Referenzsupport

Cloud Insights

NetApp
March 30, 2023

Inhaltsverzeichnis

Referenzsupport

Support Wird Angefordert

Sie können auf die Support-Optionen in Cloud Insights zugreifen, indem Sie auf **Hilfe > Support** klicken. Die verfügbaren Support-Optionen hängen davon ab, ob Sie sich im Test- oder Abonnementmodus befinden.

[Support-Seite]

Aktivieren der Supportberechtigung

Cloud Insights bietet Self-Service und E-Mail-Support bei Ausführung im Testmodus. Sobald Sie den Service abonniert haben, wird dringend empfohlen, den Supportanspruch zu aktivieren. Durch die Aktivierung der Supportberechtigung können Sie über den Online-Chat, das Web-Ticketing-System und das Telefon auf den technischen Support zugreifen. Der Standard-Support-Modus ist bis zum Abschluss der Registrierung Self-Service. Siehe "Details" Unten.

Während des ersten Abonnementvorgangs generiert Ihre Cloud Insights Instanz eine 20-stellige NetApp Seriennummer ab der „950“. Diese NetApp Seriennummer steht für das Cloud Insights Abonnement Ihres Kontos. Sie müssen die NetApp Seriennummer registrieren, um die Support-Berechtigung zu aktivieren. Wir bieten zwei Optionen für die Support-Registrierung:

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

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

Schritte

1. Öffnen Sie die Website für die Registrierung von NetApp https://register.netapp.com
2. Wählen Sie „Ich bin bereits als NetApp Kunde registriert“ und wählen Sie *Cloud Insights* als Produktlinie aus. Wählen Sie Ihren Billing Provider (NetApp oder AWS) aus und geben Sie Ihre Seriennummer und Ihren NetApp Abonnementnamen oder Ihre AWS Kunden-ID an. Geben Sie dazu im Menü „Hilfe > Support“ innerhalb der Cloud Insights Benutzeroberfläche Ihre Seriennummer an:

   [SN_Screen]

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

   [Bestehendes Kundenformular]

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 Cloud Insights Seriennummer.

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

Schritte

1. Öffnen Sie die Website für die Registrierung von NetApp https://register.netapp.com
2. Wählen Sie „Ich bin kein registrierter NetApp Kunde“ und füllen Sie die erforderlichen Informationen im folgenden Beispielformular aus:

[Neues Kundenformular]

1. Wählen Sie *Cloud Insights* als Produktlinie aus. Wählen Sie Ihren Billing Provider (NetApp oder AWS) aus und geben Sie Ihre Seriennummer und Ihren NetApp Abonnementnamen oder Ihre AWS Kunden-ID an. Geben Sie dazu im Menü „Hilfe > Support“ innerhalb der Cloud Insights Benutzeroberfläche Ihre Seriennummer an:

   [SN_Screen]

2. Wenn keine Fehler auftreten, wird der Benutzer auf eine Seite „Registrierung erfolgreich übermittelt“ weitergeleitet. Die E-Mail-Adresse, die mit dem NSS SSO-Benutzernamen verbunden ist, der für die Registrierung verwendet wird, erhält innerhalb weniger Stunden eine E-Mail mit der Angabe „Ihr Produkt ist jetzt für Support berechtigt“.
3. Als neuer NetApp Kunde müssen Sie außerdem ein NSS-Benutzerkonto für die zukünftige Registrierung auf der NetApp Support Site erstellen und auf das Support-Portal für den Chat des technischen Supports und die Ticketausstellung im Web zugreifen. Dieser Link befindet sich unter https://mysupport.netapp.com/eservice/public/now.do. Sie können Ihre neu registrierte Cloud Insights Seriennummer angeben, um den Prozess zu beschleunigen.
4. Dies ist eine einmalige Registrierung für die Cloud Insights Seriennummer.

Abrufen Von Support-Informationen

NetApp bietet auf verschiedene Weise Unterstützung für Cloud Insights. Umfassende kostenlose Self-Support-Optionen stehen rund um die Uhr zur Verfügung, wie etwa Knowledgebase-Artikel (KB) oder die NetApp Community. Für Benutzer, die eine der Cloud Insights-Editionen (Basic*, Standard, Premium) abonniert haben, steht der technische Support per Telefon oder Web-Ticketing zur Verfügung. Für Webticket und die Case-Verwaltung ist ein NSS-Konto (NetApp Support Site) erforderlich.

*Der Support ist bei Basic Edition verfügbar, sofern alle NetApp Speichersysteme mindestens auf Premium Support Level abgedeckt sind.

Self-Service-Support:

Diese Support-Optionen sind im Testmodus verfügbar und stehen rund um die Uhr kostenlos zur Verfügung:

- **"Knowledgebase"**

  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"**

  Wenn Sie auf den Community-Link klicken, gelangen Sie zur NetApp Cloud Insights Community, in der sich mit Kollegen und Experten austauschen können.

Es gibt auch einen Link zur Verfügung zu stellen xref:{relative_path}**"Feedback"** Um uns bei der Verbesserung der Cloud Insights zu unterstützen.

Abonnementunterstützung

Wenn Sie über ein Cloud Insights-Abonnement oder einen bezahlten Support für überwachte NetApp Produkte oder Services verfügen, können Sie sich mit einem NetApp Support-Techniker an die oben genannten Self-Support-Optionen wenden, um Ihr Problem zu lösen.

Sie müssen sich registrieren, um Aktivieren Sie den Support Für NetApp Cloud-Produkte. Registrieren Sie sich unter NetApp "Support-Registrierung Für Cloud-Datenservices".

Es wird dringend empfohlen, dieses Kontrollkästchen zu aktivieren, damit ein NetApp Support Engineer während Ihrer Support-Sitzung auf Ihre Cloud Insights Umgebung zugreifen kann. 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 diese Support-Optionen nutzen zu können, benötigen Sie ein aktives Cloud Insights Abonnement:

- "* Telefon*"
- **"Support-Ticket"**
- **Chat** - Sie werden mit dem NetApp Support-Personal in Verbindung stehen (nur an Wochentagen). Der Chat ist in der Menüoption **Hilfe > Live-Chat** oben rechts auf einem beliebigen Cloud Insights-Bildschirm verfügbar.

Sie können auch Unterstützung für den Vertrieb anfordern, indem Sie auf die klicken **"Vertrieb Kontaktieren"** Verlinken:

Die Cloud Insights-Seriennummer wird im Dienst über das Menü * Hilfe > Support* angezeigt. Wenn beim Zugriff auf den Service Probleme auftreten und bereits eine Seriennummer bei NetApp registriert wurde, können Sie sich auch die Seriennummern der Cloud Insights auf der NetApp Support Site wie folgt ansehen:

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

[Support SN anzeigen]

Supportmatrix Für Cloud Insights Data Collector

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

Learning Center

Unabhängig von Ihrem Abonnement **Hilfe > Support** Links zu verschiedenen Kursangeboten der NetApp University, damit Sie den größtmöglichen Nutzen aus Cloud Insights ziehen können. Erfahren Sie mehr darüber!

Supportmatrix Für Cloud Insights Data Collector

Die Supportmatrix für Data Collector enthält eine Referenz für Data Collectors, die von Cloud Insights unterstützt werden, einschließlich Hersteller- und Modellinformationen.

Die Matrix ist im PDF-Format verfügbar.

Klicken Sie zum Öffnen auf den Link. Klicken Sie mit der rechten Maustaste, und wählen Sie *Speichern unter…*, um eine Kopie herunterzuladen.

"* Data Collector Support Matrix*"

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

Cloud Insights erfasst mit dem Amazon EC2 Data Collector Bestands- und Performance-Daten von EC2 Instanzen.

Anforderungen

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

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

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

Konfiguration

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

Feld	Beschreibung
AWS Region	Wählen Sie die Region AWS
IAM-Rolle	Nur zur Verwendung bei Übernahme auf einer AU in AWS. Siehe unten für weitere Informationen über "IAM-Rollen".
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	Sehen Sie sich dies an, um zu überprüfen, ob AWS Sie mit API-Anfragen von Cloud Insights-Umfragen in Rechnung stellt.

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 Cloud Insights die umbenannten Daten möglicherweise nicht erfassen. Es wird empfohlen, die standardmäßigen metrischen Namen zu belassen.

IAM-Zugriffsschlüssel

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

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

IAM-Rolle

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

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

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

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

Weitere Informationen finden Sie in der Amazon-Dokumentation auf "IAM-Rollen".

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

Zuordnen von Amazon Tags zu Cloud Insights-Annotationen

Der Amazon EC2 Data Collector bietet eine Option, mit der Sie Cloud Insights Annotationen mit Tags ausfüllen können, die auf EC2 konfiguriert sind. Die Anmerkungen müssen genau wie die EC2-Tags benannt werden. Cloud Insights wird immer die gleichen Textanmerkungen mit dem gleichen Namen ausfüllen und versucht, Anmerkungen anderer Typen (Nummer, boolescher Wert usw.) am besten auszufüllen. 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 werden die Groß-/Kleinschreibung berücksichtigt, während die Groß-/Kleinschreibung von Cloud Insights nicht berücksichtigt wird. Wenn Sie also eine Annotation mit dem Namen „EIGENTÜMER“ in Cloud Insights und den Tags mit dem Namen „EIGENTÜMER“, „Eigentümer“ und „Eigentümer“ in EC2 erstellen, wird all die EC2-Varianten des „EIGENTÜMERS“ der Annotation von Cloud Insight zugeordnet.

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

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

- Sie müssen jedes Child-Konto so konfigurieren, dass eine AWS Rolle zugewiesen wird, die es der Haupt-Account-ID ermöglicht, über das Children-Konto auf EC2 Details zuzugreifen.
- Für jedes untergeordnete Konto muss der Rollenname mit demselben String konfiguriert sein.
- Geben Sie diese Zeichenfolge für den Rollennamen im Abschnitt Cloud Insights AWS Data Collector **Erweiterte Konfiguration** im Feld * Kontotrole* ein.

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.

Informationen zum Konfigurieren Ihrer Umgebung, damit Cloud Insights von den AWS-Child-Konten erfasst werden kann, finden Sie im folgenden Abschnitt:

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

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

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

Fehlerbehebung

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

Amazon FSX für NetApp ONTAP Datensammler

Dieser Datensammler erfasst Bestands- und Performance-Daten von Amazon FSX für NetApp ONTAP. Dieser Datensammler wird schrittweise in allen Cloud Insights-Servicegebieten zur Verfügung gestellt. Wenden Sie sich an Ihren Vertriebsmitarbeiter, wenn das Symbol für diesen Sammler in Ihrer Cloud Insights-Umgebung nicht angezeigt wird.

Terminologie

Cloud Insights erfasst Bestands- und Performance-Daten des FSX-NetApp Datensammlers. 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	Laufzeit Für Cloud Insights
Cluster	Storage
LUN	Datenmenge

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
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 beziehen Cloud Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Anstelle des Arrays, die dies anbieten, führt Cloud Insights in der Regel eine IOPS-gewichtete Berechnung durch, die aus den Statistiken der einzelnen internen Volumen abgeleitet wird.
- Durchsatz: Aggregiert aus internen Volumes. Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Erstellung programmgesteuert durch die Cloud Insights Datenquelle im Rahmen 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 Administratorkonto haben, das für schreibgeschützte API-Aufrufe konfiguriert ist.
- Zu den Kontodetails gehören Benutzername und Passwort.
- Port-Anforderungen: 80 oder 443

Konfiguration

Feld	Beschreibung
NetApp Management IP	IP-Adresse oder vollqualifizierter Domain-Name des NetApp Clusters

Feld	Beschreibung
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

Fehlerbehebung

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

Inventar

Problem:	Versuchen Sie dies:
Erhalten Sie 401 HTTP-Antwort oder 13003 ZAPI-Fehlercode und ZAPI gibt „unzureichende Berechtigungen“ oder „nicht autorisiert für diesen Befehl“ zurück	Benutzernamen und Kennwort sowie Benutzerrechte/Berechtigungen überprüfen.
ZAPI gibt zurück „Cluster-Rolle ist keine Cluster_Mgmt LIF“	AU muss mit Cluster Management IP sprechen. Überprüfen Sie die IP und wechseln Sie ggf. auf eine andere IP
ZAPI-Befehl schlägt nach dem erneuten Versuch fehl	AU hat ein Kommunikationsproblem mit dem Cluster. Überprüfen Sie Netzwerk, Port-Nummer und IP-Adresse. Der Benutzer sollte auch versuchen, einen Befehl von der Befehlszeile aus dem AU-Rechner auszuführen.
AU konnte über HTTP keine Verbindung mit ZAPI herstellen	Prüfen Sie, ob der ZAPI-Port Klartext akzeptiert. Wenn AU versucht, Klartext an einen SSL-Socket zu senden, schlägt die Kommunikation fehl.

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.

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

Konfigurieren des Azure Compute-Datensammlers

Cloud Insights erfasst mithilfe des Azure Computing-Datensammlers Bestands- und Performance-Daten aus Azure Computing-Instanzen.

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 Cloud Insights-Erkennung 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 Cloud 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

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Broadcom

Datensammler Brocade Network Advisor

Cloud Insights erfasst mithilfe des Brocade Network Advisor Datensammlers Inventar- und Performance-Daten von Brocade Switches.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom Datensammler Brocade Network Advisor. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Switch	Switch
Port	Port

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
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 Cloud Insights-Erfassungseinheit führt Verbindungen zum TCP-Port 443 auf dem BNA-Server ein. BNA-Server muss Version 14.2.1 oder höher ausführen.
- IP-Adresse des Brocade Network Advisor Servers
- Benutzername und Kennwort für ein Administratorkonto
- Port-Anforderung: HTTP/HTTPS 443

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Inventar

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

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

Datensammler Brocade FC Switch

Cloud Insights verwendet die Brocade FC Switch (SSH) Datenquelle, um Inventar für Brocade oder umbenannte Switch-Geräte zu ermitteln, auf denen FOS-Firmware (FOS) 4.2 und höher ausgeführt wird. Geräte werden sowohl im FC-Switch- als auch im Access Gateway-Modus unterstützt.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom Datensammler des Brocade FC Switch. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Switch	Switch
Port	Port
Virtual Fabric, Physische Fabric	Fabric
Zone	Zone
Logischer Switch	Logischer Switch
Virtual Volume	Datenmenge
LSAN-Zone zu erreichen	IVR-Zone

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

Anforderungen

- Die Cloud Insights Acquisition Unit (AU) leitet Verbindungen zum TCP-Port 22 auf Brocade Switches ein, um Bestandsdaten zu erfassen. Die AU wird auch Verbindungen zu UDP Port 161 für die Sammlung von Leistungsdaten initiieren.
- Für alle Switches in der Fabric muss eine IP-Konnektivität vorhanden sein. Wenn Sie das Kontrollkästchen Alle Switches in der Fabric erkennen auswählen, erkennt Cloud Insights alle Switches in der Fabric. Für die Erkennung ist jedoch eine IP-Konnektivität für diese zusätzlichen Switches erforderlich.
- Weltweit ist dasselbe Konto über alle Switches in der Fabric erforderlich. Sie können PuTTY (Open Source Terminal Emulator) verwenden, um den Zugriff zu bestätigen.

- Die Ports 161 und 162 müssen offen sein für alle Switches im Fabric für SNMP-Performance-Abfragen.
- SNMP Read-Only Community String

Konfiguration

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

Erweiterte Konfiguration

Feld	Beschreibung
Fabric-Name	Der Fabric-Name wird vom Data Collector gemeldet. Lassen Sie das Feld leer, um den Fabric-Namen als WWN zu melden.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 15.
Ausgeschlossene Geräte	Kommagetrennte Liste der Geräte-IDs, die von der Abfrage ausgeschlossen werden sollen
Admin-Domänen Aktiv	Wählen Sie, wenn Sie Admin-Domains verwenden
MPR-Daten abrufen	Wählen Sie diese Option aus, um Routing-Daten von Ihrem Multiprotokoll-Router zu erhalten.
Trapping Aktivieren	Wählen Sie diese Option aus, um die Erfassung beim Empfang eines SNMP-Trap vom Gerät zu aktivieren. Wenn Sie Trapping aktivieren auswählen, müssen Sie auch SNMP aktivieren.
Mindestzeit zwischen Traps (s)	Mindestzeit zwischen durch Traps ausgelösten Erfassungsversuchen. Der Standardwert ist 10.
Erkennung aller Switches in der Fabric	Wählen Sie diese Option, um alle Switches in der Fabric zu erkennen
Entscheiden Sie sich für HBA vs Zonenaliase	Wählen Sie, ob HBA- oder Zonenaliasen bevorzugt werden sollen
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.
SNMP-Auth-Protokoll	SNMP-Authentifizierungsprotokoll (nur SNMP v3)

Feld	Beschreibung
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 Cloud Insights, die Zeitüberschreitung „*SSH Banner Wait Timeout“ (sec)* auf einen höheren Wert zu erhöhen.
Fehler: „Cloud Insights hat ungültige Gehäuserolle erhalten“	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.
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.

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

Cisco MDS Fabric Switches Datensammler

Cloud Insights verwendet den Datensammler der Cisco MDS Fabric Switches, um Inventar für Cisco MDS Fabric Switches sowie eine Vielzahl von Cisco Nexus FCoE Switches zu ermitteln, auf denen der FC-Service aktiviert ist.

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

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom Datensammler des Cisco FC Switch. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Switch	Switch
Port	Port
VSAN	Fabric
Zone	Zone
Logischer Switch	Logischer Switch
Name Server-Eintrag	Name Server-Eintrag
Inter-VSAN Routing-Zone (IVR	IVR-Zone

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

Anforderungen

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

Konfiguration

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

Erweiterte Konfiguration

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

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

Fehlerbehebung

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

Inventar

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

Leistung

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

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

Datensammler Cohesity SmartFiles

Dieser REST API-basierte Collector erwirbt einen Cohesity Cluster und ermittelt die „Ansichten“ (als interne Cloud Insights Volumes), die verschiedenen Nodes sowie Performance-Kennzahlen.

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Dell

Datensammler der Dell EMC XC-Serie

Cloud Insights verwendet diesen Datensammler, um Bestands- und Performanceinformationen für die Dell EMC XC-Speicher-Arrays zu ermitteln.

Konfiguration

Feld	Beschreibung
Externe IP-Adresse des Prism	IP-Adresse des XC-Servers
Benutzername	Benutzername für den XC-Server
Passwort	Passwort, das für den XC-Server verwendet wird

Erweiterte Konfiguration

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

Fehlerbehebung

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

Dell EMC

DELL EMC Data Domain-Datensammler

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

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom Data Domain-Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Festplatte	Festplatte
Array Erledigen	Storage
FC-Port	Port
File-System	Internes Volumen
Kontingente	Kontingente
NFS- und CIFS-Freigabe	Dateifreigabe

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

Anforderungen

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

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Konfigurieren des EMC ECS-Datensammlers

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

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

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom 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	Laufzeit Für Cloud Insights
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 der ECS Management Console
- Domain-Konto auf Administratorebene für das ECS-System
- Port 443 (HTTPS): Erfordert eine ausgehende Verbindung zum TCP-Port 443 des ECS-Systems.
- 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
ECS Host	IP-Adresse oder vollqualifizierter Domain-Name des ECS-Systems
ECS-Host-Port	Port, der für die Kommunikation mit ECS Host verwendet wird
ECS Anbieter-ID	Anbieter-ID für ECS
Passwort	Passwort wird für ECS verwendet

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 360 Minuten.

Fehlerbehebung

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

Dell EMC PowerScale Datensammler

Cloud Insights erfasst mithilfe des Dell EMC PowerScale (bisher Isilon) SSH Data Collector Bestands- und Performance-Daten von PowerScale Scale Scale Scale-out NAS Storage.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen von diesem Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Laufwerk	Festplatte
Cluster	Storage
Knoten	Storage-Node
File-System	Internes Volumen

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

Anforderungen

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

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Inventar

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

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

Rest-Datensammler Dell EMC Isilon/PowerScale

Cloud Insights erfasst mithilfe des Dell EMC Isilon/PowerScale REST Data Collector Bestands- und Performance-Daten von Dell EMC Isilon oder PowerScale Storage.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen von diesem Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt.

Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
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

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

Berechtigungsname	Beschreibung	r(Lesen) oder rw (Lesen+Schreiben)
ISI_PRIV_SWIFT	Swift	r
ISI_PRIV_JOB_ENGINE	Job-Engine	r

Konfiguration

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

Erweiterte Konfiguration

Feld	Beschreibung
HTTPS-Port	Der Standardwert ist 8080.
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20.
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300.

Fehlerbehebung

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

Inventar

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

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

Dell EMC PowerStore-Datensammler

Der EMC PowerStore Data Collector sammelt Bestandsdaten aus dem EMC PowerStore-

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

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

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen von diesem Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Host	Host
Host_Volume_Zuordnung	Host_Volume_Zuordnung
Hardware (es hat Laufwerke unter „extra_Details“-Objekt): Laufwerke	Festplatte
Appliance	Storage Pool
Cluster	Storage Array Durchführt
Knoten	StorageNode
fc_Port	Port
Datenmenge	Datenmenge
InternalVolume	File_System

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

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Informationen erforderlich:

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

Konfiguration

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

Erweiterte Konfiguration

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

Die PowerStore Performance-Sammlung von Cloud Insight nutzt die 5-minütigen Granularitätsquelldaten von PowerStore. Beispielsweise fragt Cloud Insights alle fünf Minuten nach diesen Daten ab. Dies ist nicht konfigurierbar.

Fehlerbehebung

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

Dell EMC RecoverPoint Data Collector

Der primäre Anwendungsfall des EMC RecoverPoint Data Collector ist die Ermittlung von Replikationsbeziehungen zwischen Volumes, die von der RecoverPoint-Speicher-Appliance unterstützt werden. Dieser Sammler entdeckt auch das RecoverPoint-Gerät selbst. Bitte beachten Sie, dass Dell/EMC eine VMware Backup-Lösung für VMs--„RecoverPoint for VMs“ verkauft, die von diesem Collector nicht unterstützt wird

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

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

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Informationen erforderlich:

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

DELL EMC ScaleIO Datensammler

Der ScaleIO Datensammler erfasst Inventarinformationen aus dem ScaleIO Storage. Für die Konfiguration benötigt dieser Datensammler die ScaleIO Gateway-Adresse und einen Admin-Benutzernamen und ein Passwort.

Terminologie

Cloud Insights erhält die folgenden Bestandsinformationen vom ScaleIO Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
MDM-Cluster (Meta Data Manager	Storage
SDS (ScaleIO 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 Gateway(s)	IP-Adressen oder FQDNs von ScaleIO-Gateways, getrennt durch Komma (,) oder Semikolon (;)

Feld	Beschreibung
Benutzername	Administratorbenutzername zur Anmeldung beim ScaleIO-Gerät
Passwort	Passwort zur Anmeldung beim ScaleIO-Gerät

Erweiterte Konfiguration

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

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

Fehlerbehebung

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

Konfigurieren des EMC Unity Data Collector

DER DELL EMC Unity (ehemals VNXe)-Datensammler bietet Bestandsunterstützung für VNXe Unified Storage-Arrays. Cloud 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 Inventarisierung. Fibre Channel-Volumes werden erkannt, Cloud Insights erstellt jedoch keine Berichte über FC-Zuordnung, Maskierung oder Storage-Ports.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom Datensammler Unity. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Festplatte	Festplatte

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Storage Array Durchführt	Storage
Prozessor	Storage-Node
Storage-Pool	Storage-Pool
Allgemeine iSCSI-Block-Informationen, 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“	* Überprüfen Sie die korrekte IP-Adresse, den Benutzernamen und das Kennwort * Bestätigen Sie, dass Unisphere CLI auf der Cloud Insights-Erfassungseinheit installiert ist * Bestätigen Sie, dass das Installationsverzeichnis der Unisphere CLI in der Datasource-Konfiguration korrekt ist. * Bestätigen Sie, dass die IP-Adresse der VNXe in der Konfiguration der Datenquelle korrekt ist. Öffnen Sie in der Cloud Insights Acquisition Unit einen CMD, und wechseln Sie in das konfigurierte Installationsverzeichnis: €{INSTALLDIR. Versuchen Sie, eine Verbindung zum VNXe-Gerät herzustellen, indem Sie Folgendes eingeben: Uemcli -d <Ihre IP> -U <Ihre ID> /sys/General show

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

Datensammler der Dell EMC VMAX- und PowerMax-Gerätefamilie

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

Anforderungen

Bevor Sie diese Datensammlung konfigurieren, sollten Sie sicherstellen, dass Cloud Insights über eine TCP-Verbindung zu Port 2707 auf dem vorhandenen Solutions Enabler-Server verfügt. Cloud Insights erkennt alle Symmetrix-Arrays, die auf diesem Server „lokal“ sind, wie in der Ausgabe der „symcfg-Liste“ dieses Servers zu sehen ist.

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

SMI-S (auch bekannt als „ECOM“) vorgesehen. Sie erhalten ein Login-Popup.

- Berechtigungen müssen in der Daemon-Konfigurationsdatei des Solutions Enabler Servers deklariert werden, die üblicherweise hier zu finden ist: */var/symapi/config/daemon_Users*

  Hier ist eine Beispieldatei mit den richtigen Cisys Berechtigungen.

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

Terminologie

Cloud Insights erfasst die folgenden Bestandsinformationen aus der Datenquelle EMC VMAX/PowerMax. 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	Laufzeit Für Cloud Insights
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 Cloud Insights-Datensammler ignoriert.

Feld	Beschreibung
Name Des Service	Dienstname wie in der Datei *netcnfg* angegeben

Feld	Beschreibung
Vollständiger Pfad zur CLI	Vollständiger Pfad zu dem Ordner, der die Symmetrix CLI enthält
SMI-S-Host-IP-Adresse	IP-Adresse des SMI-S-Hosts

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40 Minuten.
Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben	Geben Sie an, ob die unten aufgeführte Array-Liste beim Sammeln von Daten aufgenommen oder ausgeschlossen werden soll.
Bestandsfilter Geräteliste	Kommagetrennte Liste der Geräte-IDs, die einbezogen oder ausgeschlossen werden sollen
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 das Cloud Insights-Verhalten nicht in Bezug auf die Arrays, die durch die Ausgabe "symcfg list" als REMOTE aufgeführt werden. Cloud Insights erfasst Daten nur auf 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.

Feld	Beschreibung
SMIS-Port überschreiben	Wenn Sie leer sind, verwenden Sie den Standardport im Feld Verbindungstyp. Andernfalls geben Sie den zu verwendenden Anschluss ein
SMI-S-Benutzername	Benutzername für den SMI-S Provider Host
SMI-S-Passwort	Benutzername für den SMI-S Provider Host
Leistungsintervall (Sek.)	Intervall zwischen Performance-Abstimmungen (standardmäßig 1000 Sekunden)
hoose 'exclude' oder 'include', um eine Liste anzugeben	Geben Sie an, ob die unten aufgeführte Array-Liste beim Erfassen von Performancedaten einbezogen oder ausgeschlossen werden soll
Geräteliste Für Leistungsfilter	Kommagetrennte Liste der Geräte-IDs, die einbezogen oder ausgeschlossen werden sollen

Fehlerbehebung

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

Problem:	Versuchen Sie dies:
Fehler: Die angeforderte Funktion ist derzeit nicht lizenziert	Installieren Sie die SYMAPI-Serverlizenz.
Fehler: Es wurden keine Geräte gefunden	Stellen Sie sicher, dass Symmetrix-Geräte vom Solutions Enabler-Server verwaltet werden: - Führen Sie die symcfg-Liste -V aus, um die Liste der konfigurierten Symmetrix-Geräte anzuzeigen.
Fehler: Ein angeforderter Netzwerkdienst wurde in der Servicedatei nicht gefunden	Stellen Sie sicher, dass der Solutions Enabler Service Name die netcnfg-Datei für Solutions Enabler definiert hat. Diese Datei befindet sich in der Regel unter SYMAPI\config\ in der Installation des Solutions Enabler-Clients.
Fehler: Die Handshake des Remote-Clients/Servers ist fehlgeschlagen	Überprüfen Sie die letzten speichersrvd.log*-Dateien auf dem Solutions Enabler-Host, den wir zu entdecken versuchen.
Fehler: Allgemeiner Name im Clientzertifikat ungültig	Bearbeiten Sie die Datei *Hosts* auf dem Solutions Enabler-Server, damit der Hostname der Acquisition Unit wie in der storsrvd.log auf dem Solutions Enabler-Server angegeben auf der IP-Adresse auflöst.
Fehler: Die Funktion konnte keinen Speicher abrufen	Stellen Sie sicher, dass genügend freier Speicherplatz im System vorhanden ist, um Solutions Enabler auszuführen
Fehler: Solutions Enabler konnte nicht alle erforderlichen Daten bereitstellen.	Untersuchen Sie den Integritätsstatus und das Lastprofil von Solutions Enabler

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

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

Datensammler Dell EMC VNX Block Storage (NaviCLI

Cloud Insights verwendet den Dell EMC VNX Block Storage (NaviSec) Data Collector (ehemals CLARiiON), um Bestands- und Performancedaten zu erfassen.

Terminologie

Cloud Insights erfasst die folgenden Bestandsinformationen vom Datensammler EMC VNX Block Storage. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

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

Syntax der Navisphere Befehlszeilenschnittstelle

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Inventar

Problem:	Versuchen Sie dies:
Fehler: • Agent wird nicht ausgeführt • konnte naviseccli • keinen Befehl ausführen	• Bestätigen Sie, dass Navisphere CLI auf der Cloud Insight Acquisition Unit installiert ist • Sie haben die Option „Secure Client verwenden“ im Data Collector-Konfigurationsassistenten nicht ausgewählt und verfügen nicht über eine nicht sichere Version der Navisphere CLI. • Bestätigen Sie, dass das Installationsverzeichnis Navisphere CLI in der Konfiguration des Datensammlers korrekt ist • Bestätigen Sie, dass die IP des VNX-Blockspeichers in der Konfiguration des Datensammlers korrekt ist: • Von der Cloud Insights-Erfassungseinheit: - Öffnen Sie einen CMD. - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis - Versuchen Sie, eine Verbindung mit dem VNX Block-Speicher-Gerät herzustellen, indem Sie „navicli -h {ip} getagent“ eingeben (ersetzen Sie die {ip} durch die tatsächliche IP)
Fehler: 4.29 emc235848 emc241018 getall konnte keine Host-Alias-Info analysieren	Dies wird wahrscheinlich durch eine FLARE 29-Fehlerproblematik der Host-Initiator-Datenbank auf dem Array selbst verursacht. Siehe EMC Knowledge Base Artikel: Emc235848, emc241018. Sie können auch prüfen https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128
Fehler: Die Meta-LUNs können nicht abgerufen werden. Fehler beim Ausführen von java -jar navicli.jar	• Ändern Sie die Konfiguration des Datensammlers, um den sicheren Client zu verwenden (empfohlen) • Installieren von navicli.jar im CLI-Pfad zu navicli.exe ODER NaviSECCLI.exe • Hinweis: navicli.jar ist veraltet ab EMC Navisphere Version 6.26 • die Version navicli.jar ist unter Umständen verfügbar http://powerlink.emc.com
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 in der Regel durch die Aktualisierung der Firmware auf dem VNX-Block-Speicher-Gerät verursacht, aber nicht 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). • Stellen Sie sicher, dass das Gerät und der Host beide identische Versionen der Software ausführen: - Öffnen Sie von der Cloud Insights-Erfassungseinheit ein Befehlszeilenfenster - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis - Verbinden Sie mit dem CLARiiON-Gerät, indem Sie “navicli -h €{ip} getagent“ eingeben - suchen Sie nach der Versionsnummer auf den ersten paar Zeilen. Beispiel: „Agent Rev: 6.16.2 (0.1)“ - Suche nach und vergleiche die Version in der ersten Zeile. Beispiel: „Navisphere CLI Revision 6.07.00.04.07“
Fehler: Nicht Unterstützte Konfiguration - Keine Fibre-Channel-Ports	Das Gerät ist nicht mit Fibre-Channel-Ports konfiguriert. Aktuell werden nur FC-Konfigurationen unterstützt. Überprüfen Sie, ob diese Version/Firmware unterstützt wird.

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

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

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

Terminologie

Cloud Insights erfasst die folgenden Bestandsinformationen vom VNX File Data Collector. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Celerra Network Server/Celerra Storage-Pool	Storage-Pool
File-System	Internes Volumen
Data Mover	Controller
Auf einem Data Mover gemountet	Dateifreigabe
CIFS- und NFS-Exporte	Share
Festplatten-Volume	Back-End LUN

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

Anforderungen

Sie benötigen Folgendes, um diesen Datensammler zu konfigurieren:

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

Konfiguration

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

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (Minuten)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20 Minuten.

Fehlerbehebung

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

Inventar

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

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

Konfigurieren des Dell EMC VNX Unified Data Collectors

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

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen von diesem Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

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

Anforderungen

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

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

Konfiguration

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

Erweiterte Konfigiration

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

Fehlerbehebung

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

Konfigurieren des EMC VPLEX-Datensammlers

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

Für die Performance-Erfassung durch VPLEX-Cluster von Cloud Insights muss der Performance-Archivierungsservice betriebsbereit sein, um die CSV-Dateien und Protokolle aufzufüllen, die Cloud 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 Abfrage, ob alle erwarteten Dateien vorhanden sind und ob sie ordnungsgemäß aktualisiert werden. Wenn sie fehlen oder veraltet sind, protokolliert Cloud Insights Ausfälle bei der Performance-Erfassung.

Terminologie

Cloud Insightst erwirbt die folgenden Bestandsinformationen vom VPLEX 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	Laufzeit Für Cloud Insights
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
ITLS	Back-End-Pfad

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

Anforderungen

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

- Für die Leistung ist Port 22 erforderlich.

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Inventar

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

Leistung

Problem:	Versuchen Sie dies:
Fehler: VPLEX-Performance für Version unter 5.3 wird nicht unterstützt.	Aktualisieren Sie VPLEX auf 5.3 oder höher

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

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

Dell EMC XtremeIO-Datensammler

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

Anforderungen

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

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

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom EMC XtremIO Data Collector. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Festplatte (SSD)	Festplatte
Cluster	Storage
Controller	Storage-Node
Datenmenge	Datenmenge
LUN-Zuordnung	Volume-Zuordnung

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Ziel-FC-Initiator	Volume-Maske

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

Anforderungen

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Fujitsu ETERNUS Datensammler

Der Fujitsu ETERNUS-Datensammler erfasst Bestandsdaten über administrativen Zugriff auf das Speichersystem.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom Fujitsu ETERNUS Storage. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Festplatte	Festplatte
Storage	Storage
Thin Pool, Flexible Tier Pool, Raid-Gruppe	Storage-Pool
Standard-Volume, Snap Data Volume (SDV), Snap Data Pool Volume (SDPV), Thin Provisioning Volume (TPV), Flexible Tier Volume (FTV), Wide Striping Volume (WSV)	Datenmenge
Channel-Adapter	Controller

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

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

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

Konfiguration

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

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 20 Minuten.

Fehlerbehebung

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

Inventar

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

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

NetApp Google Compute Data Collector

Dieser Datensammler unterstützt Inventar- und Performance-Erfassung aus Google Compute Cloud-Plattformkonfigurationen. Dieser Sammler wird versuchen, alle Computing-Ressourcen in allen Projekten innerhalb einer Google-Organisation zu entdecken. Wenn Sie mehrere Google-Organisationen haben, die Sie mit Cloud Insights entdecken möchten, möchten Sie einen Cloud Insights-Collector pro Organisation bereitstellen.

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

HP Enterprise

HP Enterprise Alletra 9000 / Primera Storage Datensammler

Cloud Insights verwendet den Datensammler HP Enterprise Alletra 9000/HP Enterprise Primera (zuvor 3PAR), um Inventar und Performance zu ermitteln.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen von diesem Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ 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 Datenkolletors sind folgende Voraussetzungen erforderlich:

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Inventar

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

Leistung

Problem:	Versuchen Sie dies:
Verbindung oder Anmeldung fehlgeschlagen. Fehler bei der Initialisierung des Providers.	Ein Name eines rein numerischen Arrays kann Probleme mit dem SMI-S-Server verursachen. Versuchen Sie, den Namen des Arrays zu ändern.
Der konfigurierte SMI-S-Benutzer verfügt über keine Domäne	Gewähren Sie dem konfigurierten SMI-S-Benutzer entsprechende Domänenberechtigungen
Laut Cloud Insights kann die Verbindung zum SMI-S-Dienst nicht hergestellt/angemeldet werden.	Vergewissern Sie sich, dass es keine Firewall zwischen der CI AU und dem Array gibt, die die CI AU daran versperren würde, TCP-Verbindungen zu 5988 oder 5989 zu machen. Sobald das geschehen ist, und wenn Sie bestätigt haben, dass es keine Firewall gibt, sollten Sie SSH auf das Array, und verwenden Sie den "showcim" Befehl zu bestätigen. Überprüfen Sie, dass: * Dienst aktiviert ist * HTTPS-Port sollte 5989 sein. Wenn alle diese sind, können Sie versuchen, „stopcim“ und dann ein „startcim“, um den CIM neu zu starten (d.h. SMI-S-Service).

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

HP Enterprise Command View-Datensammler

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

Terminologie

Cloud Insights erfasst die folgenden Bestandsinformationen vom Datensammler HP Enterprise Command View. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
PDEV	Festplatte
Journalpool	Festplattengruppe
Storage Array Durchführt	Storage
Port Controller	Storage-Node
Array-Gruppe, DP-Pool	Storage-Pool

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
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 Exportwerkzeug (Export.exe) muss in die Cloud 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 Cloud Insights AU installiert.
- Netzwerkanforderungen
  - Die Exportwerkzeuge sind Java-basiert und verwenden RMI, um mit dem Array zu sprechen. Diese Tools sind möglicherweise nicht für die Firewall geeignet, da sie auf jedem Aufruf dynamisch die Quell- und Ziel-TCP-Ports aushandeln können. Außerdem verhalten sich die Export-Tools der verschiedenen Modell-Arrays im Netzwerk möglicherweise unterschiedlich - Fragen Sie HPE nach den Anforderungen Ihres Modells

Konfiguration

Feld	Beschreibung
Command View Server	IP-Adresse oder vollqualifizierter Domain-Name des Command View Servers
Benutzername	Benutzername für den Command View Server.
Passwort	Passwort, das für den Command View-Server verwendet wird.

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

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Inventar

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

Leistung

Problem:	Versuchen Sie dies:
Fehler: * Fehler beim Ausführen des Exportdienstprogramms * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass Exportdienstprogramm auf der Cloud Insights-Erfassungseinheit installiert ist * Bestätigen Sie, dass der Speicherort des Exportdienstprogramms in der Konfiguration des Datensammlers korrekt ist * Bestätigen Sie, dass die IP des USP/R600-Arrays in der Konfiguration des Datensammlers korrekt ist. * Bestätigen Sie den Benutzernamen Und das Passwort ist in der Konfiguration des Datensammlers korrekt. * Bestätigen Sie, dass die Version des Exportdienstprogramms mit der Microcode-Version des Speicherarrays * von der Cloud Insights-Erfassungseinheit kompatibel ist, öffnen Sie eine CMD-Eingabeaufforderung und gehen Sie wie folgt vor: - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis - Versuchen Sie, eine Verbindung mit dem konfigurierten Speicher-Array herzustellen, indem Sie die Batch-Datei runWin.bat ausführen
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

Problem:	Versuchen Sie dies:
Fehler: Exportwerkzeuge protokolliert "Zeitbereich für Überwachung nicht abrufen".	* Bestätigung der Leistungsüberwachung auf dem Array ist aktiviert. * Versuchen Sie, die Exportwerkzeuge außerhalb von Cloud Insights zu aktivieren, um zu bestätigen, dass das Problem außerhalb von Cloud 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 Speicher-Navigator Modular CLI auf der Cloud Insights-Erfassungseinheit installiert ist * Bestätigen Sie, dass der modulare Speicher-CLI-Standort in der Datenerfassungs-Konfiguration korrekt ist * Bestätigen Sie, dass die IP des WMS/SMS/SMS-Arrays in der Konfiguration des Datensammlers korrekt ist * Bestätigen Dass Speicher-Navigator Modular CLI-Version mit einer Mikrocode-Version des Speicherarrays kompatibel ist, die im Datensammler * von der Cloud Insights-Erfassungseinheit konfiguriert ist, öffnen Sie eine CMD-Eingabeaufforderung und gehen Sie wie folgt vor: - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis - Versuchen Sie, eine Verbindung mit dem konfigurierten Speicher-Array herzustellen, indem Sie den folgenden Befehl „auunitref.exe“ ausführen.
Fehler: Konfigurationsfehler: Speicher-Array wird vom Inventory nicht gemeldet	Überprüfen Sie, ob Speicher-Array in Frage im Command View-Server konfiguriert ist
Fehler: * Kein Array ist beim Speicher Navigator Modular 2 CLI registriert * Array ist nicht bei der Speicher Navigator Modular 2 CLI registriert * Konfigurationsfehler: Speicher-Array nicht bei StorageNavigator Modular CLI registriert	* Eingabeaufforderung öffnen und Verzeichnis auf den konfigurierten Pfad ändern * Ausführen des Befehls „set=STONAVM_HOME=.“ * Ausführen des Befehls „auunitref“ * Bestätigen Sie, dass die Befehlsausgabe Details des Arrays mit IP * enthält. Wenn die Ausgabe nicht die Array-Details enthält, registrieren Sie das Array mit Storage Navigator CLI: - Eingabeaufforderung öffnen und Verzeichnis auf den konfigurierten Pfad ändern - Befehl „set=STONAVM_HOME= ausführen.“ - Ausführen des Befehls „auunitaddAuto -ip €{ip}“. Ersetzen Sie{ip} durch echtes IP

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

HPE Alletra 6000 Datensammler

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

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen von diesem Sammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
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 NimbleOS hat sich für Volumes entwickelt, und alle Statistiken Cloud Insights Berichte wurden aus den Statistiken zu Volumes abgeleitet

Konfiguration

Feld	Beschreibung
Array-Management-IP-Adresse	Vollständig qualifizierter Domain-Name (FQDN) oder Array-Management-IP-Adresse.

Feld	Beschreibung
Benutzername	Benutzername für das Array
Passwort	Kennwort für das Array

Erweiterte Konfiguration

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

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

Hitachi Data Systems (Hds)

Datensammler der Hitachi Vantara Command Suite

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

Terminologie

Cloud Insights erfasst die folgenden Bestandsinformationen vom Datensammler der Hitachi Vantara Command Suite. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
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:

    Cloud Insights ist ein starker Standpunkt, um eine doppelte Zählung von Kapazität bei allen Kosten zu vermeiden. 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 Cloud Insights sowohl die zugrunde liegenden RAID Gruppen als auch die Pools gemeldet hat, würde die Summe ihrer Bruttokapazität die Summe der Festplatten deutlich übersteigen.

  Stattdessen reduziert der Datensammler der Cloud Insights HDS Command Suite die Größe von RAID-Gruppen willkürlich um die Kapazität von Pool Volumes. Dies kann dazu führen, dass Cloud Insights die RAID-Gruppe überhaupt nicht meldet. Darüber hinaus werden alle resultierenden RAID-Gruppen so gekennzeichnet, dass sie in der Cloud Insights WebUI nicht sichtbar sind, doch fließen sie in das Cloud Insights Data Warehouse (DWH). 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 Exportwerkzeug (Export.exe) muss in die Cloud Insights AU kopiert werden.
  - Die Version des Exportwerkzeugs muss mit der Microcode-Version des Ziel-Arrays übereinstimmen.
- AMS-Leistung:
  - NetApp empfiehlt: Erstellen eines dedizierten Servicekontos auf AMS Arrays für Cloud Insights zum Abrufen von Performance-Daten. Storage Navigator ermöglicht nur ein Benutzerkonto, das gleichzeitig mit dem Array angemeldet ist. Wenn Cloud Insights dasselbe Benutzerkonto wie Verwaltungsskripte oder HiCommand verwendet, kann dies dazu führen, dass Cloud Insights, Verwaltungsskripte oder HiCommand aufgrund der Eins-Grenze für gleichzeitige Benutzerkontoanmeldedaten nicht mit dem Array kommunizieren kann
  - Performance Monitor muss lizenziert sein.
  - Das CLI-Dienstprogramm Storage Navigator Modular 2 (SNM2) muss auf der Cloud Insights AU installiert sein.

Konfiguration

Feld	Beschreibung
HiCommand Server	IP-Adresse oder vollqualifizierter Domänenname des HiCommand Device Manager-Servers

Feld	Beschreibung
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.

Leistung

Problem:	Versuchen Sie dies:
Fehler: * Fehler beim Ausführen des Exportdienstprogramms * Fehler beim Ausführen des externen Befehls	* Bestätigen Sie, dass Exportdienstprogramm auf der Cloud Insights-Erfassungseinheit installiert ist * Bestätigen Sie, dass der Speicherort des Exportdienstprogramms in der Konfiguration des Datensammlers korrekt ist * Bestätigen Sie, dass die IP des USP/R600-Arrays in der Konfiguration des Datensammlers korrekt ist. * Bestätigen Sie den Benutzernamen Und das Passwort ist in der Konfiguration des Datensammlers korrekt. * Bestätigen Sie, dass die Version des Exportdienstprogramms mit der Microcode-Version des Speicherarrays * von der Cloud Insights-Erfassungseinheit kompatibel ist, öffnen Sie eine CMD-Eingabeaufforderung und gehen Sie wie folgt vor: - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis - Versuchen Sie, eine Verbindung mit dem konfigurierten Speicher-Array herzustellen, indem Sie die Batch-Datei runWin.bat ausführen
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

Problem:	Versuchen Sie dies:
Fehler: Exportwerkzeuge protokolliert "Zeitbereich für Überwachung nicht abrufen".	* Bestätigung der Leistungsüberwachung auf dem Array ist aktiviert. * Versuchen Sie, die Exportwerkzeuge außerhalb von Cloud Insights zu aktivieren, um zu bestätigen, dass das Problem außerhalb von Cloud 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 Speicher-Navigator Modular CLI auf der Cloud Insights-Erfassungseinheit installiert ist * Bestätigen Sie, dass der modulare Speicher-CLI-Standort in der Datenerfassungs-Konfiguration korrekt ist * Bestätigen Sie, dass die IP des WMS/SMS/SMS-Arrays in der Konfiguration des Datensammlers korrekt ist * Bestätigen Dass Speicher-Navigator Modular CLI-Version mit einer Mikrocode-Version des Speicherarrays kompatibel ist, die im Datensammler * von der Cloud Insights-Erfassungseinheit konfiguriert ist, öffnen Sie eine CMD-Eingabeaufforderung und gehen Sie wie folgt vor: - Ändern Sie das Verzeichnis in das konfigurierte Installationsverzeichnis - Versuchen Sie, eine Verbindung mit dem konfigurierten Speicher-Array herzustellen, indem Sie den folgenden Befehl „auunitref.exe“ ausführen.
Fehler: Konfigurationsfehler: Speicher-Array wird vom Inventory nicht gemeldet	Überprüfen Sie, ob Speicher-Array in Frage im HiCommand-Server konfiguriert ist
Fehler: * Kein Array ist beim Speicher Navigator Modular 2 CLI registriert * Array ist nicht bei der Speicher Navigator Modular 2 CLI registriert * Konfigurationsfehler: Speicher-Array nicht bei StorageNavigator Modular CLI registriert	* Eingabeaufforderung öffnen und Verzeichnis auf den konfigurierten Pfad ändern * Ausführen des Befehls „set=STONAVM_HOME=.“ * Ausführen des Befehls „auunitref“ * Bestätigen Sie, dass die Befehlsausgabe Details des Arrays mit IP * enthält. Wenn die Ausgabe nicht die Array-Details enthält, registrieren Sie das Array mit Storage Navigator CLI: - Eingabeaufforderung öffnen und Verzeichnis auf den konfigurierten Pfad ändern - Befehl „set=STONAVM_HOME= ausführen.“ - Ausführen des Befehls „auunitaddAuto -ip €{ip}“. Ersetzen Sie{ip} durch echtes IP

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

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. Cloud Insights unterstützt die Erkennung von NFS- und CIFS-Freigaben, Dateisystemen (interne Volumes) und Spannungs (Storage-Pools).

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom HNAS-Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Ebene	Festplattengruppe
Cluster	Storage
Knoten	Storage-Node
Span	Storage-Pool
Systemlaufwerk	Back-End Lun
File System	Internes Volumen

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

Anforderungen

- IP-Adresse des Geräts
- Port 22, SSH-Protokoll
- Benutzername und Passwort - Berechtigungsebene: Supervisor
- Hinweis: Dieser Datensammler ist SSH-basiert, also muss die AU, die auf dem HNAS selbst SSH-Sitzungen auf TCP 22 oder auf der Systemverwaltungseinheit (SMU) initiieren können, mit der das Cluster verbunden ist.

Konfiguration

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

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 30 Minuten.

Fehlerbehebung

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

Inventar

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

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

Datensammler Hitachi Ops Center

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

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen von diesem Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
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

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Host-Gruppen	Volume-Zuordnung und -Maskierung
Volume-Paare	Storage-Synchronisierung

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

Inventaranforderungen

Zur Erfassung von Bestandsdaten müssen Sie Folgendes haben:

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

Performance-Anforderungen erfüllt

Zur Erfassung von Leistungsdaten müssen die folgenden Anforderungen erfüllt sein:

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

Konfiguration

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

Erweiterte Konfiguration

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

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

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

Infiniat InfiniBox Datensammler

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

Terminologie

Cloud Insights erwirbt folgende Bestandsinformationen vom Datensammler Infiniat InfiniBox. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Storage-Pool	Storage-Pool
Knoten	Controller
Dateisystem	Internes Volumen
Dateisystem	Dateifreigabe
Dateisystem-Exporte	Share

Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration dieses Datensammlers.

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

Konfiguration

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

Erweiterte Konfiguration

Feld	Beschreibung
TCP-Port	TCP-Port zur Verbindung mit InfiniBox-Server. Der Standardwert ist 443.

Feld	Beschreibung
Abfrageintervall Für Bestand	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60 Minuten.

Fehlerbehebung

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

Huawei OceanStor Datensammler

Cloud Insights verwendet den Datensammler Huawei OceanStor (REST/HTTPS), um Inventar und Performance für Huawei OceanStor und OceanStor Dorado Storage zu ermitteln.

Terminologie

Cloud Insights erwirbt die folgenden Bestands- und Leistungsinformationen vom Huawei OceanStor. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Storage-Pool	Storage-Pool
File-System	Internes Volumen
Controller	Storage-Node
FC-Port (zugeordnet)	Volume-Zuordnung
Host FC Initiator (zugeordnet)	Volume-Maske
NFS/CIFS-Freigabe	Share
ISCSI-Link-Ziel	ISCSI-Ziel-Node
ISCSI-Link-Initiator	ISCSI-Initiator-Node
Festplatte	Festplatte
LUN	Datenmenge

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Anforderungen erforderlich:

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

IBM

IBM Cleversafe Datensammler

Cloud Insights verwendet diese Datensammlung, um Bestands- und Performancedaten für IBM Cleversafe Speichersysteme zu ermitteln.

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

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom IBM Cleversafe Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Storage-Pool	Storage-Pool
Container	Internes Volumen
Container	Dateifreigabe
NFS-Share	Share

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

Anforderungen

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

IBM CS Datensammler

Cloud Insights verwendet diese Datensammlung, um Bestands- und Performance-Daten für IBM CS Storage-Systeme zu ermitteln.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom IBM CS Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Storage-Pool	Storage-Pool
Container	Internes Volumen
Container	Dateifreigabe
NFS-Share	Share

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen

Datensammler möglicherweise nicht alle Fälle dar.

Anforderungen

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Datensammler der IBM System Storage DS8000-Serie

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

DS3xxx-, DS4xxx- und DS5xxx-Geräte werden von unterstützt "NetApp E-Series Datensammler". Sie finden in der Cloud Insights Supportmatrix weitere Informationen zu unterstützten Modellen und Firmware-Versionen.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom IBM DS Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Festplattenmodul	Festplatte

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
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
- Auf der Cloud Insights AU installierte Software von Drittanbietern: IBM *dscli*
- Zugriffsvalidierung: Führen Sie die Befehle *dscli* mit dem Benutzernamen und Passwort aus
- Port-Anforderungen: 80, 443 und 1750

Konfiguration

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

Erweiterte Konfiguration

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

Feld	Beschreibung
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 zu kommunizieren https://${ip}:8452/DS8000/Console. Ersetzen Sie die €{ip} durch die konfigurierte IP-Adresse des Datensammlers.
Fehler: * Programm kann nicht ausgeführt werden * Fehler beim Ausführen des Befehls	* Von der Cloud Insights-Erfassungseinheit Öffnen Sie eine CMD * Öffnen Sie CLI.CFG-Datei im Home Directory/lib von CLI und überprüfen Sie die Eigenschaft JAVA_INSTALL, bearbeiten Sie den Wert entsprechend Ihrer Umgebung * Anzeigen Sie die auf diesem Computer installierte Java-Version, und geben Sie Folgendes ein: „java -Version“ * Ping die IP-Adresse des im CLI-Befehl angegebenen IBM-Speichergeräts wurde ausgegeben. * Wenn alle oben genannten gut funktioniert haben, dann führen Sie manuell einen CLI-Befehl aus

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

Konfigurieren des IBM PowerVM-Datensammlers

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

Terminologie

Cloud Insights erfasst Inventarinformationen 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	Laufzeit Für Cloud Insights
Hdisk	Virtuelles Laufwerk
Managed System	Host
LPAR, VIO Server	Virtual Machine

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Volume-Gruppe	Datastore
Physisches Volume	LUN

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

Anforderungen

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

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

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

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

Konfiguration

Feld	Beschreibung
IP-Adresse für Hardware Management Console (HMC)	IP-Adresse oder vollqualifizierter Domänenname der PowerVM Hardware Management Console
HMC-Benutzer	Benutzername für die Hardware Management Console
Passwort	Kennwort, das für die Hardware-Verwaltungskonsole verwendet wird

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20 Minuten.
SSH-Port	Port, der für SSH zu PowerVM verwendet wird

Feld	Beschreibung
Passwort	Kennwort, das für die Hardware-Verwaltungskonsole verwendet wird
Anzahl Wiederholungen	Anzahl der Versuche für einen erneuten Versuch in der Bestandsaufnahme
Geräte Ausschließen	Kommagetrennte Liste von Geräte-IDs oder zu schließenden Anzeigenamen

Fehlerbehebung

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

Konfigurieren des IBM SAN Volume Controller-Datensammlers

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

Die Liste der unterstützten Geräte umfasst Modelle wie SVC, v7000, v5000 und v3700. In der Cloud Insights Supportmatrix finden Sie weitere Informationen zu unterstützten Modellen und Firmware-Versionen.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom IBM SVC Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Laufwerk	Festplatte
Cluster	Storage
Knoten	Storage-Node
Mdisk-Gruppe	Storage-Pool
Vdisk	Datenmenge
Mdisk	Back-End-LUNs und -Pfade

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

Inventaranforderungen

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

Performance-Anforderungen Erfüllt

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

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

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

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

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

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

Konfiguration des IBM XIV/A9000 Datensammlers

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

Terminologie

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
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.
- Unter folgendem Link finden Sie Informationen zur Erstellung eines Kontos für die SMI-S-Performance-Sammlung: http://publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp?topic=%2Fcom.ibm.tpc_V41.doc%2Ffqz0_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

Feld	Beschreibung
Vollständiger Pfad zu XIV CLI Directory	Vollständiger Pfad zum Ordner mit der XIV CLI
SMI-S-Host-IP-Adresse	IP-Adresse des SMI-S-Hosts

Erweiterte Konfiguration

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

Fehlerbehebung

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

Lenovo Datensammler

Cloud Insights ermittelt mit dem Lenovo Datensammler Bestands- und Performancedaten für Lenovo HX-Speichersysteme.

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

Anforderungen

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Microsoft

Konfigurieren des Azure NetApp Files-Datensammlers

Cloud Insights erfasst mit dem Azure NetApp Files Datensammler Bestands- und Performancedaten.

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 Cloud Insights-Erkennung 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 Cloud 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

Feld	Beschreibung
Ich verstehe, dass Microsoft mir API-Anforderungen in Rechnung stellt	Überprüfen Sie dies, um zu überprüfen, ob Microsoft Ihnen die durch eine Insight-Umfrage gestellten API-Anforderungen abrechnungen aufstellt.

Erweiterte Konfiguration

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

Fehlerbehebung

- Die von Ihrem ANF-Datensammler verwendeten Anmeldedaten dürfen keinen Zugriff auf Azure-Abonnements haben, die ANF-Volumes enthalten.
- Wenn der Zugang zum Reader dazu führt, dass die Leistensammlung fehlschlägt, versuchen Sie, den Zugriff auf Mitarbeiter auf Ressourcengruppenebene zu gewähren.

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

Microsoft Hyper-V Datensammler

Der Microsoft Hyper-V Datensammler erfasst Bestands- und Performancedaten aus der virtualisierten Server Computing-Umgebung.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom Microsoft Hyper-V (WMI). Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Virtuelle Festplatte	Virtuelles Laufwerk
Host	Host
Virtual Machine	Virtual Machine
Cluster Shared Volumes (CSV), Partition Volume	Datastore
Internet SCSI-Gerät, Multi Path SCSI LUN	LUN
Fibre Channel-Port	Port

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

Anforderungen

Zur Konfiguration dieses Datensammlers sind folgende Voraussetzungen erforderlich:

- Für die Hyper-V muss Port 5985 geöffnet sein, damit Daten erfasst und Remote-Zugriff/-Management erfolgen können.

- IP-Adresse des Knoten der Clustering-Gruppe
- Lokaler Administrator-Benutzer und Passwort auf dem Hypervisor
- Benutzerkonto auf Administratorebene
- Windows Management Instrumentation (WMI)-Befehl, der Standard, der von Windows installiert wird.
- 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 auf jedem Gast mehr Daten für Cloud Insights zur Verfügung stellen. 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
IP-Adresse des physischen Hosts	Die IP-Adresse oder der vollqualifizierte Domänenname für den physischen Host (Hypervisor).
Benutzername	Administrator-Benutzername für den Hypervisor
Passwort	Kennwort für den Hypervisor
NT-Domäne	Der von den Nodes im Cluster verwendete DNS-Name

Erweiterte Konfiguration

Feld	Beschreibung
Abfrageintervall für Bestand (min)	Der Standardwert ist 20 Minuten.

Fehlerbehebung

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

NetApp

NetApp Cloud Connection für ONTAP 9.9 oder höher

Dieser Datensammler erstellt eine Cloud-Verbindung, um Daten aus ONTAP 9.9+ CVO, AFF und FAS zu erfassen.

Dieser Datensammler ist "Veraltet" Stand: 1. Januar 2023. Informationen zum Übergang zur AU-basierten Datenerfassung finden Sie im "Knowledgebase".

Konfiguration

Cloud Insights sammelt Daten von ONTAP 9.9+ über eine **Cloud-Verbindung**, sodass keine externe Erfassungseinheit installiert werden muss. Dies vereinfacht die Fehlerbehebung, die Wartung und die Erstbereitstellung. Zur Konfiguration der Cloud-Verbindung für den ONTAP 9.9+-Datensammler müssen Sie einen **Pairing-Code** auf den ONTAP-System-Manager kopieren, der dann eine Verbindung zu Ihrer Cloud Insights-Umgebung herstellen wird. Nachdem die Verbindung hergestellt wurde, sind die erfassten Daten identisch mit denen, wenn sie über eine Akquisitionseinheit gesammelt wurden.

Dieser Datensammler unterstützt ONTAP 9.9+ CVO, AFF und FAS.

[Konfiguration Von Cloud Agent Data Collector]

Führen Sie die folgenden Schritte aus, um die Verbindung zu konfigurieren:

- Erstellen Sie ein eindeutiges Token, das zur Herstellung der Verbindung zum ONTAP-System verwendet wird.
- Kopieren Sie den Pairing Code, der das Token enthält. Sie können den Kopplungscode anzeigen, indem Sie auf *[+] Code Snippet* aufdecken.

  Sobald Sie den Kopplungscode kopiert haben, wird auf dem Konfigurationsbildschirm des Datensammlers ein Schritt 6 angezeigt, in dem Sie aufgefordert werden, auf den Verbindungsaufbau zu warten. Auf diesem Bildschirm muss erst die Verbindung hergestellt werden.

  [Warten auf Verbindung]

- Melden Sie sich auf der neuen Registerkarte „Browser“ beim ONTAP System Manager an, und navigieren Sie zu „*Cluster* > *Einstellungen* > *Cloud-Verbindungen*“.
- Klicken Sie auf *Cloud-Verbindung hinzufügen* und fügen Sie den Kopplungscode ein.
- Kehren Sie zur Registerkarte Cloud Insights-Browser zurück, und warten Sie, bis die Verbindung hergestellt ist. Sobald er eingerichtet ist, wird eine Schaltfläche *complete* angezeigt.
- Klicken Sie Auf *Complete*.

Fehlerbehebung

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

Problem:	Versuchen Sie dies:
Ich sehe den folgenden Fehler beim Versuch, sich mit Azure CVO zu verbinden: „Die Anfrage zum Signieren des Zertifikats an den Broker/Manager CA Service wurde nicht abgeschlossen.“	Vergewissern Sie sich, dass die Proxy-Einstellungen Ihres Cloud Manager auf die private IP-Adresse von Cloud Manager festgelegt sind. Für die Installation von Cloud Manager kann ein anderer Proxy festgelegt werden. Sobald der Proxy auf die richtige IP gesetzt ist und Sie den Proxy im Dialogfeld Cloud Connector referenzieren, sollte die Verbindung zu Cloud Insights erfolgreich hergestellt werden.

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

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	Überprüfen Sie, ob Cloud Insights die erweiterten Metriken aus der folgenden Liste erfasst.

Fehlerbehebung

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

NetApp Cloud Volumes Services für AWS Data Collector

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Problem:	Versuchen Sie dies:
Ich habe einen ähnlichen Fehler wie dieser erhalten: 'Anfrage konnte nicht ausgeführt werden: Verbinden mit <AWS region endpoint>:8080 [<AWS region endpoint>/AWS Region Endpunkt IP>] fehlgeschlagen: Verbindungszeitlimit: GET https://<AWS FQDN des regionalen Endpunkts>:8080/v1/Speicher/IPRanges HTTP/1.1'	Der "Proxy" Die von Cloud Insights zur Kommunikation mit der Erfassungseinheit verwendete Verbindung kommuniziert nicht zwischen Cloud Insights und dem Data Collector selbst. Hier sind einige Dinge, die Sie versuchen können: Stellen Sie sicher, dass die Erfassungseinheit in der Lage ist, den fqdn aufzulösen und den erforderlichen Port zu erreichen. Vergewissern Sie sich, dass kein Proxy erforderlich ist, um den angegebenen Endpunkt in der Fehlermeldung zu erreichen. Curl kann verwendet werden, um die Kommunikation zwischen der Akquisitionseinheit und dem Endpunkt zu testen. Stellen Sie sicher, dass Sie für diesen Test **nicht** einen Proxy verwenden. Beispiel: Root@acquitionunit# curl -s -H Accept:Application/json -H "Inhaltstyp: Anwendung/json" -H API-Schlüssel:<api key used in the data collector credentials -H secret-key:<secret key used in the data collector credentials> -X GET https://<AWS Regionaler Endpunkt>:8080/v1/Speicher/IPRanges Siehe dies "NetApp KB-Artikel".

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

NetApp Config Advisor Datensammler

Dieser Datensammler erfasst Konfigurationsdaten von Storage-Systemen, auf denen ONTAP ausgeführt wird, und verbundene Switches mit schreibgeschützten Anrufen. Dieser Datensammler führt außerdem Konfigurationsänderungen und Zustandsprüfungen auf dem gesamten Stack der ONTAP Cluster-Konfiguration durch, um Kabel-, Konfigurations-, Resiliency-, Verfügbarkeits- und Sicherheitsprobleme zu identifizieren.

Dieser Datensammler ist "Veraltet".

Terminologie

Cloud Insights erfasst Konfigurationsdaten von ONTAP und Switches mit dem Config Advisor Data Collector. 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	Laufzeit Für Cloud Insights
Festplatte	Festplatte
Switch	Switch
Cluster	Storage
Knoten	Storage-Node
Aggregat	Storage-Pool
LUN	Datenmenge
Datenmenge	Internes Volumen

Beachten Sie außerdem, dass die Config Advisor-Kennzahlen über das *netapp_ontap.configAdvisor*-Tag im Dashboard und anderen Anfragen zur Verfügung stehen.[Dropdown-Liste mit dem Kennzahlenschild für configAdvisor]

Config Advisor-Terminologie

Die folgenden Begriffe gelten für Objekte oder Referenzen, die Sie auf Config Advisor Dashboards finden können.

Zusammenfassung Des Geräts

- 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.
- Gerätetyp/Typ – Typ des Geräts in der Datenquelle – Storage Controller/Switch
- Anbieter/Untertyp – derselbe Anbietername, den Sie sehen würden, ob 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.
- Hostname: Hostname(s) wie in der Datenquelle konfiguriert.
- Version – Version des Betriebssystems oder der Firmware.

Regelergebnisse

- Regel – eine Prüfung, die mit dem System ausgeführt wird, die Abweichungen der Konfiguration von empfohlenen Methoden analysiert oder bekannte Probleme identifiziert.
- Regelname – Kurzname für die Regel oder Prüfung, die ausgeführt wird.
- Regel-ID – Kennung für die Regel.

- Ziel – Komponente, auf die die Regel angewendet wird. Es handelt sich hierbei um einen Cluster-Namen, einen Node-Namen oder einen Switch-Namen.
- Auswirkungen – Auswirkungen des Risikos auf das System. Die Wirkungsgrade werden wie unten aufgeführt
  - Hohe Auswirkungen: Potenzielle Verluste beim Datenzugriff oder längerer Verlust von Node-Redundanz
  - Mittlere Auswirkungen: Performance-Verschlechterung oder kurzfristiger Verlust von Node-Redundanz
  - Low Impact: Szenarien mit geringen Auswirkungen
  - Best Practice: Abweichungen von dokumentierten Best Practices
- Beschreibung – kurze Beschreibung des Fehlers.
- Details – ausführliche Beschreibung des Fehlers, der die betroffenen Komponenten auflistet
  - Empfehlungen – Links zu KB-Artikeln oder zur NetApp Dokumentation mit zusätzlichen Details zum Risiko oder zur Problembehebung

Anforderungen

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

- Sie müssen Zugriff auf ein Administratorkonto haben, das für schreibgeschützten Zugriff für SSH- und ONTAPi-Anrufe auf ONTAP konfiguriert ist.
- Sie müssen Zugriff auf ein Administratorkonto haben, das für schreibgeschützten Zugriff auf SSH-Anrufe auf Switches konfiguriert ist, wenn diese Teil der Sammlung sind
- Zu den Kontodetails gehören Benutzername und Passwort. Optional kann der private SSH-Schlüssel übergeben werden, wenn ONTAP für die SSH-Schlüsselauthentifizierung oder Multi-Faktor-Authentifizierung (MFA) konfiguriert ist
- Port-Anforderungen: 22, 80 oder 443
- Kontoberechtigungen:
  - Lesen Sie den einzigen Rollennamen in ssh oder/und ontapi-Anwendung auf den Standard-Vserver
  - Administratorkonto mit mindestens schreibgeschütztem Zugriff auf Switches

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
Aktivieren Sie MFA für ONTAP	Aktivieren Sie diese Option, um die Multi-Faktor-Authentifizierung bei ONTAP zu aktivieren

Privater SSH-Schlüssel	Fügen Sie den Inhalt des privaten SSH-Schlüssels ein, wenn ONTAP eine SSH-Schlüsselauthentifizierung oder MFA verwendet
Verbindungstyp	Wählen Sie HTTP (Standardport 80) oder HTTPS (Standardport 443). Die Standardeinstellung ist HTTPS
ONTAP SSH-Port	Ermöglicht die Angabe eines benutzerdefinierten SSH-Ports für die ONTAP-Verbindung
Switch-SSH-Port	Ermöglicht die Angabe eines benutzerdefinierten SSH-Ports für die Switch-Verbindung
Abfrageintervall (min)	Der Standardwert ist 1440 Minuten oder 24 Stunden. Kann mindestens 60 Minuten einstellen

Unterstützte Betriebssysteme

Config Advisor kann auf folgenden Betriebssystemen ausgeführt werden. Wenn Collector auf einer Erfassungseinheit installiert ist, in der das Betriebssystem nicht in dieser Liste enthalten ist, würden Sammlungen fehlschlagen.

- Windows 10 (64 Bit)
- Windows 2012 R2 Server (64 Bit)
- Windows 2016 Server (64 Bit)
- Windows 2019 Server (64 Bit)
- Red hat Enterprise Linux (RHEL) 7.7 und höher (64 Bit)
- Ubuntu 14.0 und höher

Support und Video

In den folgenden Videos erfahren Sie, wie Sie den Data Collector installieren und mithilfe von Dashboards Config Advisor in Cloud Insights optimal nutzen.

Installieren und Konfigurieren des Datensammlers:

[] | *Installing and Configuring the Config Advisor data collector*

Erstellen eines Config Advisor Dashboards:

[] | *Using dashboards to view Config Advisor data*

Anderer Support

Öffnen Sie bei anderen Fragen im Zusammenhang mit Config Advisor über das Config Advisor-Tool ein Ticket, indem Sie auf Hilfe → Support-Ticket öffnen klicken.

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

Datensammler der NetApp ONTAP Datenmanagement-Software

Diese Datensammlung erfasst Bestands- und Performancedaten von Storage-Systemen

mit ONTAP unter Verwendung von schreibgeschützten API-Aufrufen eines ONTAP-Kontos. Dieser Datensammler erstellt auch einen Datensatz in der Cluster-Anwendungsregistrierung, um den Support zu beschleunigen.

Terminologie

Cloud Insights erfasst Bestands- und Performancedaten des ONTAP Datensammlers. 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	Laufzeit Für Cloud Insights
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 beziehen Cloud Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Anstelle des Arrays, die dies anbieten, führt Cloud Insights in der Regel eine IOPS-gewichtete Berechnung durch, die aus den Statistiken der einzelnen internen Volumen abgeleitet wird.
- Durchsatz: Aggregiert aus internen Volumes. Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Erstellung programmgesteuert durch die Cloud Insights Datenquelle im Rahmen der Bestandsberichterstattung.

Storage-Pool

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

Storage-Node

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

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

Anforderungen

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

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

Konfiguration

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

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	Wählen Sie HTTP (Standardport 80) oder HTTPS (Standardport 443). Die Standardeinstellung ist HTTPS
Kommunikations-Port Überschreiben	Geben Sie einen anderen Port an, wenn Sie den Standardwert nicht verwenden möchten
Abfrageintervall für Bestand (min)	Der Standardwert ist 60 Minuten.
Für TLS für HTTPS	TLS nur als Protokoll bei Verwendung von HTTPS zulassen
Netzgruppen Automatisch Suchen	Aktivieren Sie die automatische Suche der Netzgruppe nach den Regeln für die Exportrichtlinie
Netzgruppenerweiterung	Erweiterungsstrategie Für Netzgruppen: Wählen Sie_file_ oder_Shell_. Der Standardwert ist *shell*.
HTTP-Lesezeit Sekunden	Der Standardwert ist 30

Feld	Beschreibung
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.

Ein Hinweis zu Berechtigungen

Da eine Reihe von Cloud Insights ONTAP Dashboards auf erweiterte ONTAP-Zähler angewiesen sind, müssen Sie im Abschnitt Data Collector Advanced Configuration **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 Cloud Insights auf Cluster-Ebene zu erstellen, melden Sie sich mit dem Cluster Management Administrator-Benutzernamen/Passwort 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
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
```

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.

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.

Leistung

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

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

NetApp 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

Cloud Insights erwirbt die folgenden Bestandsinformationen vom NetApp 7-Mode 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:

Dieser Datensammler ist "Veraltet".

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Festplatte	Festplatte
Raid-Gruppe	Festplattengruppe
Filer	Storage
Filer	Storage-Node
Aggregat	Storage-Pool
LUN	Datenmenge
Datenmenge	Internes Volumen

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

Anforderungen

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

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

Konfiguration

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

Erweiterte Konfiguration

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

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

Storage-Systemverbindung

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

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

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

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

- Mit den folgenden Befehlen werden die Fähigkeiten der Benutzerrolle definiert:
  - „api-*“: Nutzen Sie diese, um Cloud Insights die Ausführung aller NetApp Storage-API-Befehle zu ermöglichen.

    Dieser Befehl ist erforderlich, um das ZAPI zu verwenden.

  - „login-http-admin“: Hiermit kann Cloud Insights über HTTP eine Verbindung mit dem NetApp Storage herstellen. Dieser Befehl ist erforderlich, um das ZAPI zu verwenden.
  - „Security-API-vfiler“: Nutzen Sie dies, um Cloud Insights zu ermöglichen, NetApp Storage API Befehle auszuführen, um vFiler Einheitsinformationen 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 über die folgende Berechtigung auf dem Gerät verfügt: • API-* • cli-date • cli-df • cli-ifconfig • cli-lun • cli-Operations • cli-rdfile • cli-Snap • Login-http-admin • Security-API-vfiler prüfen Sie auch, ob die ONTAP-Version von Cloud Insights unterstützt wird und überprüfen Sie, ob die verwendeten Anmeldedaten 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.
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.

Problem:	Versuchen Sie dies:
Socket-Zeitüberschreitungsfehler mit ZAPI	Prüfen Sie die Filer-Konnektivität und/oder erhöhen Sie die Zeitüberschreitung.
„C-Modus-Cluster werden nicht durch den 7-Mode-Datenquelle unterstützt“-Fehler	Überprüfen Sie die IP und ändern Sie die IP in ein 7-Mode-Cluster.
Fehler „Verbindung zum vFiler konnte nicht hergestellt werden“	Überprüfen Sie, ob die Fähigkeiten des Erwerbs von Benutzern mindestens folgende Fähigkeiten enthalten: api-* Security-API-vfiler Login-http-admin Bestätigen Sie, dass Filer mindestens ONTAPI Version 1.7 läuft.

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

NetApp E-Series Datensammler

Die NetApp E-Series Datensammlung sammelt Bestands- 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	Laufzeit Für Cloud Insights
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 beziehen Cloud Insights diesen Wert direkt ein, ist dies jedoch häufig nicht der Fall. Anstelle des Arrays, die dies anbieten, führt Cloud 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. Idealerweise direkt aus dem Array bezogen, falls nicht verfügbar, fasst Cloud Insights den Durchsatz der Volumes zusammen, um diesen Wert abzuleiten
- Verwaltung – dieser kann einen Hyperlink für die Verwaltungsschnittstelle des Geräts enthalten. Erstellt programmgesteuert durch die Cloud Insights Datenquelle im Rahmen der Bestandsberichterstattung

Storage-Pool

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

Storage-Node

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

Anforderungen

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Konfigurieren des Datensammlers des NetApp HCI-Verwaltungsservers

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

Dieser Datensammler erwirbt nur vom **NetApp HCI Management Server**. Um Daten aus dem Storage-System zu erfassen, müssen Sie außerdem den konfigurieren "NetApp SolidFire" Datensammler.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen von 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	Laufzeit Für Cloud Insights
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.

Problem:	Versuchen Sie dies:
Fehler: VirtualCenter at IP verfügt über kein von JVM einkonformes Zertifikat	Mögliche Lösungen: * Empfohlen: Zertifikat für Virtual Center durch Verwendung von Stronger (z.B. neu generieren 1024-Bit) RSA-Schlüssel * Nicht empfohlen: Ändern Sie die JVM java.security-Konfiguration, um die Einschränkung jdk.certpath.diabledAlgorithms zu nutzen, um einen 512-Bit-RSA-Schlüssel zu ermöglichen. Siehe Versionshinweise zu JDK 7 Update 40 unter "http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

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

NetApp SolidFire All-Flash Array Datensammler

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

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

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom NetApp SolidFire All-Flash Array Data Collector. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Laufwerk	Festplatte
Cluster	Storage
Knoten	Storage-Node
Datenmenge	Datenmenge
Fibre-Channel-Port	Port
Volume Access Group, LUN-Zuweisung	Volume-Zuordnung
ISCSI-Sitzung	Volume-Maske

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

Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration dieses Datensammlers:

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

Konfiguration

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

Erweiterte Konfiguration

Feld	Beschreibung
Verbindungstyp	Wählen Sie den Verbindungstyp
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 Cloud Insights wie folgt angezeigt:

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

Wo?

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

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

NetApp StorageGRID Datensammler

Der NetApp StorageGRID Datensammler unterstützt Inventar- und Performance-Sammlung aus StorageGRID Konfigurationen.

StorageGRID wird mit einem eigenen Raw TB für die gemanagte Einheit gemessen. Jede unformatierte StorageGRID-Kapazität von 40 TB wird als 1 berechnet "Verwaltete Einheit (ME)".

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom 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	Laufzeit Für Cloud Insights
StorageGRID	Storage
Knoten	Knoten
Mandant	Storage-Pool
Eimer	Internes Volumen

Anforderungen

Für die Konfiguration dieser Datenquelle gelten folgende Anforderungen:

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

Konfiguration

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

Erweiterte Konfiguration

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

Single Sign On (SSO)

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

Die Firmware-Version	API-Version	Unterstützung von Single Sign On (SSO)
11.1	2	Nein
11.2	3.0	Ja.

11.5	3.3	Ja.

Fehlerbehebung

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

Nutanix NX-Datensammler

Cloud Insights ermittelt mit dem Nutanix Datensammler Bestands- und Performance-Daten für Nutanix NX Storage-Systeme.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom Nutanix Data Collector, Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Storage-Pool	Storage-Pool
Nutanix Container	Internes Volumen
Nutanix Container	Dateifreigabe
NFS-Share	Share

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

Anforderungen

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

OpenStack Data Collector

Der OpenStack (REST API/KVM) Data Collector erfasst Bestandsdaten für alle OpenStack Instanzen und optional VM-Performance-Daten.

Anforderungen

- IP-Adresse des OpenStack Controllers
- Anmeldeinformationen für OpenStack Admin-Rollen und Zugriff auf den Linux-KVM-Hypervisor. Wenn Sie das Administratorkonto oder die entsprechenden Administratorrechte nicht verwenden, müssen Sie die Standardrichtlinien mithilfe von „Trial and Error“ ermitteln, um sich für Ihre Benutzer-ID für Datensammler zu entspannen.
- Das OpenStack Ceilometer-Modul muss für die Performance-Erfassung installiert und konfiguriert sein. Die Konfiguration des Ceilometers erfolgt durch Bearbeiten der Nova.conf-Datei für jeden Hypervisor und dann durch Neustart des Nova Compute Service auf jedem Hypervisor. Die Optionsnamen ändern sich für verschiedene OpenStack Versionen:
  - Icehouse
  - Juno
  - Kilo
  - Freiheit
  - Mitaka
  - Newton
  - Kata
- Für CPU-Statistiken muss „Compute_Monitors=ComputeDriverCPUMonitor“ in /etc/Nova/Nova.conf auf Computing-Knoten eingeschaltet werden.
- Port-Anforderungen:
  - 5000 für http und 13000 für https, für den Keystone Service
  - 22 für KVM SSH
  - 8774 für Nova Compute Service
  - 8776 für Cinder Block Service
  - 8777 für den Ceilometer Performance Service

◦ 9292 für Glance Image Service **Hinweis** der Port bindet sich an den spezifischen Dienst, und der Dienst kann auf dem Controller oder einem anderen Host in größeren Umgebungen ausgeführt werden.

Konfiguration

Feld	Beschreibung
OpenStack-Controller-IP-Adresse	IP-Adresse oder vollqualifizierter Domain-Name des OpenStack Controllers
OpenStack Administrator	Benutzername für einen OpenStack Admin
OpenStack Passwort	Passwort, das für den OpenStack Admin verwendet wird
OpenStack Administrator-Mandant	Mandantenname des OpenStack Administrator
KVM-Sudo-Benutzer	KVM sudo Benutzername
Wählen Sie „Kennwort“ oder „OpenSSH-Schlüsseldatei“, um den Anmeldeinformationstyp anzugeben	Anmeldeinformationstyp, der für die Verbindung zum Gerät über SSH verwendet wird
Vollständiger Pfad zum privaten Bestandsschlüssel	Vollständiger Pfad zum privaten Bestandsschlüssel
KVM-Sudo-Kennwort	KVM-Sudo-Kennwort

Erweiterte Konfiguration

Feld	Beschreibung
Aktivieren der Erkennung des Hypervisor-Inventars über SSH	Aktivieren Sie diese Option, um die Erkennung des Hypervisor-Inventars über SSH zu aktivieren
OpenStack Admin-URL-Port	OpenStack Admin-URL-Port
Verwenden Sie HTTPS	Überprüfen Sie, ob sicheres HTTP verwendet wird
SSH-Port	Port, der für SSH verwendet wird
SSH-Prozess wird erneut ausgeführt	Anzahl der Versuche für einen erneuten Versuch in der Bestandsaufnahme
Abfrageintervall für Bestand (min)	Intervall zwischen Bestandsabstimmungen Der Standardwert ist 20 Minuten.

Fehlerbehebung

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

Inventar

Problem:	Versuchen Sie dies:
„Konfigurationsfehler“ mit Fehlermeldungen beginnen mit „Policy lässt nicht zu“ oder „Sie sind nicht autorisiert“	* ip-Adresse prüfen * Benutzername und Passwort überprüfen

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

Datensammler der Oracle ZFS Storage Appliance

Cloud Insights verwendet den Datensammler der Oracle ZFS Storage Appliance, um Bestands- und Performance-Daten zu erfassen.

Terminologie

Cloud Insights erfasst Bestandsinformationen mit dem Oracle ZFS Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
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. Cloud Insights erwartet, dass Sie jeden_-Controller in einem Hochverfügbarkeitspaar konfiguriert haben, um die folgenden Metriken zu erfassen:

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

Wenn der Controller nicht oder alle diese erfasst werden, führt dies wahrscheinlich dazu, dass Cloud Insights den Workload auf den „internen Volumes“ nicht oder nur unzureichend meldet.

Konfiguration

Feld	Beschreibung
ZFS Controller-1-Hostname	Host Name für Storage Controller 1
ZFS Controller-2-Hostname	Host-Name für Storage Controller 2
Benutzername	Benutzername für das Benutzerkonto des Speichersystemadministrators
Passwort	Kennwort für das Administratorbenutzerkonto

Erweiterte Konfiguration

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

Fehlerbehebung

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

Inventar

Problem:	Versuchen Sie dies:
„Ungültige Anmeldeinformationen“	ZFS-Benutzerkonto und -Passwort validieren
„Konfigurationsfehler“ mit Fehlermeldung „REST Service ist deaktiviert“	Vergewissern Sie sich, dass DER REST-Dienst auf diesem Gerät aktiviert ist.
„Konfigurationsfehler“ mit Fehlermeldung „Benutzer nicht autorisiert für Befehl“	Wahrscheinlich aufgrund bestimmter Rollen (z. B. 'Advanced_Analytics') sind für den konfigurierten Benutzer <username> nicht enthalten. Mögliche Lösung: * Korrigieren Sie den Umfang der Analyse (Statistik) für den Benutzer €{user} mit der nur lesenden Rolle: - Aus dem Bildschirm Konfiguration → Benutzer, legen Sie Ihre Maus über die Rolle und doppelklicken Sie, um das Bearbeiten zu ermöglichen - Wählen Sie "Analyse" aus dem Dropdown-Menü Bereich. Eine Liste der möglichen Eigenschaften wird angezeigt. - Klicken Sie am häufigsten auf das Kontrollkästchen, und es wird alle drei Eigenschaften auswählen. - Klicken Sie auf die Schaltfläche Hinzufügen auf der rechten Seite. - Klicken Sie oben rechts im Popup-Fenster auf die Schaltfläche Übernehmen. Das Popup-Fenster wird geschlossen.

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

Datensammler Pure Storage FlashArray

Cloud Insights erfasst mithilfe des Datensammlers Pure Storage FlashArray Bestands- und Performance-Daten.

Terminologie

Für jeden von Cloud Insights erfassten Asset-Typ wird die am häufigsten für die Ressource verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Laufwerk (SSD)	Festplatte
Array Erledigen	Storage
Controller	Storage-Node
Datenmenge	Datenmenge
LUN-Zuordnung	Volume-Zuordnung
Initiator, Ziel	Volume-Maske

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

Anforderungen

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

Konfiguration

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

Erweiterte Konfiguration

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

Feld	Beschreibung
Leistungsintervall (Sek.)	Der Standardwert ist 300

Fehlerbehebung

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

Inventar

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

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

Datensammler Red hat Virtualization

Cloud Insights verwendet den Red hat Virtualization Data Collector, um Bestandsdaten von virtualisierten Linux- und Microsoft Windows-Workloads zu erfassen.

Terminologie

Für jeden von Cloud Insights erfassten Asset-Typ wird die am häufigsten für die Ressource verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
Festplatte	Virtuelles Laufwerk
Host	Host
Virtual Machine	Virtual Machine
Storage Domain	Datastore
Logische Einheit	LUN

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

Anforderungen

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

Konfiguration

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

Erweiterte Konfiguration

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

Fehlerbehebung

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

Rubrik CDM Data Collector

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

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom Rubrik Datensammler. Die am häufigsten für diese Ressource verwendete Terminologie wird für jeden von Cloud Insights erfassten Asset-Typ angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

Anbieter-/Modelllaufzeit	Laufzeit Für Cloud Insights
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 Cloud Insights-Erfassungseinheit initiiert Verbindungen zum TCP-Port 443 zum Cluster Rubrik. Ein Collector pro Cluster.
- IP-Adresse des Rubrik Clusters.
- Benutzername und Passwort für das Cluster.
- Port-Anforderung: HTTPS 443

Konfiguration

Feld	Beschreibung
IP	IP-Adresse des Clusters Rubrik
Benutzername	Benutzername für das Cluster
Passwort	Passwort für das Cluster

Erweiterte Konfiguration

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

Fehlerbehebung

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

Inventar

Problem:	Versuchen Sie dies:
Ich erhielt die Nachricht, dass mehr als ein Speicher erstellt wird.	Überprüfen Sie, ob das Cluster ordnungsgemäß konfiguriert ist und der Collector auf ein einzelnes Cluster verweist.
Ich erhielt eine Warnung, dass die Disk API mehr Daten zurückgegeben hat	Wenden Sie sich an den Support, um zusätzliche Daten zu erhalten.

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

VMware vSphere Data Collector konfigurieren

Der Datensammler für VMware vSphere sammelt ESX Host-Informationen und benötigt schreibgeschützte Berechtigungen auf allen Objekten im Virtual Center.

Terminologie

Cloud Insights erwirbt die folgenden Bestandsinformationen vom VMware vSphere Data Collector. 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	Laufzeit Für Cloud Insights
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 durch Komma getrennte Liste mit den genauen „Namen“ Ihrer ESX-Hosts erstellen, wie sowohl in Cloud Insights als auch 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. Beim Filtern nach CLUSTER Verwenden Sie die Cloud Insights-ähnlichen Cluster-Namen wie von CI auf Hypervisoren gemeldet - Cloud Insights prepends the vSphere Cluster Name with the vSphere Datacenter Name and a forward slash - „DC1/clusterA“ ist der Clustername, den Cloud Insights über einen Hypervisor in clusterA innerhalb des Rechenzentrums DC1 berichten würde.
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 den VMware Infrastructure Client zu kommunizieren. * Versuchen Sie, mit Virtual Center über Managed Object Browser (z. B. MOB) zu kommunizieren.
Fehler: VirtualCenter at IP verfügt über kein von JVM einkonformes Zertifikat	Mögliche Lösungen: * Empfohlen: Zertifikat für Virtual Center durch Verwendung von Stronger (z.B. neu generieren 1024-Bit) RSA-Schlüssel * Nicht empfohlen: Ändern Sie die JVM java.security-Konfiguration, um die Einschränkung jdk.certpath.diabledAlgorithms zu nutzen, um einen 512-Bit-RSA-Schlüssel zu ermöglichen. Siehe Versionshinweise zu JDK 7 Update 40 unter "http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

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

Data Collector Reference - Dienste

Erfassung Von Node-Daten

Cloud Insights sammelt Kennzahlen von dem Knoten, auf dem Sie einen Agent installieren.

Installation

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

Objekte und Zähler

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

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

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

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

Einrichtung

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

MacOS-Speicherauslastung

Cloud Insights (via Telegraf) und macOS berichten über verschiedene Nummern für die Speichernutzung. Sowohl Telegraf als auch der Mac-Aktivitätsmonitor verwenden Metriken, die von *vm_stat* gesammelt wurden, jedoch wird die Gesamtspeichernutzung jeweils unterschiedlich berechnet.

Telegraf berechnet *Memory Used Total* wie folgt:

```
 Memory Used Total = Memory Total - Memory Available Total
Wobei _Memory Available Total_ aus der Summe von „Pages free“ und „Pages inactive“ in _vm_stat_ abgeleitet wird.
```

Der Mac-Aktivitätsmonitor berechnet hingegen den verwendeten Speicher wie folgt:

```
 Memory Used = App Memory + Wired Memory + Compressed
Wo?
```

- *App Memory* wird aus dem Unterschied zwischen „Anonymen Seiten“ und „Seiten auffindbar“ in *vm_stat*,
- *Wired Memory* wird von „Pages Wired Down“ in *vm_stat*, und abgeleitet
- *Compressed* wird aus „Seiten, die durch Kompressor belegt sind“ in *vm_stat* abgeleitet.

ActiveMQ Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken aus ActiveMQ zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** ActiveMQ.

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

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

[ActiveMQ-Konfiguration]

Einrichtung

Informationen finden Sie unter "ActiveMQ-Dokumentation"

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

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

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Apache Data Collector

Dieser Datensammler ermöglicht die Erfassung von Daten von Apache-Servern in Ihrer Umgebung.

Voraussetzungen

- Sie müssen Ihren Apache HTTP Server einrichten und ordnungsgemäß ausführen lassen

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

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Apache aus.

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

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

[Apache-Konfiguration]

Einrichtung

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

Kompatibilität:

Die Konfiguration wurde gegen Apache HTTP Server Version 2.4.38 entwickelt.

Aktivieren von mod_Status:

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

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

Modul aktivieren:

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

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

Statistiken aus dem Modul offenlegen:

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

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

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

Detaillierte Anweisungen zum Modul „MOD_Status“ finden Sie im "Apache-Dokumentation"

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

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

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Consul Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken von Consul zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option Konsul.

   Wenn Sie keinen Agenten für die Sammlung konfiguriert haben, werden Sie aufgefordert "Installieren Sie einen Agenten" Ihrer Umgebung zu unterstützen.

   Wenn Sie bereits einen Agenten konfiguriert haben, wählen Sie das entsprechende Betriebssystem oder die entsprechende Plattform aus, und klicken Sie auf **Weiter**.

2. Befolgen Sie die Anweisungen auf dem Bildschirm Consul Configuration, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

Einrichtung

Informationen finden Sie unter "Dokumentation für Konsul".

Objekte und Zähler für Konsul

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Konsul	Namespace-ID-Service-Node prüfen	Node-IP Node OS Node UUID Node Name Service Name Check Name Service Service ID Status	Warnung Bei Kritischem Durchgang

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Couchbase Data Collector

Cloud Insights verwendet diese Datensammlung, um die Kennzahlen von Couchbase zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option Couchbase.

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

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

[Konfiguration von Couchbase]

Einrichtung

Informationen finden Sie unter "Couchbase Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Couchbase Node	Namespace Cluster Couchbase Node-Hostname	Node Name Node-IP	Speicher Insgesamt
Couchbase Bucket	Namespace-Bucket-Cluster	Node Name Node-IP	Daten Verwendete Daten Abrufen Verwendete Elemente Anzahl Verwendete Elemente Speicher Verwendete Operationen Pro Sekunde Kontingent Verwendet

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

CouchDB Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken von CouchDB zu sammeln.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** CouchDB.

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

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

[Konfiguration von CouchDB]

Einrichtung

Informationen finden Sie unter "CouchDB-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
CouchDB	Namespace-Server	Node Name Node-IP	Authentifizierung Cache Treffer Authentifizierung Cache Fräulein Datenbank liest Datenbank schreibt Datenbanken Open OS Files Max Anfragenzeit Min Anfragestzeit httpd Request Methoden httpd Request Methoden httpd Request löschen httpd Request Methods Get httpd Request Methods Head httpd Request Methods Post httpd Request Methods Put Status Codes 200 Status Codes 201 Statuscodes 202 Statuscodes 301 Statuscodes 304 Statuscodes 400 Statuscodes 401 Statuscodes 403 Statuscodes 404 Statuscodes 405 Statuscodes 409 Statuscodes 412 Statuscodes 500

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Docker Data Collector

Cloud Insights verwendet diese Datenerfassung zum Erfassen von Kennzahlen aus Docker.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Docker aus.

   Wenn Sie keinen Agenten für die Sammlung konfiguriert haben, werden Sie aufgefordert "Installieren Sie einen Agenten" Ihrer Umgebung zu unterstützen.

   Wenn Sie bereits einen Agenten konfiguriert haben, wählen Sie das entsprechende Betriebssystem oder die entsprechende Plattform aus, und klicken Sie auf **Weiter**.

2. Befolgen Sie die Anweisungen im Bildschirm Docker-Konfiguration, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Docker-Konfiguration]

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 sich das für die Kubernetes-Plattform bereitgestellte Cloud Insights-Installationsprogramm automatisch um diese Zuordnung kümmert.

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:
Nach den Anweisungen auf der Konfigurationsseite sehe ich meine Docker-Metriken in Cloud Insights nicht.	Prüfen Sie die Telegraf-Agentenprotokolle, um zu sehen, ob es folgenden Fehler meldet: E! Fehler im Plugin [inputs.docker]: Berechtigung verweigert beim Versuch, eine Verbindung zum Docker Daemon-Socket herzustellen.Falls dies der Fall ist, ergreifen Sie die erforderlichen Schritte, um den Telegraf-Agent-Zugriff auf den Docker Unix-Sockel wie oben angegeben zu ermöglichen.

Weitere Informationen finden Sie im "Unterstützung" Seite.

Elasticsearch Data Collector

Cloud Insights verwendet diese Datenerfassung zum Erfassen von Metriken aus Elasticsearch.

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Elasticsearch.

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

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

[Elasticsearch-Konfiguration]

Einrichtung

Informationen finden Sie unter "Elasticsearch-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Elasticsearch-Cluster	Namespace-Cluster	Node-IP Node-Name Cluster-Status	Gesamtknotenanzahl Gesamtknotenanzahl Dateidatenmenge (Bytes) Dateidatenfreiwert (Bytes) Dateisystem-Daten gesamt (Bytes) JVM Threads BS zugewiesene Prozesse Betriebssystem Verfügbare Prozessoren Betriebssystem Mem Free (Bytes) Betriebssystem Mem Free OS Mem Total (Bytes) verwendetes Betriebssystem Mem verwendeter Prozess CPU Indexes Abschlussgröße (Bytes) Indizes Anzahl Indizes Indexen Anzahl Indizes Indizes Docs gelöschte Indizes Feld Datendiktionen Indices Field Data Memory Size (Bytes) Indizes Abfrage Cache-Anzahl Indizes Cache Größe Indizes Anzahl Segmente Anzahl Indizes Segmente Doc Values Speicher (Bytes) Indizes Shards Index Primärarten AVG Indizes Shards Index Primärindizes Indizes Max Indizes Shards Index Primärindizes Index Indizes Min Indizes. Indizes Shards Index Replication Avg Indizes Shards Index Replication Max Indizes Shards Index Replikation Min Indizes Shards durchschn. Indizes Shards Max Indizes Shards Primaries Indizes Indizes Shards Replication Indizes Shards Storage-Größe (Bytes)

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Elasticsearch-Node	Namespace Cluster es Node ID es Node IP es Node	Zone-ID	Machine Learning Enabled Machine Learning Memory Machine Learning Max Open Jobs X-Pack installierte Breakers Accounting Estimated Size (Bytes) Breakers Accounting Limit Size (Bytes) Breakers Accounting Overhead Breakers Accounting Tripped Breakers Field Data Estimated Size (Bytes) Breakers Field Data Overhead Breakers Field Data Tripped Breakers Field Data Breakers Field Data Stimulated Size (Bytes) Breakers in-Flight Limit Size (Bytes) Breakers in-Flight Overhead Breakers in-Flight Dripped Breakers Parent Estimated Size (Bytes) Breakers Parent Limit Size (Bytes) Breakers Parent Overhead Breakers Parent Tripped Breakers Request Estimated Size (Bytes) Breakers Request availed Filesystem Data available (Bytes) Filesystem Data Free (Bytes) Filesystem Data Total (Bytes) Dateisystem IO Stats Devices Ops Filesystem IO Stats Devices (kb) Schreib-I/O-Stats-Geräte Lese-Ops-Filesystem IO Statistik-Geräte EITE (kb) Dateisystem IO Stats Devices Write Ops Dateisystem IO Stats Total Ops Filesystem IO Stats Total Read (kb) Filesystem IO Stats Read Ops-Filesystem – IO-Statistik (KB) Dateisystem-IO-Stats-Write-Ops-Filesystem Least Usage Estimate Available (Bytes)

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Flik Data Collector

Cloud Insights verwendet diese Datenerfassung zum Erfassen von Kennzahlen aus Flink.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option Flink.

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

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

[Flik-Konfiguration]

Einrichtung

Eine vollständige Flink-Implementierung umfasst die folgenden Komponenten:

JobManager: Das Primärsystem Flik. Koordiniert eine Reihe von TaskManagers. In einer Konfiguration mit hoher Verfügbarkeit verfügt das System über mehr als einen JobManager. Taskmanager: Hier werden Flik-Operatoren ausgeführt. Das Flink Plugin basiert auf dem telegraf Jolokia Plugin. Als Voraussetzung für die Erfassung von Informationen aus allen Flik-Komponenten muss JMX auf allen Komponenten konfiguriert und über Jolokia freigelegt werden.

Kompatibilität

Die Konfiguration wurde gegen die Version 1.7 von Flink entwickelt.

Einrichtung

Jolokia Agent Jar

Für alle einzelnen Komponenten muss eine Version der Jolokia Agent JAR-Datei heruntergeladen werden. Die gegen getestete Version war "Jolokia Agent 1.6.0".

Anweisungen unten gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-Agent.jar) unter dem Speicherort '/opt/flink/lib/' platziert wird.

JobManager

Um JobManager so zu konfigurieren, dass die Jolokia API freigegeben wird, können Sie die folgende Umgebungsvariable auf Ihren Knoten einrichten und dann den JobManager neu starten:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Sie können einen anderen Port für Jolokia (8778) wählen. Wenn Sie eine
interne IP haben, um Jolokia zu sperren, können Sie die „Catch all“
0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP über
das telegraf-Plugin zugänglich sein muss.
```

Taskmanager

So konfigurieren Sie TaskManager(s), um die Jolokia-API zu öffnen, können Sie die folgende Umgebungsvariable auf Ihren Knoten einrichten und dann den TaskManager neu starten:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Sie können einen anderen Port für Jolokia (8778) wählen. Wenn Sie eine
interne IP haben, um Jolokia zu sperren, können Sie die „Catch all“
0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP über
das telegraf-Plugin zugänglich sein muss.
```

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik Task Manager	Cluster Namespace-Server	Node Name Task-Manager-ID-Knoten-IP	Netzwerk verfügbar Speichersegmente Netzwerk Speichersegmente Speichersegmente Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scavenge Time Heap Memory Comstived Heap Memory Init Heap Memory Max Heap Memory Used Thread Count Daemon Thread Count Thread Count Spitzenanzahl Thread Count Thread Count Insgesamt Gestartet

Objekt:	Kennungen:	Attribute:	Datenpunkte:
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
Flik Job Manager	Cluster Namespace-Server	Node Name Node-IP	Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scravenge Time Heap Memory Comstived Heap Memory Init Heap Memory Max Heap Memory Used Number Registrierte Task-Manager Anzahl laufende Jobs Taskleisten verfügbare Task-Steckplätze Gesamt-Thread-Anzahl Daemon-Thread-Anzahl Maximale Anzahl Der Threads Anzahl Der Threads Insgesamt Begonnen

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik-Aufgabe	Cluster Namespace Job-ID Task-ID	Server Node Name Job Name Sub Task-Index Task-Versuch-ID Task-Versuch Nummer Task-Name Task-Manager-ID Knoten-IP Aktuelle Eingabe-Wasserzeichen	Puffer in Pool Nutzung Buffers in Warteschlange Länge Buffer Out Pool Nutzung Buffer Out Queue Länge Anzahl Puffer in Lokale Anzahl Buffers in Local per Second Anzahl Puffer in Local per second Rate Anzahl Puffer in Remote Number Buffers in Remote per second Anzahl Puffer in Remote per second Anzahl der Puffer in Remote per Anzahl Der Auspuffer Anzahl Der Auspuffer Pro Sekunde Anzahl Auspuffer Pro Sekunde Anzahl Bytes Pro Sekunde Anzahl Bytes In Lokale Anzahl Bytes Pro Sekunde Anzahl Bytes In Lokal Pro Sekunde Anzahl Bytes In Lokal Pro Sekunde Anzahl Bytes In Remote Number Bytes In Remote Per Second Anzahl Bytes In Remote Pro Sekunde Rate Anzahl Bytes Out Anzahl Bytes Out Pro Sekunde Anzahl Bytes Out Pro Sekunde Anzahl Datensätze In Number Datensätze In Per Second Anzahl Datensätze Pro Sekunde Anzahl Datensätze Pro Sekunde Anzahl Datensätze Pro Sekunde Anzahl Datensätze Aus Anzahl Datensätze Pro Sekunde Anzahl Datensätze Aus Pro Sekunde

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Flik Task Operator	Cluster Namespace Job-ID Operator-ID Task-ID	Server Node Name Job Name Operator Name Sub Task-Index Task-Versuch-ID Task-Versuch-Nummer Task-Name Task-Manager-ID-Knoten-IP	Aktuelle Eingabe Watermark Current Output Watermark Number Records In Number Records In Per Second Count Anzahl Datensätze In Pro Sekunde Anzahl Datensätze Pro Sekunde Anzahl Datensätze Aus Anzahl Datensätze Pro Sekunde Anzahl Anzahl Datensätze Aus Pro Sekunde Anzahl Verspätete Datensätze Verworfen Zugewiesene Partitionen Bytes Verbrauchte Rate Commit Latenz Durchschn. Commit-Latenz Max. Commit Rate Commits faciert fehlgeschlagene Verbindungen Close Rate Verbindungsanzahl Verbindungserzeugung Rate Anzahl Abholen Latenz durchschn. Abholen Max. Abholen Rate Abholen Größe Max. Abholen Drosselzeit durchschn. Abrufdauer Max. Heartbeat Rate Incoming Byte Rate I/O-Zeit durchschn. (Ns) I/O Wartezeit I/O Wartezeit durchschn. (Ns) Verbindungsrate Verbindungszeit durchschn. Letzter Heartbeat ago Netzwerk-I/O-Rate ausgehende Byte-Datensätze verbrauchte Rate Datensätze lag max. Datensätze pro Anforderung durchschn. Anfragemgröße Durchschnittl. Anfragengröße max. Ansprechrate Wählen Rate Synchronisierungszeit durchschn. Heartbeat Antwort Zeit Max. Verbindungszeit Max. Synchronisierungszeit

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Hadoop Data Collector

Cloud Insights verwendet diese Datenerfassung zum Erfassen von Kennzahlen aus Hadoop.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Hadoop.

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

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

[Hadoop Konfiguration] [Hadoop Konfiguration]

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.

Jolokia Agent Jar

Für alle einzelnen Komponenten muss eine Version der Jolokia Agent JAR-Datei heruntergeladen werden. Die gegen getestete Version war "Jolokia Agent 1.6.0".

Die nachfolgende Anleitung setzt voraus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-Agent.jar) unter der Adresse '/opt/hadoop/lib/' abgelegt wird.

NameNode

Um NameNode zu konfigurieren, um die Jolokia API freizugeben, können Sie unter <HADOOP_HOME>/etc/hadoop/hadoop-env.sh Folgendes einrichten:

```
export HADOOP_NAMENODE_OPTS="$HADOOP_NAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7800,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8000
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8000 above) and Jolokia (7800).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Sekundärer NameNode

Um den sekundären NameNode zu konfigurieren, um die Jolokia API freizugeben, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export HADOOP_SECONDARYNAMENODE_OPTS="$HADOOP_SECONDARYNAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7802,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8002
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8002 above) and Jolokia (7802).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

DataNode

Um die DataNodes so zu konfigurieren, dass sie die Jolokia API aussetzen, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export HADOOP_DATANODE_OPTS="$HADOOP_DATANODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7801,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8001
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8001 above) and Jolokia (7801).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

ResourceManager

Um den ResourceManager so zu konfigurieren, dass die Jolokia API zur Verfügung gestellt wird, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export YARN_RESOURCEMANAGER_OPTS="$YARN_RESOURCEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7803,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8003
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8003 above) and Jolokia (7803).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

NodeManager

Um die NodeManagers so zu konfigurieren, dass sie die Jolokia API aussetzen, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export YARN_NODEMANAGER_OPTS="$YARN_NODEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7804,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8004
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8004 above) and Jolokia (7804).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

JobGeschichteServer

Um den JobHistorieServer so zu konfigurieren, dass die Jolokia API zur Verfügung gestellt wird, können Sie Folgendes in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh einrichten:

```
export HADOOP_JOB_HISTORYSERVER_OPTS="$HADOOP_JOB_HISTORYSERVER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7805,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8005
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8005 above) and Jolokia (7805).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Sekundärer Hadoop NameNode	Cluster Namespace-Server	Node Name Node IP Compile Info Version	GC-Anzahl GC-Kopien Anzahl GC-Markierungen Sweep Compact-Anzahl GC-Nummer Info Schwellenwert überschritten GC-Nummer Warnungsschwellenwert überschritten GC-Zeit kopieren GC-Markierungen Sweep Compact-Zeit GC Gesamtdauer Extra Sleep Time Logs Anzahl der Fehler Protokolle Anzahl der fatalen Protokolle Info-Anzahl Warnmeldungen SpeicherHeap-Comstied Speicher Heap Max Speicher Heap Verwendeter Speicher Max Speicher Nicht Heap Speicher Nicht Heap Max Speicher Nicht Heap Verwendete Threads Blockierte Threads Neue Threads Runnable Threads Beendet Threads Timed Waiting Threads

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop NodeManager	Cluster Namespace-Server	Node Name Node-IP	Container Zugewiesener Speicher Zugewiesener Speicher Zuweisen Oportunistic Virtual Cores Allocchortunistic Virtual Cores Zugeordnete Speichernutzung Verfügbare Kerne Verfügbare Verzeichnisse Bad Lokale Verzeichnisse Bad Log Cache Größe Vor Clean Container Starten Dauer Durchschn. Dauer Container Starten Dauer Anzahl Operationen Container Abgeschlossen Container Container Container Container Container Container Inting Container Killed Containers Started Containers Container Reiniting Container gerollt zurück auf Fehler-Container ausgeführt Plattenauslastung gut Lokale Verzeichnisse Datenträgernutzung gut Log-Verzeichnisse Bytes gelöscht Private Bytes gelöscht Öffentliche Container mit opportunistischen Bytes gelöscht Gesamtanzahl Shuffle Verbindungen Shuffle Ausgabe Bytes Shuffle Outputs fehlgeschlagen Shuffle Outputs OK GC-Anzahl GC-Kopien Anzahl GC-Markierungen Sweep Compact Count GC-Nummer Info Schwellenwert überschritten GC-Nummer Warnungsschwellenwert überschritten GC-Zeit kopieren GC-Markierungen Sweep Compact Time GC Gesamtdauer Extra Sleep Time Logs Anzahl Protokolle Fatal Count Protokolle Warnungszahl Speicher Heap Max

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop ResourceManager	Cluster Namespace-Server	Node Name Node-IP	AnwendungMaster-Startverzögerung durchschn. AnwendungMaster-Startverzögerung AnwendungMaster-Register Verzögerung durchschn. AnwendungMaster Register Verzögerung Nummer NodeManager Aktive Nummer NodeManager Decomissierte Nummer NodeManager Decomissioning Nummer NodeManager Lost Number NodeManager neu gestartet Nummer NodeManager Herunterfahren Nummer NodeManager Healthy Number NodeManager Memory Limit NodeManager Virtual Cores Limit used Capacity Active Applications Active Users Aggregierter Container Zugewiesene Aggregatcontainer Freigegebene Aggregate-Speicher Sekunden Ersatz Für Aggregat-Node Lokale Container Zugewiesene Aggregat-Aus Switch-Container Zugewiesenes Aggregat Ack Lokale Container Zugewiesenes Aggregat Virtuelle Kerne Sekunden Vorweggenommen Container Zugewiesener Speicher Zugewiesene Virtuelle Kerne Applikationsversuch Erster Container-Zuweisungsverzögerung Durchschn. Time Application-Versuch Erste Containerzuordnungsverzögerung Anzahl der Anwendungen Abgeschlossene Anwendungen Anwendungen

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop DataNode	Cluster Namespace-Server	Node Name Node-IP Cluster-ID-Version	Transceiver-Anzahl überträgt in Bearbeitung Cache Kapazität Cache verwendete Kapazität DFS verwendete geschätzte Kapazität verloren Gesamt Letztes Volume Ausfall Rate Blöcke Anzahl gecachte Blöcke Anzahl fehlgeschlagener Cache-Blöcke Anzahl nicht in Cache-Blöcke Anzahl nicht übertragene Volumes Anzahl Restkapazität GC-Kopien Anzahl GC-Mark Sweep Compact-Anzahl GC-Nummer Info Schwellenwert überschritten GC-Nummer Warnschwellenwert überschritten GC-Zeit Kopieren GC-Zeit GC-Markierungen Sweep Compact Time GC Gesamt Extra Sleep Time Logs Anzahl Protokolle tödliche Anzahl Protokolle Info Anzahl Protokolle Warnungszahl Speicher Heap-Speicher Heap Max Speicher Heap verwendeter Speicher Max Speicher nicht Heap-belegt Speicher Nicht Heap Max Speicher Nicht Heap Verwendet Threads Blockiert Threads Neue Threads Runnable Threads Beendet Threads Timed Warting Threads Wartend

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop NameNode	Cluster Namespace-Server	Node Name Node IP Transaktions-ID Letzte geschriebene Zeit seit Letzte geladen Edits HA State File System Status Block Pool ID Cluster ID Compile Info unterschiedliche Version Anzahl Version	Block Kapazität Blöcke Gesamtkapazität genutzte Gesamtkapazität nicht DFS-Blöcke beschädigt geschätzte Kapazität verloren Gesamtblöcke Überschuss Herzschläge abgelaufen Dateien Gesamt File System Lock Queue Länge Blöcke fehlende Blöcke fehlende Replizierung mit Faktor 1 Clients Aktive Daten Knoten Dead Data Nodes Deaktivieren Dead Data Nodes Decommissioning Live Data Nodes Decomissieren Verschlüsselungszonen Anzahl Daten Knoten, die Wartungsdateien unter Baudaten Knoten eingeben in Wartung Daten Knoten leben in Wartung Daten Knoten Live-Speicher Inches Replikation Ausstehende Timeouts Datenknoten Nachricht Ausstehende Blöcke Ausstehende Löschblöcke ausstehende Replikationsblöcke Ausstehende Replikationsblöcke Ausstehende Replikationsblöcke mehrere verschobene Blöcke geplante Snapshot-Verzeichnisse Daten-Nodes veraltete Dateien Gesamt Last Sync Anzahl der gesamten Transaktionen seit letzten Checkpoint-Transaktionen seit Last Log Roll-Blocks UnderReplicated Volume Failures gesamte Synchronisierungszeiten Gesamtes Objekt Max Operationen hinzufügen Operationen Snapshots zulassen Batched Operations Block Queued Operations Block

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Hadoop JobGeschichteServer	Cluster Namespace-Server	Node Name Node-IP	GC-Anzahl GC-Kopien Anzahl GC-Markierungen Sweep Compact-Anzahl GC-Nummer Info Schwellenwert überschritten GC-Nummer Warnungsschwellenwert überschritten GC-Zeit kopieren GC-Markierungen Sweep Compact-Zeit GC Gesamtdauer Extra Sleep Time Logs Anzahl der Fehler Protokolle Anzahl der fatalen Protokolle Info-Anzahl Warnmeldungen SpeicherHeap-Comstied Speicher Heap Max Speicher Heap Verwendeter Speicher Max Speicher Nicht Heap Speicher Nicht Heap Max Speicher Nicht Heap Verwendete Threads Blockierte Threads Neue Threads Runnable Threads Beendet Threads Timed Waiting Threads

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

HAProxy Data Collector

Cloud Insights verwendet diese Datensammlung, um Kennzahlen von HAProxy zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option HAProxy.

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

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.
3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten,

zum Beispiel nach Betriebssystem/Plattform.

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

[HAProxy-Konfiguration]

Einrichtung

Telegraf's Plugin für HAProxy setzt auf HAProxy Stats Aktivierung. Diese Konfiguration ist in HAProxy integriert, ist jedoch nicht sofort aktiviert. Wenn HAProxy aktiviert ist, wird ein HTML-Endpunkt angezeigt, der in Ihrem Browser angezeigt werden kann oder für die Extraktion des Status aller HAProxy-Konfigurationen abgekratzt werden kann.

Kompatibilität:

Die Konfiguration wurde gegen HAProxy-Version 1.9.4 entwickelt.

Einrichtung:

Um Statistiken zu aktivieren, bearbeiten Sie Ihre haproxy-Konfigurationsdatei und fügen Sie nach dem Abschnitt 'Standards' die folgenden Zeilen hinzu: Verwenden Sie Ihren eigenen Benutzer/Ihr Passwort und/oder die haproxy-URL:

```
stats enable
stats auth myuser:mypassword
stats uri  /haproxy?stats
```

Im Folgenden finden Sie eine vereinfachte Beispiel-Konfigurationsdatei mit aktivierten Statistiken:

```
global
  daemon
  maxconn 256

defaults
  mode http
  stats enable
  stats uri /haproxy?stats
  stats auth myuser:mypassword
  timeout connect 5000ms
  timeout client 50000ms
  timeout server 50000ms

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

backend servers
  server server1 10.128.0.55:8080 check ssl verify none
  server server2 10.128.0.56:8080 check ssl verify none

backend servers_2
  server server3 10.128.0.57:8080 check ssl verify none
  server server4 10.128.0.58:8080 check ssl verify none
```

Vollständige und aktuelle Anweisungen finden Sie im "HAProxy-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
HAProxy Frontend	Namespace-Adressenproproxy	Node-IP-Knotenname Proxy-ID-Modus Prozess-id Sitzungen Ratenlimit Server-id Sitzungen Limit Status	Bytes in Bytes Out Cache Hits Cache Lookups Komprimierung Bytes umgangen Komprimierung Bytes in Komprimierung Bytes Out Komprimierung Reaktionen Verbindungsrate Verbindungsrate Max Verbindungen insgesamt Anträge, die von der Verbindung abgelehnt werden Rule Requests verweigert durch Sicherheitsbedenken Antworten verweigert durch Sicherheitsbedenken Anfragen abgelehnt durch Session Rule Requests erfragt Fehler Antworten 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten andere Anfragen Abfangen Sitzungen Rate Sitzungen Max Anfragen Rate Max Anfragen Rate Max Anforderungen Total Sessions Sitzungen Max Sitzungen Antworten Neuschreibung Total Requests

Objekt:	Kennungen:	Attribute:	Datenpunkte:
HAProxy-Server	Namespace-Adresse-Proxy-Server	Node-IP-Knotenname Check Time to Finish Check Fall Configuration Check Health Value Check RISE Configuration Check Status Proxy ID Last Change Time Last Session Time Mode Process id Server Status Weight	Aktive Server Backup Server Bytes in Bytes Out Downs Check Downs Check Fails Client abgebrochen Verbindungen Verbindung Verbindung Durchschnittliche Zeit Ausfallzeit Gesamt Denied Responses Verbindungsfehler Antwort 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten anderer Server ausgewählt Total Queue Current Queue Max. Durchschnittliche Zeit Sitzungen pro Zweite Sitzungen pro Sekunde Max. Wiederverwendbarkeit der Verbindung Reaktionszeit Durchschnittliche Sitzungen Sitzungen Max Server Transfer bricht Sitzungen gesamte Sitzungen Gesamtzeit Durchschnittliche Anforderungen Redispatches Anfragen Wiederholungen Anfragen Neuschreibung Anfragen

Objekt:	Kennungen:	Attribute:	Datenpunkte:
HAProxy-Back-End	Namespace-Adressenproproxy	Node-IP-Node-Name Proxy-ID Letzte Änderung Zeit Letzte Sitzung Zeitmodus Prozess-id Server-id Sitzungen Limit Status Gewicht	Aktive Server Backup Server Bytes in Bytes Out Cache Aufrufe Cache Lookups überprüfen Downs Client abbricht Komprimierung Bytes umgangen Komprimierung Bytes in Komprimierung Bytes out Komprimierungsantworten Verbindung Durchschnittliche Zeit Ausfallzeit Total Requests verweigert durch Sicherheitsbedenken Antworten verweigert durch Sicherheit Bedenken Verbindungsfehler Antworten Reaktion 1xx Antworten 2xx Antworten 3xx Antworten 4xx Antworten 5xx Antworten anderer Server ausgewählt Total Queue Current Queue Max. Warteschlange Durchschnittliche Zeit Sitzungen pro Sekunde Sitzungen pro Sekunde Max. Anfragen Gesamt Verbindungswiederverwendung Reaktionszeit Durchschnittliche Sitzungen Sitzungen Max. Serverübertragung Abtreibungen Sitzungen Gesamtzeit Durchschnittliche Anfragen Neuzuweisen Wiederholungsanfragen Wiederholungsanfragen Wiederholungsanfragen Wiederholungsanfragen Anträge Neu Schreiben

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

JVM Data Collector

Cloud Insights verwendet diese Datenerfassung zum Erfassen von Kennzahlen aus JVM.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** JVM.

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

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

[JVM-Konfiguration]

Einrichtung

Informationen finden Sie unter "JVM-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
JVM	Namespace-JVM	OS Architektur OS Name OS Version Laufzeit Spezifikation Laufzeit Spezifikation Hersteller Laufzeit Spezifikation Version Uptime Laufzeit VM Name Laufzeit VM Anbieter Laufzeit VM Version Node Name Node IP	Class Loaded Class Loaded Class Memory Unloaded Memory Heap Init Memory Heap used Max Memory Heap Used Memory Non Heap Innit Memory Non Heap Max Memory nicht Heap Used Memory Objects Ausstehende Fertigstellung von Betriebssystemprozessoren verfügbar Betriebssystem engagierte virtuelle Speichergröße OS Kostenlos Physikalische Speichergröße OS Freier Swap Speicherplatz Größe OS Max Datei Descriptor Anzahl OS Open File Descriptors Anzahl Betriebssystem Prozessor CPU Load OS CPU Time OS System CPU Load OS System Load Average OS Gesamt Physical Memory Size OS Gesamt Swap Space Size Thread Daemon Anzahl der Threads Spitzenanzahl Thread Count Thread Total Started Count Garbage Collector Copy Collection Count Garbage Collector Copy Collection Time Garbage Collector Sammlung von Mark-Sweep Sammlungszeit Zeitabfälle Collector G1 Sammlung der Alten Generation Speicherbage Collector G1 Zeitabbage der Jungen Generation Sammlungszähler Garbage Collector G1 Young Generation Collection Time Garbage Collector Zeitabfälle Sammlung der aktuellen Mark-Sweep Sammlung Zeitgarage Collector Parallel Collection Count Garbage Collector Parallel

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Kafka Data Collector

Cloud Insights verwendet diese Datensammler, um Metriken aus Kafka zu sammeln.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Kafka.

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

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

[Konfiguration von Kafka]

Einrichtung

Das Kafka Plugin basiert auf dem telegraf's Jolokia Plugin. Um Informationen aus allen Kafka-Brokern zu sammeln, muss JMX über Jolokia auf allen Komponenten konfiguriert und zugänglich gemacht werden.

Kompatibilität

Konfiguration wurde gegen Kafka Version 0.11.0 entwickelt.

Einrichtung

Alle Anweisungen unten Nehmen wir an, dass Ihr Installationsort für kafka '/opt/kafka' ist. Sie können die nachfolgenden Anweisungen an Ihren Installationsort anpassen.

Jolokia Agent Jar

Eine Version die Jolokia Agent jar-Datei muss sein "Heruntergeladen". Die gegen die Version getestete war Jolokia Agent 1.6.0.

Anweisungen unten gehen davon aus, dass die heruntergeladene JAR-Datei (jolokia-jvm-1.6.0-Agent.jar) unter dem Speicherort '/opt/kafka/libs/' abgelegt wird.

Kafka Brokers

Um Kafka Brokers so zu konfigurieren, dass sie die Jolokia API aussetzen, können Sie in <KAFKA_HOME>/bin/kafka-Server-Start.sh kurz vor dem Anruf „kafka-run-class.sh“ Folgendes hinzufügen:

```
export JMX_PORT=9999
export RMI_HOSTNAME=`hostname -I`
export KAFKA_JMX_OPTS="-javaagent:/opt/kafka/libs/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0
-Dcom.sun.management.jmxremote.password.file=/opt/kafka/config/jmxremote.p
assword -Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=$RMI_HOSTNAME
-Dcom.sun.management.jmxremote.rmi.port=$JMX_PORT"
```

Beachten Sie, dass das obige Beispiel 'Hostname -i' verwendet, um die Umgebungsvariable 'RMI_HOSTNAME' einzurichten. In mehreren IP-Maschinen muss dies optimiert werden, um die IP, die Sie für RMI-Verbindungen interessieren, zu erfassen.

Sie können einen anderen Port für JMX (9999 oben) und Jolokia (8778) wählen. Wenn Sie eine interne IP haben, um Jolokia zu sperren, können Sie die „Catch all“ 0.0.0.0 durch Ihre eigene IP ersetzen. Beachten Sie, dass diese IP über das telegraf-Plugin zugänglich sein muss. Sie können die Option '-Dcom.sun.management.jmxremote.authenticate=false' verwenden, wenn Sie nicht authentifizieren möchten. Nutzung auf eigenes Risiko.

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Kafka Broker	Cluster Namespace Broker	Node Name Node-IP	Replikatmanager Fetcher Max Lag Zookeeper Client-Verbindungen Zookeeper Client-Verbindungen (15 m Rate) Zookeeper Client-Verbindungen (5 m Rate) Zookeeper Client-Verbindungen (mittlere Rate) Zookeeper Client-Verbindungen (1 m Rate) Anzahl der Threads des Replikatmanagers Anzahl der Threads Anzahl der Threads Anzahl der Threads Anzahl der aktuellen Lesevorgänge Anzahl der insgesamt gestarteten Offline-Partitionen Anfragen Gesamtzeit (50. Perzentil) Anfragen produzieren Gesamtzeit (75. Perzentil) Anfragen produzieren Gesamtzeit (98 Perzentil) Anfragen produzieren Gesamtzeit (999. Perzentil) Erstellen von Anfragen Gesamtzeit (9th Perzentil) Erstellen von Anfragen Gesamt Zeit produzieren Anfragen Gesamt Zeit produzieren Max produzieren Anfragen Gesamt Zeit Mittelwert produzieren Anfragen Gesamtzeit Min Erzeugungsanforderunge n Total Zeit Max Gesamtzeit Gesamt Zeit Stddev Replica Manager ISR reduziert Replikatmanager verkleinert ISR (15 m Rate) Replica Manager ISR reduziert (5 m Rate) Replica Manager ISR reduziert (Mittlere Rate) Replica Manager ISR-Shrink (1-m-Rate) Anforderung Handler durchschn. Leerlaufanfrage (15-m-Rate) Anforderung

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Kibana Data Collector

Cloud Insights verwendet diesen Datensammler, um Kennzahlen von Kibana zu sammeln.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option Kibana.

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

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

[Kibana-Konfiguration]

Einrichtung

Informationen finden Sie unter "Kibana Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Kibana	Namespace-Adresse	Versionsstatus des Node-IP-Node-Namens	Gleichzeitige Verbindungen Heap Max Heap verwendete Anforderungen pro Sekunde Antwortzeit Max. Betriebszeit

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Memcached Data Collector

Cloud Insights verwendet diese Datensammlung, um Kennzahlen aus Memcached zu

erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Memcached.

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

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

[Konfiguration mit Memcached]

Einrichtung

Informationen finden Sie unter "Wiki mit Memcached".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Gememcachte	Namespace-Server	Node-IP-Node-Name	Akzeptieren von Verbindungen verarbeitet Authentifizierungsanforderungen fehlgeschlagene Authentifizierungen verwendete Bytes (pro Sekunde) geschriebene Bytes (pro Sek.) CAS Badval CAS Hits CAS Misses Flush Reqs (pro Sek.) Get Reqs (pro Sek.) Set Reqs (pro Sek.) Touch Reqs (pro Sek.) Verbindungserträge (pro Sek.) Verbindungsstrukturen Verbindungen öffnen Aktuelle gespeicherte Objekte Decr fordert Zugriffe (pro Sek.) Decr fordert Fehlschläge (pro Sek.) Löschen von Anfragen Treffer (pro Sek.) Löschen von Anfragen Fehlschläge (pro Sek.) entfernte Objekte gültige Abtreibungen abgelaufene Objekte Get Hits (pro Sek.) Get Misses (pro Sek.) Gebrauchte Hash Bytes Hash-Bytes erweitert Hash Power Level Inc. Hash Power Level Inc. Zugriffe (pro Sek.) Infr Anfragen Misses (pro Sek.) Server Max Bytes anhören deaktiviert Num zurückgewonnener Mitarbeiter Threads Anzahl geöffnete Verbindungen Gesamtzahl der gespeicherten Elemente Touch Hits Touch Misses Server Uptime

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

MongoDB Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken von MongoDB zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option MongoDB aus.

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

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

[MongoDB Konfiguration]

Einrichtung

Informationen finden Sie unter "MongoDB Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
MongoDB	Namespace-Hostname		
MongoDB Datenbank	Name der Namespace-Hostname-Datenbank		

Fehlerbehebung

Informationen können im gefunden werden "Unterstützung" Seite.

MySQL Data Collector

Cloud Insights verwendet diese Datensammlung, um Kennzahlen von MySQL zu sammeln.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** MySQL.

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

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

[MySQL-Konfiguration]

Einrichtung

Informationen finden Sie unter "MySQL-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
MySQL	Namespace für MySQL Server	Node-IP-Node-Name	Abgebrochene Clients (pro s) abgebrochene Verbindungen (pro s) RX Byte (pro s) TX Bytes (pro Sek.) Befehle Admin (pro Sek.) Befehle Alter Ereignisbefehle Alter Funktion Befehle Alter Instanz Befehle Alter Prozedur Befehle Alter Server Befehle Alter Tabelle Befehle Alter Tablespace Befehle Alter Benutzer Befehle Analyse Befehle Zuweisen zu Keycache-Befehlen Begin-Befehle Binlog-Befehle Aufruf Procedure-Befehle DB-Befehle Change Master befiehlt Change Repl Filter Befehle Check Commands Prüfsummenbefehle Befehle Commit-Befehle DB-Befehle erstellen Ereignisbefehle erstellen Befehle erstellen Index-Befehle erstellen Maßnahmen-Befehle erstellen Serverbefehle erstellen Trigger-Befehle erstellen UDF-Befehle erstellen Benutzerbefehle erstellen Befehle anzeigen erstellen Dealloc SQL-Verbindungsfehler akzeptieren erstellte tmp-Disk-Tabellen verzögerte Fehler Flush-Befehle Handler Commit Innodb Buffer Pool Bytes Daten Schlüsselblöcke Nicht Gespült Schlüssel Leseanforderungen Schlüssel Schreib Schlüssel Schreibvorgänge Max Ausführungszeit Überschritten Max Verwendete Verbindungen Open Files Performance Schema Konten Lost Prepared Stmt Count Qcache Freie Blöcke

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Netstat Data Collector

Cloud Insights verwendet diese Datensammlung, um netstat-Kennzahlen zu sammeln.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** netstat aus.

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

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

[Windows Netstat-Konfiguration]

Einrichtung

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Netstat	Node-UUID	Node-IP-Node-Name	

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Nginx Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken von Nginx zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Nginx.

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

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.

3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Linux-Nginx-Konfiguration] [Linux-Nginx-Konfiguration]

Einrichtung

Für die nginx-metrische Sammlung ist Nginx erforderlich "http_stub_Status_Module" Aktiviert sein.

Weitere Informationen finden Sie im "Nginx-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Nginx	Namespace-Server	Node-IP-Node-Name-Port	Akzeptiert Aktive Bearbeitet Leseanforderungen, Die Auf Das Schreiben Warten

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

PostgreSQL Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken aus PostgreSQL zu sammeln.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** die Option PostgreSQL.

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

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

[PostgreSQL-Konfiguration]

Einrichtung

Informationen finden Sie unter "PostgreSQL-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
PostgreSQL Server	Namespace-Datenbankserver	Node Name Node-IP	Puffer Zugeordnete Buffers Back-End-Puffer Dateisynchronisation Buffers Checkpoint Puffer Clean Checkpoints Sync Time Checkpoints Write Time Checkpoints Requests Checkpoints Timed Max Geschrieben Sauber
PostgreSQL Datenbank	Namespace-Datenbankserver	Datenbank OID Node Name Node IP	Blöcke Lesezeit Blöcke Write Time Blocks Treffer Blöcke Liest Konflikte Deadlocks Client-Nummer Temp-Dateien Bytes Temp-Dateien Anzahl Zeilen Gelöschte Zeilen Abgeholt Zeilen Zeilenanzahl Zeilenanzahl Zeilenanzahl Zeilenumeinfügen Letzte Transaktionen Letzte Transaktionen Übertragen Rollbacks

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Puppet Agent Data Collector

Cloud Insights verwendet diesen Datensammler, um Metriken vom Puppet Agent zu erfassen.

Installation

1. Klicken Sie in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Puppet.

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

2. Wenn Sie noch keinen Agent für die Sammlung installiert haben oder einen Agent für ein anderes

Betriebssystem oder eine andere Plattform installieren möchten, klicken Sie auf *Anweisungen anzeigen*, um das zu erweitern "Agenten-Installation" Anweisungen.

3. Wählen Sie den Agent-Zugriffsschlüssel für diesen Datensammler aus. Sie können einen neuen Agent-Zugriffsschlüssel hinzufügen, indem Sie auf die Schaltfläche **+ Agent Access Key** klicken. Best Practice: Verwenden Sie einen anderen Agent-Zugriffsschlüssel nur, wenn Sie Datensammler gruppieren möchten, zum Beispiel nach Betriebssystem/Plattform.
4. Befolgen Sie die Konfigurationsschritte, um den Datensammler zu konfigurieren. Die Anweisungen hängen vom Betriebssystem oder der Plattform ab, die Sie zur Datenerfassung verwenden.

[Puppet-Konfiguration]

Einrichtung

Informationen finden Sie unter "Puppet-Dokumentation"

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Puppet Agent	Namespace-Node-UUID	Node Name Ort Node-IP-Version Konfigstring Version Puppet	Änderungen Total Events Failure Ereignisse Success Events Summe Ressourcen Geänderte Ressourcen Fehlgeschlagen Ressourcen Konnten Nicht Neu Starten Ressourcen Outofsync Ressourcen Neustart Ressourcen Geplante Ressourcen Übersprungene Ressourcen Gesamtzeit Ankerzeit Abruf Configtime Cron Time Exec Time File Time Filebucket Time Lastrun Time Package Time Zeitplanzeit Service Time Sshauorizedkey Time Total Time User

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Redis Data Collector

Cloud Insights verwendet 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 in **Admin > Data Collectors** auf **+Data Collector**. Wählen Sie unter **Services** Redis.

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

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

[Redis Data Collector Konfiguration]

Einrichtung

Informationen finden Sie unter "Redis-Dokumentation".

Objekte und Zähler

Folgende Objekte und ihre Zähler werden gesammelt:

Objekt:	Kennungen:	Attribute:	Datenpunkte:
Redis	Namespace-Server		

Fehlerbehebung

Weitere Informationen finden Sie im "Unterstützung" Seite.

Objekt Symbol Referenz

Ein kurzer Verweis auf Objektsymbole, die in Cloud Insights verwendet werden.

[Symbolreferenz]