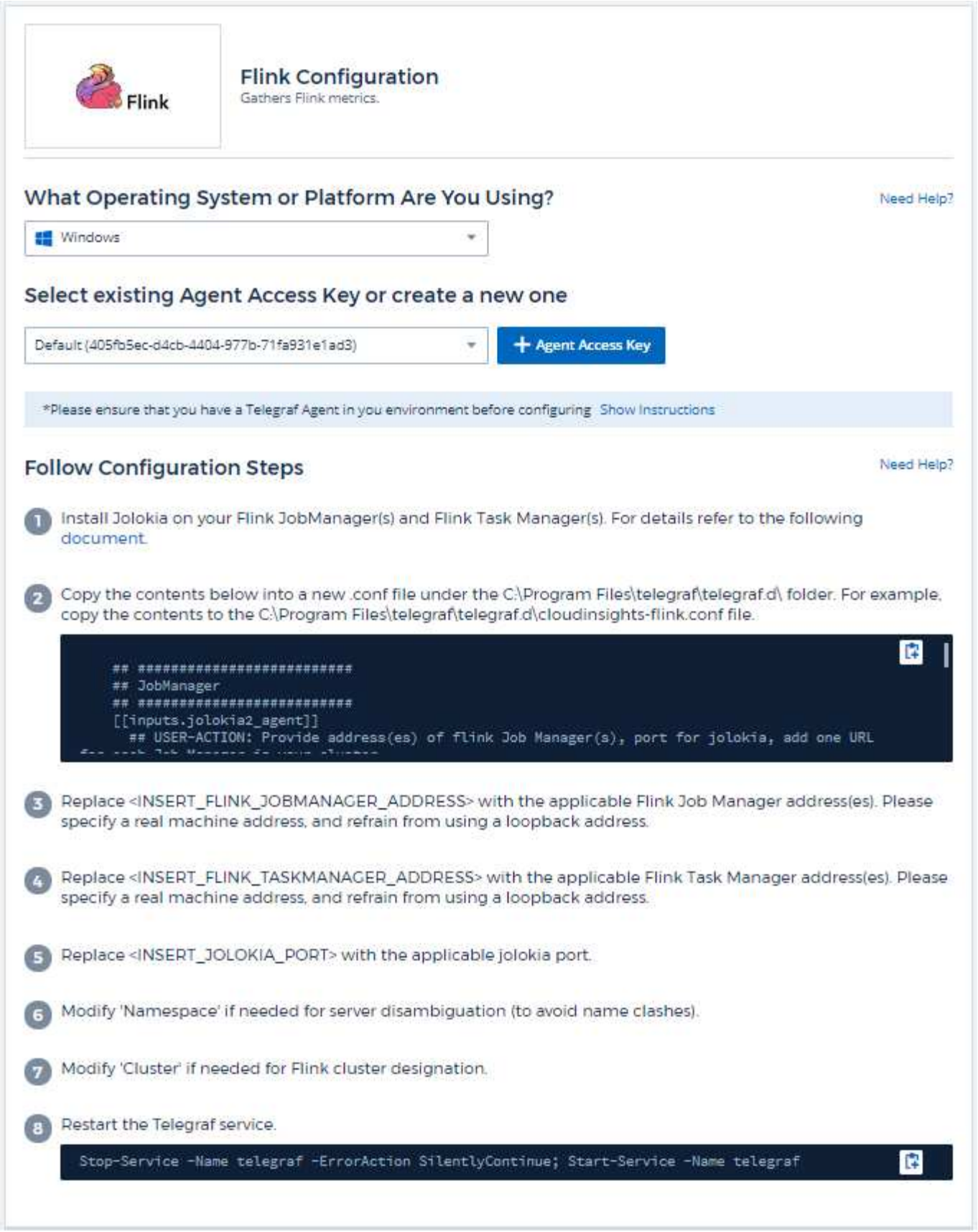
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen von Flink zu erfassen.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie „Flink“.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Eine vollständige Flink-Implementierung umfasst die folgenden Komponenten:

JobManager: Das Primärsystem Flik. Koordiniert eine Reihe von TaskManagers. In einer Konfiguration mit hoher Verfügbarkeit verfügt das System über mehr als einen JobManager. Taskmanager: Hier werden Flik-Operatoren ausgeführt. Das Flink Plugin basiert auf dem telegraf Jolokia Plugin. Als Voraussetzung für die Erfassung von Informationen aus allen Flik-Komponenten muss JMX auf allen Komponenten konfiguriert und über Jolokia freigelegt werden.

Kompatibilität

Die Konfiguration wurde gegen die Version 1.7 von Flink entwickelt.

Einrichtung

Jolokia Agent Jar

Für alle einzelnen Komponenten muss eine Version der Jolokia Agent JAR-Datei heruntergeladen werden. Die Version wurde getestet gegen war "Jolokia Agent 1.6.0".

Anweisungen unten gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-Agent.jar) unter dem Speicherort '/opt/flink/lib/' platziert wird.

JobManager

Um JobManager so zu konfigurieren, dass die Jolokia API freigegeben wird, können Sie die folgende Umgebungsvariable auf Ihren Knoten einrichten und dann den JobManager neu starten:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Sie können einen anderen Port für Jolokia (8778) wählen. Wenn Sie eine
interne IP haben, um Jolokia zu sperren, können Sie die „Catch all“
0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP über
das telegraf-Plugin zugänglich sein muss.
```

Taskmanager

So konfigurieren Sie TaskManager(s), um die Jolokia-API zu öffnen, können Sie die folgende Umgebungsvariable auf Ihren Knoten einrichten und dann den TaskManager neu starten:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Sie können einen anderen Port für Jolokia (8778) wählen. Wenn Sie eine
interne IP haben, um Jolokia zu sperren, können Sie die „Catch all“
0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP über
das telegraf-Plugin zugänglich sein muss.
```

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik Task Manager	Cluster Namespace-Server	Node Name Task-Manager-ID-Knoten-IP	Netzwerk verfügbar Speichersegmente Netzwerk Speichersegmente Speichersegmente Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scavenge Time Heap Memory Comstived Heap Memory Init Heap Memory Max Heap Memory Used Thread Count Daemon Thread Count Thread Count Spitzenanzahl Thread Count Thread Count Insgesamt Gestartet
Druckauftrag Einflken	Job-ID des Cluster-Namespace-Servers	Node Name Job Name Node-IP Letzte Checkpoint External Path-Neustartzeit	Ausfall Vollneustarts Last Checkpoint Alignment Buffered Last Checkpoint Duration Last Checkpoint Size Anzahl der abgeschlossenen Checkpoints Anzahl der fehlgeschlagenen Checkpoints Anzahl der laufenden Checkpoints Anzahl der Kontrollpunkte Betriebszeit

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik Job Manager	Cluster Namespace-Server	Node Name Node-IP	Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scravenge Time Heap Memory Comstived Heap Memory Init Heap Memory Max Heap Memory Used Number Registrierte Task-Manager Anzahl laufende Jobs Taskleisten verfügbare Task-Steckplätze Gesamt-Thread-Anzahl Daemon-Thread-Anzahl Maximale Anzahl Der Threads Anzahl Der Threads Insgesamt Begonnen

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik-Aufgabe	Cluster Namespace Job-ID Task-ID	Server Node Name Job Name Sub Task-Index Task-Versuch-ID Task-Versuch Nummer Task-Name Task-Manager-ID Knoten-IP Aktuelle Eingabe-Wasserzeichen	Puffer in Pool Nutzung Buffers in Warteschlange Länge Buffer Out Pool Nutzung Buffer Out Queue Länge Anzahl Puffer in Lokale Anzahl Buffers in Local per Second Anzahl Puffer in Local per second Rate Anzahl Puffer in Remote Number Buffers in Remote per second Anzahl Puffer in Remote per second Anzahl der Puffer in Remote per Anzahl Der Auspuffer Anzahl Der Auspuffer Pro Sekunde Anzahl Auspuffer Pro Sekunde Anzahl Bytes Pro Sekunde Anzahl Bytes In Lokale Anzahl Bytes Pro Sekunde Anzahl Bytes In Lokal Pro Sekunde Anzahl Bytes In Lokal Pro Sekunde Anzahl Bytes In Remote Number Bytes In Remote Per Second Anzahl Bytes In Remote Pro Sekunde Rate Anzahl Bytes Out Anzahl Bytes Out Pro Sekunde Anzahl Bytes Out Pro Sekunde Anzahl Datensätze In Number Datensätze In Per Second Anzahl Datensätze Pro Sekunde Anzahl Datensätze Pro Sekunde Anzahl Datensätze Pro Sekunde Anzahl Datensätze Aus Anzahl Datensätze Pro Sekunde Anzahl Datensätze Aus Pro Sekunde

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik Task Operator	Cluster Namespace Job-ID Operator-ID Task-ID	Server Node Name Job Name Operator Name Sub Task-Index Task-Versuch-ID Task-Versuch-Nummer Task-Name Task-Manager-ID-Knoten-IP	Aktuelle Eingabe Watermark Current Output Watermark Number Records In Number Records In Per Second Count Anzahl Datensätze In Pro Sekunde Anzahl Datensätze Pro Sekunde Anzahl Datensätze Aus Anzahl Datensätze Pro Sekunde Anzahl Anzahl Datensätze Aus Pro Sekunde Anzahl Verspätete Datensätze Verworfen Zugewiesene Partitionen Bytes Verbrauchte Rate Commit Latenz Durchschn. Commit-Latenz Max. Commit Rate Commits faciert fehlgeschlagene Verbindungen Close Rate Verbindungsanzahl Verbindungserzeugung Rate Anzahl Abholen Latenz durchschn. Abholen Max. Abholen Rate Abholen Größe Max. Abholen Drosselzeit durchschn. Abrufdauer Max. Heartbeat Rate Incoming Byte Rate I/O-Zeit durchschn. (Ns) I/O Wartezeit I/O Wartezeit durchschn. (Ns) Verbindungsrate Verbindungszeit durchschn. Letzter Heartbeat ago Netzwerk-I/O-Rate ausgehende Byte-Datensätze verbrauchte Rate Datensätze lag max. Datensätze pro Anforderung durchschn. Anfragemgröße Durchschnittl. Anfragengröße max. Ansprechrate Wählen Rate Synchronisierungszeit durchschn. Heartbeat Antwort Zeit Max. Verbindungszeit Max. Synchronisierungszeit

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

Hadoop Data Collector

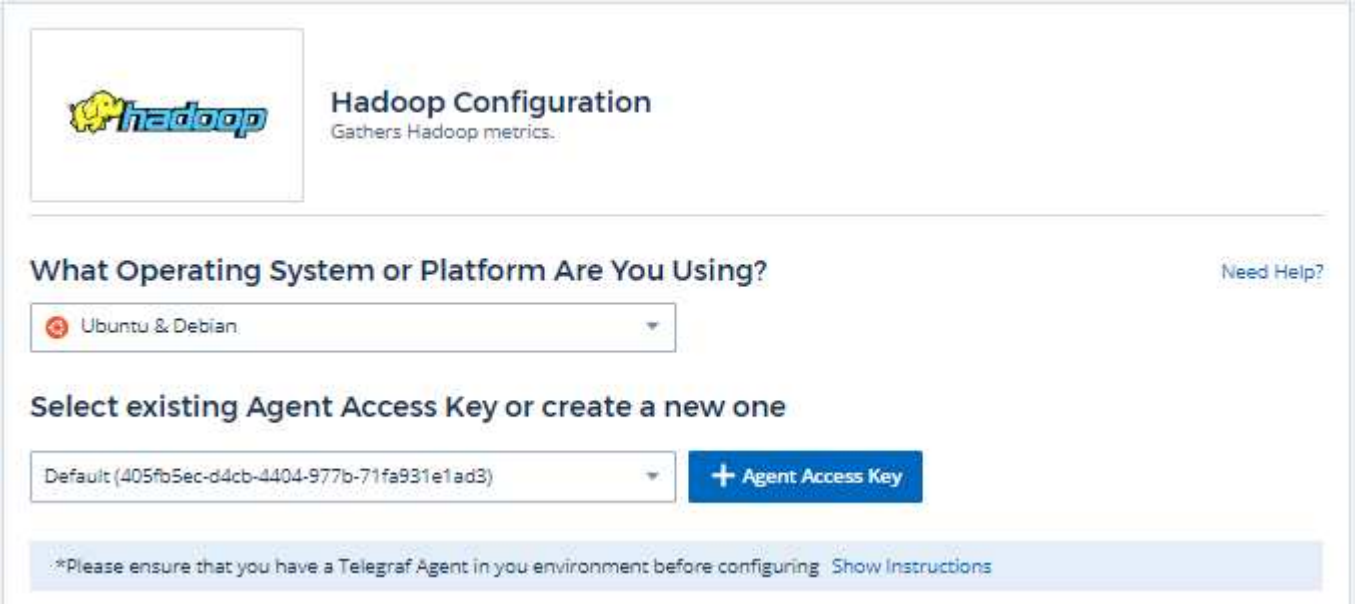
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen aus Hadoop zu sammeln.

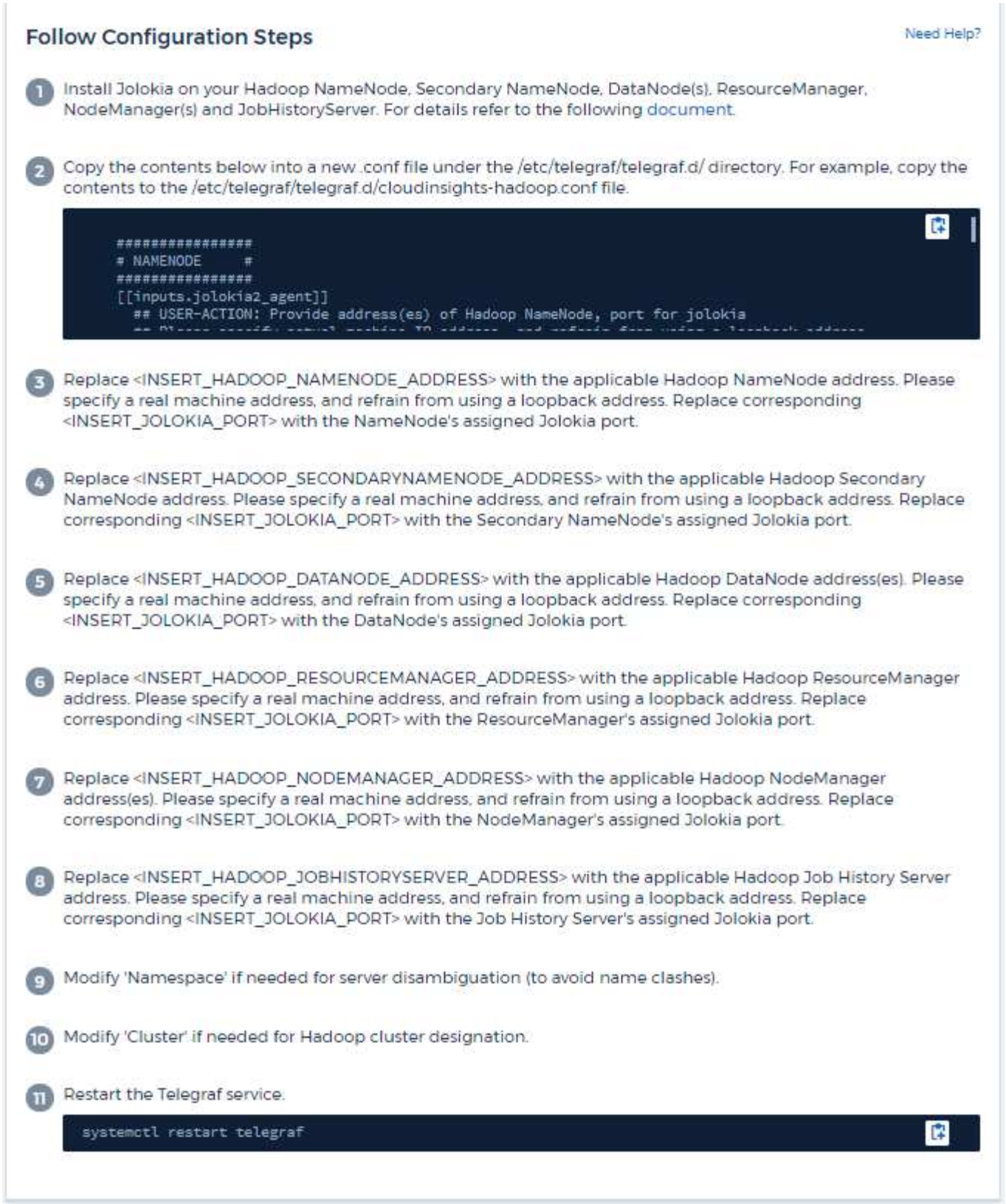
Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Für Hadoop.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.





Einrichtung

Eine vollständige Hadoop Implementierung umfasst die folgenden Komponenten:

- NameNode: Das primäre System Hadoop Distributed File System (HDFS) Koordiniert eine Reihe von DataNodes.

- Sekundärer NameNode: Ein warmer Failover für den NameNode. In Hadoop erfolgt die Heraufstufung auf NameNode nicht automatisch. Secondary NameNode sammelt Informationen von NameNode, damit sie bei Bedarf heraufgestuft werden können.
- DataNode: Tatsächlicher Eigentümer von Daten.
- ResourceManager: Das primäre Computersystem (Yarn). Koordiniert eine Reihe von NodeManagers.
- NodeManager: Die Ressource für Computing. Aktueller Speicherort für das Ausführen von Anwendungen.
- JobHistorieServer: Verantwortlich für die Bearbeitung aller Anfragen im Zusammenhang mit der Jobhistorie.

Das Hadoop Plugin basiert auf dem telegraf Jolokia Plugin. Um Informationen aus allen Hadoop Komponenten zu sammeln, muss JMX auf allen Komponenten konfiguriert und zugänglich gemacht werden.

Kompatibilität

Die Konfiguration wurde mit Hadoop Version 2.9 entwickelt.

Einrichtung

Jolokia Agent Jar

Für alle einzelnen Komponenten muss eine Version der Jolokia Agent JAR-Datei heruntergeladen werden. Die Version wurde getestet gegen war "Jolokia Agent 1.6.0".

Die nachfolgende Anleitung setzt voraus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-Agent.jar) unter der Adresse '/opt/hadoop/lib/' abgelegt wird.

NameNode

Um NameNode zu konfigurieren, um die Jolokia API freizugeben, können Sie unter <HADOOP_HOME>/etc/hadoop/hadoop-env.sh Folgendes einrichten:

```
export HADOOP_NAMENODE_OPTS="$HADOOP_NAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7800,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8000
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8000 above) and Jolokia (7800).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Sekundärer NameNode

Um den sekundären NameNode zu konfigurieren, um die Jolokia API freizugeben, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export HADOOP_SECONDARYNAMENODE_OPTS="$HADOOP_SECONDARYNAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7802,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8002
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8002 above) and Jolokia (7802).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

DataNode

Um die DataNodes so zu konfigurieren, dass sie die Jolokia API aussetzen, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export HADOOP_DATANODE_OPTS="$HADOOP_DATANODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7801,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8001
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8001 above) and Jolokia (7801).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

ResourceManager

Um den ResourceManager so zu konfigurieren, dass die Jolokia API zur Verfügung gestellt wird, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export YARN_RESOURCEMANAGER_OPTS="$YARN_RESOURCEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7803,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8003
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8003 above) and Jolokia (7803).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

NodeManager

Um die NodeManagers so zu konfigurieren, dass sie die Jolokia API aussetzen, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export YARN_NODEMANAGER_OPTS="$YARN_NODEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7804,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8004
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8004 above) and Jolokia (7804).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

JobGeschichteServer

Um den JobHistorieServer so zu konfigurieren, dass die Jolokia API zur Verfügung gestellt wird, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export HADOOP_JOB_HISTORYSERVER_OPTS="$HADOOP_JOB_HISTORYSERVER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7805,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8005
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8005 above) and Jolokia (7805).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:
Sekundärer Hadoop NameNode	Cluster Namespace-Server	Node Name Node IP Compile Info Version
Hadoop NodeManager	Cluster Namespace-Server	Node Name Node-IP
Hadoop ResourceManager	Cluster Namespace-Server	Node Name Node-IP
Hadoop DataNode	Cluster Namespace-Server	Node Name Node-IP Cluster-ID-Version
Hadoop NameNode	Cluster Namespace-Server	Node Name Node IP Transaktions-ID Letzte geschriebene Zeit seit Letzte geladen Edits HA State File System Status Block Pool ID Cluster ID Compile Info unterschiedliche Version Anzahl Version
Hadoop JobGeschichteServer	Cluster Namespace-Server	Node Name Node-IP

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

HAProxy Data Collector

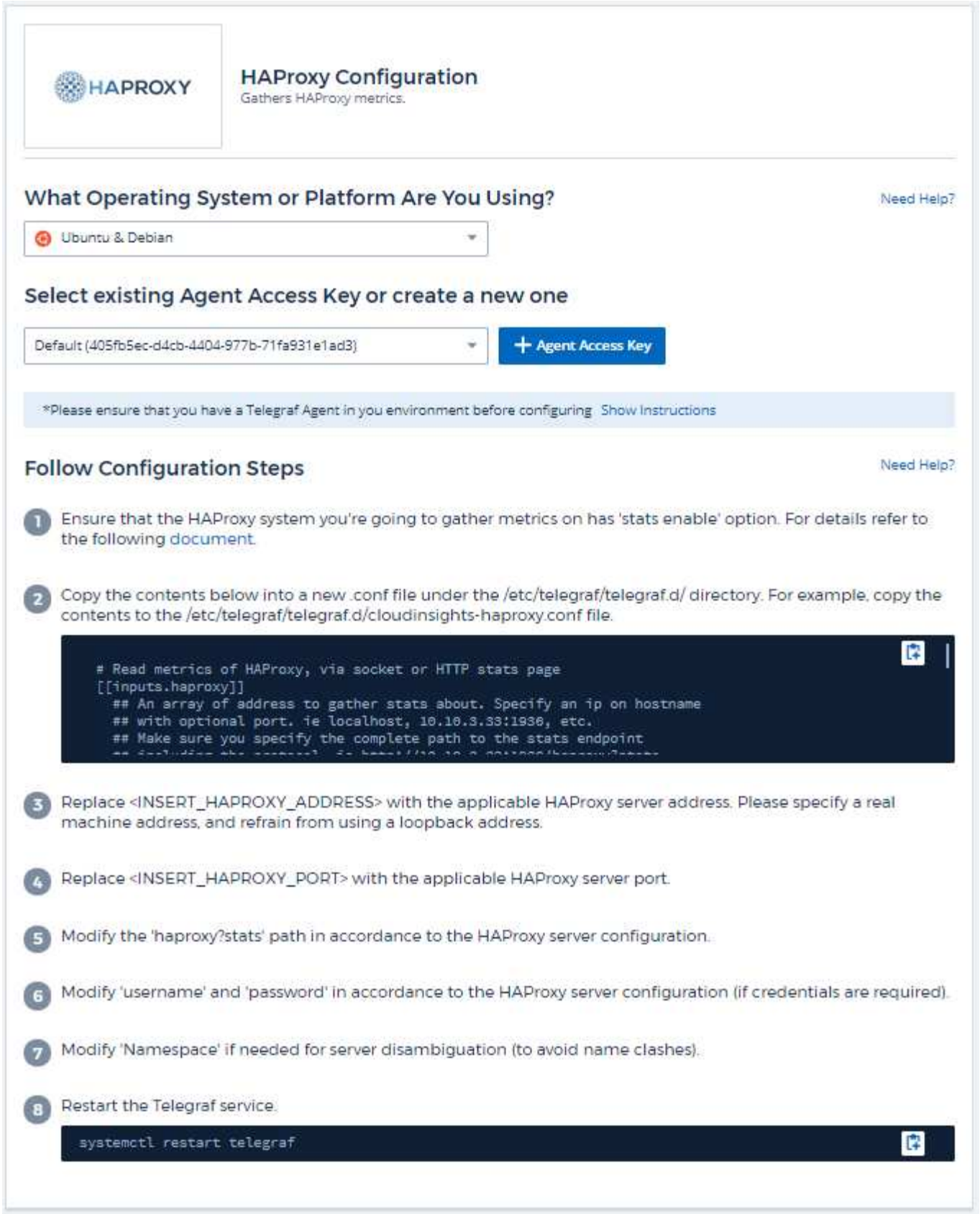
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen von HAProxy zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie HAProxy.

Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Telegraf's Plugin für HAProxy setzt auf HAProxy Stats Aktivierung. Diese Konfiguration ist in HAProxy integriert, ist jedoch nicht sofort aktiviert. Wenn HAProxy aktiviert ist, wird ein HTML-Endpunkt angezeigt, der

in Ihrem Browser angezeigt werden kann oder für die Extraktion des Status aller HAProxy-Konfigurationen abgekratzt werden kann.

Kompatibilität:

Die Konfiguration wurde gegen HAProxy-Version 1.9.4 entwickelt.

Einrichtung:

Um Statistiken zu aktivieren, bearbeiten Sie Ihre haproxy-Konfigurationsdatei und fügen Sie nach dem Abschnitt 'Standards' die folgenden Zeilen hinzu: Verwenden Sie Ihren eigenen Benutzer/Ihr Passwort und/oder die haproxy-URL:

```
stats enable
stats auth myuser:mypassword
stats uri  /haproxy?stats
```

Im Folgenden finden Sie eine vereinfachte Beispiel-Konfigurationsdatei mit aktivierten Statistiken:

```
global
  daemon
  maxconn 256

defaults
  mode http
  stats enable
  stats uri /haproxy?stats
  stats auth myuser:mypassword
  timeout connect 5000ms
  timeout client 50000ms
  timeout server 50000ms

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

backend servers
  server server1 10.128.0.55:8080 check ssl verify none
  server server2 10.128.0.56:8080 check ssl verify none

backend servers_2
  server server3 10.128.0.57:8080 check ssl verify none
  server server4 10.128.0.58:8080 check ssl verify none
```

Vollständige und aktuelle Anweisungen finden Sie im "HAProxy-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
HAProxy Frontend	Namespace-Adressenproproxy	Node-IP-Knotenname Proxy-ID-Modus Prozess-id Sitzungen Ratenlimit Server-id Sitzungen Limit Status	Bytes in Bytes Out Cache Hits Cache Lookups Komprimierung Bytes umgangen Komprimierung Bytes in Komprimierung Bytes Out Komprimierung Reaktionen Verbindungsrate Verbindungsrate Max Verbindungen insgesamt Anträge, die von der Verbindung abgelehnt werden Rule Requests verweigert durch Sicherheitsbedenken Antworten verweigert durch Sicherheitsbedenken Anfragen abgelehnt durch Session Rule Requests erfragt Fehler Antworten 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten andere Anfragen Abfangen Sitzungen Rate Sitzungen Max Anfragen Rate Max Anfragen Rate Max Anforderungen Total Sessions Sitzungen Max Sitzungen Antworten Neuschreibung Total Requests

Objekt:	Kennungen:	Attribute:	Datenpunkte:
HAProxy-Server	Namespace-Adresse-Proxy-Server	Node-IP-Knotenname Check Time to Finish Check Fall Configuration Check Health Value Check RISE Configuration Check Status Proxy ID Last Change Time Last Session Time Mode Process id Server Status Weight	Aktive Server Backup Server Bytes in Bytes Out Downs Check Downs Check Fails Client abgebrochen Verbindungen Verbindung Verbindung Durchschnittliche Zeit Ausfallzeit Gesamt Denied Responses Verbindungsfehler Antwort 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten anderer Server ausgewählt Total Queue Current Queue Max. Durchschnittliche Zeit Sitzungen pro Zweite Sitzungen pro Sekunde Max. Wiederverwendbarkeit der Verbindung Reaktionszeit Durchschnittliche Sitzungen Sitzungen Max Server Transfer bricht Sitzungen gesamte Sitzungen Gesamtzeit Durchschnittliche Anforderungen Redispatches Anfragen Wiederholungen Anfragen Neuschreibung Anfragen

Objekt:	Kennungen:	Attribute:	Datenpunkte:
HAProxy-Back-End	Namespace-Adressenproproxy	Node-IP-Node-Name Proxy-ID Letzte Änderung Zeit Letzte Sitzung Zeitmodus Prozess-id Server-id Sitzungen Limit Status Gewicht	Aktive Server Backup Server Bytes in Bytes Out Cache Aufrufe Cache Lookups überprüfen Downs Client abbricht Komprimierung Bytes umgangen Komprimierung Bytes in Komprimierung Bytes out Komprimierungsantworten Verbindung Durchschnittliche Zeit Ausfallzeit Total Requests verweigert durch Sicherheitsbedenken Antworten verweigert durch Sicherheit Bedenken Verbindungsfehler Antworten Reaktion 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten anderer Server ausgewählt Total Queue Current Queue Max. Warteschlange Durchschnittliche Zeit Sitzungen pro Sekunde Sitzungen pro Sekunde Max. Anfragen Gesamt Verbindungswiederverwendung Reaktionszeit Durchschnittliche Sitzungen Sitzungen Max. Serverübertragung Abtreibungen Sitzungen Gesamtzeit Durchschnittliche Anfragen Neuzuweisen Wiederholungsanfragen Wiederholungsanfragen Wiederholungsanfragen Wiederholungsanfragen Anträge Neu Schreiben

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

JVM Data Collector

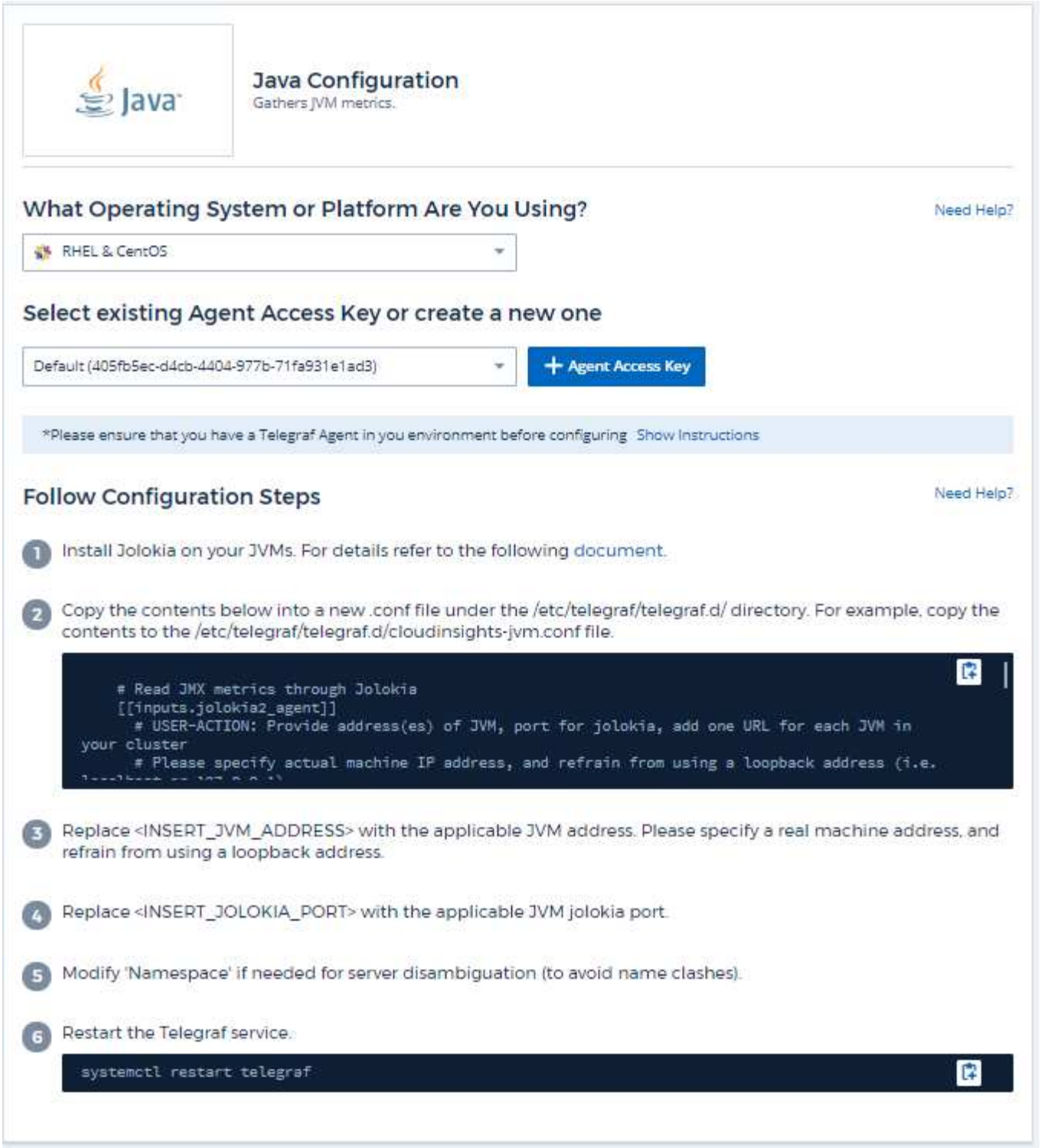
Data Infrastructure Insights verwendet diesen Datensammler zur Erfassung von Kennzahlen aus JVM.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie JVM.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie unter "JVM-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
JVM	Namespace-JVM	OS Architektur OS Name OS Version Laufzeit Spezifikation Laufzeit Spezifikation Hersteller Laufzeit Spezifikation Version Uptime Laufzeit VM Name Laufzeit VM Anbieter Laufzeit VM Version Node Name Node IP	Class Loaded Class Loaded Class Memory Unloaded Memory Heap Init Memory Heap used Max Memory Heap Used Memory Non Heap Innit Memory Non Heap Max Memory nicht Heap Used Memory Objects Ausstehende Fertigstellung von Betriebssystemprozessoren verfügbar Betriebssystem engagierte virtuelle Speichergröße OS Kostenlos Physikalische Speichergröße OS Freier Swap Speicherplatz Größe OS Max Datei Descriptor Anzahl OS Open File Descriptors Anzahl Betriebssystem Prozessor CPU Load OS CPU Time OS System CPU Load OS System Load Average OS Gesamt Physical Memory Size OS Gesamt Swap Space Size Thread Daemon Anzahl der Threads Spitzenanzahl Thread Count Thread Total Started Count Garbage Collector Copy Collection Count Garbage Collector Copy Collection Time Garbage Collector Sammlung von Mark-Sweep Sammlungszeit Zeitabfälle Collector G1 Sammlung der Alten Generation Speicherbage Collector G1 Zeitabbage der Jungen Generation Sammlungszähler Garbage Collector G1 Young Generation Collection Time Garbage Collector Zeitabfälle Sammlung der aktuellen Mark-Sweep Sammlung Zeitgarage Collector Parallel Collection Count Garbage Collector Parallel

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

Kafka Data Collector

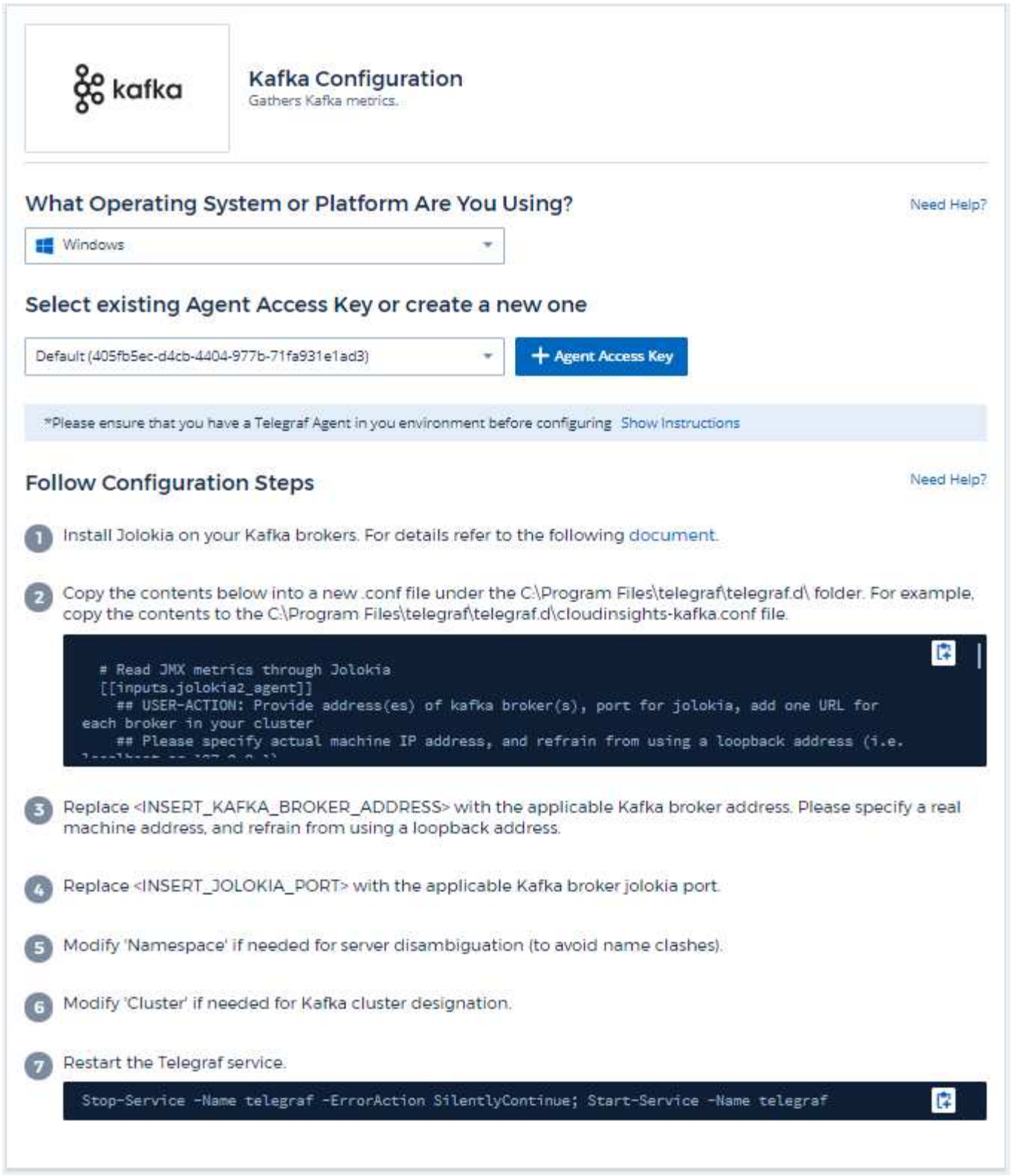
Data Infrastructure Insights nutzt diesen Datensammler, um Kennzahlen aus Kafka zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Kafka.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Das Kafka Plugin basiert auf dem telegraf's Jolokia Plugin. Um Informationen aus allen Kafka-Brokern zu sammeln, muss JMX über Jolokia auf allen Komponenten konfiguriert und zugänglich gemacht werden.

Kompatibilität

Konfiguration wurde gegen Kafka Version 0.11.0 entwickelt.

Einrichtung

Alle Anweisungen unten Nehmen wir an, dass Ihr Installationsort für kafka '/opt/kafka' ist. Sie können die nachfolgenden Anweisungen an Ihren Installationsort anpassen.

Jolokia Agent Jar

Eine Version die Jolokia Agent jar-Datei muss sein"Heruntergeladen". Die gegen die Version getestete war Jolokia Agent 1.6.0.

Anweisungen unten gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-Agent.jar) unter dem Speicherort '/opt/kafka/libs/' abgelegt wird.

Kafka Brokers

Um Kafka Brokers so zu konfigurieren, dass sie die Jolokia API aussetzen, können Sie in <KAFKA_HOME>/bin/kafka-Server-Start.sh kurz vor dem Anruf „kafka-run-class.sh“ Folgendes hinzufügen:

```
export JMX_PORT=9999
export RMI_HOSTNAME=`hostname -I`
export KAFKA_JMX_OPTS="-javaagent:/opt/kafka/libs/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0
-Dcom.sun.management.jmxremote.password.file=/opt/kafka/config/jmxremote.p
assword -Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=$RMI_HOSTNAME
-Dcom.sun.management.jmxremote.rmi.port=$JMX_PORT"
```

Beachten Sie, dass das obige Beispiel 'Hostname -i' verwendet, um die Umgebungsvariable 'RMI_HOSTNAME' einzurichten. In mehreren IP-Maschinen muss dies optimiert werden, um die IP, die Sie für RMI-Verbindungen interessieren, zu erfassen.

Sie können einen anderen Port für JMX (9999 oben) und Jolokia (8778) wählen. Wenn Sie eine interne IP haben, um Jolokia zu sperren, können Sie die „Catch all“ 0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP über das telegraf-Plugin zugänglich sein muss. Sie können die Option '-Dcom.sun.management.jmxremote.authenticate=false' verwenden, wenn Sie nicht authentifizieren möchten. Nutzung auf eigenes Risiko.

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:
Kafka Broker	Cluster Namespace Broker	Node Name Node-IP

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

Kibana Data Collector

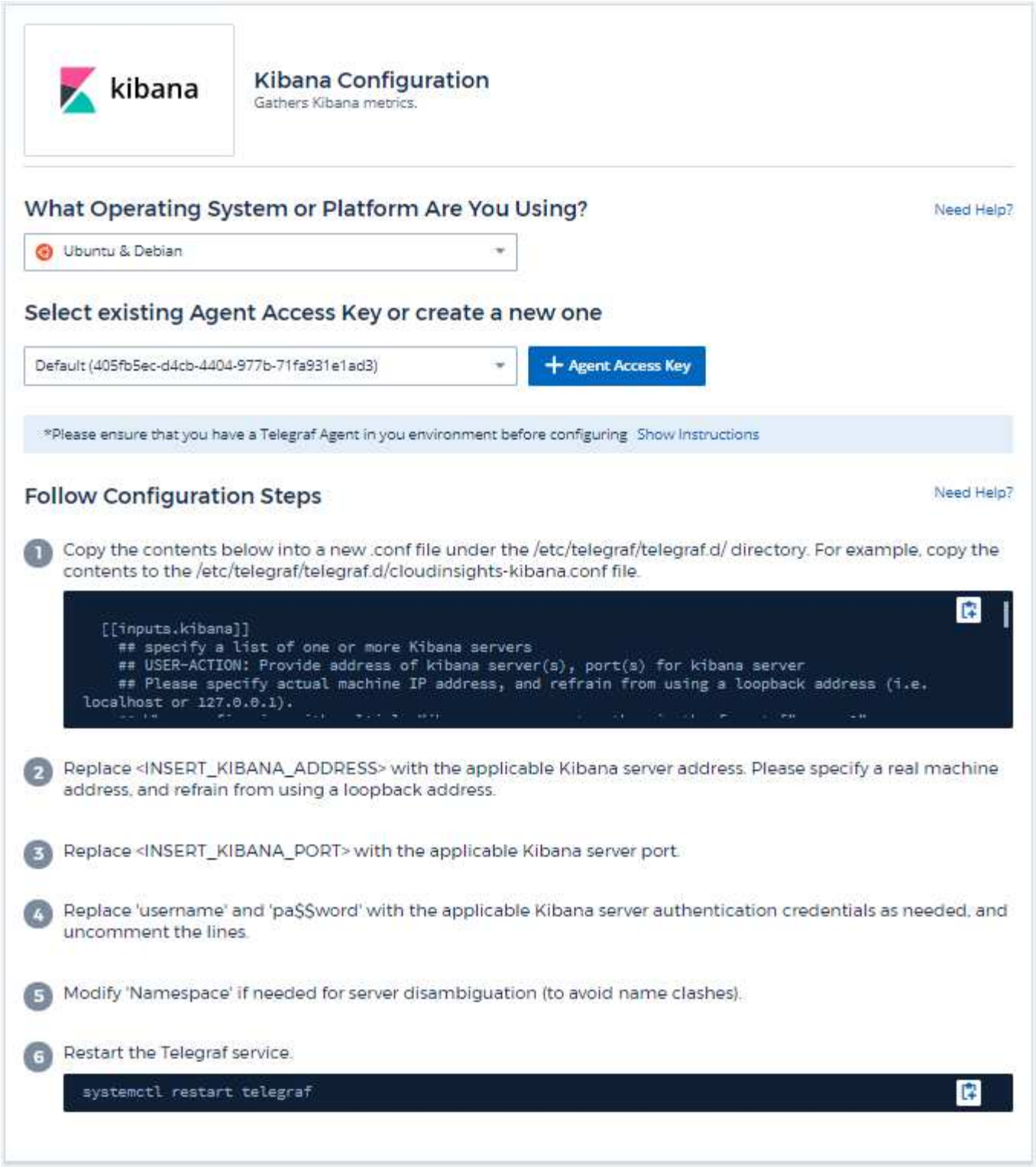
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen von Kibana zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Kibana.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie im "Kibana Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Kibana	Namespace-Adresse	Versionsstatus des Node-IP-Node-Namens	Gleichzeitige Verbindungen Heap Max Heap verwendete Anforderungen pro Sekunde Antwortzeit Max. Betriebszeit

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

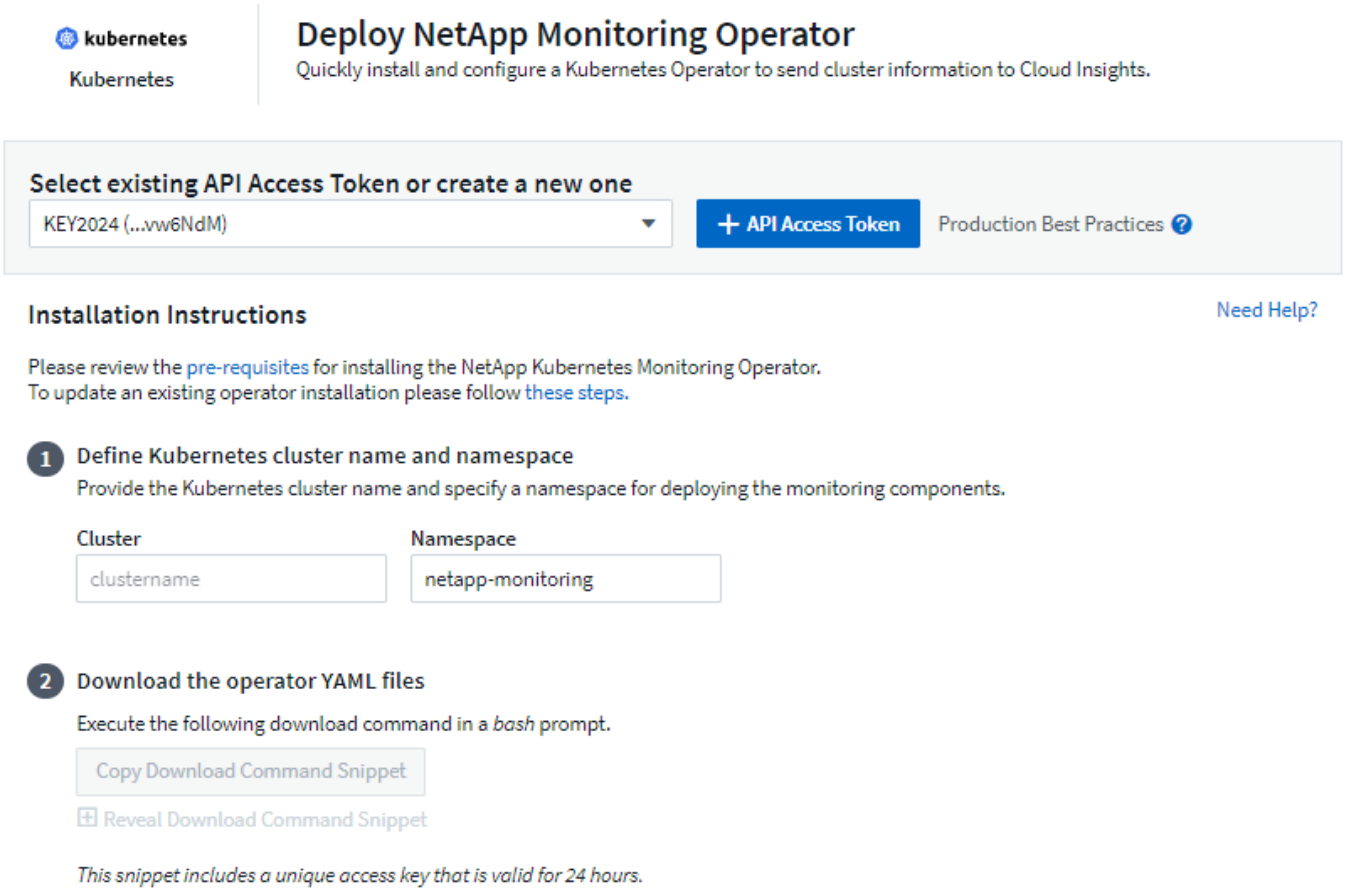
Installation und Konfiguration des Kubernetes Monitoring Operator

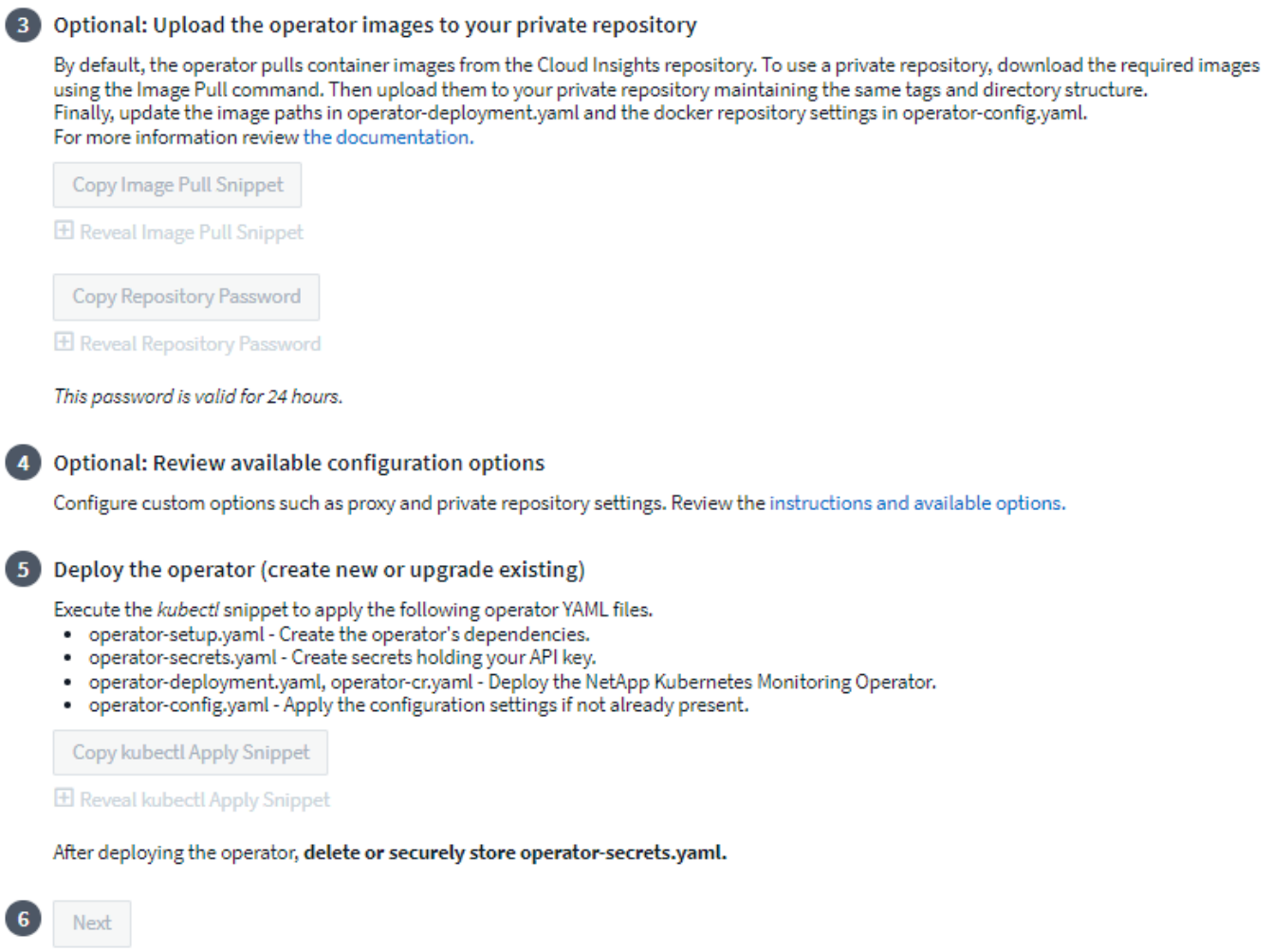
Data Infrastructure Insights bietet den **Kubernetes Monitoring Operator** für die Kubernetes-Sammlung an. Navigieren Sie zu **Kubernetes > Collectors > +Kubernetes Collector**, um einen neuen Operator bereitzustellen.

Bevor Sie den Kubernetes Monitoring Operator installieren

Lesen Sie die "Voraussetzungen" Dokumentation, bevor Sie den Kubernetes Monitoring Operator installieren oder aktualisieren.

Installieren des Kubernetes Monitoring Operator





Schritte zum Installieren des Kubernetes Monitoring Operator Agent auf Kubernetes:

1. Geben Sie einen eindeutigen Cluster-Namen und einen eindeutigen Namespace ein. Wenn Sie von einem früheren Kubernetes-Operator stammenAktualisierung, verwenden Sie den gleichen Cluster-Namen und den gleichen Namespace.
2. Sobald diese eingegeben wurden, können Sie den Download-Befehl-Snippet in die Zwischenablage kopieren.
3. Fügen Sie das Snippet in ein *bash* Fenster ein und führen Sie es aus. Die Installationsdateien des Bedieners werden heruntergeladen. Beachten Sie, dass das Snippet einen eindeutigen Schlüssel hat und für 24 Stunden gültig ist.
4. Wenn Sie ein benutzerdefiniertes oder privates Repository haben, kopieren Sie das optionale Bild-Pull-Snippet, fügen Sie es in eine *bash*-Shell ein und führen Sie es aus. Nachdem die Bilder gezogen wurden, kopieren Sie sie in Ihr privates Repository. Stellen Sie sicher, dass Sie dieselben Tags und Ordnerstrukturen beibehalten. Aktualisieren Sie die Pfade in *Operator-Deployment.yaml* sowie die Einstellungen des Docker-Repository in *Operator-config.yaml*.
5. Prüfen Sie bei Bedarf die verfügbaren Konfigurationsoptionen, z. B. Proxy- oder private Repository-Einstellungen. Lesen Sie mehr über "Konfigurationsoptionen".
6. Wenn Sie bereit sind, stellen Sie den Operator bereit, indem Sie den kubectl Apply-Snippet kopieren, herunterladen und ausführen.
7. Die Installation wird automatisch ausgeführt. Klicken Sie anschließend auf die Schaltfläche „*Next*“.

8. Wenn die Installation abgeschlossen ist, klicken Sie auf die Schaltfläche „*Next*“. Achten Sie darauf, auch die Datei *Operator-Secrets.yaml* zu löschen oder sicher zu speichern.

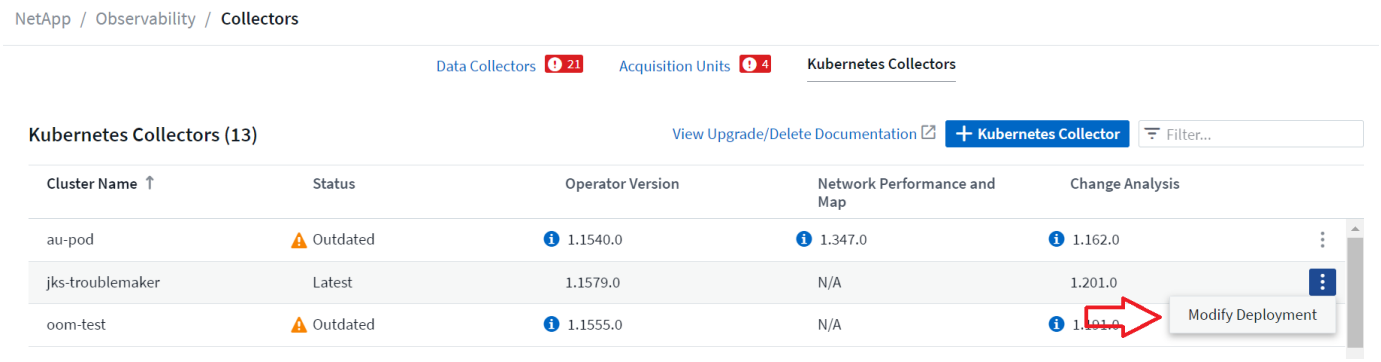
Wenn Sie ein benutzerdefiniertes Repository haben, lesen Sie über Ein benutzerdefiniertes/privates Docker-Repository verwenden.

Kubernetes-Monitoring-Komponenten

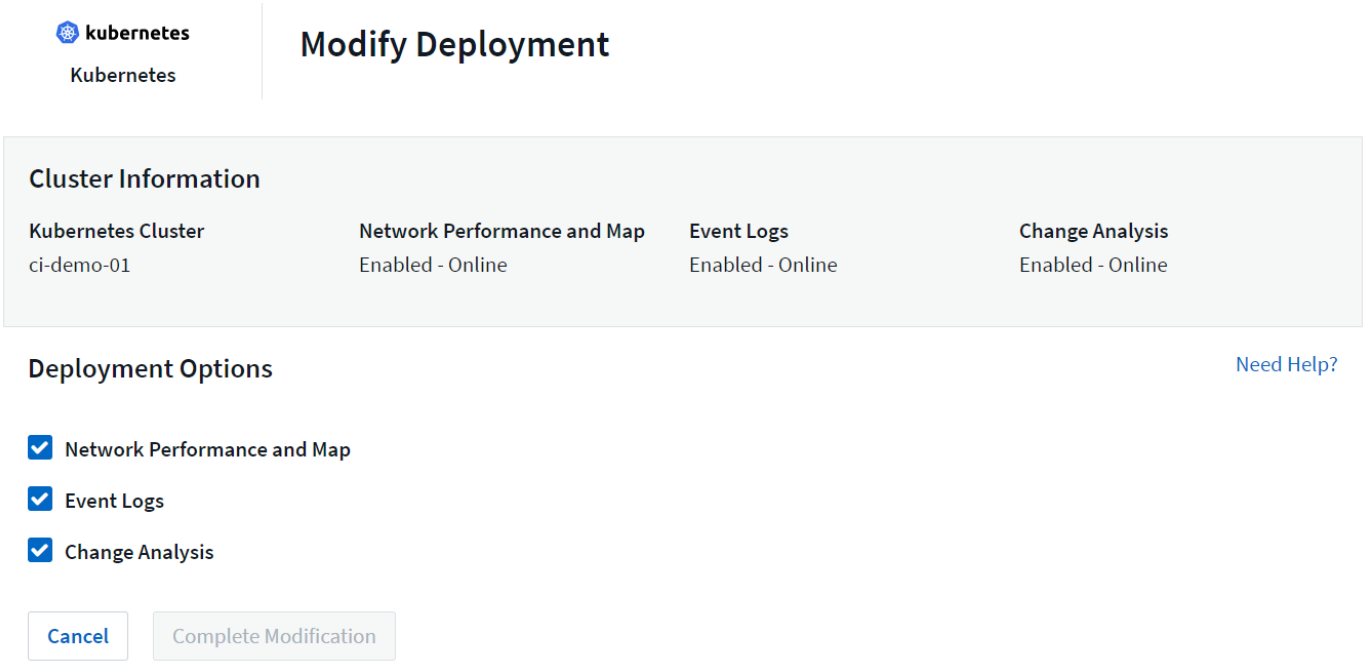
Data Infrastructure Insights Kubernetes Monitoring besteht aus vier Monitoring-Komponenten:

- Cluster-Kennzahlen
- Netzwerkleistung und -Zuordnung (optional)
- Ereignisprotokolle (optional)
- Änderungsanalyse (optional)

Die oben aufgeführten optionalen Komponenten sind standardmäßig für jeden Kubernetes-Collector aktiviert. Wenn Sie sich entscheiden, keine Komponente für einen bestimmten Collector zu benötigen, können Sie sie deaktivieren, indem Sie zu **Kubernetes > Collectors** navigieren und im Collector-Menü „drei Punkte“ rechts auf dem Bildschirm *Modify Deployment* auswählen.



Der Bildschirm zeigt den aktuellen Status jeder Komponente an und ermöglicht es Ihnen, Komponenten für diesen Collector nach Bedarf zu deaktivieren oder zu aktivieren.



Upgrade auf den neuesten Kubernetes Monitoring Operator

DII-Upgrades per Knopfdruck

Sie können den Kubernetes Monitoring Operator über die Seite DII Kubernetes Collectors aktualisieren. Klicken Sie auf das Menü neben dem Cluster, den Sie aktualisieren möchten, und wählen Sie *Upgrade*. Der Bediener überprüft die Bildsignaturen, führt einen Snapshot Ihrer aktuellen Installation durch und führt die Aktualisierung durch. Innerhalb weniger Minuten sollten Sie den Fortschritt des Bedienerstatus über die Aktualisierung auf die neueste Version anzeigen. Wenn ein Fehler auftritt, können Sie den Fehlerstatus für weitere Details auswählen und in der Tabelle zur Fehlerbehebung bei Upgrades auf Tastendruck unten nachsehen.

Upgrades mit privaten Repositorys per Knopfdruck

Wenn Ihr Operator für die Verwendung eines privaten Repositorys konfiguriert ist, stellen Sie sicher, dass alle zum Ausführen des Operators erforderlichen Bilder und deren Signaturen in Ihrem Repository verfügbar sind. Wenn beim Upgrade ein Fehler bei fehlenden Images auftritt, fügen Sie diese einfach zu Ihrem Repository hinzu und wiederholen Sie das Upgrade. Um die Bildsignaturen in Ihr Projektarchiv hochzuladen, verwenden Sie bitte das Cosigns-Tool wie folgt. Stellen Sie sicher, dass Sie Signaturen für alle unter 3 angegebenen Bilder hochladen. Optional: Laden Sie die Operatorbilder in Ihr privates Projektarchiv hoch > Bild-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 „Upgrades per Knopfdruck“ durchgeführt haben und innerhalb von sieben Tagen nach dem Upgrade Probleme mit der aktuellen Version des Bedieners auftreten, können Sie mithilfe des während des Aktualisierungsvorgangs erstellten Snapshots auf die zuvor ausgeführte Version

herunterstufen. Klicken Sie auf das Menü neben dem Cluster, den Sie wiederherstellen möchten, und wählen Sie *Rollback*.

Manuelle Upgrades

Ermitteln Sie, ob eine AgentConfiguration bei dem vorhandenen Operator vorhanden ist (wenn Ihr Namespace nicht der Standardwert *netapp-Monitoring* ist, ersetzen Sie den entsprechenden Namespace):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Wenn eine AgentConfiguration vorhanden ist:
```

- Installieren Der letzte Operator über den vorhandenen Operator.
  - Stellen Sie sicher, dass Die neuesten Container-Bilder werden angezeigtSie ein benutzerdefiniertes Repository verwenden.

Wenn AgentConfiguration nicht vorhanden ist:

- Notieren Sie sich den von Data Infrastructure Insights erkannten Cluster-Namen (wenn Ihr Namespace nicht das standardmäßige NetApp-Monitoring ist, ersetzen Sie den entsprechenden Namespace):

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Erstellen Sie eine Sicherung des bestehenden Operators (wenn Ihr
Namespace nicht der Standard-netapp-Überwachung ist, ersetzen Sie den
entsprechenden Namespace):
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,Deinstallieren>> Der
vorhandene Operator.
* <<installing-the-kubernetes-monitoring-operator,Installieren>> Der
neueste Bediener.
```

  - Verwenden Sie denselben Cluster-Namen.
  - Nachdem Sie die neuesten Operator YAML-Dateien heruntergeladen haben, können Sie alle in Agent_Backup.yaml gefundenen Anpassungen vor der Bereitstellung an den heruntergeladenen Operator-config.yaml übertragen.
  - Stellen Sie sicher, dass Die neuesten Container-Bilder werden angezeigtSie ein benutzerdefiniertes Repository verwenden.

Anhalten und Starten des Kubernetes Monitoring Operator

So beenden Sie den Kubernetes Monitoring Operator:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
So starten Sie den Kubernetes Monitoring Operator:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Deinstallation

Um den Kubernetes Monitoring Operator zu entfernen

Beachten Sie, dass der Standard-Namespace für den Kubernetes Monitoring Operator „netapp-Monitoring“ ist. Wenn Sie Ihren eigenen Namespace festgelegt haben, ersetzen Sie diesen Namespace in diesen und allen nachfolgenden Befehlen und Dateien.

Neuere Versionen des Überwachungsoperators können mit den folgenden Befehlen deinstalliert werden:

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

Wenn der Überwachungsoperator in seinem eigenen dedizierten Namespace bereitgestellt wurde, löschen Sie den Namespace:

```
 kubectl delete ns <NAMESPACE>
Hinweis: Wenn der erste Befehl „Keine Ressourcen gefunden“ zurückgibt,
verwenden Sie die folgenden Anweisungen, um ältere Versionen des
Überwachungsoperators zu deinstallieren.
```

Führen Sie jeden der folgenden Befehle in der Reihenfolge aus. Abhängig von Ihrer aktuellen Installation geben einige dieser Befehle möglicherweise Meldungen „Object not found“ zurück. Diese Meldungen können sicher ignoriert werden.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Wenn zuvor eine Sicherheitskontextbeschränkung erstellt wurde:

```
kubectl delete scc telegraf-hostaccess
```

Über Kube-State-Metrics

Der NetApp Kubernetes Monitoring Operator installiert seine eigenen kube-State-Metriken, um Konflikte mit anderen Instanzen zu vermeiden.

Informationen über Kube-State-Metrics finden Sie unter "Auf dieser Seite".

Konfigurieren/Anpassen des Bedieners

Diese Abschnitte enthalten Informationen zur Anpassung Ihrer Bedienerkonfiguration, zur Arbeit mit Proxy, zur Verwendung eines benutzerdefinierten oder privaten Docker-Repositorys oder zur Arbeit mit OpenShift.

Konfigurationsoptionen

Die am häufigsten geänderten Einstellungen können in der benutzerdefinierten Ressource *AgentConfiguration* konfiguriert werden. Sie können diese Ressource bearbeiten, bevor Sie den Operator bereitstellen, indem Sie die Datei *Operator-config.yaml* bearbeiten. Diese Datei enthält kommentierte Beispiele für Einstellungen. In der Liste "Verfügbare Einstellungen"finden Sie die aktuellste 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 die bereitgestellte Version des Operators
AgentConfiguration unterstützt, führen Sie den folgenden Befehl aus:
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Wenn die Meldung „Fehler vom Server (notfound)“ angezeigt wird, muss Ihr
Bediener aktualisiert werden, bevor Sie die AgentConfiguration verwenden
können.
```

Proxy-Unterstützung Wird Konfiguriert

An zwei Stellen können Sie einen Proxy für Ihren Mandanten verwenden, um den Kubernetes Monitoring Operator zu installieren. Es kann sich um dieselben oder separate Proxy-Systeme handelt:

- Proxy wird während der Ausführung des Installationscode-Snippets (mit „Curl“) benötigt, um das System zu verbinden, auf dem das Snippet ausgeführt wird, mit Ihrer Data Infrastructure Insights-Umgebung
- Der vom Kubernetes Ziel-Cluster benötigte Proxy für die Kommunikation mit der Insights Umgebung Ihrer Dateninfrastruktur ist erforderlich

Wenn Sie einen Proxy für eine oder beide dieser Optionen verwenden, müssen Sie zur Installation des Kubernetes Operating Monitor zunächst sicherstellen, dass Ihr Proxy so konfiguriert ist, dass eine gute Kommunikation mit Ihrer Data Infrastructure Insights-Umgebung möglich ist. Wenn Sie über einen Proxy verfügen und von dem Server/der VM, von dem aus Sie den Operator installieren möchten, auf Data Infrastructure Insights zugreifen können, ist Ihr Proxy wahrscheinlich richtig konfiguriert.

Für den Proxy, der zur Installation des Kubernetes Operating Monitor verwendet wird, legen Sie vor der Installation des Operators die Umgebungsvariablen *http_Proxy/https_Proxy* fest. In einigen Proxy-Umgebungen müssen Sie möglicherweise auch die Variable *no_Proxy Environment* festlegen.

Um die Variablen festzulegen, führen Sie die folgenden Schritte auf Ihrem System aus * bevor* den Kubernetes Monitoring Operator installiert:

1. Legen Sie die Umgebungsvariable *https_Proxy* und/oder *http_Proxy* für den aktuellen Benutzer fest:
   a. Wenn der Proxy, der eingerichtet wird, keine Authentifizierung (Benutzername/Passwort) aufweist, führen Sie den folgenden Befehl aus:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Wenn der Proxy, der eingerichtet wird, über Authentifizierung
(Benutzername/Passwort) verfügt, führen Sie folgenden Befehl aus:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Wenn der Proxy, der für das Kubernetes-Cluster zur Kommunikation mit der Insights Umgebung Ihrer Dateninfrastruktur verwendet wird, verwendet wird, installieren Sie den Kubernetes Monitoring Operator, nachdem Sie alle diese Anweisungen gelesen haben.

Konfigurieren Sie den Proxy-Abschnitt von AgentConfiguration in Operator-config.yaml, bevor Sie den Kubernetes Monitoring Operator bereitstellen.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Verwenden eines benutzerdefinierten oder privaten Docker Repositorys

Standardmäßig zieht der Kubernetes Monitoring Operator Container-Images aus dem Repository Data Infrastructure Insights. Wenn Sie ein Kubernetes-Cluster als Ziel für das Monitoring verwenden und der Cluster so konfiguriert ist, dass er nur Container-Images aus einem benutzerdefinierten oder privaten Docker-Repository oder der Container-Registrierung zieht, müssen Sie den Zugriff auf die Container konfigurieren, die vom Kubernetes Monitoring Operator benötigt werden.

Führen Sie das „Image Pull Snippet“ aus der NetApp Monitoring Operator Installationskachel aus. Dieser Befehl meldet sich beim Repository Data Infrastructure Insights an, zieht alle Image-Abhängigkeiten für den Operator ab und meldet sich vom Repository Data Infrastructure Insights ab. Wenn Sie dazu aufgefordert werden, geben Sie das angegebene temporäre Repository-Passwort ein. Mit diesem Befehl werden alle vom Bediener verwendeten Bilder heruntergeladen, einschließlich optionaler Funktionen. Nachfolgend sehen Sie, für welche Funktionen diese Bilder verwendet werden.

Core Operator-Funktionalität und Kubernetes Monitoring

- netapp Monitoring
- ci-kube-rbac-Proxy
- ci-ksm
- ci-telegraf
- Distroless-root-user

Ereignisprotokoll

- ci-Fluent-Bit

- ci-kubernetes-Event-Exporteur

Netzwerkleistung und -Zuordnung

- ci-Netz-Beobachter

Übertragen Sie das Operator-Docker-Image gemäß Ihren Unternehmensrichtlinien in das private/lokale/unternehmenseigene Docker-Repository. Stellen Sie sicher, dass die Bild-Tags und Verzeichnispfade zu diesen Images in Ihrem Repository mit denen im Data Infrastructure Insights Repository übereinstimmen.

Bearbeiten Sie die Bereitstellung des Monitoring-Operators in Operator-Deployment.yaml, und ändern Sie alle Bildverweise, um Ihr privates Docker-Repository zu verwenden.

```
image: <docker repo of the enterprise/corp docker repo>/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 die neue Position des Docker-Repo zu berücksichtigen. Erstellen Sie ein neues imagePullSecret für Ihr privates Repository. Weitere Informationen finden Sie unter *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

OpenShift-Anweisungen

Wenn Sie OpenShift 4.6 oder höher ausführen, müssen Sie die AgentConfiguration in *Operator-config.yaml* bearbeiten, um die Einstellung *runPrivileged* zu aktivieren:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

OpenShift kann zusätzliche Sicherheitsstufen implementieren, die den Zugriff auf einige Kubernetes-Komponenten blockieren könnten.

Toleranzen und Verfleckungen

Die DemonSets *netapp-CI-telegraf-ds*, *netapp-CI-Fluent-Bit-ds* und *netapp-CI-net-Observer-l4-ds* müssen für jeden Node im Cluster einen Pod planen, damit Daten auf allen Nodes korrekt erfasst werden. Der Operator wurde so konfiguriert, dass er einige bekannte **Fehler** toleriert. Wenn Sie auf Ihren Knoten benutzerdefinierte Taints konfiguriert haben und damit verhindern, dass Pods auf jedem Knoten ausgeführt werden, können Sie für diese Taints eine **Toleration** erstellen"In der *AgentConfiguration*". Wenn Sie auf alle Nodes im Cluster benutzerdefinierte Taints angewendet haben, müssen Sie der Operator-Bereitstellung auch die erforderlichen Toleranzen hinzufügen, damit der Operator-Pod geplant und ausgeführt werden kann.

Erfahren Sie mehr über Kubernetes "Tönungen und Tolerationen".

Kehren Sie zum zurück **"NetApp Kubernetes Monitoring Operator Installation** Seite"

Ein Hinweis über Geheimnisse

Um die Berechtigung für den Kubernetes Monitoring Operator zum Anzeigen der geheimen Daten im gesamten Cluster zu entfernen, löschen Sie vor der Installation die folgenden Ressourcen aus der Datei *Operator-Setup.yaml*:

```
 ClusterRole/netapp-ci<namespace>-agent-secret
 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 Optionen *AgentConfiguration* oder *Operator-config.yaml*, um den Änderungsmanagementabschnitt zu entkommentieren und *kindsToIgnoreFromWatch: '"Secrets"* im Bereich Change-Management aufzunehmen. Notieren Sie sich das Vorhandensein und die Position von einfachen und doppelten Anführungszeichen in dieser Zeile.

```
change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Überprüfen Der Signaturen Der Kubernetes Monitoring Operator Images

Das Bild für den Betreiber und alle damit verbundenen Bilder werden von NetApp signiert. Sie können die Images vor der Installation mit dem cosign-Tool manuell überprüfen oder einen Kubernetes-Aufnahme-

Controller konfigurieren. Weitere Informationen finden Sie im "Kubernetes-Dokumentation".

Der öffentliche Schlüssel, der zur Überprüfung der Bildsignaturen verwendet wird, ist in der Kachel Monitoring Operator install unter *Optional: Laden Sie die Operatorbilder in Ihr privates Repository > Image Signature Public Key*

So überprüfen Sie eine Bildsignatur manuell:

1. Kopieren Sie das Bild-Pull-Snippet, und führen Sie es aus
2. Kopieren Sie das Repository-Kennwort, und geben Sie es ein, wenn Sie dazu aufgefordert werden
3. Speichern Sie den Public Key der Bildsignatur (im Beispiel dii-image-signing.Pub).
4. Überprüfen Sie die Bilder mit cosign. Beachten Sie 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

Bei Problemen beim Einrichten des Kubernetes Monitoring Operator sollten Sie Folgendes versuchen:

Problem:	Versuchen Sie dies:
Ich sehe keinen Hyperlink/Verbindung zwischen meinem Kubernetes Persistent Volume und dem entsprechenden Back-End Storage-Gerät. Mein Kubernetes Persistent Volume wird mit dem Hostnamen des Storage-Servers konfiguriert.	Befolgen Sie die Schritte, um den bestehenden Telegraf-Agent zu deinstallieren, und installieren Sie dann den neuesten Telegraf-Agent erneut. Sie müssen Telegraf Version 2.0 oder höher verwenden. Der Kubernetes-Cluster-Storage muss aktiv durch Data Infrastructure Insights überwacht werden.

Problem:	Versuchen Sie dies:
Ich sehe Meldungen in den Protokollen, die folgende ähneln: E0901 15 352:21:39.962145 1 Reflektor.go:178] k8s.io/kube-State-metrics/internal/Store/Builder.go:352: Fehler beim Auflisten *v1.MutatingWebhookKonfiguration: Der Server konnte die angeforderte Ressource E0901 15:21:43.168161 1 Reflector.go:178] k8s.io/kube-Builder nicht finden	Diese Nachrichten können auftreten, wenn Sie kube-State-Metrics Version 2.0.0 oder höher mit Kubernetes-Versionen unter 1.20 ausführen. Um die Kubernetes-Version zu erhalten: *Kubectl Version* um die kube-State-metrics-Version zu erhalten: *Kubectl get Deploy/kube-State-metrics -o jsonpath='{..image}'* um zu verhindern, dass diese Nachrichten passieren, können Benutzer ihre kube-State-Metrics-Implementierung ändern, um die folgenden Elemente zu deaktivieren: _Mutingwebhookkonfigurationen___volumehaWeitere Resources=certificationesigningrequests,configmaps, cronjobs,dämsets, Bereitstellungen,Endpunkte,HorizontalpodAutoscaler, nesresses,Jobs,Begrenzungsbereiche,Namensräume, Netzwerkrichtlinien,Knoten,Persistenz,stagemasnesmases,nesmasnesmases,nesmasnesmasnesmasnesnesmasnesequets,ndecoses,nescontascrises,nesequequequesefises,nesequequesequesefiscones,mases,nesequidatequesequesefiscones,nesequesequesefiscrises,nesequesequesefiscones,nesefisconesefisconmases,mases,nesequesequesefiscones,necequesequeseques Validatingwebhookkonfigurationen, Volumeanhänge“
Ich sehe Fehlermeldungen von Telegraf ähnlich wie die folgenden, aber Telegraf startet und läuft: Okt 11 14:23:41 ip-172-31-39-47 systemd[1]: Startete den Plugin-getriebenen Server Agent für das Reporting von Metriken in InfluxDB. Okt 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Time=„2021-10-11T14:23:41Z“ Level=error msg=„konnte kein Cache-Verzeichnis erstellen. /Etc/telegraf/.Cache/snowflake, err: Mkdir /etc/telegraf/.ca che: Berechtigung verweigert. Ignored\n" func=„gosnowflake.(*defaultLogger).Errorf“ file=„log.go:1827 23“ Okt 31 2021:39-47 10 ip-172-11 14-23:41 telegraf[120]: Time=„41-11TZ Fehler“:41T14=. Ignored. Open /etc/telegraf/.Cache/snowflake/ocsp_response_Cache .json: No such file or Directory\n" func=„gosnowflake.(*defaultLogger).Errorf“ file=„log.go:23“ Okt 2021:10 ip-1827-31-39-47 telegraf[172]: 11 14-23:41-11T11T14:120:41Z I! Telegraf 1.19.3 Starten	Dies ist ein bekanntes Problem. "Dieser GitHub-Artikel"Weitere Informationen finden Sie unter. Solange Telegraf läuft, können Benutzer diese Fehlermeldungen ignorieren.
Auf Kubernetes meldet mein Telegraf pod(s) den folgenden Fehler: „Fehler in der Verarbeitung von mountstats-Infos: Habe mountstats-Datei nicht geöffnet: /Hostfs/proc/1/mountstats, Fehler: Open /hostfs/proc/1/mountstats: Permission dementied“	Wenn SELinux aktiviert und durchgesetzt wird, wird wahrscheinlich verhindert, dass die Telegraf PODs auf die Datei /proc/1/mountstats auf dem Kubernetes-Knoten zugreifen. Um diese Einschränkung zu überwinden, bearbeiten Sie die Agentkonfiguration und aktivieren Sie die runPrivileged-Einstellung. Weitere Einzelheiten finden Sie in den OpenShift-Anweisungen.

Problem:	Versuchen Sie dies:
Auf Kubernetes meldet mein Telegraf ReplicaSet POD den folgenden Fehler: [inputs.prometheus] Fehler im Plugin: Konnte keine keypair /etc/kubernetes/pki/etcd/Server.crt:/etc/kubernetes/pki /etcd/Server.key: Öffnen /etc/kubernetes/pki/etcd/Server.crt: Keine solche Datei oder Verzeichnis	Der Pod Telegraf ReplicaSet soll auf einem Knoten ausgeführt werden, der als Master oder für etc bestimmt ist. Wenn der ReplicaSet-Pod auf einem dieser Knoten nicht ausgeführt wird, werden diese Fehler angezeigt. Überprüfen Sie, ob Ihre Master/etcd-Knoten eine Tönungswalle haben. Fügen Sie in diesem Fall die erforderlichen Verträgungen in das Telegraf ReplicaSet, telegraf-rs ein. Bearbeiten Sie zum Beispiel die Datei ReplicaSet… kubectl edit rs telegraf-rs …und fügen Sie die entsprechenden Verträgungen der Spezifikation hinzu. Starten Sie anschließend den Pod ReplicaSet neu.
Ich habe eine PSP/PSA Umgebung. Hat dies Auswirkungen auf meinen Überwachungsperator?	Wenn Ihr Kubernetes-Cluster mit Pod-Sicherheitsrichtlinie (PSP) oder Pod Security Admission (PSA) ausgeführt wird, müssen Sie ein Upgrade auf den aktuellen Kubernetes Monitoring Operator durchführen. Gehen Sie wie folgt vor, um auf den aktuellen Operator mit Unterstützung für PSP/PSA zu aktualisieren: 1. Deinstallieren Der bisherige Monitoring-Operator: Kubectl delete Agent-Monitoring-NetApp -n NetApp-Monitoring kubectl delete ns NetApp-Monitoring kubectl delete crd Agents.Monitoring.NetApp.com kubectl delete clusterrole Agent-Manager-role Agent-Proxy-role Agent-metrics-reader kubectl delete clusterrolebinding Agent-Manager-rolebinding Agent-Proxy-rolebinding Agent-rolebinding Agent-Cluster-admin-rolebinding 2. Installieren Die neueste Version des Überwachungsbedieners.
Ich habe Probleme beim Versuch, den Operator bereitzustellen, und ich habe PSP/PSA in Gebrauch.	1. Bearbeiten Sie den Agenten mit folgendem Befehl: Kubectl -n <name-space> edit Agent 2. Markieren Sie „Sicherheitspolitik aktiviert“ als „falsch“. Dadurch werden Pod-Sicherheitsrichtlinien und Pod-Sicherheitszulassung deaktiviert und der Bediener kann die Bereitstellung durchführen. Bestätigung mit den folgenden Befehlen: Kubectl get psp (sollte Pod Security Policy entfernt zeigen) kubectl get all -n <Namespace> grep -i psp (sollte zeigen, dass nichts gefunden wird)
„ImagePullBackoff“-Fehler erkannt	Diese Fehler können auftreten, wenn Sie über ein benutzerdefiniertes oder privates Docker-Repository verfügen und den Kubernetes Monitoring Operator noch nicht so konfiguriert haben, dass er es richtig erkennt. Weitere Informationen Info über die Konfiguration für benutzerdefinierte/private Repo.

Problem:	Versuchen Sie dies:

Ich habe ein Problem mit der Installation meines Monitoring-Bedieners, und die aktuelle Dokumentation hilft mir nicht, es zu lösen.	Erfassen oder notieren Sie die Ausgabe der folgenden Befehle, und wenden Sie sich an den technischen Support.
	
	`kubectl -n netapp-monitoring get all`
	`kubectl -n netapp-monitoring describe all`
	`kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true`
	`kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true`

NET-Observer (Workload Map)-Pods im Operator Namespace befinden sich in CrashLoopBackOff	Diese Pods entsprechen dem Workload Map-Datensammler für Network Observability. Versuchen Sie Folgendes: • Überprüfen Sie die Protokolle eines der Pods, um die minimale Kernel-Version zu bestätigen. Beispiel: --- {"CI-Tenant-id":"your-Tenant-id","Collector-Cluster":"your-k8s-Cluster-Name","Environment":"prod","Level":"error","msg":"failed in validation. Grund: Kernel-Version 3.10.0 ist kleiner als die minimale Kernel-Version von 4.18.0","Time":"2022-11-09T08:23:08Z"} ---- • Net-Observer-Pods erfordern die Linux-Kernel-Version mindestens 4.18.0. Überprüfen Sie die Kernel-Version mit dem Befehl „uname -r“ und stellen Sie sicher, dass sie >= 4.18.0 sind
Pods werden im Operator Namespace ausgeführt (Standard: netapp-Monitoring), es werden jedoch keine Daten in der UI für die Workload-Zuordnung oder Kubernetes-Metriken in Abfragen angezeigt	Überprüfen Sie die Zeiteinstellung auf den Knoten des K8S-Clusters. Für eine genaue Prüfung und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Agent-Rechner mit Network Time Protocol (NTP) oder Simple Network Time Protocol (SNTP) zu synchronisieren.
Einige der Net-Observer-Pods im Namespace Operator befinden sich im Status „Ausstehend“	NET-Observer ist ein DemonSet und führt in jedem Knoten des K8s-Clusters einen Pod aus. • Beachten Sie den Pod, der sich im Status „Ausstehend“ befindet, und prüfen Sie, ob ein Ressourcenproblem für CPU oder Speicher vorliegt. Stellen Sie sicher, dass der erforderliche Arbeitsspeicher und die erforderliche CPU im Knoten verfügbar sind.

Problem:	Versuchen Sie dies:
Ich sehe Folgendes in meinen Protokollen sofort nach der Installation des Kubernetes Monitoring Operators: [inputs.prometheus] Fehler im Plugin: Fehler beim Erstellen einer HTTP-Anforderung an http://kube-state-metrics.<namespace>.svc.Cluster.local:8080/metrics: Get http://kube-state-metrics.<namespace>.svc.Cluster.local:8080/metrics: Dial tcp: Lookup kube-State-metrics.<namespace>.svc.Cluster.local: Kein solcher Host	Diese Meldung wird normalerweise nur angezeigt, wenn ein neuer Operator installiert ist und der Pod „*telegraf-rs*“ vor dem Einschalten des Pod „*ksm*“ steht. Diese Meldungen sollten beendet werden, sobald alle Pods ausgeführt werden.
Ich sehe keine Kennzahlen für die Kubernetes-Kronjobs, die in meinem Cluster vorhanden sind, erfasst.	Überprüfen Sie Ihre Kubernetes-Version (d. h. `kubectl version`). Wenn es v1.20.x oder niedriger ist, ist dies eine erwartete Einschränkung. Die mit dem Kubernetes Monitoring Operator implementierte Version von kube-State-Metrics unterstützt nur v1.cronjob. Bei Kubernetes 1.20.x und niedriger befindet sich die Ressource cronjob unter v1beta.cronjob. Daher können kube-State-Metriken die Ressource cronjob nicht finden.
Nach der Installation des Bedieners geben die telegraf-ds-Pods CrashLoopBackOff ein und die POD-Protokolle zeigen „su: Authentication failure“ an.	Bearbeiten Sie den Abschnitt telegraf in *AgentConfiguration*, und setzen Sie *dockerMetricCollectionEnabled* auf false. Weitere Informationen finden Sie im "Konfigurationsoptionen". … Spec: … telegraf: … - Name: docker Run-Mode: - DemonSet Ersetzungen: - Schlüssel: DOCKER_UNIX_SOCK_PLACEHOLDER Wert: unix:///run/Docker.Sock … …
Ich sehe wiederholte Fehlermeldungen wie die folgenden in meinen Telegraf-Logs: E! [Agent] Fehler beim Schreiben in Outputs.http: Post "https://<tenant_url>/Rest/v1/Lake/ingest/influxdb": Kontext-Deadline überschritten (Client. Zeitüberschreitung beim Warten auf Header überschritten)	Bearbeiten Sie den Abschnitt telegraf in *AgentConfiguration*, und erhöhen Sie *outputTimeout* auf 10s. Weitere Informationen finden Sie im "Konfigurationsoptionen".
Ich vermisse *involvedobject* Daten für einige Event Logs.	Stellen Sie sicher, dass Sie die Schritte im Abschnitt oben befolgt haben"Berechtigungen".
Wieso werden zwei Monitoring Operator Pods ausgeführt, einer mit dem Namen netapp-CI-Monitoring-Operator-<pod> und der andere mit dem Namen Monitoring-Operator-<pod>?	Seit dem 12. Oktober 2023 hat Data Infrastructure Insights den Betreiber refaktorisiert, um unseren Benutzern besser dienen zu können. Damit diese Änderungen vollständig umgesetzt werden, müssen Sie Entfernen Sie den alten Bedienerund Installieren Sie den neuen.

Problem:	Versuchen Sie dies:
Meine kubernetes-Ereignisse haben unerwartet aufgehört, Daten bei Infrastruktur-Insights zu melden.	Rufen Sie den Namen des POD für den Event-Exporter ab: `kubectl -n netapp-monitoring get pods`
grep event-exporter	awk '{print $1}'
sed 's/event-exporter./event-exporter/'` Es sollte entweder „netapp-CI-Event-Exporteur“ oder „Event-Exporteur“ sein. Bearbeiten Sie anschließend den Überwachungsagenten `kubectl -n netapp-monitoring edit agent`und legen Sie den Wert für LOG_FILE so fest, dass der entsprechende POD-Name des Ereignisexporteurs im vorherigen Schritt angezeigt wird. Genauer gesagt sollte LOG_FILE auf "/var/log/Containers/netapp-CI-Event-exporteur.log" oder "/var/log/Containers/Event-exporteur*.log" gesetzt werden …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Alternativ kann man auch Deinstallieren und Neu installieren den Agenten.	Ich sehe POD(s), die vom Kubernetes-Monitoring-Operator bereitgestellt werden, aufgrund unzureichender Ressourcen.
Informationen zum Erhöhen der CPU- und/oder Speichergrenzen finden Sie im Kubernetes Monitoring Operator"Konfigurationsoptionen".	Durch ein fehlendes Image oder eine ungültige Konfiguration wurden die netapp-CI-kube-State-metrics Pods nicht gestartet oder nicht einsatzbereit gemacht. Jetzt bleibt StatefulSet stecken und Konfigurationsänderungen werden nicht auf die Pods mit den netapp-CI-kube-State-Metriken angewendet.
StatefulSet befindet sich in einem "Defekt" Status. Nachdem Sie Konfigurationsprobleme behoben haben, springen die netapp-CI-kube-State-metrics-Pods an.	Pods mit netapp-CI-kube-Status-Metriken können nicht gestartet werden, nachdem ein Kubernetes Operator Upgrade ausgeführt wurde. Es wird ErrImagePull geworfen (es konnte nicht das Image entfernt werden).
Versuchen Sie, die Pods manuell zurückzusetzen.	„Event disorded as being alder then maxEventAgeSeconds“ Meldungen werden für meinen Kubernetes Cluster unter Log Analysis beobachtet.

Problem:	Versuchen Sie dies:
Ändern Sie den Operator *agentkonfiguration*, und erhöhen Sie die Erweiterung *Event-exporteur-maxEventAgeSeconds* (d. h. auf 60s), *Event-exporteur-kubeQPS* (d. h. auf 100) und *Event-exporteur-kubeBurst* (d. h. auf 500). Weitere Informationen zu diesen Konfigurationsoptionen finden Sie auf der "Konfigurationsoptionen" Seite.	Telegraf warnt vor unzureichenden, abschließbaren Speichern oder stürzt ab.
Versuchen Sie, die Grenze des abschließbaren Speichers für Telegraf im zugrunde liegenden Betriebssystem/Knoten zu erhöhen. Wenn eine Erhöhung des Limits keine Option ist, ändern Sie die NKMO-Agentkonfiguration und setzen Sie *Unprotected* auf *true*. Dadurch wird Telegraf angewiesen, keine gesperrten Speicherseiten zu reservieren. Dies kann zwar ein Sicherheitsrisiko darstellen, da entschlüsselte Geheimnisse möglicherweise auf die Festplatte ausgetauscht werden, ermöglicht aber die Ausführung in Umgebungen, in denen das Reservieren von gesperrtem Speicher nicht möglich ist. Weitere Informationen zu den Konfigurationsoptionen *Unprotected* finden Sie auf der "Konfigurationsoptionen" Seite.	Ich sehe Warnhinweise von Telegraf wie folgt: *W! [Inputs.diskio] der Datenträgername für „vdc“ kann nicht erfasst werden: Fehler beim Lesen von /dev/vdc: Keine Datei oder Verzeichnis*
Für den Kubernetes Monitoring Operator sind diese Warnmeldungen gutartig und können sicher ignoriert werden. Alternativ können Sie den telegraf-Abschnitt in AgentConfiguration bearbeiten und *runDsPrivileged* auf true setzen. Weitere Informationen finden Sie im "Konfigurationsoptionen des Bedieners".	Mein Fluent-Bit-Pod schlägt mit den folgenden Fehlern fehl: [2024/10/16 14:16:23] [error] [/src/Fluent-Bit/Plugins/in_tail/tail_fs_inotify.c:360 errno=10/16 14] zu viele geöffnete Dateien [16/23:16:23] [error] initialisieren des Input tail.0 [2024/24:2024:10/16 14] [error] die Eingabe-Initialisierung ist fehlgeschlagen

Problem:	Versuchen Sie dies:

Versuchen Sie, Ihre *fsnotify*-Einstellungen im Cluster zu ändern:
 	
`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>`
 	
Starten Sie Fluent-Bit neu.
 	
Hinweis: Um diese Einstellungen über einen Node hinweg dauerhaft neu zu starten, müssen Sie die folgenden Zeilen in */etc/sysctl.conf* eingeben
 	
`fs.inotify.max_user_instances=<something larger than current setting>`
`fs.inotify.max_user_watches=<something larger than current setting>`
	Die telegraf DS-Pods melden Fehler, die das kubernetes-Input-Plug-in betreffen und keine HTTP-Anforderungen stellen, da das TLS-Zertifikat nicht validiert werden kann. Zum Beispiel: E! [Inputs.kubernetes] Fehler im Plugin: Fehler beim Erbringen der HTTP-Anforderung zum "<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": Abrufen von "<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

Weitere Informationen finden Sie auf der "Support" Seite oder im "Data Collector Supportmatrix".

Memcached Data Collector

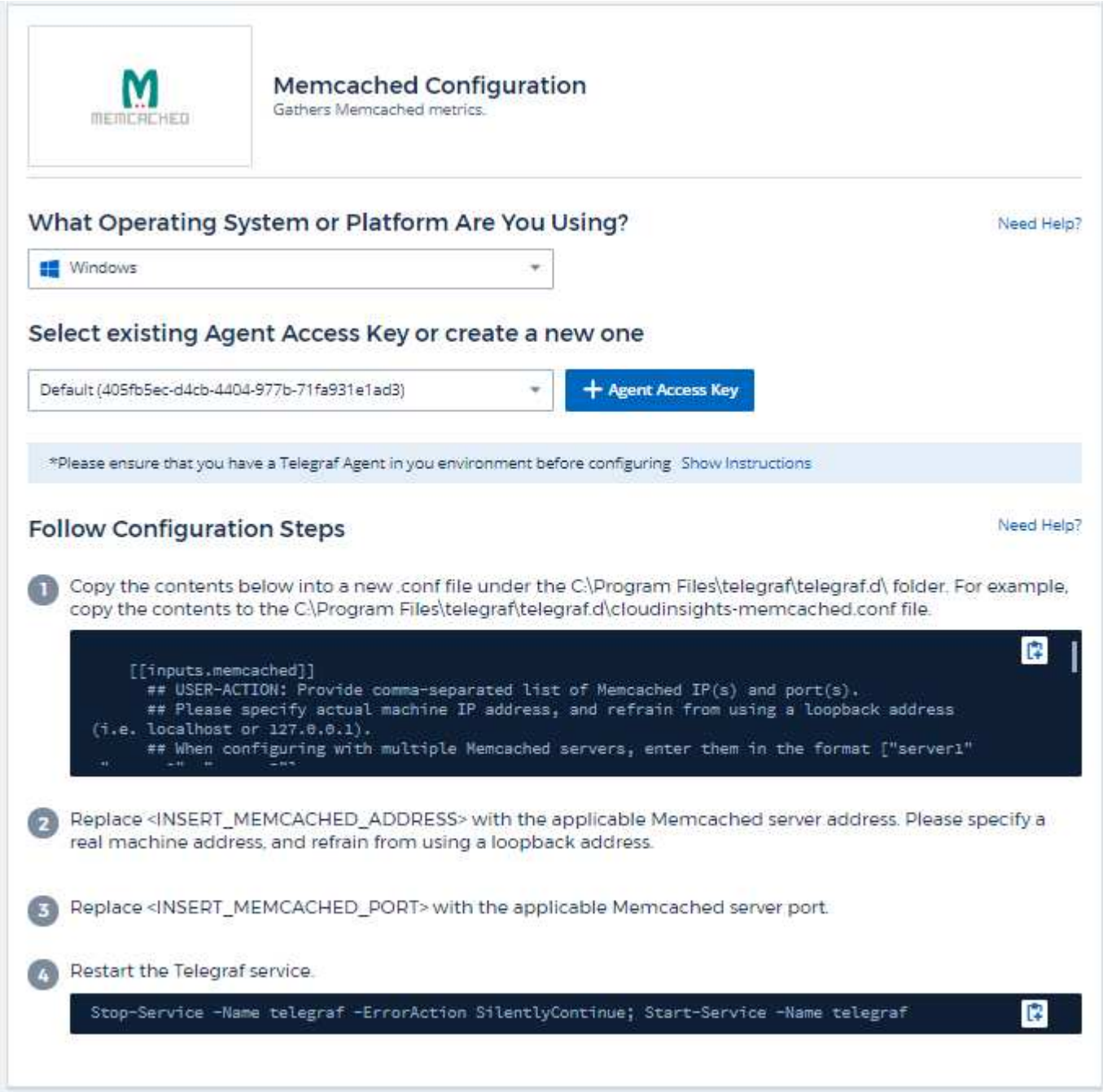
Data Infrastructure Insights nutzt diesen Datensammler, um Kennzahlen aus Memcached zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Memcached.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie im "Wiki mit Memcached".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Gememcachte	Namespace-Server	Node-IP-Node-Name	Akzeptieren von Verbindungen verarbeitet Authentifizierungsanforderungen fehlgeschlagene Authentifizierungen verwendete Bytes (pro Sekunde) geschriebene Bytes (pro Sek.) CAS Badval CAS Hits CAS Misses Flush Reqs (pro Sek.) Get Reqs (pro Sek.) Set Reqs (pro Sek.) Touch Reqs (pro Sek.) Verbindungserträge (pro Sek.) Verbindungsstrukturen Verbindungen öffnen Aktuelle gespeicherte Objekte Decr fordert Zugriffe (pro Sek.) Decr fordert Fehlschläge (pro Sek.) Löschen von Anfragen Treffer (pro Sek.) Löschen von Anfragen Fehlschläge (pro Sek.) entfernte Objekte gültige Abtreibungen abgelaufene Objekte Get Hits (pro Sek.) Get Misses (pro Sek.) Gebrauchte Hash Bytes Hash-Bytes erweitert Hash Power Level Inc. Hash Power Level Inc. Zugriffe (pro Sek.) Infr Anfragen Misses (pro Sek.) Server Max Bytes anhören deaktiviert Num zurückgewonnener Mitarbeiter Threads Anzahl geöffnete Verbindungen Gesamtzahl der gespeicherten Elemente Touch Hits Touch Misses Server Uptime

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

MongoDB Data Collector

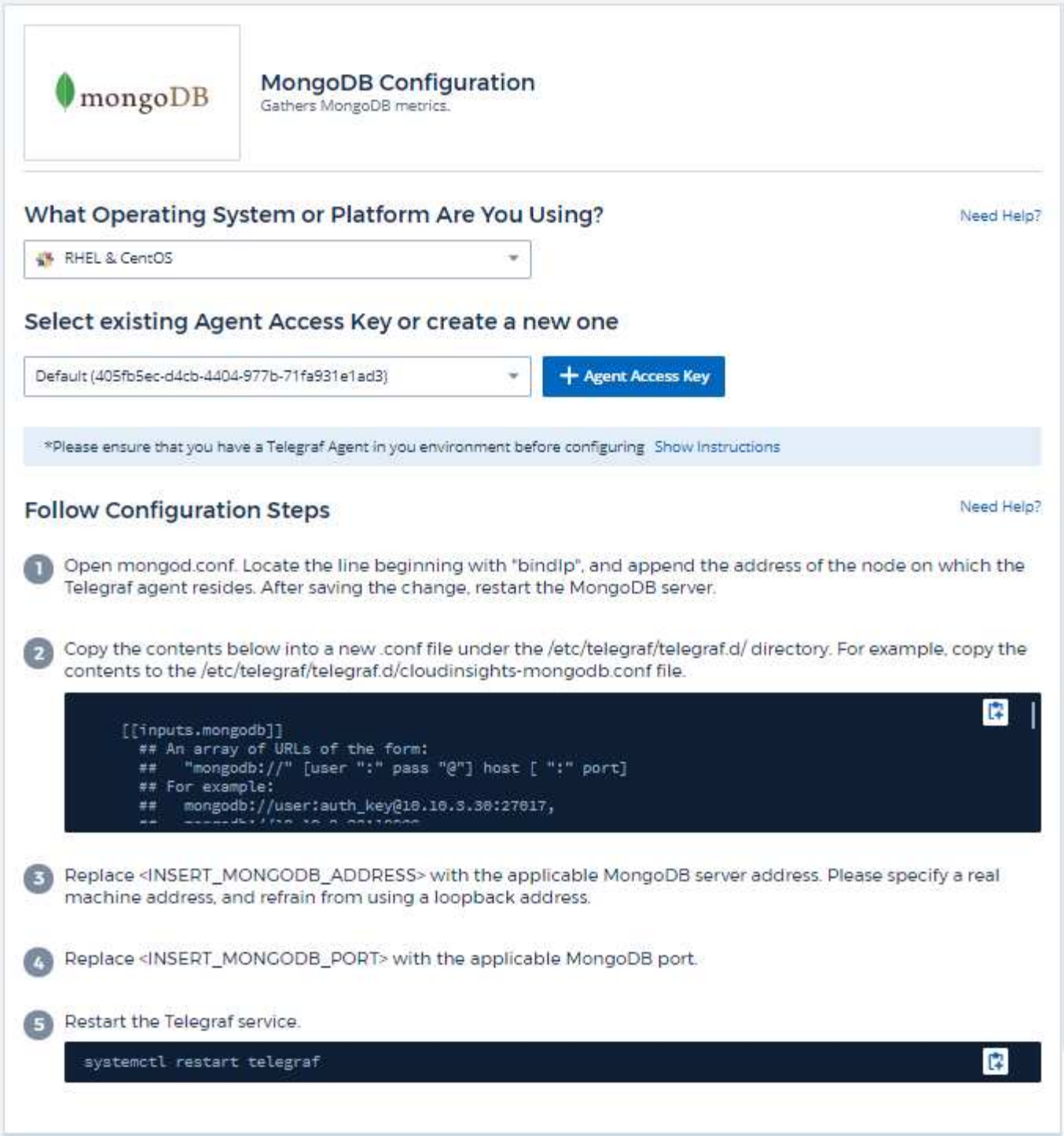
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen von MongoDB zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie MongoDB.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie im "MongoDB Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
MongoDB	Namespace-Hostname		

Objekt:	Kennungen:	Attribute:	Datenpunkte:
MongoDB Datenbank	Name der Namespace-Hostname-Datenbank		

Fehlerbehebung

Informationen finden Sie auf der "Support" Seite.

MySQL Data Collector

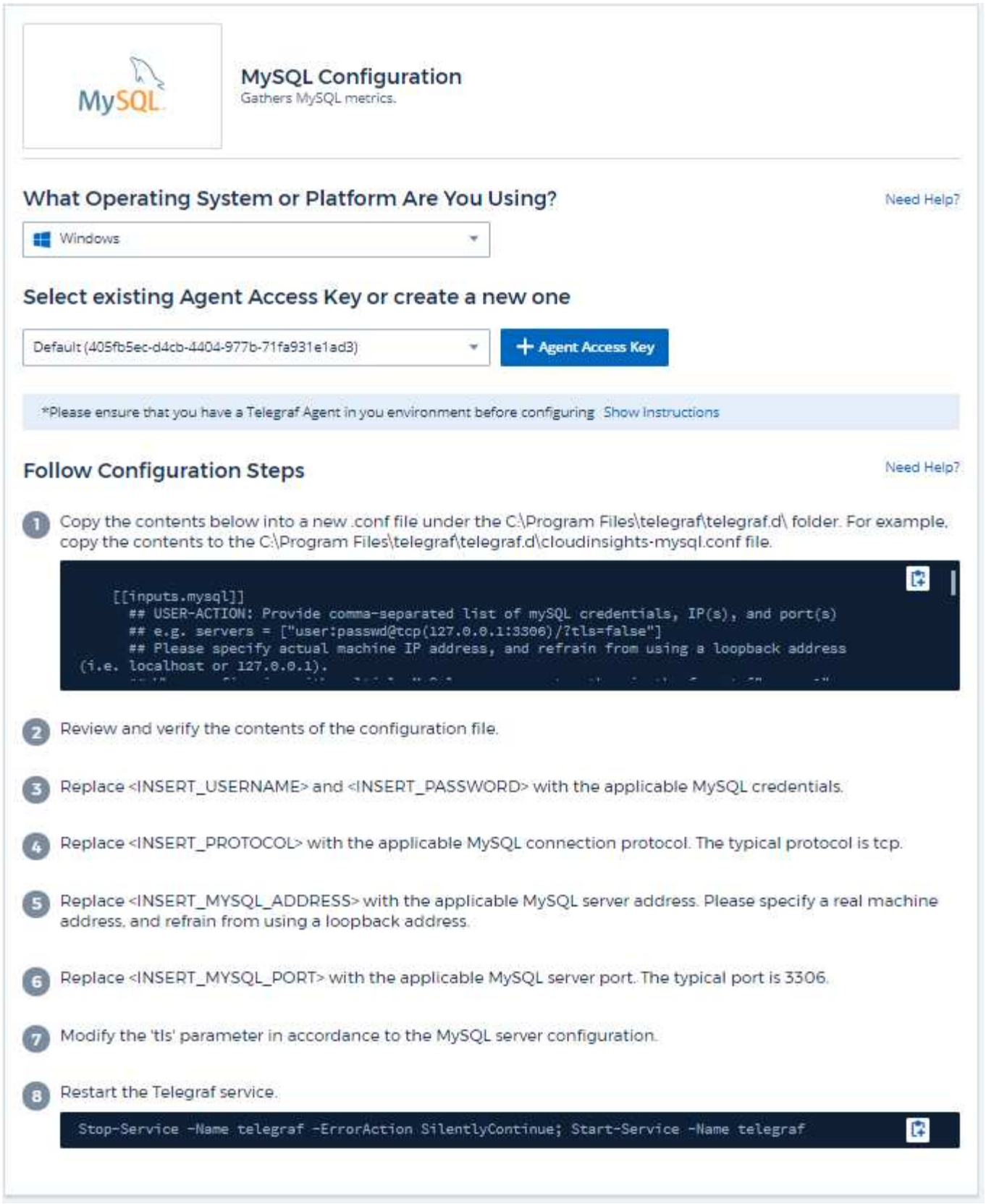
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen aus MySQL zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie MySQL.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie im "MySQL-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
MySQL	Namespace für MySQL Server	Node-IP-Node-Name	Abgebrochene Clients (pro s) abgebrochene Verbindungen (pro s) RX Byte (pro s) TX Bytes (pro Sek.) Befehle Admin (pro Sek.) Befehle Alter Ereignisbefehle Alter Funktion Befehle Alter Instanz Befehle Alter Prozedur Befehle Alter Server Befehle Alter Tabelle Befehle Alter Tablespace Befehle Alter Benutzer Befehle Analyse Befehle Zuweisen zu Keycache-Befehlen Begin-Befehle Binlog-Befehle Aufruf Procedure-Befehle DB-Befehle Change Master befiehlt Change Repl Filter Befehle Check Commands Prüfsummenbefehle Befehle Commit-Befehle DB-Befehle erstellen Ereignisbefehle erstellen Befehle erstellen Index-Befehle erstellen Maßnahmen-Befehle erstellen Serverbefehle erstellen Trigger-Befehle erstellen UDF-Befehle erstellen Benutzerbefehle erstellen Befehle anzeigen erstellen Dealloc SQL-Verbindungsfehler akzeptieren erstellte tmp-Disk-Tabellen verzögerte Fehler Flush-Befehle Handler Commit Innodb Buffer Pool Bytes Daten Schlüsselblöcke Nicht Gespült Schlüssel Leseanforderungen Schlüssel Schreib Schlüssel Schreibvorgänge Max Ausführungszeit Überschritten Max Verwendete Verbindungen Open Files Performance Schema Konten Lost Prepared Stmt Count Qcache Freie Blöcke

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

Netstat Data Collector

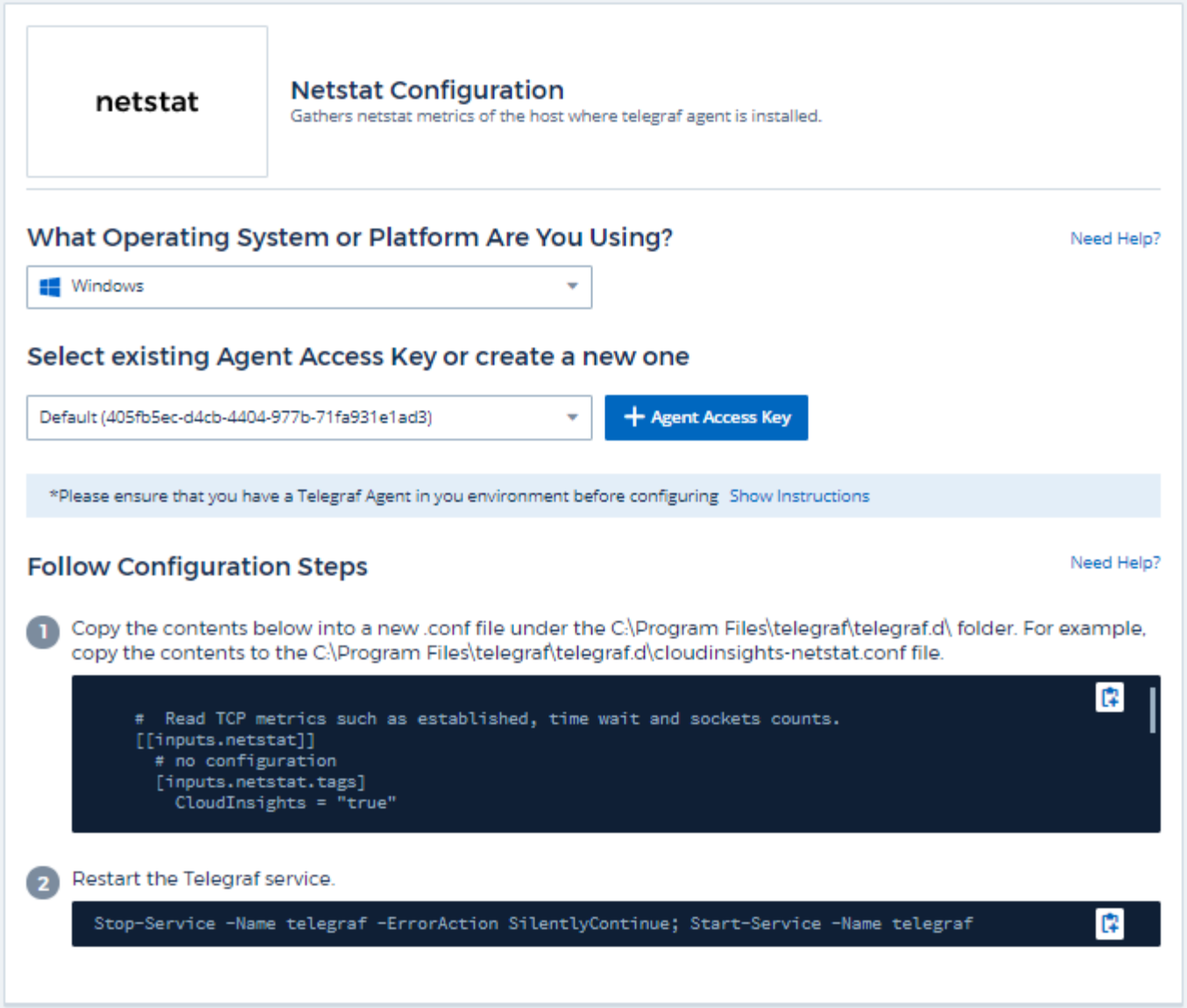
Data Infrastructure Insights verwendet diesen Datensammler, um netstat-Metriken zu erfassen.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Netstat.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Netstat	Node-UUID	Node-IP-Node-Name	

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

Nginx Data Collector

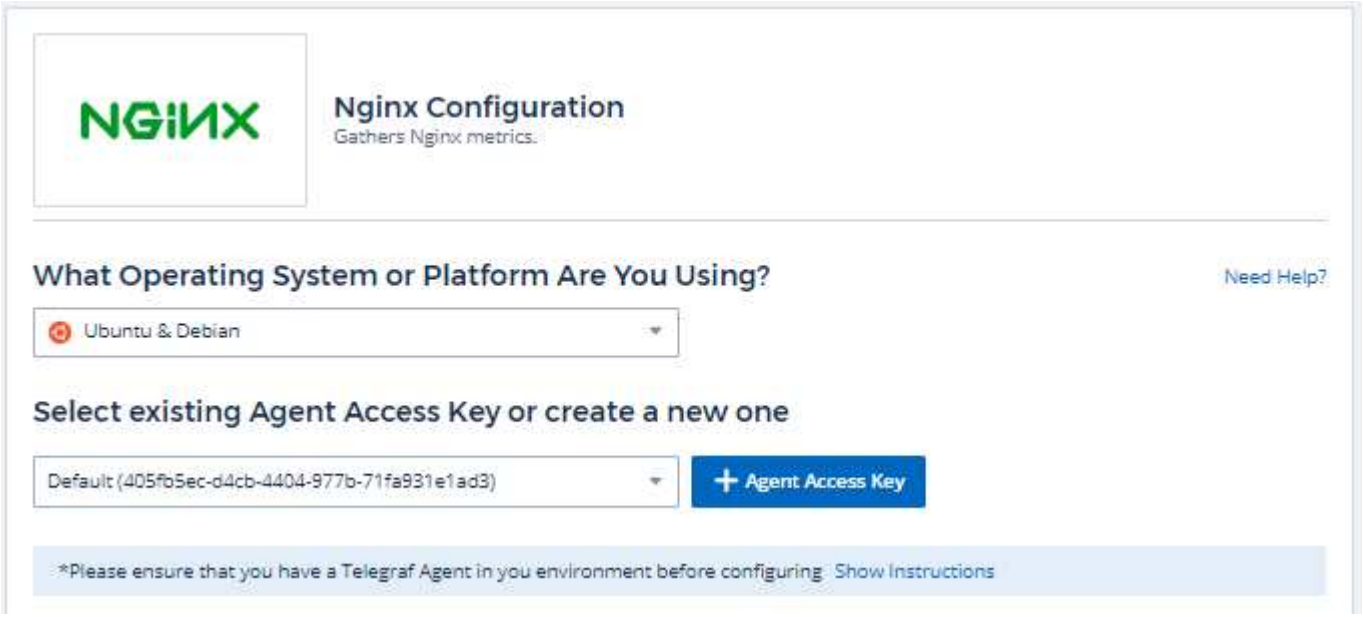
Data Infrastructure Insights verwendet diesen Datensammler, um Kennzahlen von Nginx zu sammeln.

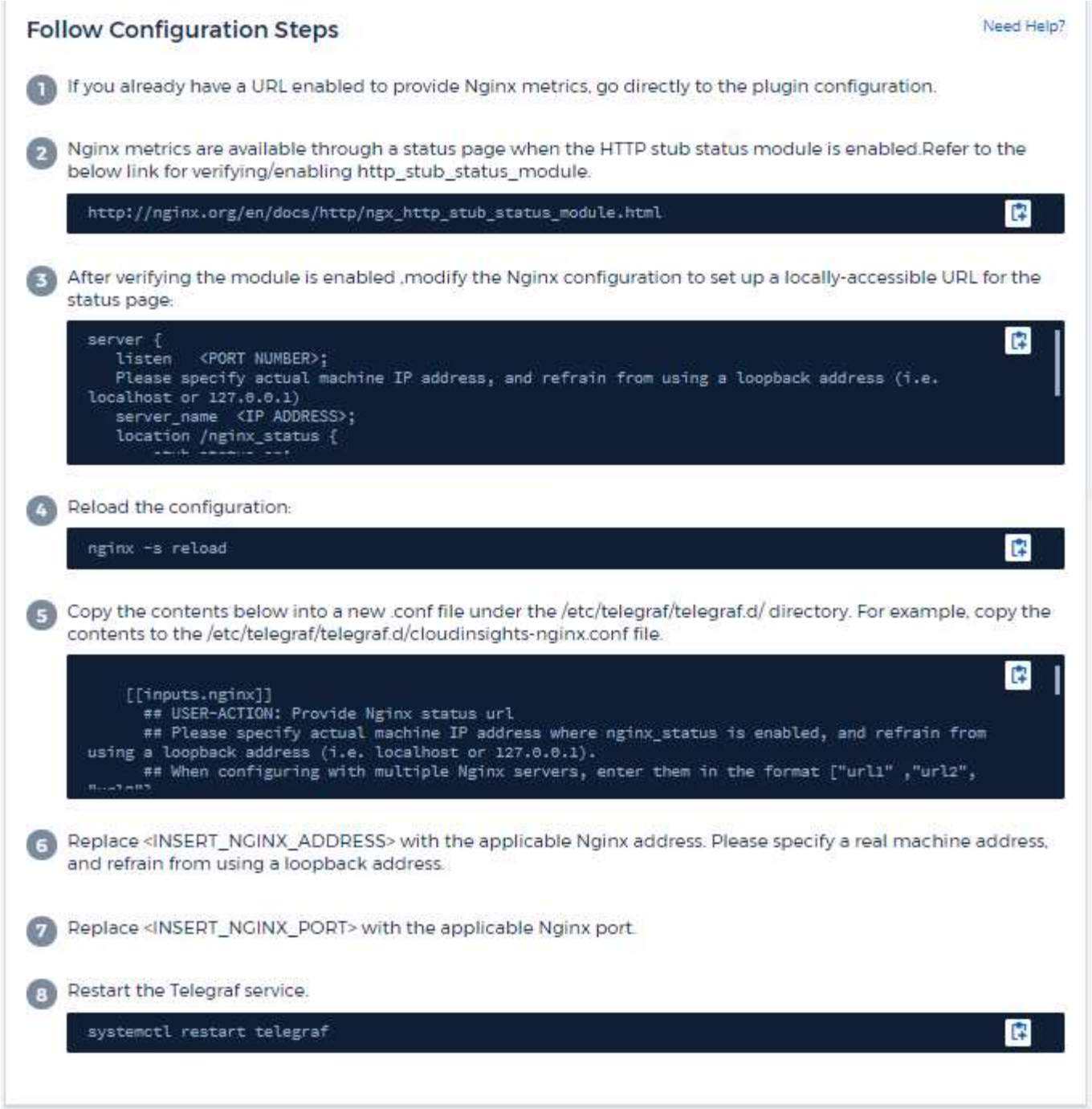
Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Nginx.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.





Einrichtung

Für die Nginx-Metrik muss Nginx "http_stub_Status_Module"aktiviert sein.

Weitere Informationen finden Sie im "Nginx-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Nginx	Namespace-Server	Node-IP-Node-Name-Port	Akzeptiert Aktive Bearbeitet Leseanforderungen, Die Auf Das Schreiben Warten

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

PostgreSQL Data Collector

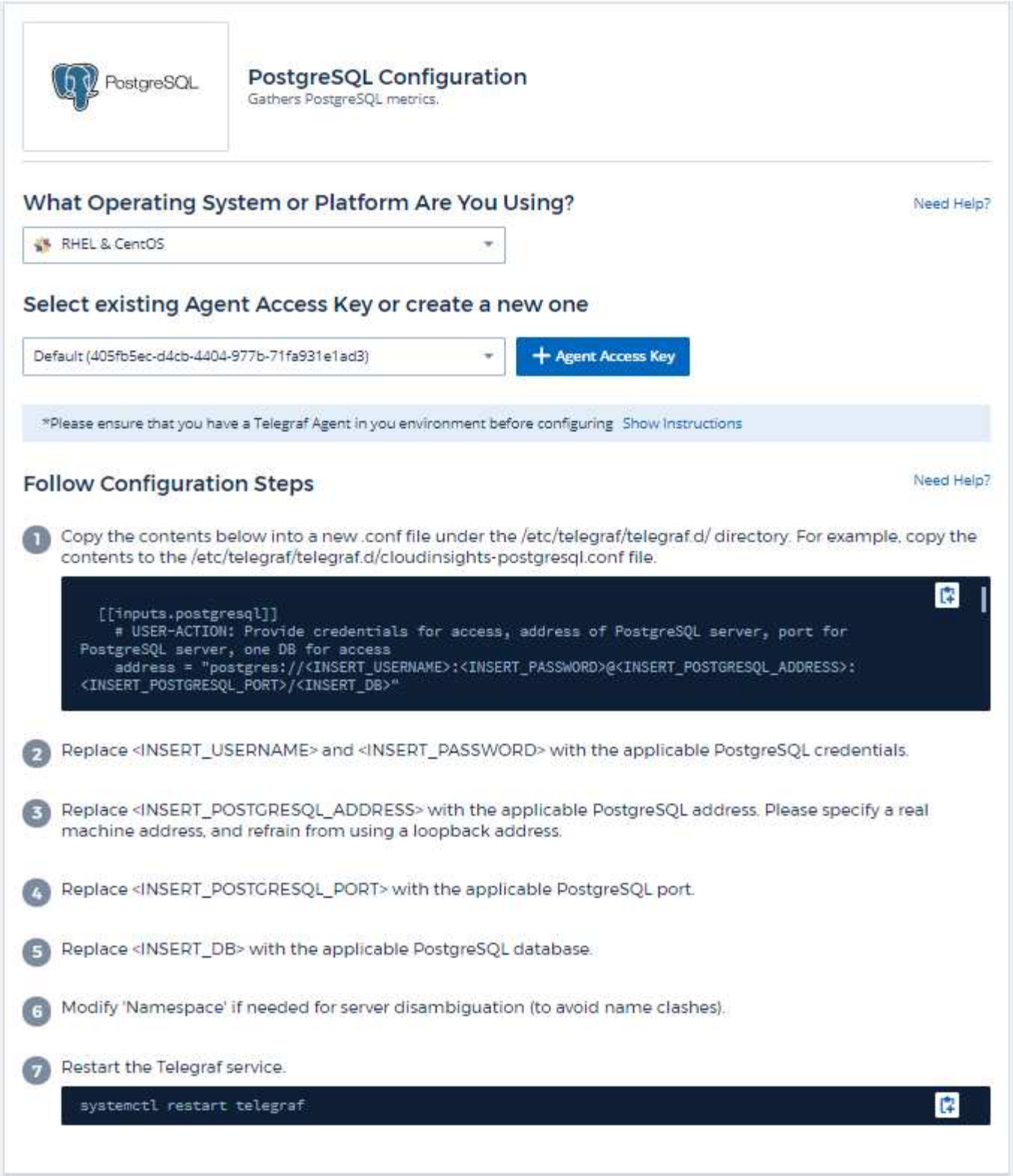
Data Infrastructure Insights nutzt diesen Datensammler, um Metriken aus PostgreSQL zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie PostgreSQL.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie im "PostgreSQL-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
PostgreSQL Server	Namespace-Datenbankserver	Node Name Node-IP	Puffer Zugeordnete Buffers Back-End-Puffer Dateisynchronisation Buffers Checkpoint Puffer Clean Checkpoints Sync Time Checkpoints Write Time Checkpoints Requests Checkpoints Timed Max Geschrieben Sauber
PostgreSQL Datenbank	Namespace-Datenbankserver	Datenbank OID Node Name Node IP	Blöcke Lesezeit Blöcke Write Time Blocks Treffer Blöcke Liest Konflikte Deadlocks Client-Nummer Temp-Dateien Bytes Temp-Dateien Anzahl Zeilen Gelöschte Zeilen Abgeholt Zeilen Zeilenanzahl Zeilenanzahl Zeilenanzahl Zeilenumeinfügen Letzte Transaktionen Letzte Transaktionen Übertragen Rollbacks

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

Puppet Agent Data Collector

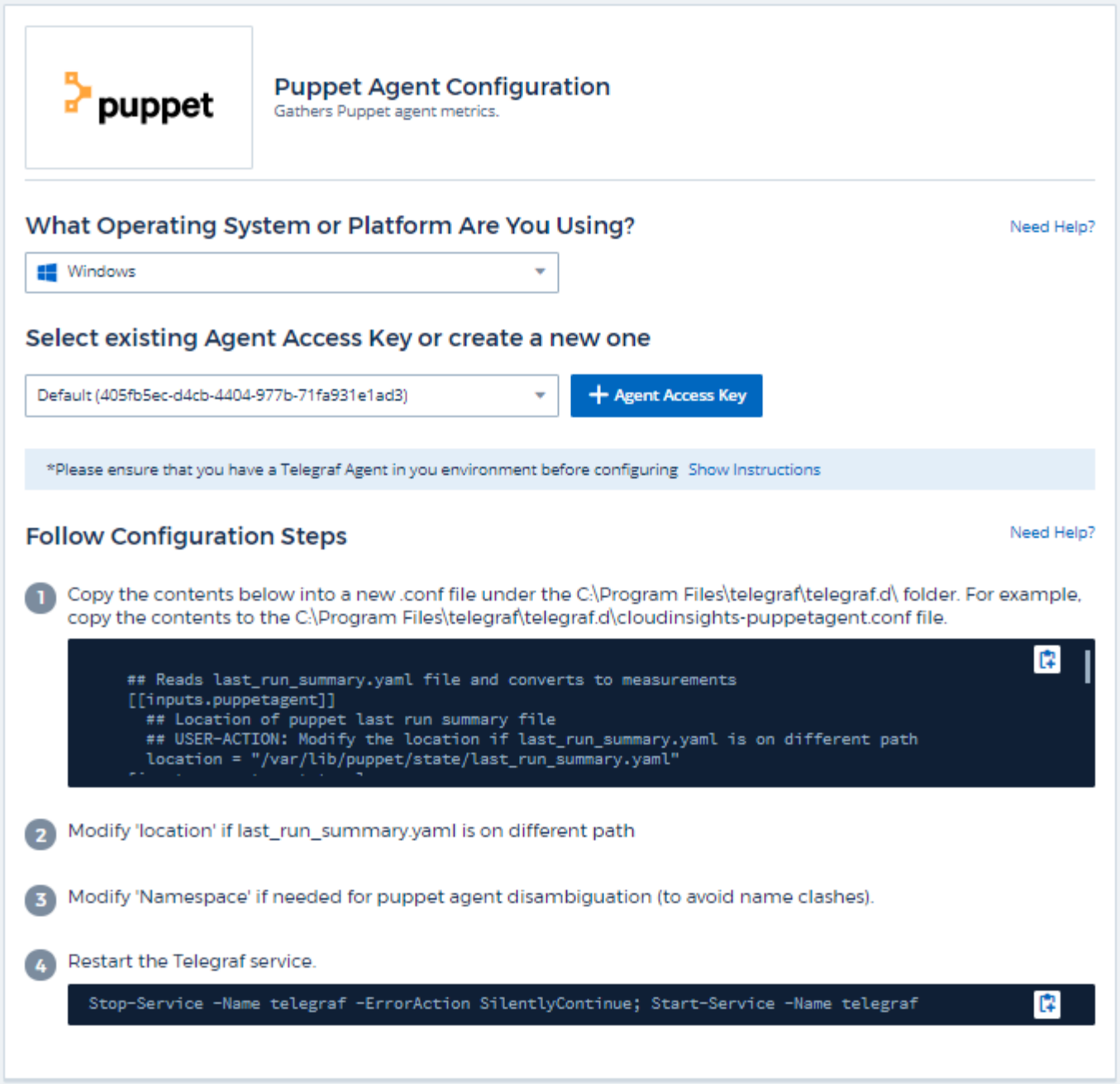
Data Infrastructure Insights nutzt diesen Datensammler, um Kennzahlen von Puppet Agent zu sammeln.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie Puppet.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie im "Puppet-Dokumentation"

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:

Puppet Agent	Namespace-Node-UUID	Node Name Ort Node-IP-Version Konfigstring Version Puppet	Änderungen Total Events Failure Ereignisse Success Events Summe Ressourcen Geänderte Ressourcen Fehlgeschlagen Ressourcen Konnten Nicht Neu Starten Ressourcen Outofsync Ressourcen Neustart Ressourcen Geplante Ressourcen Übersprungene Ressourcen Gesamtzeit Ankerzeit Abruf Configtime Cron Time Exec Time File Time Filebucket Time Lastrun Time Package Time Zeitplanzeit Service Time Sshauorizedkey Time Total Time User

Fehlerbehebung

Weitere Informationen finden Sie auf der "Support" Seite.

Redis Data Collector

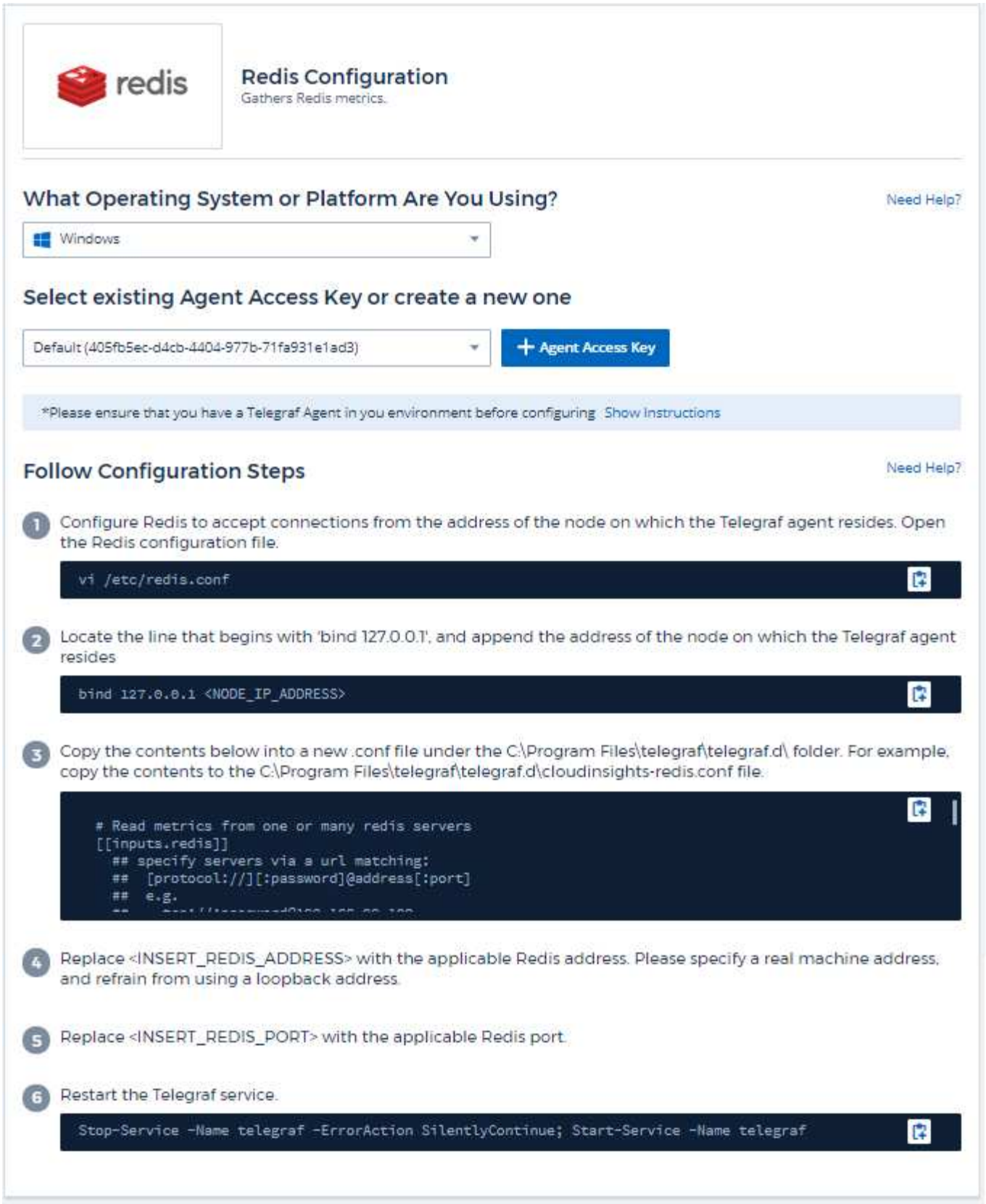
Data Infrastructure Insights nutzt diesen Datensammler, um Kennzahlen von Redis zu sammeln. Redis ist ein Open Source, in-Memory Data Structure Store, der als Datenbank-, Cache- und Nachrichten-Broker verwendet wird und die folgenden Datenstrukturen unterstützt: Strings, Hash-Funktionen, Listen, Sätze und mehr.

Installation

1. Klicken Sie unter **Observability > Collectors** auf **+Data Collector**. Wählen Sie „Redis“.

   Wählen Sie das Betriebssystem oder die Plattform aus, auf dem der Telegraf-Agent installiert ist.

2. Wenn Sie noch keinen Agenten zur Sammlung installiert haben oder einen Agenten für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um die Anweisungen zu erweitern"Agenten-Installation".
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.



Einrichtung

Informationen finden Sie im "Redis-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Redis	Namespace-Server		

Fehlerbehebung

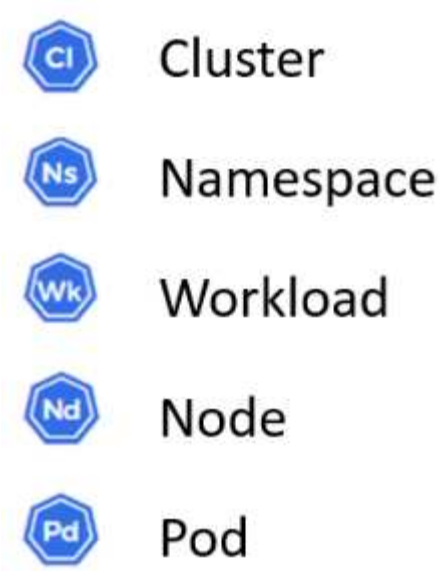
Weitere Informationen finden Sie auf der "Support" Seite.

Objekt Symbol Referenz

In Data Infrastructure Insights verwendete Objektsymbole:

Infrastruktursymbole:

Kubernetes-Symbole:



Symbole für die Kubernetes-Netzwerkleistungsüberwachung und -Zuordnung:

Copyright-Informationen

Copyright © 2025 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 IRGENDEINER 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.