Daten Werden Erfasst

Cloud Insights

NetApp
April 16, 2024

Inhalt

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.

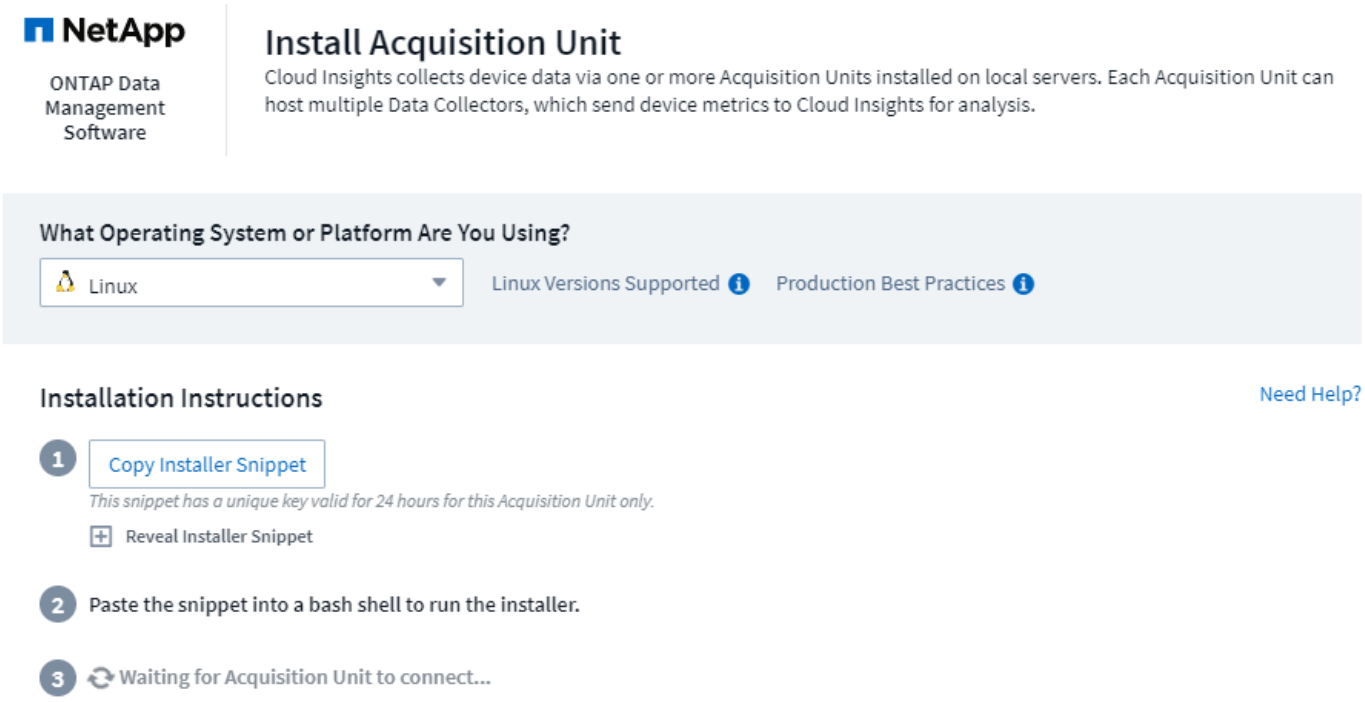
Cloud Insights bietet drei Arten von Datensammlern an:

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

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

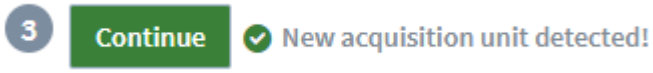
Installieren Sie eine Akquisitionseinheit

Wenn Sie einen 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.



- Folgen Sie den "Anweisungen" Wird angezeigt, um Ihre Akquisitionseinheit zu installieren. Sobald die

Software für die Erfassungseinheit installiert ist, wird die Schaltfläche Weiter angezeigt, und Sie können mit dem nächsten Schritt fortfahren.



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

Konfigurieren Sie den Data Collector - Infrastruktur

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

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

Sie können später zusätzliche Datensammler konfigurieren.

Konfigurieren Sie den Data Collector - Betriebssysteme und Dienste

Betriebssystem:

Wählen Sie für *Betriebssystem* Datensammler eine Plattform (Linux, Windows) aus, um einen Cloud Insights-Agenten 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, auf dem eine lizenzierte Version einer der folgenden Versionen ausgeführt wird: * CentOS (64 Bit): 7.2 bis 7.9, 8.1 bis 8.4, Stream 8, Stream 9 * Debian (64-bit): 9 und 10 * OpenSUSE Leap 15.1 bis 15.5 * Oracle Enterprise Linux (64 Bit): 7.5 bis 7.9, 8.1 bis 8.8 * Red hat Enterprise Linux (64 Bit): 7.2 bis 7.9, 8.1 bis 8.8, 9.1, 9.2 * Rocky 9.0, 9.1, 9.3 * SUSE Enterprise Linux Server 15, 15 SP2 bis 15 SP5 * Ubuntu Server: 18.04, 20.04, 22.04 LTS * SELinux auf den oben genannten Plattformen Auf diesem Computer sollte keine andere Software auf Anwendungsebene ausgeführt werden. Es wird ein dedizierter Server empfohlen. Wenn Sie mit SELinux arbeiten, wird empfohlen, die folgenden Befehle auf dem Erfassungseinheitssystem auszuführen: Sudo semanage fcontext -a -t usr_t "/opt/netapp/Cloudinsights(/.*)?“ Sudo restorecon -R /opt/netapp/Cloud Insights	Ein Computer mit einer lizenzierten Version von einer der folgenden Komponenten: * Microsoft Windows 10 64-Bit * Microsoft Windows Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows 11 auf diesem Computer sollte keine andere Software auf Anwendungsebene ausgeführt werden. Es wird ein dedizierter Server empfohlen.
CPU	2 CPU-Kerne	Gleich
Speicher	8 GB RAM	Gleich

Verfügbarer Festplattenspeicher	50 GB (100 GB empfohlen) Bei Linux sollte der Speicherplatz folgendermaßen zugewiesen werden: /Opt/netapp 10 GB (20 GB für große Umgebungen) /Var/log/netapp 40 GB (80 GB für große Umgebungen) /Tmp mindestens 1 GB während der Installation verfügbar	50 GB
Netzwerk	Ethernet-Verbindung mit 100 Mbit/s/1 Gbit/s, statische IP-Adresse und Anschluss 80 oder 443 von der Erfassungseinheit zu *.cloudinsights.netapp.com oder Ihrer Cloud Insights-Umgebung (d. h. https://<environment_id>.c01.cloudinsights.netapp.com) sind 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? Wenn dies der Fall ist, müssen Sie die folgende Domäne der Ausnahmeliste hinzufügen: *.cloudinsights.netapp.com Weitere Informationen finden Sie unter Proxys "Hier (Linux)" Oder "Hier (Windows)".	Gleich
Berechtigungen	Sudo-Berechtigungen auf dem Akquisitionsgruppenserver. /Tmp muss mit exec-Funktionen montiert werden.	Administratorberechtigungen auf dem Akquisitionsbereiches-Server

Virenscan		Während der Installation müssen Sie alle Virenscanner vollständig deaktivieren. Nach der Installation müssen die Pfade, die von der Software Acquisition Unit verwendet werden, vom Virenscan ausgeschlossen werden.

Zusätzliche Empfehlungen

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

Bezüglich Der Größenanpassung

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.

Zusätzliche Federal Edition-Anforderung

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

Konfigurieren Von Akquisitionseinheiten

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.

Erfahren Sie mehr über Cloud Insights Sicherheit "Hier".

Hinzufügen einer Linux-Akquisitionseinheit

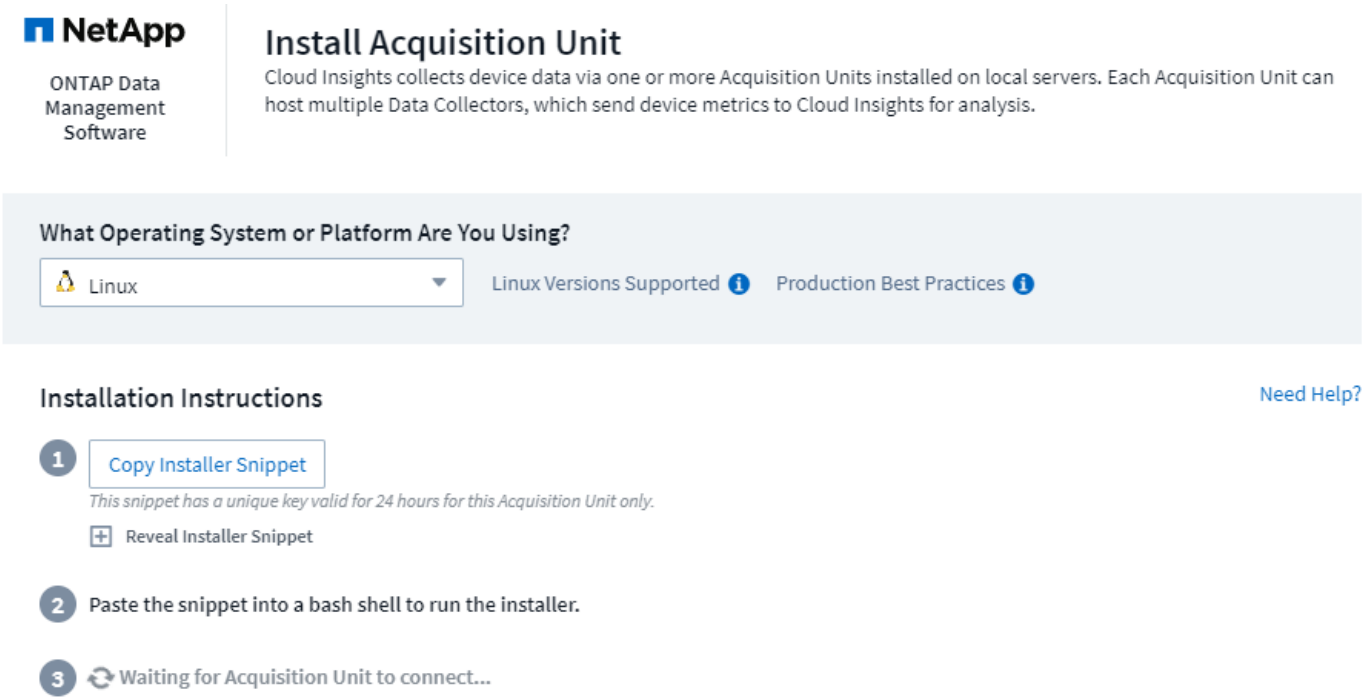
Bevor Sie beginnen

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

Schritte für die Installation der Linux-Erfassungseinheit

1. Melden Sie sich als Administrator oder Account-Inhaber in Ihrer Cloud Insights-Umgebung an.
2. Klicken Sie Auf **Observability > Collectors > Acquisition Units > +Acquisition Unit**

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



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

Nachdem Sie fertig sind

- Klicken Sie auf **Observability > Collectors > Acquisition Units**, um den Status von Acquisition Units zu

überprüfen.

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

Festlegen von Proxy-Umgebungsvariablen

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

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

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

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

Proxy-Konfiguration

Die 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.:

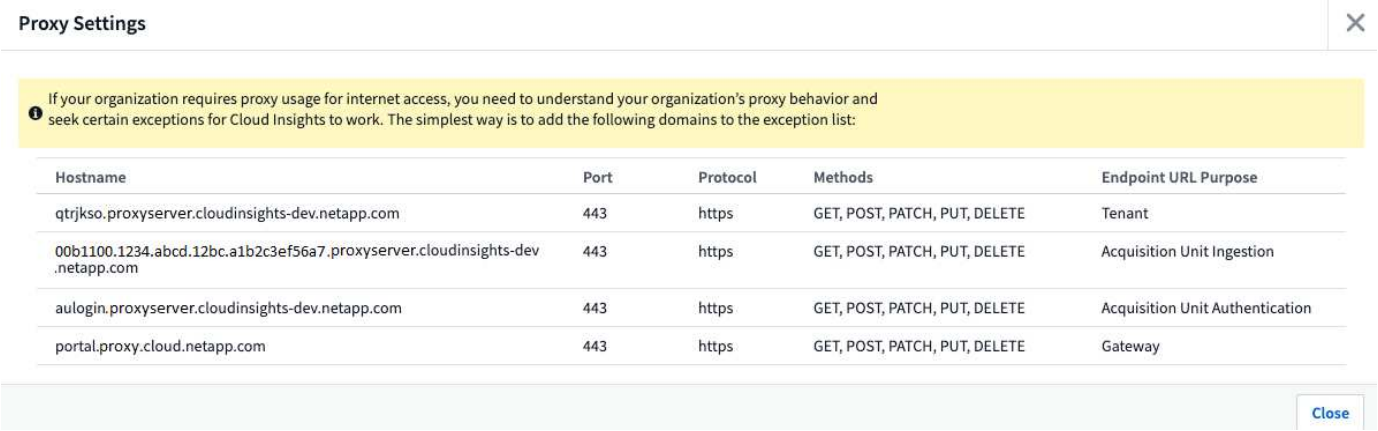
```
*.cloudinsights.netapp.com
```

> 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.



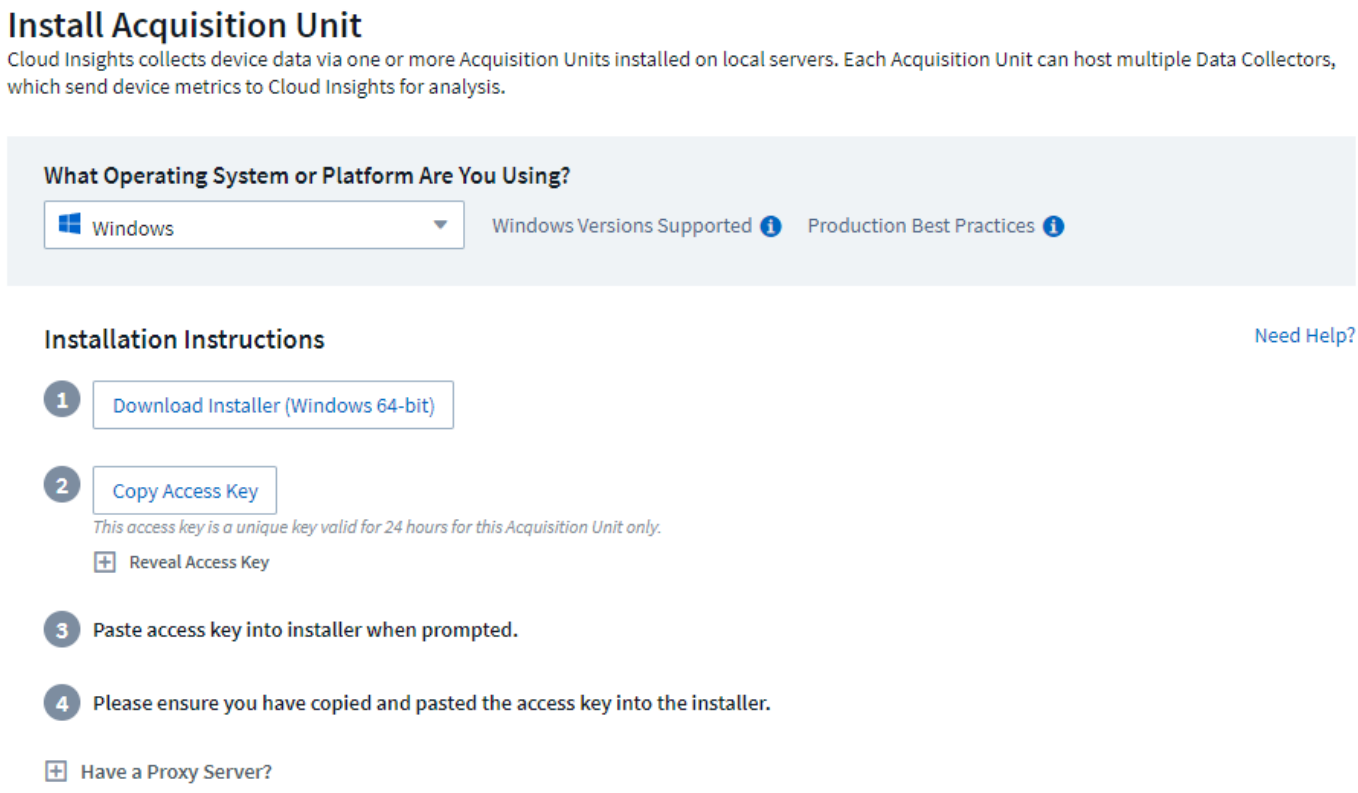
Wenn Sie Workload Security in Ihrer Umgebung haben, werden auch die konfigurierten Endpunkt-URLs in dieser Liste angezeigt.

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 **Observability > Collectors > Acquisition Units > +Acquisition Unit** .

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



1. Vergewissern Sie sich, dass der Server oder die VM, auf dem die Erfassungseinheit gehostet wird, die empfohlenen Systemanforderungen erfüllt.

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

Nachdem Sie fertig sind

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

```
cloudinsights-service.sh
```

Proxy-Konfiguration

Die 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.:

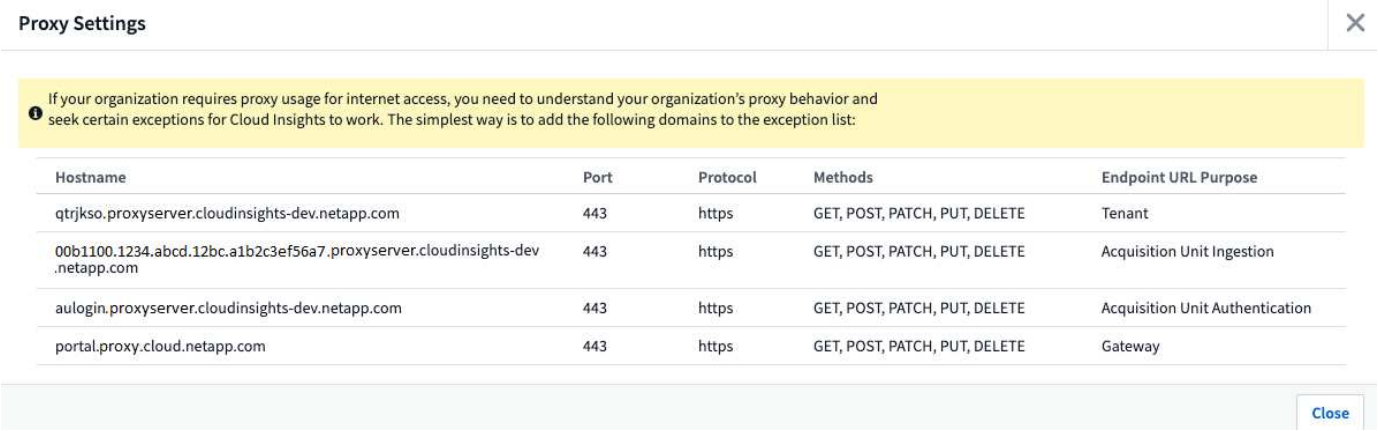
```
*.cloudinsights.netapp.com
```

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

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

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

Erneutes Installieren einer Erfassungseinheit

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

Bevor Sie beginnen

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

Schritte

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

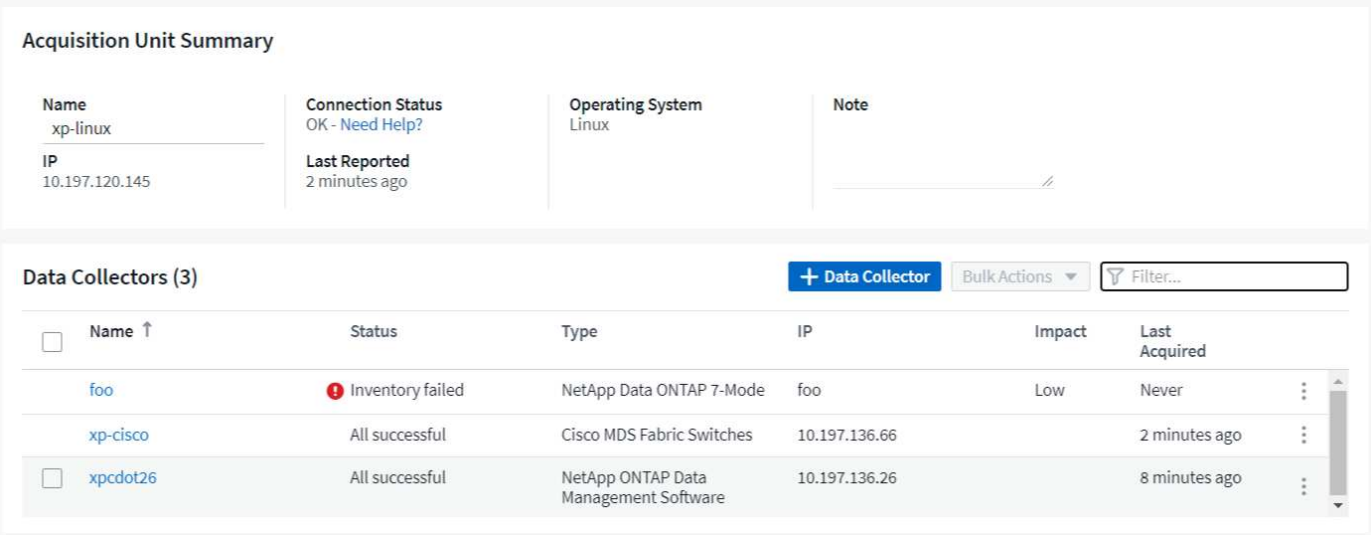
   Sie können auch mehrere Datensammler desselben Typs auswählen und auf die Schaltfläche **Massenaktionen** klicken. Wählen Sie *Bearbeiten* und weisen Sie die Datensammler der temporären Erfassungseinheit zu.

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

Anzeigen von AU-Details

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

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



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

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

Konfigurieren eines Agenten zur Datenerfassung (Windows/Linux)

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**.

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

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

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

Installieren eines Agenten

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

- Windows
- RHEL und CentOS
- Ubuntu und Debian

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

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

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

Sobald Sie einen 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.

Speicherorte Protokollieren

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

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

Windows

Voraussetzungen:

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

Proxy-Unterstützung für Windows wird konfiguriert

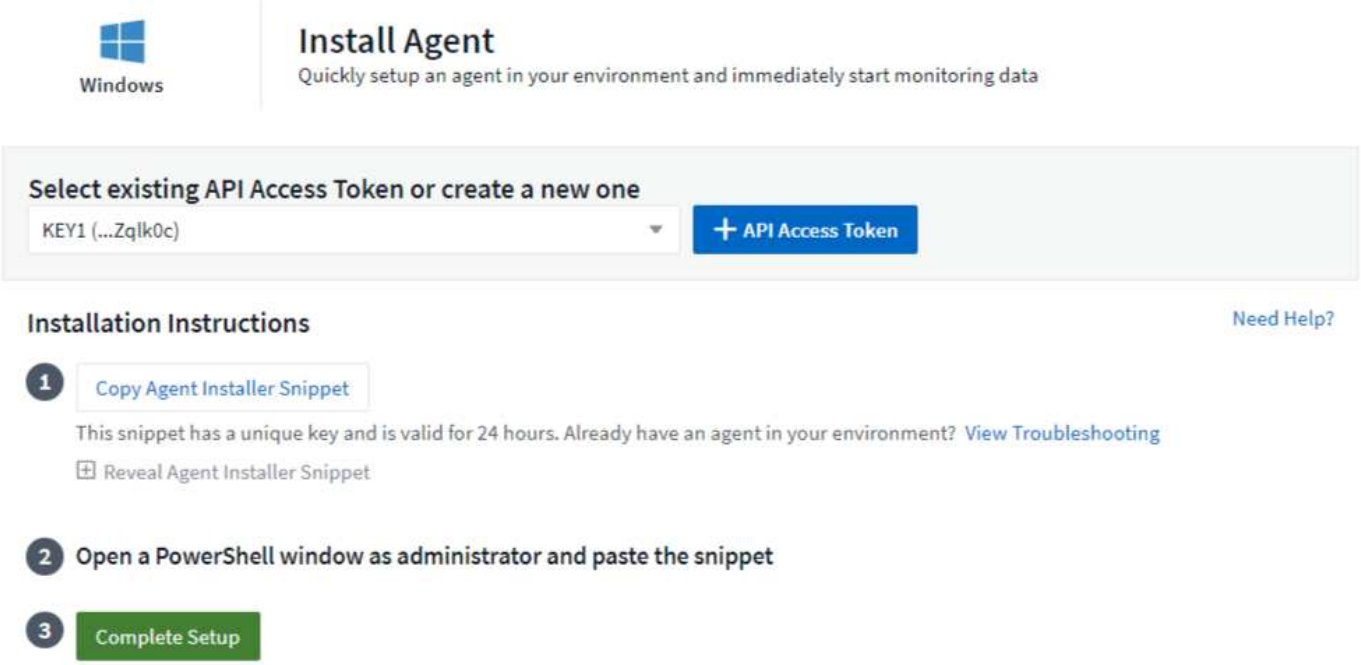
Wenn in Ihrer Umgebung ein Proxy verwendet wird, lesen Sie diesen Abschnitt vor der Installation.

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

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

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

Installieren des Agenten



Schritte zur Installation von Agent unter Windows:

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

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

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

Deinstallieren des Agenten

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

1. Stoppen und löschen Sie den Telegraf-Dienst:

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

2. Entfernen Sie das Zertifikat aus dem trustore:

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

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

Aktualisieren des Agenten

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

1. Stoppen und löschen sie den telegraf-Dienst:

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

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

RHEL und CentOS

Voraussetzungen:

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

Proxy-Unterstützung für RHEL/CentOS wird konfiguriert

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

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

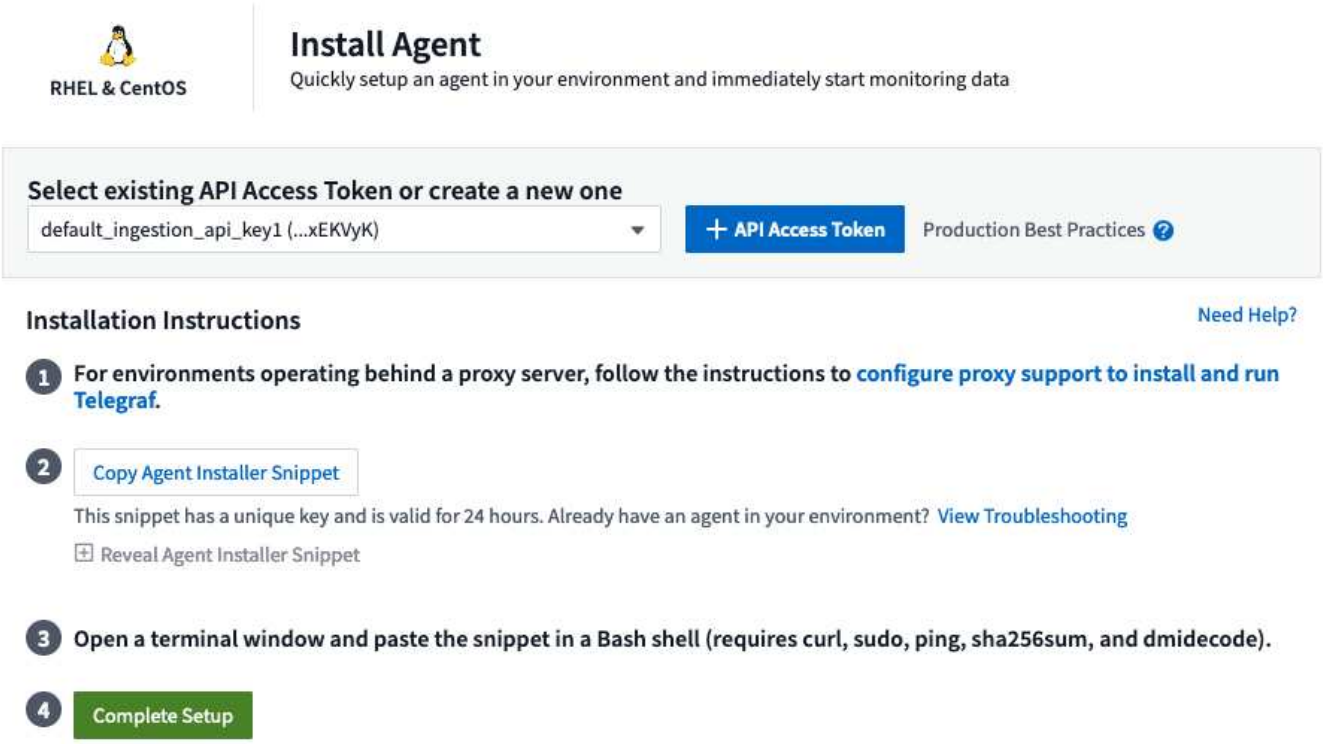
Führen Sie für Systeme, die sich hinter einem Proxy befinden, die folgenden Schritte vor der Installation des Telegraf-Agenten durch:

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

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

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

Installieren des Agenten



Schritte zum Installieren von Agent auf RHEL/CentOS:

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

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

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

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

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

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

Deinstallieren des Agenten

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

1. Stoppen Sie den Telegraf-Service:

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

2. Entfernen Sie den Telegraf-Agent:

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

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

Aktualisieren des Agenten

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

1. Stoppen sie den telegraf-Service:

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

2. Entfernen Sie den vorherigen telegraf-Agent:

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

Ubuntu und Debian

Voraussetzungen:

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

Proxy-Unterstützung für Ubuntu/Debian konfigurieren

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

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

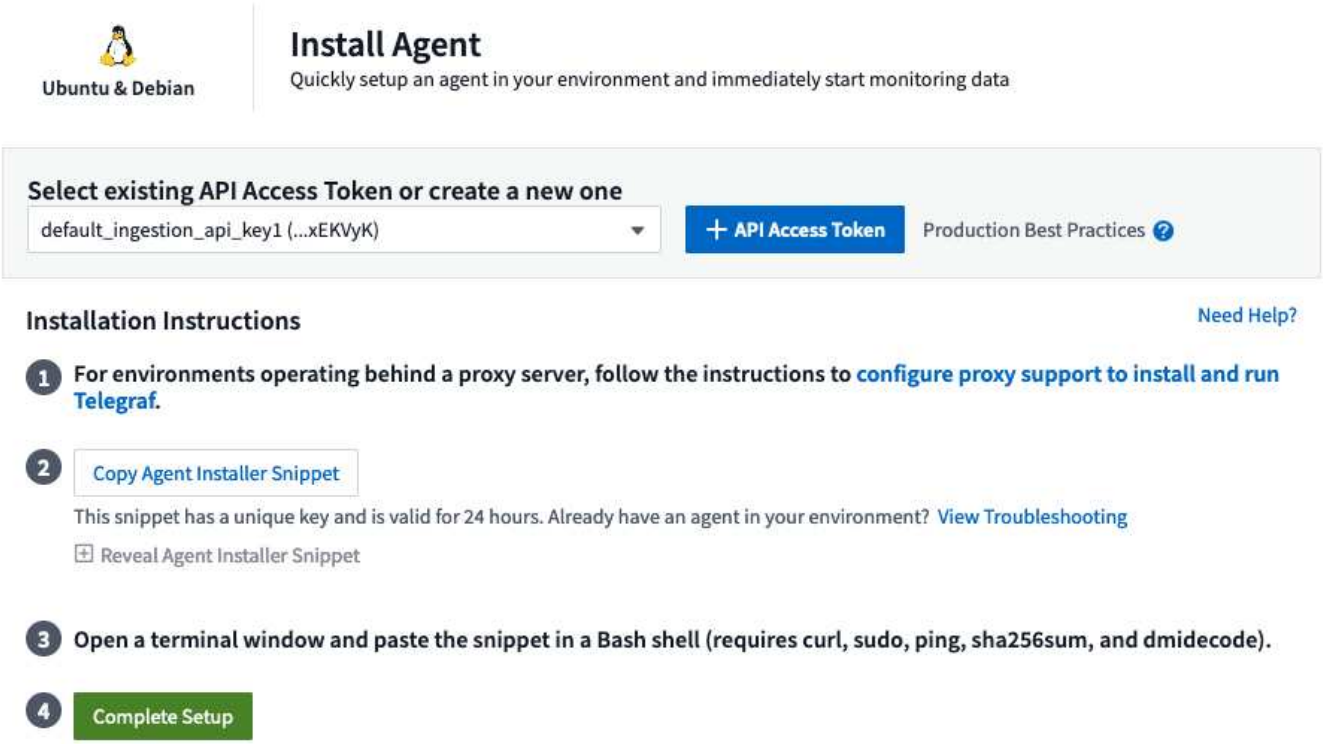
Führen Sie für Systeme, die sich hinter einem Proxy befinden, die folgenden Schritte vor der Installation des Telegraf-Agenten durch:

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

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

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

Installieren des Agenten



Schritte zur Installation von Agent auf Debian oder Ubuntu:

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

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

Wenn Ihr Betriebssystem systemd verwendet:

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

Wenn Ihr Betriebssystem keine systemd verwendet:

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

Deinstallieren des Agenten

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

1. Stoppen Sie den Telegraf-Service:

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

2. Entfernen Sie den Telegraf-Agent:

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

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

Aktualisieren des Agenten

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

1. Stoppen sie den telegraf-Service:

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

2. Entfernen Sie den vorherigen telegraf-Agent:

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

Prüfsummen Werden Überprüft

Das 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 nachstehende „--install“ (Linux) oder „-install“ (Windows) aus dem Befehl.
4. Kopieren Sie den gesamten Befehl aus dem Texteditor.
5. Fügen Sie es nun in Ihr Befehlsfenster ein (in einem Arbeitsverzeichnis) und führen Sie es aus.

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

- Download und Installation (Standard):

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

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

Windows:

- Download und Installation (Standard):

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

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

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 Prüfsummendatei (endet mit sha256.signed oder sha256.ps1)

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

Prüfsummenwert generieren

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

- RHEL/Ubuntu:

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

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

Überprüfen Sie die Prüfsumme

Extrahieren Sie die erwartete Prüfsumme aus der Prüfsummendatei

- Nicht Windows:

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

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

Installieren Sie das heruntergeladene Paket

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

Nicht Windows:

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

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

Fehlerbehebung

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

Problem:	Versuchen Sie dies:
Nach der Konfiguration eines neuen Plugins und dem Neustart von Telegraf startet Telegraf Telegraf nicht. Die Protokolle zeigen an, dass ein Fehler wie folgt auftritt: "[telegraf] Fehler laufende Agent: Fehler beim Laden der Konfigurationsdatei /etc/telegraf/telegraf.d/cloudinsights-default.conf: Plugin Outputs.http: Line <linenumber>: Configuration specified the fields ["use_System_Proxy"], they were't used"	Die installierte Telegraf-Version ist veraltet. Befolgen Sie die Schritte auf dieser Seite, um **Upgrade the Agent** für Ihre entsprechende Plattform.
Ich habe das Installer-Skript auf einer alten Installation ausgeführt und jetzt sendet der Agent keine Daten	Deinstallieren Sie den telegraf-Agent und führen Sie dann das Installationsskript erneut aus. Folgen Sie den Schritten **Upgrade the Agent** auf dieser Seite für Ihre entsprechende Plattform.
Ich habe bereits einen 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".

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 **Observability > Collectors**

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

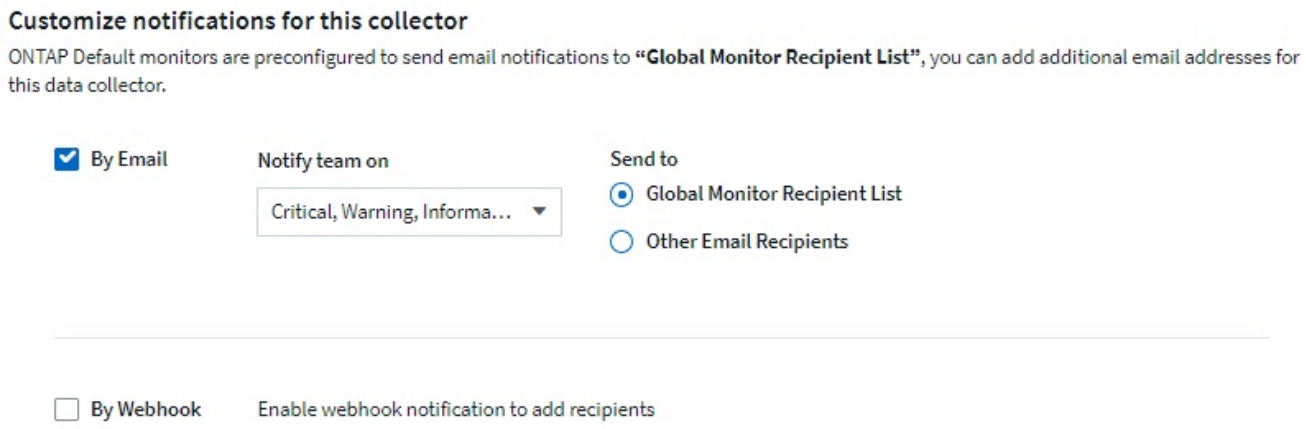
2. Klicken Sie auf **+ Collector**, und wählen Sie den zu konfigurierenden Data Collector aus.

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

3. Geben Sie einen Namen für den Datensammler ein.

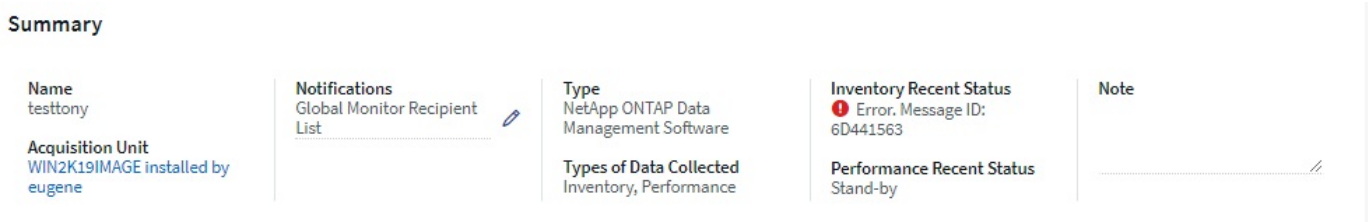
   Namen können Buchstaben (a-z), Zahlen (0-9), Bindestriche (-), Unterstriche (_), Apostrophe ('), Und Perioden (.).

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**.



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.



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 **Observability > Collectors**

   Der Bildschirm Verfügbare Datensammler wird angezeigt.

2. Klicken Sie Auf **Installierte Datensammler**

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

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

Kontrollieren der Data Collector-Umfrage

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

Schritte

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

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

Bearbeiten von Daten-Collector-Informationen

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

So bearbeiten Sie einen einzelnen Datensammler:

1. Klicken Sie im Menü Cloud Insights auf **Observability > Collectors**, 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 **Observability > Collectors**.
2. Klicken Sie Auf **Installierte Datensammler**.

3. Klicken Sie auf das Kontrollkästchen links neben dem zu kopierenden Datensammler.
4. Klicken Sie im Optionsmenü rechts neben dem ausgewählten Datensammler auf **Clone**.

   Das Dialogfeld Data Collector klonen wird angezeigt.

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

Nachdem Sie fertig sind

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

Ausführen von Massenaktionen auf Datensammlern

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

Schritte

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

Nachdem Sie fertig sind

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

Recherchieren eines fehlgeschlagenen Datensammlers

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

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

Schritte

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

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

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