Daten Werden Erfasst

Cloud Insights

NetApp
March 30, 2023

Inhaltsverzeichnis

Daten Werden Erfasst

Erste Schritte zum Sammeln von Daten

Nachdem Sie sich zum ersten Mal bei Cloud Insights angemeldet haben und sich zum ersten Mal in Ihrer Umgebung anmelden, führen Sie die folgenden Schritte durch, um mit der Erfassung und dem Management der Daten zu beginnen.

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

Cloud Insights bietet drei Arten von Datensammlern an:

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

Wählen Sie Ihren ersten Datensammler von den unterstützten Anbietern und Modellen aus. Sie können später ganz einfach weitere Datensammler hinzufügen.

Installieren Sie eine Akquisitionseinheit

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

[Anweisungen für Linux AU]

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

[Neue AU erkannt]

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

Konfigurieren Sie den Data Collector - Infrastruktur

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

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

Sie können später zusätzliche Datensammler konfigurieren.

Konfigurieren Sie den Data Collector - Betriebssysteme und Dienste

Betriebssystem:

Wählen Sie für Datensammler *Betriebssystem* eine Plattform (MacOS, Linux, Windows) aus, um einen Cloud Insights-Agent zu installieren. Sie müssen mindestens einen Agenten haben, um Daten von Services zu erfassen. Der Agent erfasst auch Daten vom Host selbst, zur Verwendung in Cloud Insights. Diese Daten werden in Widgets usw. als „Knoten“-Daten kategorisiert

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

Dienste:

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

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

Dashboards Hinzufügen

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

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

Mehr ist nicht nötig

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

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

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

Nützliche Definitionen

Die folgenden Definitionen können nützlich sein, wenn Sie über Cloud Insights-Datensammler oder -Funktionen sprechen:

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

gehören:

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

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

Anforderungen An Die Erfassungseinheit

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

Anforderungen

Komponente	Linux-Anforderungen Erfüllt	Windows Anforderungen
Betriebssystem	Ein Computer mit einer lizenzierten Version von einer der folgenden: * CentOS (64-Bit): 7.2 bis 7.9, Stream 8, Stream 9 * Debian (64-Bit): 9 und 10 * Oracle Enterprise Linux (64-Bit): 7.5 bis 7.9, 8.1 bis 8.4 * Red hat Enterprise Linux (64-Bit): 7.2 bis 7.9, 8.1 bis 8.6 * Ubuntu Server: 18.04 und 20.04 LTS auf diesem Computer sollte keine andere Software auf Anwendungsebene ausgeführt werden. Es wird ein dedizierter Server empfohlen.	Ein Computer mit einer lizenzierten Version von einer der folgenden Komponenten: * Microsoft Windows 10 64-Bit * Microsoft Windows Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows 11 auf diesem Computer sollte keine andere Software auf Anwendungsebene ausgeführt werden. Es wird ein dedizierter Server empfohlen.
CPU	2 CPU-Kerne	Gleich
Speicher	8 GB RAM	Gleich

Verfügbarer Festplattenspeicher	50 GB bei Linux sollte auf diese Weise Speicherplatz zugeteilt werden: /Opt/netapp 10 GB /var/log/netapp 40 GB/tmp mindestens 1 GB während der Installation zur Verfügung stehen	50 GB
Netzwerk	100 Mbit/s/1 Gbit/s Ethernet-Verbindung, statische IP-Adresse und Port 80 oder 443-Konnektivität von Acquisition Unit zu *.cloudinsights.netapp.com oder Ihrer Cloud Insights-Umgebung (d. h. https://<environment_id>.c01.cloudinsights.netapp.com) erforderlich. Informationen zu Anforderungen zwischen Erfassungseinheit und jedem Data Collector finden Sie in der Anleitung für "Data Collector". Wenn Ihr Unternehmen Proxy-Nutzung für den Internet-Zugriff erfordert, müssen Sie möglicherweise das Proxy-Verhalten Ihrer Organisation verstehen und bestimmte Ausnahmen für Cloud Insights zu arbeiten suchen. Blockiert Ihr Unternehmen beispielsweise standardmäßig den Zugriff und gewährt ausnahmsweise nur Zugriff auf bestimmte Websites/Domänen? In diesem Fall müssen Sie die folgende Domain zur Ausnahmeliste hinzugefügt bekommen: *.cloudinsights.netapp.com für weitere Informationen, bereit über Proxys "Hier" Oder "Hier".	Gleich
Berechtigungen	Sudo-Berechtigungen auf dem Akquisitionsgruppenserver. /Tmp muss mit exec-Funktionen montiert werden.	Administratorberechtigungen auf dem Akquisitionsbereiches-Server
Virenscan		Während der Installation müssen Sie alle Virenscanner vollständig deaktivieren. Nach der Installation müssen die Pfade, die von der Software Acquisition Unit verwendet werden, vom Virenscan ausgeschlossen werden.

Zusätzliche Empfehlungen

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

Bezüglich Der Größenanpassung

Sie können mit einer Cloud Insights Acquisition Unit mit nur 8 GB Speicher und 50 GB Festplattenspeicher beginnen. In größeren Umgebungen sollten Sie sich jedoch die folgenden Fragen stellen:

Vorteile:

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

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

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

Konfigurieren Von Akquisitionseinheiten

Cloud Insights erfasst Gerätedaten mit einer oder mehreren auf lokalen Servern installierten Erfassungseinheiten. Jede Erfassungseinheit kann mehrere Datensammler hosten, die Gerätemetriken zur Analyse an Cloud Insights senden.

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

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

Hinzufügen einer Linux-Akquisitionseinheit

Bevor Sie beginnen

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

Schritte für die Installation der Linux-Erfassungseinheit

1. Melden Sie sich als Administrator oder Account-Inhaber in Ihrer Cloud Insights-Umgebung an.
2. Klicken Sie Auf **Admin > Datensammler > Akquisitionseinheiten > +Akquisitionseinheit**

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

[Anweisungen für Linux AU]

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

Nachdem Sie fertig sind

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

Festlegen von Proxy-Umgebungsvariablen

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

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

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

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

Proxy-Konfiguration

Die Akquisitionseinheit verwendet eine 2-Wege-/gegenseitige Authentifizierung, um eine Verbindung zum Cloud Insights-Server herzustellen. Das Clientzertifikat muss an den Cloud Insights-Server zur Authentifizierung übergeben werden. Dazu muss der Proxy so eingerichtet sein, dass er die https-Anforderung an den Cloud Insights-Server weitergibt, ohne die Daten zu entschlüsseln.

Am einfachsten ist es, die Platzhalterkonfiguration in Ihrem Proxy/Firewall anzugeben, um mit Cloud Insights zu kommunizieren, z.B.:

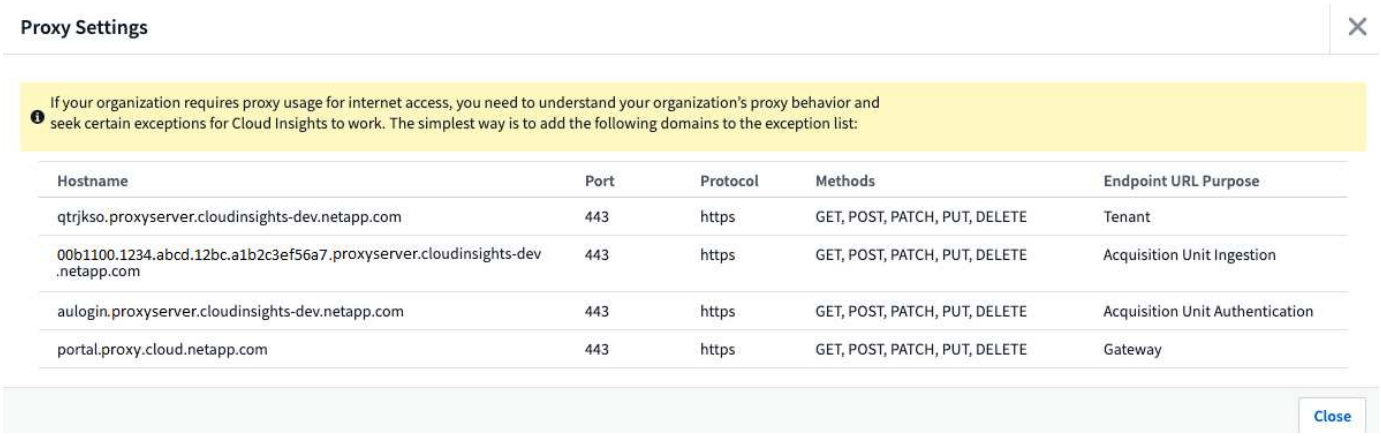
```
*.cloudinsights.netapp.com
```

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

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

Anzeigen von Proxy-URLs

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



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

Hinzufügen einer Windows-Erfassungseinheit

Schritte für die Installation der Windows-Erfassungseinheit

1. Melden Sie sich als Benutzer mit Administratorrechten beim Server/der VM der Erfassungseinheit an.
2. Öffnen Sie auf diesem Server ein Browserfenster, und melden Sie sich als Administrator oder Kontoinhaber in Ihrer Cloud Insights-Umgebung an.
3. Klicken Sie Auf **Admin > Datensammler > Akquisitionseinheiten > +Akquisitionseinheit** .

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

[Windows AU Installation] | *NewWindowsAUInstall.png*

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

Nachdem Sie fertig sind

- Klicken Sie auf **Admin > Data Collectors > Acquisition Units**, um den Status der Akquisitionseinheiten zu überprüfen.

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

```
cloudinsights-service.sh
```

Proxy-Konfiguration

Die Akquisitionseinheit verwendet eine 2-Wege-/gegenseitige Authentifizierung, um eine Verbindung zum Cloud Insights-Server herzustellen. Das Clientzertifikat muss an den Cloud Insights-Server zur Authentifizierung übergeben werden. Dazu muss der Proxy so eingerichtet sein, dass er die https-Anforderung an den Cloud Insights-Server weitergibt, ohne die Daten zu entschlüsseln.

Am einfachsten ist es, die Platzhalterkonfiguration in Ihrem Proxy/Firewall anzugeben, um mit Cloud Insights zu kommunizieren, z.B.:

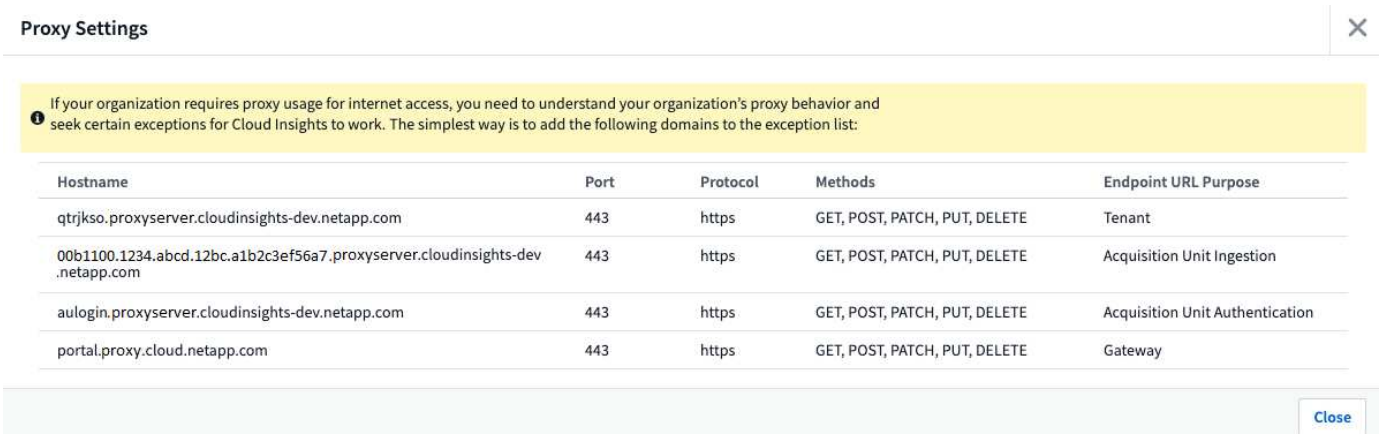
```
*.cloudinsights.netapp.com
```

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

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

Anzeigen von Proxy-URLs

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



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

Deinstallation einer Akquisitionseinheit

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

Windows:

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

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

Linux:

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

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

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

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

Windows und Linux:

Nach die AU deinstallieren:

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

HINWEIS: Die Standarderfassungseinheit kann nicht gelöscht werden. Wählen Sie eine andere AU als Standard aus, bevor Sie die alte löschen.

Erneutes Installieren einer Erfassungseinheit

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

Bevor Sie beginnen

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

Schritte

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

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

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

Anzeigen von AU-Details

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

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

[BEISPIEL FÜR DIE SEITE AU Detail]

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

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

Konfigurieren eines Agenten zum Erfassen von Daten (Windows/Linux/Mac)

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

Die aktuelle Telegraf-Version für Cloud Insights ist **1.24.0**.

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

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

Installieren eines Agenten

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

- Windows
- RHEL und CentOS
- Ubuntu und Debian
- MacOS
- Kubernetes

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

1. Melden Sie sich beim Host an, den Sie für Ihren Agenten verwenden werden.
2. Melden Sie sich auf Ihrer Cloud Insights-Website an und gehen Sie zu **Admin > Datensammler**.

3. Klicken Sie auf **+Data Collector** und wählen Sie einen zu installierenden Datensammler aus.
4. Wählen Sie die geeignete Plattform für Ihren Host (Windows, Linux, macOS usw.)
5. Befolgen Sie die verbleibenden Schritte für jede Plattform.

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

Sobald Sie einen Agent auf einem Server/einer VM installiert haben, sammelt Cloud Insights Kennzahlen von diesem System und sammelt Daten von allen von Ihnen konfigurierten Datensammlern. Diese Kennzahlen werden als erfasst "Node-Metriken".

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

Windows

Voraussetzungen:

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

Proxy-Unterstützung für Windows wird konfiguriert

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

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

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

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

Installieren des Agenten

[Windows Agent-Installation]

Schritte zur Installation von Agent unter Windows:

1. Wählen Sie einen Agent-Zugriffsschlüssel aus.
2. Kopieren Sie den Befehlsblock aus dem Agent-Installationsdialog. Sie können auf das Clipboard-Symbol klicken, um den Befehl schnell in die Zwischenablage zu kopieren.
3. Öffnen Sie ein PowerShell-Fenster

4. Fügen Sie den Befehl in das PowerShell Fenster ein, und drücken Sie die Eingabetaste.
5. Der Befehl lädt das entsprechende Agent-Installationsprogramm herunter, installiert es und legt eine Standardkonfiguration fest. Nach Abschluss des Vorgangs wird der Agent-Service neu gestartet. Der Befehl hat einen eindeutigen Schlüssel und ist 24 Stunden lang gültig.
6. Klicken Sie auf **Fertig** oder **Weiter**

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

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

Deinstallieren des Agenten

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

1. Stoppen und löschen Sie den Telegraf-Dienst:

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

2. Entfernen Sie das Zertifikat aus dem trustore:

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

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

Aktualisieren des Agenten

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

1. Stoppen und löschen sie den telegraf-Dienst:

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

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

5. "Installieren Sie den neuen Agenten".

RHEL und CentOS

Voraussetzungen:

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

Proxy-Unterstützung für RHEL/CentOS wird konfiguriert

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

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

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

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

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

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

Installieren des Agenten

[RHEL/CentOS Agent Installation]

Schritte zum Installieren von Agent auf RHEL/CentOS:

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

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

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

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

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

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

Deinstallieren des Agenten

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

1. Stoppen Sie den Telegraf-Service:

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

2. Entfernen Sie den Telegraf-Agent:

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

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

Aktualisieren des Agenten

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

1. Stoppen sie den telegraf-Service:

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

2. Entfernen Sie den vorherigen telegraf-Agent:

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

Ubuntu und Debian

Voraussetzungen:

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

Proxy-Unterstützung für Ubuntu/Debian konfigurieren

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

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

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

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

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

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

Installieren des Agenten

[Ubuntu/Debian Agent Install]

Schritte zur Installation von Agent auf Debian oder Ubuntu:

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

Befehl hat einen eindeutigen Schlüssel und ist 24 Stunden lang gültig.

6. Klicken Sie auf **Fertig** oder **Weiter**

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

Wenn Ihr Betriebssystem systemd verwendet:

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

Wenn Ihr Betriebssystem keine systemd verwendet:

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

Deinstallieren des Agenten

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

1. Stoppen Sie den Telegraf-Service:

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

2. Entfernen Sie den Telegraf-Agent:

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

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

Aktualisieren des Agenten

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

1. Stoppen sie den telegraf-Service:

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

2. Entfernen Sie den vorherigen telegraf-Agent:

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

MacOS

Voraussetzungen:

- Folgende Befehle müssen verfügbar sein: Curl, sudo, openssl und shasum
- Wenn Sie sich hinter einem Proxy befinden, müssen Sie die Anweisungen im Abschnitt * Proxy-Unterstützung für macOS* befolgen.

Proxy-Unterstützung für macOS wird konfiguriert

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

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

Führen Sie bei Systemen, die sich hinter einem Proxy befinden, folgende Schritte aus, um die Umgebungsvariable *https_Proxy* und/oder *http_Proxy* für den aktuellen Benutzer **VOR** zur Installation des Telegraf-Agenten festzulegen:

```
 export https_proxy=<proxy_server>:<proxy_port>
*NACH* Installation des Telegraf-Agenten, fügen Sie die entsprechende
_https_Proxy_ und/oder _http_Proxy_ Variable(en) in
_/Applications/telegraf.App/Contents/telegraf.plist_: hinzu und setzen Sie
sie ein
```

```
…
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
   <key>EnvironmentVariables</key>
   <dict>
          <key>https_proxy</key>
          <string><proxy_server>:<proxy_port></string>
   </dict>
   <key>Program</key>
   <string>/Applications/telegraf.app/Contents/MacOS/telegraf</string>
   <key>Label</key>
   <string>telegraf</string>
   <key>ProgramArguments</key>
   <array>
     <string>/Applications/telegraf.app/Contents/MacOS/telegraf</string>
     <string>--config</string>
     <string>/usr/local/etc/telegraf.conf</string>
     <string>--config-directory</string>
     <string>/usr/local/etc/telegraf.d</string>
   </array>
   <key>RunAtLoad</key>
   <true/>
</dict>
</plist>
…
```

Starten Sie dann Telegraf nach dem Laden der oben genannten Änderungen neu:

```
sudo launchctl stop telegraf
sudo launchctl unload -w /Library/LaunchDaemons/telegraf.plist
sudo launchctl load -w /Library/LaunchDaemons/telegraf.plist
sudo launchctl start telegraf
```

Installieren des Agenten

[MacOS Agent-Installation]

Schritte zum Installieren von Agent auf macOS:

1. Wählen Sie einen Agent-Zugriffsschlüssel aus.
2. Kopieren Sie den Befehlsblock aus dem Agent-Installationsdialog. Sie können auf das Clipboard-Symbol klicken, um den Befehl schnell in die Zwischenablage zu kopieren.

3. Öffnen Sie ein Fenster „Bash“
4. Fügen Sie den Befehl in das Fenster „Bash“ ein, und drücken Sie die Eingabetaste.
5. Der Befehl lädt das entsprechende Agent-Installationsprogramm herunter, installiert es und legt eine Standardkonfiguration fest. Nach Abschluss des Vorgangs wird der Agent-Service neu gestartet. Der Befehl hat einen eindeutigen Schlüssel und ist 24 Stunden lang gültig.
6. Wenn Sie zuvor einen Telegraf-Agent mit Homebrew installiert haben, werden Sie aufgefordert, ihn zu deinstallieren. Nachdem der zuvor installierte Telegraf Agent deinstalliert wurde, führen Sie den Befehl in Schritt 5 erneut aus.
7. Klicken Sie auf **Fertig** oder **Weiter**

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

```
sudo launchctl start telegraf
sudo launchctl stop telegraf
```

Deinstallieren des Agenten

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

1. Stoppen Sie den Telegraf-Service:

```
 sudo launchctl stop telegraf
. Deinstallieren Sie den telegraf-Agent:
```

```
sudo cp /Applications/telegraf.app/scripts/uninstall /tmp
sudo /tmp/uninstall
```

2. Entfernen Sie alle Konfigurations- oder Protokolldateien, die zurückgelassen werden können:

```
sudo rm -rf /usr/local/etc/telegraf*
sudo rm -rf /usr/local/var/log/telegraf.*
```

Aktualisieren des Agenten

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

1. Stoppen sie den telegraf-Service:

```
 sudo launchctl stop telegraf
. Deinstallieren Sie den vorherigen telegraf-Agent:
```

```
sudo cp /Applications/telegraf.app/scripts/uninstall /tmp
sudo /tmp/uninstall
```

2. "Installieren Sie den neuen Agenten".

{Leer} {leer} {leer} {leer} {leer} leer {Leer}

Kubernetes

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

Bitte **"Los geht hier"** Informationen und Installationsanweisungen für den NetApp Kubernetes Monitoring Operator.

{Leer} {leer} {leer} {leer} {leer} leer {Leer}

Prüfsummen Werden Überprüft

Das Cloud Insights Agent-Installationsprogramm führt Integritätsprüfungen durch. Einige Benutzer müssen jedoch vor der Installation oder Anwendung heruntergeladener Artefakte möglicherweise ihre eigenen Überprüfungen durchführen. Dazu können Sie das Installationsprogramm herunterladen und eine Prüfsumme für das heruntergeladene Paket erstellen. Anschließend wird die Prüfsumme mit dem in der Installationsanleitung angegebenen Wert verglichen.

Laden Sie das Installationspaket herunter, ohne es zu installieren

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

Führen Sie hierzu folgende Schritte aus:

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

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

- Download und Installation (Standard):

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

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

Windows:

- Download und Installation (Standard):

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

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

Der Download-Only-Befehl lädt alle erforderlichen Artefakte vom Cloud Insights in das Arbeitsverzeichnis herunter. Die Artefakte umfassen, dürfen aber nicht beschränkt sein auf:

- Ein Installationsskript
- Einer Umgebungsdatei
- YAML-Dateien
- Eine signierte Prüfsummendatei (endet in shar256.signierte oder sha256.ps1)
- Eine PEM-Datei (netapp_cert.pem) zur Signaturverifizierung

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

Die PEM-Datei kann durch Bestätigung des Fingerabdrucks wie folgt verifiziert werden:

```
 1A918038E8E127BB5C87A202DF173B97A05B4996
Genauer gesagt,
```

- Nicht Windows:

```
 openssl x509 -fingerprint -sha1 -noout -inform pem -in netapp_cert.pem
* Windows:
```

```
Import-Certificate -Filepath .\netapp_cert.pem -CertStoreLocation
Cert:\CurrentUser\Root
```

Prüfsummenwert generieren

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

- RHEL/Ubuntu:

```
 sha256sum <package_name>
* MacOS:
```

```
 shasum -a 256 telegraf.pkg
* Windows:
```

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

Überprüfen Sie die Prüfsumme mithilfe der PEM-Datei

Die signierte Prüfsummendatei kann mit der PEM-Datei verifiziert werden:

- Nicht Windows:

```
 openssl smime -verify -in telegraf*.sha256.signed -CAfile
netapp_cert.pem -purpose any
* Windows (nach der Installation des Zertifikats über Import-Zertifikat
oben):
```

```
Get-AuthenticodeSignature -FilePath .\telegraf.zip.sha256.ps1
$result = Get-AuthenticodeSignature -FilePath .\telegraf.zip.sha256.ps1
$signer = $result.SignerCertificate
Add-Type -Assembly System.Security
[Security.Cryptography.x509Certificates.X509Certificate2UI]::DisplayCertif
icate($signer)
```

Installieren Sie das heruntergeladene Paket

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

Nicht Windows:

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

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

Fehlerbehebung

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

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

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

Konfiguration des NetApp Kubernetes Monitoring Operator

Cloud Insights verwendet u. a. verschiedene Komponenten "Fließendes Bit" Und "Telegraf", Für die Erfassung von Kubernetes-Daten. Telegraf ist ein Plug-in-gestützter Server-Agent, mit dem Kennzahlen, Ereignisse und Protokolle erfasst und protokolliert werden können. Input-Plugins werden verwendet, um die gewünschten Informationen in den Agenten zu sammeln, indem Sie direkt auf das System/Betriebssystem zugreifen, indem Sie APIs von Drittanbietern aufrufen oder konfigurierte Streams (d. h. anhören Kafka, StatsD usw.). Mit Output-Plug-ins werden die gesammelten Metriken, Ereignisse und Protokolle vom Agenten an Cloud Insights gesendet.

Cloud Insights bietet die Sammlung **NetApp Kubernetes Monitoring Operator** (NKMO) für Kubernetes an. Wählen Sie beim Hinzufügen eines Datensammlers einfach die Kachel „Kubernetes“.

[Kubernetes Data Collector]

Unten finden Sie eine allgemeine Abbildung, die zeigt, wo sich der Bediener in Ihrer Umgebung befindet. Je nach Umgebung ist *Proxy Server* möglicherweise erforderlich oder nicht.

[Eine Übersichtskarte mit NKMO im Kubernetes-Cluster. Die Pfeile zeigen, wie die Daten von den Hosts, dem Proxyserver, zum Cluster übertragen werden, wobei alles auf Cloud Insights hochläuft]

Der Betreiber (NKMO) und die Datensammler werden aus der Cloud Insights Docker Registry heruntergeladen. Nach der Installation verwaltet NKMO dann alle Operator-kompatiblen Kollektoren, die in den Kubernetes-Cluster-Knoten zur Datengewinnung bereitgestellt werden, einschließlich der Verwaltung des Lebenszyklus dieser Kollektoren. Nach dieser Kette werden die Daten von den Sammlern erfasst und an Cloud Insights gesendet.

Vor der Installation des NetApp Kubernetes Monitoring Operator

Voraussetzungen:

- Beachten Sie bitte die folgenden Komponentenversionen. Dies sind die aktuellen *required* Versionen, die vom NetApp Kubernetes Monitoring Operator enthalten sind. Diese Versionen müssen Sie besonders beachten, wenn Sie sind Verwenden eines benutzerdefinierten oder privaten Docker Repositorys:
  - Telegraf: 1.25.0
  - kube-rbac-Proxy: V0.13.0
  - kube-State-Metriken: V2.6.0
  - Fließendes Bit: 1.9.8
  - kubernetes-Event-Exporter: Version 0.10
- Die Installation des NetApp Kubernetes Monitoring Operator wird mit Kubernetes Version 1.20 oder neuer unterstützt.
- Wenn Cloud Insights den Back-End-Storage überwacht und Kubernetes bei der Laufzeit des Docker Containers verwendet wird, kann Cloud Insights POD-to-PV-to-Storage-Zuordnungen sowie Kennzahlen für NFS und iSCSI anzeigen. Andere Laufzeiten zeigen nur NFS an.
- Ab August 2022 unterstützt der NetApp Kubernetes Monitoring Operator Pod Security Policy (PSP). Unbedingt Upgrade Den neuesten NetApp Kubernetes Monitoring Operator finden, wenn in Ihrer Umgebung PSP verwendet wird.
- Wenn Sie auf OpenShift 4.6 oder höher laufen, müssen Sie die **OpenShift-Anweisungen** weiter unten befolgen. Außerdem müssen Sie sicherstellen, dass diese Voraussetzungen erfüllt sind.
- Die Überwachung ist nur auf Linux Knoten installiert

  Cloud Insights unterstützt das Monitoring von Kubernetes-Nodes, auf denen Linux ausgeführt wird, indem eine Kubernetes-Node-Auswahl angegeben wird, die auf diesen Plattformen die folgenden Kubernetes-Labels berücksichtigt:

Plattform	Etikett
Kubernetes v1.20 und höher	Kubernetes.io/os = linux
Rancher + Cattle.io als Orchestrierungs-/Kubernetes-Plattform	Cattle.io/os = linux

- Der NetApp Kubernetes Monitoring Operator und seine Abhängigkeiten (telegraf, kube-State-metrics, Fluentbit, etc.) werden nicht auf Nodes unterstützt, die mit der Arm64-Architektur ausgeführt werden.

- Folgende Befehle müssen verfügbar sein: *Curl, sudo, openssl, sha256sum,* und *kubectl*. Um optimale Ergebnisse zu erzielen, fügen Sie diese Befehle in den PFAD ein. Beachten Sie, dass *kubectl* mindestens mit Zugriff auf die folgenden kubernetes-Objekte konfiguriert werden muss: *Agents, Clusterroles, clusterrolebindings, customresourcedefinitions, Deployments, Namespaces, Rollen, Rollenbindungen, Secrets, Serviceaccounts,* und *Services*. Siehe "Hier" Beispiel für eine .yaml-Datei mit diesen minimalen Clusterrollenberechtigungen.
- Der Host, den Sie für die Installation des NetApp Kubernetes Monitoring Operator verwenden werden, muss für die Kommunikation mit dem Ziel-K8s-Cluster *kubectl* konfiguriert sein. Zudem muss eine Internetverbindung zur Cloud Insights-Umgebung vorhanden sein. Wenn für diesen Host ein Proxy erforderlich ist, um Cloud Insights zu erreichen, befolgen Sie die Anweisungen im Proxy-Unterstützung Wird Konfiguriert Abschnitt.
- Der NetApp Kubernetes Monitoring Operator installiert seine eigenen kube-State-Metriken, um Konflikte mit anderen Instanzen zu vermeiden.
- Wenn Sie sich während der Installation hinter einem Proxy befinden oder wenn Sie den zu überwachenden K8s-Cluster betreiben, befolgen Sie die Anweisungen im Proxy-Unterstützung Wird Konfiguriert Abschnitt.
- Zum Erstellen von Kubernetes-Clusterrollen und Rollenbindungen müssen Sie über die erforderlichen Berechtigungen verfügen.

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

Beachten Sie diese, bevor Sie beginnen

Wenn Sie mit einem laufen Proxy, Haben Sie eine Benutzerdefiniertes Repository, Oder verwenden OpenShift, Lesen Sie die folgenden Abschnitte sorgfältig.

Wenn Sie ein Upgrade von einer früheren Installation durchführen, lesen Sie auch den Aktualisierung Informationsdaten.

Wenn Sie die Installationsdateien vor der Installation des Agenten überprüfen möchten, lesen Sie nach Überprüfen Von Kubernetes Prüfsummen.

Proxy-Unterstützung Wird Konfiguriert

An zwei Stellen können Sie in Ihrer Umgebung einen Proxy verwenden, um den NetApp Kubernetes Monitoring Operator zu installieren. Es kann sich um dieselben oder separate Proxy-Systeme handelt:

- Proxy benötigt bei Ausführung des Installationscodes Snippet (mit "Curl"), um das System, an dem das Snippet ausgeführt wird, mit Ihrer Cloud Insights-Umgebung zu verbinden
- Proxy für die Kommunikation mit Ihrer Cloud Insights Umgebung durch das Ziel-Kubernetes-Cluster

Wenn Sie einen Proxy für diesen oder beide verwenden, müssen Sie für die Installation des NetApp Kubernetes Operating Monitor zunächst sicherstellen, dass Ihr Proxy konfiguriert ist und eine gute Kommunikation mit Ihrer Cloud Insights-Umgebung ermöglicht. Wenn Sie über einen Proxy verfügen und über den Server/die VM auf Cloud Insights zugreifen können, von dem aus Sie den Operator installieren möchten, wird Ihr Proxy wahrscheinlich richtig konfiguriert.

Legen Sie für den Proxy, der zur Installation des NetApp Kubernetes Operating Monitor verwendet wurde, vor der Installation des Operators die Umgebungsvariablen *http_Proxy/https_Proxy* fest. In einigen Proxy-Umgebungen müssen Sie möglicherweise auch die Variable *no_Proxy Environment* festlegen.

Um die Variable(en) festzulegen, führen Sie auf Ihrem System **vor** der Installation des NetApp Kubernetes

Monitoring Operators folgende Schritte aus:

1. Legen Sie die Umgebungsvariable *https_Proxy* und/oder *http_Proxy* für den aktuellen Benutzer fest:
   a. Wenn der Proxy, der eingerichtet wird, keine Authentifizierung (Benutzername/Passwort) aufweist, führen Sie den folgenden Befehl aus:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Wenn der Proxy, der eingerichtet wird, über Authentifizierung
(Benutzername/Passwort) verfügt, führen Sie folgenden Befehl aus:
```

```
export http_proxy=
<proxy_username>:<proxy_password>@<proxy_server>:<proxy_port>
```

Nachdem Sie alle diese Anweisungen gelesen haben, installieren Sie den Proxy, der für die Kommunikation Ihres Kubernetes Clusters mit Ihrer Cloud Insights-Umgebung verwendet wurde.

Um die Konfiguration abzuschließen, führen Sie folgende Schritte auf dem System durch **nach** haben Sie den NetApp Kubernetes Monitoring Operator installiert.

Öffnen Sie zunächst die Datei *Agent-Monitoring-netapp* zur Bearbeitung:

```
 kubectl -n netapp-monitoring edit agent agent-monitoring-netapp
Suchen Sie den Abschnitt *spec:* dieser Datei und fügen Sie den folgenden
Code hinzu:
```

```
proxy:

# If an AU is enabled on your cluster for monitoring
# by Cloud Insights, then isAuProxyEnabled should be set to true:
 isAuProxyEnabled: <true or false>

# If your Operator install is behind a corporate proxy,
# isTelegrafProxyEnabled should be set to true:
 isTelegrafProxyEnabled: <true or false>

# If LOGS_COLLECTION is enabled on your cluster for monitoring
# by CI, then isFluentbitProxyEnabled should be set to true:
 isFluentbitProxyEnabled: <true or false>

# Set the following values according to your proxy login:
 password: <password for proxy, optional>
 port: <port for proxy>
 server: <server for proxy>
 username: <username for proxy, optional

# In the noProxy section, enter a comma-separated list of
# IP addresses and/or resolvable hostnames that should bypass
# the proxy:
 noProxy: <comma separated list>
```

Verwenden eines benutzerdefinierten oder privaten Docker Repositorys

Standardmäßig werden in der Konfiguration des NetApp Kubernetes Monitoring Operator Container-Images aus öffentlichen Registrys übertragen. Wenn Sie über ein Kubernetes-Cluster verfügen, das als Ziel für das Monitoring verwendet wird, Dieses Cluster ist so konfiguriert, dass nur Container-Images aus einem benutzerdefinierten oder privaten Docker Repository oder einer Container-Registrierung entfernt werden. Daher müssen Sie den Zugriff auf die Container konfigurieren, die vom NetApp Kubernetes Monitoring Operator benötigt werden, damit die erforderlichen Befehle ausgeführt werden können.

Verwenden Sie die folgenden Anweisungen, um Container-Images in Ihrer Registrierung vorab zu positionieren und die Konfiguration des NetApp Kubernetes Monitoring Operator zu ändern, um auf diese Images zuzugreifen. Ersetzen Sie Ihren gewählten Installations-Namespace in den folgenden Befehlen, wenn er sich vom Standard-Namespace von „netapp-Monitoring“ unterscheidet.

1. Informieren Sie sich über den Docker:

```
 kubectl -n netapp-monitoring get secret docker -o yaml
. Den Wert von _.dockerconfigjson:_ aus der Ausgabe des obigen Befehls
kopieren/einfügen.
. Decodieren des Dockers Secret:
```

```
echo <paste from _.dockerconfigjson:_ output above> | base64 -d
```

Die Ausgabe dieser wird im folgenden JSON-Format vorliegen:

```
{ "auths":
  {"docker.<cluster>.cloudinsights.netapp.com" :
    {"username":"<tenant id>",
     "password":"<password which is the CI API token>",
     "auth"    :"<encoded username:password basic auth token. This is
internal to docker>"}
  }
}
```

Melden Sie sich beim Docker Repository an:

```
docker login docker.<cluster>.cloudinsights.netapp.com (from step #2) -u
<username from step #2>
password: <password from docker secret step above>
```

Ziehen Sie das Fahrerandockerbild aus dem Cloud Insights. Stellen Sie sicher, dass die Versionsnummer *netapp-Monitoring* aktuell ist:

```
docker pull docker.<cluster>.cloudinsights.netapp.com/netapp-
monitoring:<version>
docker pull docker.<cluster>.cloudinsights.netapp.com/distroless-root-
user:<version>
```

Suchen Sie das Feld „*netapp-Monitoring* <Version>“ mit dem folgenden Befehl:

```
 kubectl -n netapp-monitoring describe deployment monitoring-operator |
grep -i "image:" |grep netapp-monitoring
Laden Sie alle Open-Source-Abhängigkeiten in Ihre private Docker-
Registrierung herunter. Die folgenden Open-Source-Images müssen
heruntergeladen werden. Siehe <<before-installing-the-netapp-kubernetes-
monitoring-operator,Voraussetzungen>> Abschnitt oben für die aktuellsten
Versionen dieser Komponenten:
```

```
docker pull docker.<cluster>.cloudinsights.netapp.com/telegraf:<telegraf
version>
docker pull docker.<cluster>.cloudinsights.netapp.com/kube-rbac-
proxy:<kube-rbac-proxy version>
docker pull docker.<cluster>.cloudinsights.netapp.com/kube-state-
metrics:<kube-state-metrics version>
```

Wenn fließendes Bit aktiviert ist, laden Sie auch Folgendes herunter:

```
docker pull docker.<cluster>.cloudinsights.netapp.com/fluent-bit:<fluent-
bit version>
docker pull docker.<cluster>.cloudinsights.netapp.com/kubernetes-event-
exporter:<kubernetes-event-exporter version>
```

Übertragen Sie das Operator-Docker-Image gemäß Ihren Unternehmensrichtlinien in das private/lokale/unternehmenseigene Docker-Repository. Stellen Sie sicher, dass die Verzeichnispfade zu diesen Bildern in Ihrem Repository mit denen in Docker.<cluster>.cloudinsights.netapp.com übereinstimmen.

Bearbeiten Sie die Bereitstellung des Monitoring-Operators, und ändern Sie alle Bildreferenzen, um den neuen Speicherort für den Docker Repo zu verwenden:

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Bearbeiten Sie das Agent CR, um den neuen Repoort des Dockers wiederzugeben.

```
kubectl -n netapp-monitoring edit agent agent-monitoring-netapp
```

```
docker-repo: <docker repo of the enterprise/corp docker repo>
dockerRepoSecret: <optional: name of the docker secret of enterprise/corp
docker repo, this secret should be already created on the k8s cluster in
the same namespace>
```

Nehmen Sie im Abschnitt *spec:* folgende Änderungen vor:

```
spec:
  telegraf:
    - name: ksm
      substitutions:
        - key: k8s.gcr.io
          value: <same as "docker-repo" field above>
```

OpenShift-Anweisungen

Wenn Sie auf OpenShift 4.6 oder höher ausgeführt werden, müssen Sie die Einstellung „privilegierter Modus“ ändern. Führen Sie den folgenden Befehl aus, um den Agenten zum Bearbeiten zu öffnen. Wenn Sie einen anderen Namespace als „netapp-Monitoring“ verwenden, geben Sie diesen Namespace in der Befehlszeile an:

```
 kubectl edit agent agent-monitoring-netapp -n netapp-monitoring
Ändern Sie in der Datei _privilegiert-Mode: False_ in _privilegiert-Mode:
True_
```

OpenShift kann zusätzliche Sicherheitsstufen implementieren, die den Zugriff auf einige Kubernetes-Komponenten blockieren könnten.

Installation des NetApp Kubernetes Monitoring Operator

[Bedienerbasierte Installation]

Schritte zur Installation des NetApp Kubernetes Monitoring Operator Agent auf Kubernetes:

1. Geben Sie einen eindeutigen Cluster-Namen und einen eindeutigen Namespace ein. Wenn Sie es sind Aktualisierung Verwenden Sie vom Skript-basierten Agent oder einem vorherigen Kubernetes Operator denselben Cluster-Namen und denselben Namespace.
2. Sobald diese eingegeben wurden, können Sie das Snippet für den Agent Installer kopieren
3. Klicken Sie auf die Schaltfläche, um dieses Snippet in die Zwischenablage zu kopieren.
4. Fügen Sie das Snippet in ein *bash* Fenster ein und führen Sie es aus. Beachten Sie, dass das Snippet einen eindeutigen Schlüssel hat und für 24 Stunden gültig ist.
5. Die Installation wird automatisch ausgeführt. Klicken Sie nach Abschluss des Programms auf die Schaltfläche *Setup abschließen*.

Die Einrichtung ist unvollständig, bis Sie abgeschlossen sind Konfigurieren Sie Ihren Proxy.

Wenn Sie über ein benutzerdefiniertes Repository verfügen, müssen Sie die Anweisungen für befolgen Verwenden eines benutzerdefinierten/privaten Docker-Repositorys.

Aktualisierung

Wenn Sie bereits über einen skriptbasierten Agent verfügen, müssen Sie _ein Upgrade auf den NetApp Kubernetes Monitoring Operator durchführen.

Upgrade vom skriptbasierten Agent auf den NetApp Kubernetes Monitoring Operator

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

1. Notieren Sie sich den Cluster-Namen, der von Cloud Insights anerkannt ist. Sie können den Cluster-Namen anzeigen, indem Sie den folgenden Befehl ausführen. Wenn Ihr Namespace nicht der Standard (*CI-Monitoring*) ist, ersetzen Sie den entsprechenden Namespace:

```
kubectl -n ci-monitoring get cm telegraf-conf -o jsonpath='{.data}'
|grep "kubernetes_cluster ="
```

2. Speichern Sie den K8s-Clusternamen für die Verwendung während der Installation der Bedienerlösung K8s, um die Datenkontinuität zu gewährleisten.

   Wenn Sie sich den Namen des K8s-Clusters in CI nicht merken, können Sie ihn mit der folgenden Befehlszeile aus Ihrer gespeicherten Konfiguration extrahieren:

```
 cat /tmp/telegraf-configs.yaml | grep kubernetes_cluster | head -2
. Entfernen Sie die skriptbasierte Überwachung
```

   Gehen Sie wie folgt vor, um den skriptbasierten Agent auf Kubernetes zu deinstallieren:

   Wenn der Monitoring Namespace ausschließlich für Telegraf genutzt wird:

```
kubectl --namespace ci-monitoring delete
ds,rs,cm,sa,clusterrole,clusterrolebinding -l app=ci-telegraf
```

```
kubectl delete ns ci-monitoring
```

   Wenn zusätzlich zu Telegraf der Monitoring-Namespace für andere Zwecke verwendet wird:

```
 kubectl --namespace ci-monitoring delete
ds,rs,cm,sa,clusterrole,clusterrolebinding -l app=ci-telegraf
. <<installing-the-netapp-kubernetes-monitoring-operator,Installieren>>
Der aktuelle Operator. Verwenden Sie unbedingt denselben Cluster-Namen,
wie oben in Schritt 1 beschrieben.
```

Upgrade auf den aktuellen NetApp Kubernetes Monitoring Operator

Führen Sie die folgenden Befehle für die Aktualisierung der Installation durch, die auf dem Bediener basiert:

- Notieren Sie sich den Cluster-Namen, der von Cloud Insights anerkannt ist. Sie können den Cluster-Namen anzeigen, indem Sie den folgenden Befehl ausführen. Wenn Ihr Namespace nicht der Standard (*netapp-Monitoring*) ist, ersetzen Sie den entsprechenden Namespace:

```
kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
```

Deinstallieren Der aktuelle Operator.

Installieren Der neueste Operator. Verwenden Sie denselben Cluster-Namen und stellen Sie sicher, dass Sie neue Container-Images ziehen, wenn Sie eine benutzerdefinierte Repo eingerichtet haben.

Stoppen und Starten des NetApp Kubernetes Monitoring Operator

So beenden Sie den NetApp Kubernetes Monitoring Operator:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
So starten Sie den NetApp Kubernetes Monitoring Operator:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Deinstallation

Wenn Sie auf einem bereits installierten, skriptbasierten Kubernetes-Agent ausgeführt werden, müssen Sie dies unbedingt tun Upgrade Für den NetApp Kubernetes Monitoring Operator.

Um den veralteten, skriptbasierten Agent zu entfernen

Beachten Sie, dass diese Befehle den Standard-Namespace "CI-Monitoring" verwenden. Wenn Sie Ihren eigenen Namespace festgelegt haben, ersetzen Sie diesen Namespace in diesen und allen nachfolgenden Befehlen und Dateien.

Um den skriptbasierten Agent auf Kubernetes zu deinstallieren (z. B. bei einem Upgrade auf den NetApp Kubernetes Monitoring Operator), gehen Sie folgendermaßen vor:

Wenn der Monitoring Namespace ausschließlich für Telegraf genutzt wird:

```
 kubectl --namespace ci-monitoring delete
ds,rs,cm,sa,clusterrole,clusterrolebinding -l app=ci-telegraf
 kubectl delete ns ci-monitoring
Wenn zusätzlich zu Telegraf der Monitoring-Namespace für andere Zwecke
verwendet wird:
```

```
kubectl --namespace ci-monitoring delete
ds,rs,cm,sa,clusterrole,clusterrolebinding -l app=ci-telegraf
```

Um den NetApp Kubernetes Monitoring Operator zu entfernen

Beachten Sie, dass der Standard-Namespace für den NetApp Kubernetes Monitoring Operator „netapp-Monitoring“ ist. Wenn Sie Ihren eigenen Namespace festgelegt haben, ersetzen Sie diesen Namespace in diesen und allen nachfolgenden Befehlen und Dateien.

Neuere Versionen des Überwachungsoperators können mit den folgenden Befehlen deinstalliert werden:

```
kubectl delete agent -A -l installed-by=nkmo-<name-space>
kubectl delete ns,clusterrole,clusterrolebinding,crd -l installed-by=nkmo-
<name-space>
```

Wenn der erste Befehl „Keine Ressourcen gefunden“ zurückgibt, verwenden Sie die folgenden Anweisungen, um ältere Versionen des Überwachungsoperators zu deinstallieren.

Führen Sie jeden der folgenden Befehle in der Reihenfolge aus. Abhängig von Ihrer aktuellen Installation können einige dieser Befehle Nachrichten ‘object not found’ zurückgeben. Diese Meldungen können sicher ignoriert werden.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Wenn zuvor eine Security Context Constraint manuell für eine skriptbasierte Telegraf-Installation erstellt wurde:

```
kubectl delete scc telegraf-hostaccess
```

Über Kube-State-Metrics

Der NetApp Kubernetes Monitoring Operator installiert kube-State-Metriken automatisch. Gleichzeitig ist keine Interaktion mit den Benutzern erforderlich.

kube-State-Metrics Counters

Verwenden Sie die folgenden Links, um auf Informationen zu diesen kube State-Metriken zuzugreifen:

1. "Kennzahlen für die Konfigmap"

2. "DemonSet Metrics"
3. "Implementierungsmetriken"
4. "Ingress Metrics"
5. "Namespace-Kennzahlen"
6. "Node-Kennzahlen"
7. "Persistente Volume-Kennzahlen"
8. "Kenngrößen Für Die Forderung Im Persistenten Volume"
9. "Pod-Metriken"
10. "Kennzahlen für ReplicaSet"
11. "Geheimkennzahlen"
12. "Service-Kennzahlen"
13. "StatfulSet-Kennzahlen"

Überprüfen Von Kubernetes Prüfsummen

Das Cloud Insights Agent-Installationsprogramm führt Integritätsprüfungen durch. Einige Benutzer müssen jedoch vor der Installation oder Anwendung heruntergeladener Artefakte möglicherweise ihre eigenen Überprüfungen durchführen. Um einen nur-Download-Vorgang durchzuführen (im Gegensatz zum Standard-Download-and-install), können diese Benutzer den Agent-Installation Befehl erhalten von der UI und entfernen Sie die nachhängbare "Installation" Option.

Führen Sie hierzu folgende Schritte aus:

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

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

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

Der Download-Only-Befehl lädt alle erforderlichen Artefakte vom Cloud Insights in das Arbeitsverzeichnis herunter. Die Artefakte umfassen, dürfen aber nicht beschränkt sein auf:

- Ein Installationsskript
- Einer Umgebungsdatei

- YAML-Dateien
- Eine signierte Prüfsumme-Datei (sha256.signed)
- Eine PEM-Datei (netapp_cert.pem) zur Signaturverifizierung

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

Die PEM-Datei kann durch Bestätigung des Fingerabdrucks wie folgt verifiziert werden:

```
 1A918038E8E127BB5C87A202DF173B97A05B4996
Genauer gesagt,
```

```
 openssl x509 -fingerprint -sha1 -noout -inform pem -in netapp_cert.pem
Die signierte Prüfsummendatei kann mit der PEM-Datei verifiziert werden:
```

```
 openssl smime -verify -in sha256.signed -CAfile netapp_cert.pem -purpose
any
Sobald alle Artefakte zufriedenstellend überprüft wurden, kann die
Agenteninstallation durch Ausführen von gestartet werden:
```

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

Einstellung des Bedienpersonals

Sie können den NetApp Kubernetes Monitoring Operator für eine optimale Performance anpassen, indem Sie bestimmte Variablen für benutzerdefinierte Ressourcen Feinabstimmung vornehmen. Anweisungen und Listen der Variablen, die Sie einstellen können, finden Sie in der im Installationspaket enthaltenen README-Datei. Verwenden Sie nach der Installation des Operators den folgenden Befehl, um README anzuzeigen:

```
kubectl exec -c manager -it <operator-pod-name> -n <namespace> -- cat
configs/substitution-vars/README.txt
```

Fehlerbehebung

Einige Dinge, die Sie versuchen können, wenn Probleme bei der Einrichtung des NetApp Kubernetes Monitoring Operators auftreten:

Problem:	Versuchen Sie dies:
Ich sehe keinen Hyperlink/Verbindung zwischen meinem Kubernetes Persistent Volume und dem entsprechenden Back-End Storage-Gerät. Mein Kubernetes Persistent Volume wird mit dem Hostnamen des Storage-Servers konfiguriert.	Befolgen Sie die Schritte, um den bestehenden Telegraf-Agent zu deinstallieren, und installieren Sie dann den neuesten Telegraf-Agent erneut. Sie müssen Telegraf Version 2.0 oder höher verwenden, und Ihr Kubernetes Cluster Storage muss von Cloud Insights aktiv überwacht werden.
Ich sehe Nachrichten in den Protokollen, die folgenden ähneln: E0901 15:21:39.962145 1 Reflektor.go:178] k8s.io/kube-State-metrics/intern/Store/Builder.go:352: Listen fehlgeschlagen *v1.MutatingWebhookKonfiguration: Der Server konnte die angeforderte Ressource E0901 15:21 352:43.168161 1 Reflektor.GO:178] k8s.io/kukio-Verzeichnis nicht gefunden	Diese Nachrichten können auftreten, wenn Sie kube-State-Metrics Version 2.0.0 oder höher mit Kubernetes-Versionen unter 1.20 ausführen. Um die Kubernetes-Version zu erhalten: *Kubectl Version* um die kube-State-metrics-Version zu erhalten: *Kubectl get Deploy/kube-State-metrics -o jsonpath='{..image}'* um zu verhindern, dass diese Nachrichten passieren, können Benutzer ihre kube-State-Metrics-Implementierung ändern, um die folgenden Elemente zu deaktivieren: _Mutingwebhookkonfigurationen___volumehaWeitere Resources=certificationesigningrequests,configmaps, cronjobs,dämsets, Bereitstellungen,Endpunkte,HorizontalpodAutoscaler, nesresses,Jobs,Begrenzungsbereiche,Namensräume, Netzwerkrichtlinien,Knoten,Persistenz,stagemasnesmases,nesmasnesmases,nesmasnesmasnesmasnesnesmasnesequets,ndecoses,nescontascrises,nesequequequesefises,nesequequesequesefiscones,mases,nesequidatequesequesefiscones,nesequesequesefiscrises,nesequesequesefiscones,nesefisconesefisconmases,mases,nesequesequesefiscones,necequesequeseques Validatingwebhookkonfigurationen, Volumeanhänge“
Ich sehe Fehlermeldungen von Telegraf ähnlich wie die folgenden, aber Telegraf startet und läuft: Okt 11 14:23:41 ip-172-31-39-47 systemd[1]: Startete den Plugin-getriebenen Server Agent für das Reporting von Metriken in InfluxDB. Okt 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Time=„2021-10-11T14:23:41Z“ Level=error msg=„konnte kein Cache-Verzeichnis erstellen. /Etc/telegraf/.Cache/snowflake, err: Mkdir /etc/telegraf/.ca che: Berechtigung verweigert. Ignorierte\n" Funktion=„gosnowflake.(*defaultLogger).Errorf“ file=„log.go:120“ Okt 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Time=„2021-10-11T14:23:41Z“ Level=Fehler msg=„konnte nicht geöffnet werden. Ignoriert. Öffnen Sie /etc/telegraf/.Cache/snowflake/ocsp_response_Cache .json: Keine solche Datei oder Verzeichnis\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" Okt 11 14:23:41 ip-172-31-39-47 telegraf[1827 23]: 2021-10-11T14:41I! Telegraf 1.19.3 Starten	Dies ist ein bekanntes Problem. Siehe "Dieser GitHub-Artikel" Entnehmen. Solange Telegraf läuft, können Benutzer diese Fehlermeldungen ignorieren.

Problem:	Versuchen Sie dies:
Auf Kubernetes meldet mein Telegraf pod(s) den folgenden Fehler: „Fehler in der Verarbeitung von mountstats-Infos: Habe mountstats-Datei nicht geöffnet: /Hostfs/proc/1/mountstats, Fehler: Open /hostfs/proc/1/mountstats: Permission dementied“	Wenn SELinux aktiviert ist und die Durchsetzung aktiviert wird, wird wahrscheinlich verhindert, dass Telegraf Pod(s) auf die Datei /proc/1/mountstats auf den Kubernetes Nodes zugreifen. Um diese Einschränkung zu entspannen, bearbeiten Sie den Agenten (`kubectl edit agent agent-monitoring-netapp`), und ändern Sie "Privileged-Mode: False" in "Privileged-Mode: True"
Auf Kubernetes meldet mein Telegraf ReplicaSet POD den folgenden Fehler: [inputs.prometheus] Fehler im Plugin: Konnte keine keypair /etc/kubernetes/pki/etcd/Server.crt:/etc/kubernetes/pki /etcd/Server.key: Öffnen /etc/kubernetes/pki/etcd/Server.crt: Keine solche Datei oder Verzeichnis	Der Pod Telegraf ReplicaSet soll auf einem Knoten ausgeführt werden, der als Master oder für etc bestimmt ist. Wenn der ReplicaSet-Pod auf einem dieser Knoten nicht ausgeführt wird, werden diese Fehler angezeigt. Überprüfen Sie, ob Ihre Master/etcd-Knoten eine Tönungswalle haben. Fügen Sie in diesem Fall die erforderlichen Verträgungen in das Telegraf ReplicaSet, telegraf-rs ein. Bearbeiten Sie zum Beispiel die Datei ReplicaSet… kubectl edit rs telegraf-rs …und fügen Sie die entsprechenden Verträgungen der Spezifikation hinzu. Starten Sie anschließend den Pod ReplicaSet neu.
Ich habe eine PSP/PSA Umgebung. Hat dies Auswirkungen auf meinen Überwachungsperator?	Wenn Ihr Kubernetes Cluster mit der Pod Security Policy (PSP) oder PSA (Pod Security Admission) ausgeführt wird, müssen Sie ein Upgrade auf den aktuellen NetApp Kubernetes Monitoring Operator durchführen. Führen Sie die folgenden Schritte aus, um auf den aktuellen NKMO mit Unterstützung für PSP/PSA zu aktualisieren: 1. Deinstallieren Der vorherige Überwachungsoperator: Kubectl delete Agent-Monitoring-netapp -n netapp-Monitoring kubectl delete ns netapp-Monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrolle Agent-Manager-role Agent-Proxy-role Agent-metrics-reader kubectl delete clusterrolebinding Agent-Manager-rolebinding Agent-Proxy-rolebinding Agent-Proxy-rolebinding Agent-Cluster-admin-rolebinding 2. Installieren Die neueste Version des Überwachungsbedieners.
Bei der Bereitstellung des NKMO begegnete mir Probleme, und PSP/PSA ist im Einsatz.	1. Bearbeiten Sie den Agenten mit dem folgenden Befehl: Kubectl -n <Name-space> Edit Agent 2. Markieren Sie „Sicherheitspolitik aktiviert“ als „falsch“. Dadurch werden Pod Security Policies und Pod Security Admission deaktiviert und die Bereitstellung des NKMO ermöglicht. Bestätigung mit den folgenden Befehlen: Kubectl get psp (sollte Pod Security Policy entfernt zeigen) kubectl get all -n <Namespace> grep -i psp (sollte zeigen, dass nichts gefunden wird)

Problem:	Versuchen Sie dies:
„ImagePullBackoff“-Fehler erkannt	Diese Fehler treten möglicherweise auf, wenn Sie über ein benutzerdefiniertes oder privates Docker Repository verfügen und den NetApp Kubernetes Monitoring Operator noch nicht so konfiguriert haben, dass es richtig erkannt wird. Weitere Informationen Info zur Konfiguration für benutzerdefinierte/private Repo.

Ich habe ein Problem mit der Installation meines Monitoring-Bedieners, und die aktuelle Dokumentation hilft mir nicht, es zu lösen.	Erfassen oder notieren Sie die Ausgabe der folgenden Befehle, und wenden Sie sich an den technischen Support.
	`kubectl -n netapp-monitoring get all`
	`kubectl -n netapp-monitoring describe all`
	`kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true`
	`kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true`

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

Konfigurieren Von Datensammlern

Sie konfigurieren Datensammler in Ihrer Cloud Insights-Umgebung, um Daten von Geräten im Datacenter zu erfassen.

Bevor Sie beginnen

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

Schritte

1. Klicken Sie im Menü Cloud Insights auf **Admin > Datensammler**

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

2. Klicken Sie auf **+ Collector** auf dem gewünschten Anbieter und wählen Sie den zu konfigurierenden Datensammler aus.

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

3. Geben Sie einen Namen für den Datensammler ein.

   Namen können Buchstaben (a-z), Zahlen (0-9), Bindestriche (-), Unterstriche (_), Apostrophe ('), Und Perioden (.).

4. Geben Sie die Erfassungseinheit ein, die diesem Datensammler zugeordnet werden soll.
5. Geben Sie die erforderlichen Felder im Konfigurationsbildschirm ein.
6. Wenn Sie aufgefordert werden, Benachrichtigungen zu konfigurieren, wählen Sie E-Mail, Webhook oder beides und wählen Sie die Alarmtypen aus, die Sie benachrichtigen möchten (kritisch, Warnung, Information und/oder gelöst). Sie können die Liste der Empfänger für den globalen Monitor (konfiguriert in **Admin > Benachrichtigungen**) angeben oder weitere Empfänger angeben. Wenn Sie bereit sind, fortzufahren, klicken Sie auf **Setup abschließen**.

[Sammlerbenachrichtigungen]

Wenn Sie sich eine Landing Page mit **ONTAP-Datensammler** ansehen, können Sie die Benachrichtigungen ändern, indem Sie im Übersichtsbereich des Datensammlers auf das Bleistiftsymbol im Feld „Benachrichtigungen“ klicken.

ONTAP Data Collector-Benachrichtigungen haben Vorrang vor allen spezifischen Monitoring-Benachrichtigungen, die für den Cluster/den Datensammler relevant sind. Die Empfängerliste, die Sie für den Data Collector selbst festgelegt haben, erhält die Warnungen zum Datensammler. Wenn keine aktiven Warnungen zur Datenerfassung vorhanden sind, werden die von Monitor erzeugten Warnmeldungen an bestimmte Überwachungsempfänger gesendet.

[Bearbeiten Von Collector-Benachrichtigungen]

1. Klicken Sie auf **Erweiterte Konfiguration**, um weitere Konfigurationsfelder hinzuzufügen. (Nicht alle Datensammler benötigen erweiterte Konfiguration.)
2. Klicken Sie auf **Testkonfiguration**, um zu überprüfen, ob der Datensammler ordnungsgemäß konfiguriert ist.
3. Klicken Sie auf **Collector hinzufügen**, um die Konfiguration zu speichern und den Datensammler zu Ihrem Cloud Insights-Mandanten hinzuzufügen.

Nach dem Hinzufügen eines neuen Datensammlers leitet Cloud Insights drei Abstimmungen ein:

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

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

Bestimmen des Erfassungsstatus der Datensammlung

Da Datensammler die primäre Informationsquelle für Cloud Insights sind, müssen Sie unbedingt sicherstellen, dass diese im laufenden Zustand bleiben.

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

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

Verwalten von konfigurierten Datensammlern

Die Seite installierte Datensammler bietet Zugriff auf die für Cloud Insights konfigurierten Datensammler. Auf dieser Seite können Sie vorhandene Datensammler ändern.

Schritte

1. Klicken Sie im Menü Cloud Insights auf **Admin > Datensammler**

   Der Bildschirm Verfügbare Datensammler wird angezeigt.

2. Klicken Sie Auf **Installierte Datensammler**

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

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

Kontrollieren der Data Collector-Umfrage

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

Schritte

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

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

Bearbeiten von Daten-Collector-Informationen

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

So bearbeiten Sie einen einzelnen Datensammler:

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

   Das Dialogfeld Collector bearbeiten wird geöffnet.

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

Sie können auch mehrere Datensammler bearbeiten:

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

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

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

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

Klonen von Datensammlern

Mit der Clone Facility können Sie schnell eine Datenquelle hinzufügen, die dieselben Anmeldedaten und Attribute wie eine andere Datenquelle enthält. Klonen ermöglicht Ihnen die einfache Konfiguration mehrerer Instanzen desselben Gerätetyps.

Schritte

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

   Das Dialogfeld Data Collector klonen wird angezeigt.

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

Nachdem Sie fertig sind

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

Ausführen von Massenaktionen auf Datensammlern

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

Schritte

1. Klicken Sie im Menü Cloud Insights auf **Admin > Datensammler**

2. Klicken Sie Auf **Installierte Datensammler**
3. Klicken Sie auf das Kontrollkästchen links neben den Datensammlern, die Sie ändern möchten.
4. Klicken Sie im Optionsmenü rechts auf die gewünschte Option.

Nachdem Sie fertig sind

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

Recherchieren eines fehlgeschlagenen Datensammlers

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

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

Schritte

1. Klicken Sie Auf **Admin** > **Datensammler** > **Installierte Datensammler**.
2. Klicken Sie auf den verknüpften Namen des defekten Datensammlers, um die Seite Zusammenfassung zu öffnen.
3. Auf der Seite Zusammenfassung können Sie im Bereich Kommentare alle Hinweise lesen, die von einem anderen Techniker hinterlassen wurden, der möglicherweise auch diesen Fehler untersucht hat.
4. Notieren Sie alle Leistungsmeldungen.
5. Bewegen Sie den Mauszeiger über die Segmente des Ereigniskleistendiagramms, um zusätzliche Informationen anzuzeigen.
6. Wählen Sie eine Fehlermeldung für ein Gerät aus, die unter der Ereigniszeitleiste angezeigt wird, und klicken Sie auf das Symbol Fehlerdetails rechts neben der Meldung.

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

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

Copyright-Informationen

Markeninformationen