



Daten sammeln

Data Infrastructure Insights

NetApp
February 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/data-infrastructure-insights/task_getting_started_with_cloud_insights.html on February 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

Daten sammeln	1
Erste Schritte beim Sammeln von Daten	1
Installieren einer Erfassungseinheit	1
Konfigurieren des Datensammlers – Infrastruktur	1
Konfigurieren des Datensammlers – Betriebssysteme und Dienste	2
Dashboards hinzufügen	2
Das ist alles, was dazu gehört	2
Nützliche Definitionen	3
Anforderungen an die Erfassungseinheit	3
Anforderungen	3
Zusätzliche Empfehlungen	5
Zur Größenbestimmung	6
Konfigurieren von Erfassungseinheiten	6
Hinzufügen einer Linux-Erfassungseinheit	6
Hinzufügen einer Windows-Erfassungseinheit	8
Deinstallieren einer Erfassungseinheit	10
Neuinstallation einer Erfassungseinheit	12
Anzeigen von AU-Details	12
Konfigurieren eines Agenten zum Sammeln von Daten (Windows/Linux)	13
Installieren eines Agenten	14
Überprüfen der Prüfsummen von Telegraf-Paketen	21
Erstellen und Verwenden von API-Zugriffstoken	23
Fehlerbehebung	24
Konfigurieren von Datenkollektoren	25
Ermitteln des Erfassungsstatus des Datensammlers	26
Verwalten konfigurierter Datenkollektoren	26
Steuern der Datensammlerabfrage	26
Bearbeiten von Datenkollektorinformationen	27
Klonen von Datenkollektoren	27
Durchführen von Massenaktionen auf Datensammlern	28
Untersuchung eines gescheiterten Datensammlers	28

Daten sammeln

Erste Schritte beim Sammeln von Daten

Nachdem Sie sich für Data Infrastructure Insights angemeldet und sich zum ersten Mal bei Ihrer Umgebung angemeldet haben, werden Sie durch die folgenden Schritte geführt, um mit dem Sammeln und Verwalten von Daten zu beginnen.

Datensammler ermitteln Informationen aus Ihren Datenquellen, beispielsweise Speichergeräten, Netzwerk-Switches und virtuellen Maschinen. Die gesammelten Informationen werden zur Analyse, Validierung, Überwachung und Fehlerbehebung verwendet.

Data Infrastructure Insights bietet drei Arten von Datensammlern:

- Infrastruktur (Speichergeräte, Netzwerk-Switches, Computerinfrastruktur)
- Betriebssysteme (wie VMware oder Windows)
- Dienste (wie Kafka)

Wählen Sie Ihren ersten Datensammler aus den verfügbaren unterstützten Anbietern und Modellen aus. Sie können später problemlos weitere Datensammler hinzufügen.

Installieren einer Erfassungseinheit

Wenn Sie einen *Infrastruktur*-Datensammler ausgewählt haben, ist eine Erfassungseinheit erforderlich, um Daten in Data Infrastructure Insights einzuspeisen. Sie müssen die Acquisition Unit-Software herunterladen und auf einem Server oder einer VM im Rechenzentrum installieren, von dem Sie die Daten erfassen. Eine einzelne Erfassungseinheit kann für mehrere Datensammler verwendet werden.

[Linux AU-Anweisungen]

- Folgen Sie den "[Anweisungen](#)" wird angezeigt, um Ihre Erfassungseinheit zu installieren. Sobald die Software der Erfassungseinheit installiert ist, wird die Schaltfläche „Weiter“ angezeigt und Sie können mit dem nächsten Schritt fortfahren.

[Neue AU erkannt]

Bei Bedarf können Sie später weitere Erfassungseinheiten einrichten. Beispielsweise möchten Sie möglicherweise, dass verschiedene Erfassungseinheiten Informationen aus Rechenzentren in unterschiedlichen Regionen sammeln.

Konfigurieren des Datensammlers – Infrastruktur

Bei *Infrastruktur*-Datensammlern werden Sie aufgefordert, die angezeigten Datensammlerfelder auszufüllen:

- Geben Sie dem Datensammler einen eindeutigen und aussagekräftigen Namen.
- Geben Sie die Anmeldeinformationen (Benutzername und Kennwort) ein, um gegebenenfalls eine Verbindung mit dem Gerät herzustellen.
- Füllen Sie alle anderen Pflichtfelder in den Abschnitten *Konfiguration* und *Erweiterte Konfiguration* aus.
- Klicken Sie auf **Sammler hinzufügen**, um den Datensammler zu speichern.

Sie können später weitere Datensammler konfigurieren.

Konfigurieren des Datensammlers – Betriebssysteme und Dienste

Betriebssystem:

Wählen Sie für Datensammler vom Typ „Betriebssystem“ eine Plattform (Linux, Windows) aus, um einen Data Infrastructure Insights Agent zu installieren. Sie müssen mindestens einen Agenten haben, um Daten von Diensten zu sammeln. Der Agent sammelt auch Daten vom Host selbst zur Verwendung in Data Infrastructure 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 Agent zu installieren.
- Wenn die Installation abgeschlossen ist, klicken Sie auf **Setup abschließen**.

Leistungen:

Klicken Sie bei Service-Datensammlern auf eine Kachel, um die Anleitungsseite für diesen Service zu öffnen.

- Wählen Sie eine Plattform und einen Agent-Zugriffsschlüssel.
- Wenn auf dieser Plattform kein Agent installiert ist, befolgen Sie die Anweisungen zum Installieren des Agenten.
- Klicken Sie auf **Weiter**, um die Anleitungsseite zum Datensammler zu öffnen.
- Befolgen Sie die Anweisungen zum Konfigurieren des Datensammlers.
- Wenn die Konfiguration abgeschlossen ist, klicken Sie auf **Setup abschließen**.

Dashboards hinzufügen

Abhängig vom Typ des anfänglichen Datensammlers, den Sie zur Konfiguration ausgewählt haben (Speicher, Switch usw.), werden ein oder mehrere relevante Dashboards importiert. Wenn Sie beispielsweise einen Speicherdatensammler konfiguriert haben, wird eine Reihe speicherbezogener Dashboards importiert und eines davon als Ihre Data Infrastructure 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 eigenen"](#).

Das ist alles, was dazu gehört

Nachdem Sie den anfänglichen Einrichtungsprozess abgeschlossen haben, beginnt Ihre Umgebung mit der Datenerfassung.

Wenn Ihr anfänglicher Einrichtungsvorgang unterbrochen wird (z. B. wenn Sie das Browserfenster schließen), müssen Sie die Schritte manuell ausführen:

- Wählen Sie einen Datensammler
- Installieren Sie einen Agenten oder eine Erfassungseinheit, wenn Sie dazu aufgefordert werden
- Konfigurieren des Datensammlers

Nützliche Definitionen

Die folgenden Definitionen können hilfreich sein, wenn es um Datensammler oder Funktionen von Data Infrastructure Insights geht:

- Lebenszyklus des Kollektors: Ein Kollektor befindet sich in seinem Lebenszyklus in einem der folgenden Zustände:
 - **Vorschau:** In begrenzter Kapazität oder für ein begrenztes Publikum verfügbar. "[Vorschaufunktionen](#)" und es wird erwartet, dass die Datensammler nach der Vorschauphase allgemein verfügbar werden. Die Vorschauzeiträume variieren je nach Zielgruppe oder Funktionalität.
 - **GA:** Eine Funktion oder ein Datensammler, der basierend auf der Edition oder dem Funktionsumfang allgemein für alle Kunden verfügbar ist.
 - **Veraltet:** Gilt für Datensammler, deren Funktion nicht mehr aufrechterhalten werden kann oder voraussichtlich nicht mehr aufrechterhalten werden kann. Veraltete Datensammler werden häufig durch neuere, funktional aktualisierte Datensammler ersetzt.
 - **Gelöscht:** Ein Datensammler, der entfernt wurde und nicht mehr verfügbar ist.
- Erfassungseinheit: Ein Computer, der ausschließlich zum Hosten von Datensammlern dient, normalerweise eine virtuelle Maschine. Dieser Computer befindet sich normalerweise im selben Rechenzentrum/VPC wie die überwachten Elemente.
- 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 von Ihren Infrastrukturdatensammlern (Speicher, VM, Port, EC2 usw.) zu erfassen. Bevor Sie die Erfassungseinheit installieren, sollten Sie sicherstellen, dass Ihr Mandant die Anforderungen an Betriebssystem, CPU, Speicher und Festplattenspeicher erfüllt.

Anforderungen

Komponente	Linux-Anforderungen	Windows-Anforderung
------------	---------------------	---------------------

Betriebssystem	<p>Ein Computer mit einer lizenzierten Version eines der folgenden: * AlmaLinux 9.5, 10 * Centos (64-bit): Stream 9 * Debian (64-bit): 11 bis 13 * OpenSUSE Leap 15.2 bis 15.6, 16 * Oracle Enterprise Linux (64-bit): 8.10, 9.2, 9.4, 9.6, 10 * Red Hat (64-bit): 8.10, 9.2, 9.4, 9.6, 10 * Rocky 9.2 bis 9.6 * SUSE Linux Enterprise Server 15 SP4 bis 15 SP7, 16 * Ubuntu Server: 20.04, 22.04, 24.04 LTS * SELinux auf den oben genannten Plattformen Dieser Computer sollte keine weitere Anwendungssoftware ausführen. Ein dedizierter Server wird empfohlen. Wenn Sie SELinux verwenden, wird empfohlen, die folgenden Befehle auf dem System der Datenerfassungseinheit auszuführen: sudo semanage fcontext -a -t usr_t "/opt/netapp/cloudinsights(.*)" sudo restorecon -R /opt/netapp/cloudinsights</p>	<p>Ein Computer, auf dem eine lizenzierte Version einer der folgenden Windows-Versionen ausgeführt wird: * Microsoft Windows 11 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows Server 2025 Auf diesem Computer darf keine andere Anwendungssoftware ausgeführt werden. Ein dedizierter Server wird empfohlen.</p>
CPU	2 CPU-Kerne	Dasselbe
Erinnerung	8 GB RAM	Dasselbe
Verfügbarer Speicherplatz	50 GB (100 GB empfohlen) Für 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	<p>Erforderlich sind eine 100-Mbit/s-/1-Gbit/s-Ethernet-Verbindung, eine statische IP-Adresse und eine Port-80- oder Port-443-Konnektivität (ausgehend) von der Akquisitionseinheit zu *.cloudinsights.netapp.com oder Ihrem Data Infrastructure Insights Mandanten (z. B. <a href="https://<tenant_id>.c01.cloudinsights.netapp.com">https://<tenant_id>.c01.cloudinsights.netapp.com). Die Anforderungen an die Verbindung zwischen der Erfassungseinheit und den einzelnen Datensammlern entnehmen Sie bitte der Anleitung für die "Datensammler". Die Wenn Ihre Organisation die Verwendung eines Proxys für den Internetzugang erfordert, müssen Sie möglicherweise das Proxy-Verhalten Ihrer Organisation verstehen und nach bestimmten Ausnahmen suchen, damit Data Infrastructure Insights funktioniert. Blockiert Ihre Organisation beispielsweise standardmäßig den Zugriff und erlaubt den Zugriff auf bestimmte Websites/Domänen nur ausnahmsweise? In diesem Fall müssen Sie die folgende Domain zur Ausnahmeliste hinzufügen lassen: *.cloudinsights.netapp.com. Weitere Informationen finden Sie unter „Proxys“ "hier (Linux)" oder "hier (Windows)". Die</p>	Dasselbe
Berechtigungen	Sudo-Berechtigungen auf dem Acquisition Unit-Server. /tmp muss mit Exec-Funktionen gemountet werden.	Administratorberechtigungen auf dem Acquisition Unit-Server
Virenscan		Während der Installation müssen Sie alle Virenscanner vollständig deaktivieren. Nach der Installation müssen die von der Acquisition Unit-Software verwendeten Pfade vom Virenscan ausgeschlossen werden.

Zusätzliche Empfehlungen

- Für eine genaue Prüfung und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Computer der Erfassungseinheit mithilfe des **Network Time Protocol (NTP)** oder des **Simple Network Time Protocol (SNTP)** zu synchronisieren.

Zur Größenbestimmung

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

Erwarten Sie:

- Entdecken Sie mehr als 2500 virtuelle Maschinen oder 10 große (> 2 Knoten) ONTAP Cluster, Symmetrix oder HDS/HPE VSP/XP-Arrays auf dieser Erfassungseinheit?
- Sollen insgesamt 75 oder mehr Datensammler auf dieser Erfassungseinheit eingesetzt werden?

Für jede der oben aufgeführten „Ja“-Antworten wird empfohlen, der AU 8 GB Arbeitsspeicher und 50 GB Festplattenspeicher hinzuzufügen. Wenn Sie beispielsweise beide Fragen mit „Ja“ beantwortet haben, sollten Sie ein 24-GB-Speichersystem mit 150 GB oder mehr Festplattenspeicher einsetzen. Unter Linux der Speicherplatz, der dem Protokollspeicherort hinzugefügt werden soll.

Wenden Sie sich bei weiteren Fragen zur Dimensionierung an den NetApp Support.

Konfigurieren von Erfassungseinheiten

Data Infrastructure Insights sammelt Gerätedaten mithilfe einer oder mehrerer auf lokalen Servern installierter Erfassungseinheiten. Jede Erfassungseinheit kann mehrere Datensammler hosten, die Gerätemetriken zur Analyse an Data Infrastructure Insights senden.

In diesem Thema wird beschrieben, wie Sie Erfassungseinheiten hinzufügen, und es werden zusätzliche Schritte beschrieben, die erforderlich sind, wenn Ihre Umgebung einen Proxy verwendet.



Für eine genaue Prüfung und Datenberichterstattung wird dringend empfohlen, die Zeit auf dem Computer der Erfassungseinheit mithilfe des **Network Time Protocol (NTP)** oder des **Simple Network Time Protocol (SNTP)** zu synchronisieren.

Lesen Sie mehr über die Sicherheit von Data Infrastructure Insights ["hier."](#)

Hinzufügen einer Linux-Erfassungseinheit

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 zur Installation der Linux Acquisition Unit

1. Melden Sie sich als Administrator oder Kontoinhaber bei Ihrer Data Infrastructure Insights Umgebung an.
2. Klicken Sie auf **Beobachtbarkeit > Sammler > Erfassungseinheiten > +Erfassungseinheit**

Das System zeigt das Dialogfeld „Erfassungseinheit installieren“ an. Wählen Sie Linux.

Install Acquisition Unit

Cloud Insights collects device data via one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.

What Operating System or Platform Are You Using?

 LinuxLinux Versions Supported  Production Best Practices [Need Help?](#)

Installation Instructions

1[Copy Installer Snippet](#)

This snippet has a unique key valid for 24 hours for this Acquisition Unit only.

[Reveal Installer Snippet](#)**2**

Paste the snippet into a bash shell to run the installer.

3 Waiting for Acquisition Unit to connect...

1. Überprüfen Sie, ob der Server oder die VM, auf dem/der die Erfassungseinheit gehostet wird, die empfohlenen Systemanforderungen erfüllt.
2. Stellen Sie sicher, dass auf dem Server eine unterstützte Linux-Version ausgeführt wird. Klicken Sie auf **Unterstützte Betriebssystemversionen** , um eine Liste der unterstützten Versionen anzuzeigen.
3. Kopieren Sie den Installationsbefehlsausschnitt im Dialogfeld in ein Terminalfenster auf dem Server oder der VM, auf dem/der die Erfassungseinheit gehostet wird.
4. Fügen Sie den Befehl in die Bash-Shell ein und führen Sie ihn aus.

Nach Abschluss

- Klicken Sie auf **Beobachtbarkeit > Sammler > Erfassungseinheiten**, um den Status der Erfassungseinheiten zu überprüfen.
- Sie können auf die Protokolle der Erfassungseinheit unter `/var/log/netapp/cloudinsights/acq/acq.log` zugreifen.
- Verwenden Sie das folgende Skript, um die Erfassungseinheit zu steuern:
 - `cloudinsights-service.sh` (Stoppen, Starten, Neustarten, Status prüfen)
- 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 Proxy-Umgebungsvariablen festlegen, bevor Sie die Erfassungseinheit hinzufügen. Die Anweisungen zum Konfigurieren des Proxys finden Sie im Dialogfeld „Erfassungseinheit hinzufügen“.

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

Hinweis: Beachten Sie die Einschränkungen für Sonderzeichen in den Feldern für Proxy-Benutzernamen

und -Passwörter: „%“ und „!“ sind im Feld „Benutzername“ zulässig. Im Kennwortfeld sind die Zeichen „:“, „%“ und „!“ zulässig.

3. Führen Sie den bearbeiteten Befehl in einem Terminal mithilfe der Bash-Shell aus.

4. Installieren Sie die Software der Erfassungseinheit.

Proxy-Konfiguration

Die Acquisition Unit verwendet eine 2-Wege-/gegenseitige Authentifizierung, um eine Verbindung zum Data Infrastructure Insights -Server herzustellen. Zur Authentifizierung muss das Client-Zertifikat an den Data Infrastructure Insights -Server übergeben werden. Um dies zu erreichen, muss der Proxy so eingerichtet werden, dass er die https-Anfrage an den Data Infrastructure Insights -Server weiterleitet, ohne die Daten zu entschlüsseln.

Am einfachsten ist es, in Ihrem Proxy/Ihrer Firewall eine Platzhalterkonfiguration für die Kommunikation mit Data Infrastructure Insights anzugeben, zum Beispiel:

*.cloudinsights.netapp.com



Die Verwendung eines Sternchens (*) als Platzhalter ist üblich, Ihre Proxy-/Firewall-Konfiguration verwendet jedoch möglicherweise ein anderes Format. Überprüfen Sie anhand der Proxy-Dokumentation, ob die Platzhalterspezifikation in Ihrer Umgebung korrekt ist.

Weitere Informationen zur Proxy-Konfiguration finden Sie in der NetApp "[Wissensdatenbank](#)".

Anzeigen von Proxy-URLs

Sie können die URLs Ihres Proxy-Endpunkts anzeigen, indem Sie beim Auswählen eines Datensammlers während des Onboardings auf den Link **Proxy-Einstellungen** oder auf der Seite **Hilfe > Support** auf den Link unter *Proxy-Einstellungen* klicken. Es wird eine Tabelle wie die folgende angezeigt.

Proxy Settings					X
If your organization requires proxy usage for internet access, you need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. The simplest way is to add the following domains to the exception list:					
Hostname	Port	Protocol	Methods	Endpoint URL Purpose	
qtrjkso.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant	
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion	
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication	
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway	

Wenn Sie Workload Security auf Ihrem Mandanten haben, werden die konfigurierten Endpunkt-URLs auch in dieser Liste angezeigt.

Hinzufügen einer Windows-Erfassungseinheit

Schritte zur Installation der Windows-Erfassungseinheit

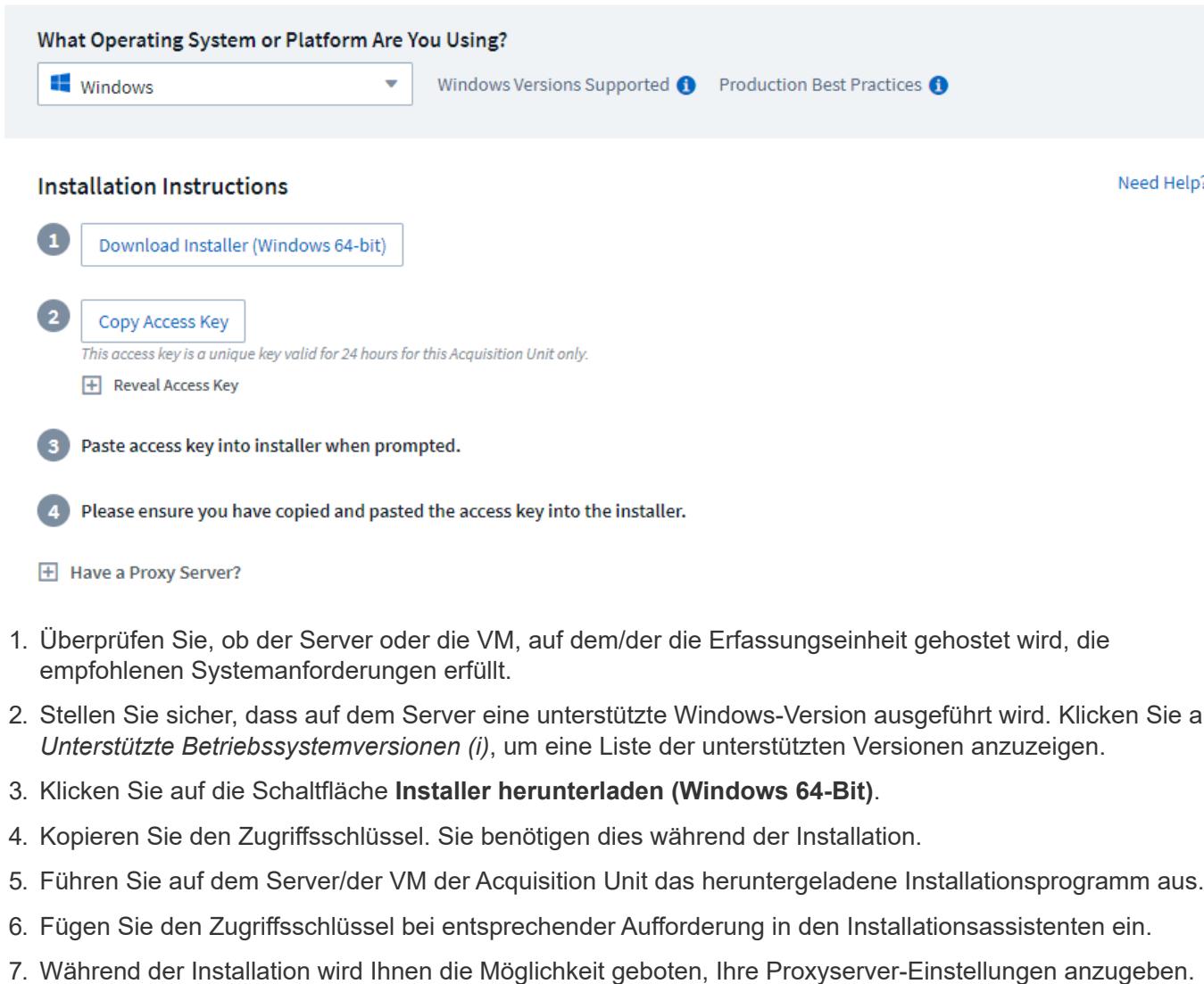
1. Melden Sie sich beim Acquisition Unit-Server/VM als Benutzer mit Administratorberechtigungen an.

2. Öffnen Sie auf diesem Server ein Browserfenster und melden Sie sich als Administrator oder Kontoinhaber bei Ihrer Data Infrastructure Insights Umgebung an.
3. Klicken Sie auf **Beobachtbarkeit > Sammler > Erfassungseinheiten > +Erfassungseinheit**.

Das System zeigt das Dialogfeld „Erfassungseinheit installieren“ an. Wählen Sie Windows.

Install Acquisition Unit

Cloud Insights collects device data via one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.



What Operating System or Platform Are You Using?

Windows

Windows Versions Supported ⓘ Production Best Practices ⓘ

Installation Instructions

1 Download Installer (Windows 64-bit)

2 Copy Access Key

This access key is a unique key valid for 24 hours for this Acquisition Unit only.

+ Reveal Access Key

3 Paste access key into installer when prompted.

4 Please ensure you have copied and pasted the access key into the installer.

+ Have a Proxy Server?

- 1 Überprüfen Sie, ob der Server oder die VM, auf dem/der die Erfassungseinheit gehostet wird, die empfohlenen Systemanforderungen erfüllt.
- 2 Stellen Sie sicher, dass auf dem Server eine unterstützte Windows-Version ausgeführt wird. Klicken Sie auf *Unterstützte Betriebssystemversionen (i)*, um eine Liste der unterstützten Versionen anzuzeigen.
- 3 Klicken Sie auf die Schaltfläche **Installer herunterladen (Windows 64-Bit)**.
- 4 Kopieren Sie den Zugriffsschlüssel. Sie benötigen dies während der Installation.
- 5 Führen Sie auf dem Server/der VM der Acquisition Unit das heruntergeladene Installationsprogramm aus.
- 6 Fügen Sie den Zugriffsschlüssel bei entsprechender Aufforderung in den Installationsassistenten ein.
- 7 Während der Installation wird Ihnen die Möglichkeit geboten, Ihre Proxyserver-Einstellungen anzugeben.

Nach Abschluss

- Klicken Sie auf * > Observability > Collectors > Acquisition Units*, um den Status der Acquisition Units zu überprüfen.
- Sie können auf das Acquisition Unit-Protokoll unter <Installationsverzeichnis>\ Cloud Insights\Acquisition Unit\log\acq.log zugreifen.
- Verwenden Sie das folgende Skript, um die Erfassungseinheit zu stoppen, zu starten, neu zu starten oder ihren Status zu überprüfen:

```
cloudinsights-service.sh
```

Proxy-Konfiguration

Die Acquisition Unit verwendet eine 2-Wege-/gegenseitige Authentifizierung, um eine Verbindung zum Data Infrastructure Insights -Server herzustellen. Zur Authentifizierung muss das Client-Zertifikat an den Data Infrastructure Insights -Server übergeben werden. Um dies zu erreichen, muss der Proxy so eingerichtet werden, dass er die https-Anfrage an den Data Infrastructure Insights -Server weiterleitet, ohne die Daten zu entschlüsseln.

Am einfachsten ist es, in Ihrem Proxy/Ihrer Firewall eine Platzhalterkonfiguration für die Kommunikation mit Data Infrastructure Insights anzugeben, zum Beispiel:

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



Die Verwendung eines Sternchens (*) als Platzhalter ist üblich, Ihre Proxy-/Firewall-Konfiguration verwendet jedoch möglicherweise ein anderes Format. Überprüfen Sie anhand der Proxy-Dokumentation, ob die Platzhalterspezifikation in Ihrer Umgebung korrekt ist.

Weitere Informationen zur Proxy-Konfiguration finden Sie in der NetApp "[Wissensdatenbank](#)".

Anzeigen von Proxy-URLs

Sie können die URLs Ihres Proxy-Endpunkts anzeigen, indem Sie beim Auswählen eines Datensammlers während des Onboardings auf den Link **Proxy-Einstellungen** oder auf der Seite **Hilfe > Support** auf den Link unter *Proxy-Einstellungen* klicken. Es wird eine Tabelle wie die folgende angezeigt.

Proxy Settings					
If your organization requires proxy usage for internet access, you need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. The simplest way is to add the following domains to the exception list:					
Hostname	Port	Protocol	Methods	Endpoint URL Purpose	
qtrjkso.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant	
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion	
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication	
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway	

Close

Wenn Sie Workload Security auf Ihrem Mandanten haben, werden die konfigurierten Endpunkt-URLs auch in dieser Liste angezeigt.

Deinstallieren einer Erfassungseinheit

Um die Software der Erfassungseinheit zu deinstallieren, gehen Sie wie folgt vor:

Windows:

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

1. Öffnen Sie auf dem Server/der VM der Erfassungseinheit die Systemsteuerung und wählen Sie **Programm deinstallieren**. Wählen Sie das Data Infrastructure Insights Acquisition Unit-Programm zum Entfernen aus.
2. Klicken Sie auf „Deinstallieren“ und folgen Sie den Anweisungen.

Linux:

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

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

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

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

Windows und Linux:

Nach der Deinstallation der AU:

1. Gehen Sie in Data Infrastructure Insights zu **Observability > Collectors** und wählen Sie die Registerkarte ***Acquisition Units** aus.
2. Klicken Sie rechts neben der Erfassungseinheit, die Sie deinstallieren möchten, auf die Schaltfläche „Optionen“ und wählen Sie „Löschen“ aus. Sie können eine Erfassungseinheit nur löschen, wenn ihr keine Datensammler zugewiesen sind.



Sie können keine Erfassungseinheit (AU) löschen, an die Datensammler angeschlossen sind. Verschieben Sie alle Datensammler der AU in eine andere AU (bearbeiten Sie den Sammler und wählen Sie einfach eine andere AU aus), bevor Sie die ursprüngliche AU löschen.

Zur Geräteauflösung wird eine Erfassungseinheit mit einem Stern daneben verwendet. Bevor Sie diese AU entfernen, müssen Sie eine andere AU zur Verwendung für die Geräteauflösung auswählen. Bewegen Sie den Mauszeiger über eine andere AU und öffnen Sie das Menü mit den drei Punkten, um „Für Geräteauflösung verwenden“ auszuwählen.



Neuinstallation einer Erfassungseinheit

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

Bevor Sie beginnen

Sie müssen eine temporäre Erfassungseinheit auf einem separaten Server/VM konfiguriert haben, bevor Sie eine Erfassungseinheit neu installieren.

Schritte

1. Melden Sie sich beim Acquisition Unit-Server/VM an und deinstallieren Sie die AU-Software.
2. Melden Sie sich bei Ihrer Data Infrastructure Insights Umgebung an und gehen Sie zu **Observability > Collectors**.
3. Klicken Sie für jeden Datensammler rechts auf das Optionsmenü 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 **Beobachtbarkeit > Sammler** 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“ aus. Sie können eine Erfassungseinheit nur löschen, wenn ihr keine Datensammler zugewiesen sind.
6. Sie können die Acquisition Unit-Software jetzt auf dem ursprünglichen Server/der ursprünglichen VM neu installieren. Klicken Sie auf **+Erfassungseinheit** und befolgen Sie die obigen Anweisungen, um die Erfassungseinheit zu installieren.
7. Nachdem die Erfassungseinheit neu installiert wurde, weisen Sie Ihre Datensammler wieder der Erfassungseinheit zu.

Anzeigen von AU-Details

Die Detailseite der Erfassungseinheit (AU) bietet nützliche Einzelheiten zu einer AU sowie Informationen zur Fehlerbehebung. Die AU-Detailseite enthält die folgenden Abschnitte:

- Ein **Zusammenfassungsabschnitt** mit folgendem Inhalt:
 - **Name** und **IP** der Erfassungseinheit
 - Aktueller Verbindungsstatus der AU
 - **Zuletzt gemeldet** erfolgreiche Datensammler-Abfragezeit
 - Das **Betriebssystem** der AU-Maschine
 - Alle aktuellen **Hinweise** 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 **Datensammler** der AU, die für jeden Datensammler Folgendes anzeigt:
 - **Name** - Klicken Sie auf diesen Link, um zur Detailseite des Datensammlers mit zusätzlichen Informationen zu gelangen
 - **Status** – Erfolgs- oder Fehlerinformationen

- **Typ** – Anbieter/Modell
- **IP-Adresse des Datensammlers**
- **Aktuelles Auswirkungsniveau**
- **Letzte Erfassung** - Zeitpunkt der letzten erfolgreichen Abfrage des Datensammlers

Acquisition Unit Summary

Name xp-linux	Connection Status OK - Need Help?	Operating System Linux	Note
IP 10.197.120.145	Last Reported 2 minutes ago		

Data Collectors (3)

<input type="checkbox"/> Name ↑	Status	Type	IP	Impact	Last Acquired	⋮
foo	! Inventory failed	NetApp Data ONTAP 7-Mode	foo	Low	Never	⋮
xp-cisco	All successful	Cisco MDS Fabric Switches	10.197.136.66		2 minutes ago	⋮
xpcdot26	All successful	NetApp ONTAP Data Management Software	10.197.136.26		8 minutes ago	⋮

Sie können bei jedem Datensammler auf das Menü mit den drei Punkten klicken, um den Datensammler zu klonen, zu bearbeiten, abzufragen oder zu löschen. Sie können in dieser Liste auch mehrere Datensammler auswählen, um Massenaktionen für sie auszuführen.

Um die Erfassungseinheit neu zu starten, klicken Sie oben auf der Seite auf die Schaltfläche **Neustart**. Klicken Sie auf diese Schaltfläche, um im Falle eines Verbindungsproblems zu versuchen, die **Verbindung wiederherzustellen**.

Konfigurieren eines Agenten zum Sammeln von Daten (Windows/Linux)

Data Infrastructure Insights verwendet "[Telegraf](#)" als dessen Agent für die Erfassung von Integrationsdaten. Telegraf ist ein Plugin-gesteuerter Server-Agent, der zum Sammeln und Melden von Metriken, Ereignissen und Protokollen verwendet werden kann. Eingabe-Plugins werden verwendet, um die gewünschten Informationen im Agenten zu sammeln, indem direkt auf das System/Betriebssystem zugegriffen wird, APIs von Drittanbietern aufgerufen werden oder konfigurierte Streams abgehört werden (z. B. Kafka, statsD usw.). Ausgabe-Plugins werden verwendet, um die gesammelten Metriken, Ereignisse und Protokolle vom Agenten an Data Infrastructure Insights zu senden.

Informationen zur Installation auf Kubernetes finden Sie im "[NetApp Kubernetes Monitoring Operator](#)" Seite.



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



Wenn Sie die Installationsdateien vor der Installation des Agenten überprüfen möchten, lesen Sie den Abschnitt weiter unten auf [Überprüfen der Prüfsummen von Telegraf-Paketen](#).

Installieren eines Agenten

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

- [Windows](#)
- [RHEL und CentOS](#)
- [Ubuntu und Debian](#)

Um einen Agenten zu installieren, müssen Sie unabhängig von der verwendeten Plattform zunächst Folgendes tun:

1. Melden Sie sich bei dem Host an, den Sie für Ihren Agenten verwenden möchten.
2. Melden Sie sich bei Ihrer Data Infrastructure Insights Umgebung an und navigieren Sie zu **Observability > Collectors**.
3. Klicken Sie auf **+Datensammler** 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.



Nachdem Sie einen Agenten auf einem Host installiert haben, müssen Sie auf diesem Host keinen weiteren Agenten installieren.



Sobald Sie einen Agenten auf einem Server/einer VM installiert haben, sammelt Data Infrastructure Insights zusätzlich zu den von Ihnen konfigurierten Datensammlern auch Metriken von diesem System. Diese Kennzahlen werden wie folgt erfasst: „[Knoten-Metriken](#)“.



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

Protokollspeicherorte

Telegraf-Protokollnachrichten werden standardmäßig von stdout in die folgenden Protokolldateien 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.

Konfigurieren der Proxy-Unterstützung für Windows



Wenn Ihre Umgebung einen Proxy verwendet, lesen Sie diesen Abschnitt vor der Installation.



Die folgenden Schritte beschreiben die Aktionen, die zum Festlegen der Umgebungsvariablen `http_proxy/https_proxy` erforderlich sind. Für einige Proxy-Umgebungen müssen Benutzer möglicherweise auch die Umgebungsvariable `no_proxy` festlegen.

Führen Sie bei Systemen, die sich hinter einem Proxy befinden, Folgendes aus, um die Umgebungsvariable(n) `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

Install Agent

Quickly setup an agent in your environment and immediately start monitoring data

Select existing API Access Token or create a new one

KEY1 (...Zqlk0c)

+ API Access Token

Installation Instructions

1 Copy Agent Installer Snippet

This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)

+ Reveal Agent Installer Snippet

2 Open a PowerShell window as administrator and paste the snippet

3 Complete Setup

Need Help?

Schritte zum Installieren des Agenten unter Windows:

1. Wählen Sie einen Agent-Zugriffsschlüssel.
2. Kopieren Sie den Befehlsblock aus dem Agent-Installationsdialog. Sie können auf das Zwischenablagen-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. Wenn der Vorgang abgeschlossen ist, wird der Agentendienst neu gestartet. Der Befehl hat einen eindeutigen Schlüssel und ist 24 Stunden gültig.
6. Klicken Sie auf **Fertig** oder **Weiter**

Nachdem der Agent installiert wurde, können Sie den Dienst mit den folgenden Befehlen starten/stoppen:

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

Deinstallation des Agenten

Um den Agenten unter Windows zu deinstallieren, führen Sie in einem PowerShell-Fenster die folgenden Schritte aus:

1. Stoppen und löschen Sie den Telegraf-Dienst:

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

2. Entfernen Sie das Zertifikat aus dem Truststore:

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

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

Aktualisieren des Agenten

Um den Telegraf-Agenten 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 Sie `C:\Programme\telegraf\telegraf.conf`
4. Löschen Sie `C:\Programme\telegraf\telegraf.exe`
5. "[Installieren des neuen Agenten](#)" .

RHEL und CentOS

Voraussetzungen:

- Die folgenden 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 konfigurieren** befolgen.

Konfigurieren der Proxy-Unterstützung für RHEL/CentOS



Wenn Ihre Umgebung einen Proxy verwendet, lesen Sie diesen Abschnitt vor der Installation.



Die folgenden Schritte beschreiben die Aktionen, die zum Festlegen der Umgebungsvariablen `http_proxy/https_proxy` erforderlich sind. Für einige Proxy-Umgebungen müssen Benutzer möglicherweise auch die Umgebungsvariable `no_proxy` festlegen.

Führen Sie bei Systemen hinter einem Proxy die folgenden Schritte **VOR** der Installation des Telegraf-Agenten aus:

1. Legen Sie die Umgebungsvariable(n) `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(n) _https_proxy_ und/oder _http_proxy_ ein:
```

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

Installieren des Agenten



RHEL & CentOS

Install Agent

Quickly setup an agent in your environment and immediately start monitoring data

Select existing API Access Token or create a new one

default_ingestion_api_key1 (...xEKVYK)

+ API Access Token

Production Best Practices

Installation Instructions

Need Help?

- 1 For environments operating behind a proxy server, follow the instructions to [configure proxy support to install and run Telegraf](#).

- 2 [Copy Agent Installer Snippet](#)

This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)

[Reveal Agent Installer Snippet](#)

- 3 Open a terminal window and paste the snippet in a Bash shell (requires curl, sudo, ping, sha256sum, and dmidecode).

- 4 [Complete Setup](#)

Schritte zum Installieren des Agenten auf RHEL/CentOS:

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

Nachdem der Agent installiert wurde, können Sie den Dienst mit den folgenden Befehlen starten/stoppen:

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

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

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

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

Deinstallation des Agenten

Um den Agenten unter RHEL/CentOS zu deinstallieren, gehen Sie in einem Bash-Terminal wie folgt vor:

1. Beenden Sie den Telegraf-Dienst:

```
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-Agenten:

```
yum remove telegraf
. Entfernen Sie alle Konfigurations- oder Protokolldateien, die
möglicherweise zurückgeblieben sind:
```

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

Aktualisieren des Agenten

Um den Telegraf-Agenten zu aktualisieren, gehen Sie wie folgt vor:

1. Stoppen Sie den Telegraf-Dienst:

```
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-Agenten:

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

Ubuntu und Debian

Voraussetzungen:

- Die folgenden 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 konfigurieren** folgen.

Konfigurieren der Proxy-Unterstützung für Ubuntu/Debian



Wenn Ihre Umgebung einen Proxy verwendet, lesen Sie diesen Abschnitt vor der Installation.



Die folgenden Schritte beschreiben die Aktionen, die zum Festlegen der Umgebungsvariablen `http_proxy/https_proxy` erforderlich sind. Für einige Proxy-Umgebungen müssen Benutzer möglicherweise auch die Umgebungsvariable `no_proxy` festlegen.

Führen Sie bei Systemen hinter einem Proxy die folgenden Schritte **VOR** der Installation des Telegraf-Agenten aus:

1. Legen Sie die Umgebungsvariable(n) `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(n) _https_proxy_ und/oder _http_proxy_ ein:
```

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

Installieren des Agenten



Ubuntu & Debian

Install Agent

Quickly setup an agent in your environment and immediately start monitoring data

Select existing API Access Token or create a new one

default_ingestion_api_key1 (...xEKVyK) ▼ + API Access Token Production Best Practices ?

Installation Instructions

Need Help?

- 1 For environments operating behind a proxy server, follow the instructions to [configure proxy support to install and run Telegraf](#).

- 2 [Copy Agent Installer Snippet](#)

This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)

[Reveal Agent Installer Snippet](#)

- 3 Open a terminal window and paste the snippet in a Bash shell (requires curl, sudo, ping, sha256sum, and dmidecode).

- 4 [Complete Setup](#)

Schritte zum Installieren des Agenten unter Debian oder Ubuntu:

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

Nachdem der Agent installiert wurde, 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 systemd nicht verwendet:

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

Deinstallation des Agenten

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

1. Beenden Sie den Telegraf-Dienst:

```
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-Agenten:

```
dpkg -r telegraf  
. Entfernen Sie alle Konfigurations- oder Protokolldateien, die  
möglicherweise zurückgeblieben sind:
```

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

Aktualisieren des Agenten

Um den Telegraf-Agenten zu aktualisieren, gehen Sie wie folgt vor:

1. Stoppen Sie den Telegraf-Dienst:

```
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-Agenten:

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

Überprüfen der Prüfsummen von Telegraf-Paketen

Das Installationsprogramm des Data Infrastructure Insights -Agenten führt Integritätsprüfungen durch, einige Benutzer möchten jedoch möglicherweise eigene Überprüfungen durchführen, bevor sie die heruntergeladene Telegraf-Binärdatei installieren. Dies kann durch Herunterladen des Installationsprogramms und Generieren einer Prüfsumme für das heruntergeladene Paket erfolgen. Anschließendes Vergleichen der Prüfsumme mit dem in den Installationsanweisungen angezeigten Wert.

Laden Sie das Installationspaket herunter, ohne es zu installieren

Um einen reinen Downloadvorgang durchzuführen (im Gegensatz zum standardmäßigen Herunterladen und Installieren), können Benutzer den von der Benutzeroberfläche erhaltenen Agenteninstallationsbefehl bearbeiten und die Option „Installieren“ entfernen.

Gehen Sie folgendermaßen vor:

1. Kopieren Sie den Agent Installer-Ausschnitt wie angegeben.
2. Fügen Sie den Codeausschnitt nicht in ein Befehlsfenster ein, sondern in einen Texteditor.
3. Entfernen Sie das abschließende „--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 (in einem Arbeitsverzeichnis) ein und führen Sie es aus.

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

- Herunterladen und installieren (Standard):

```
installerName=cloudinsights-ubuntu_debian.sh ... && ./installerName  
--download --verify && sudo -E -H ./installerName --install  
* Nur zum Herunterladen:
```

```
installerName=cloudinsights-ubuntu_debian.sh ... && ./installerName  
--download --verify
```

Windows:

- Herunterladen und installieren (Standard):

```
!$(installerName=".\\cloudinsights-windows.ps1") ... -and $(if(((Get-  
FileHash $installerName).Hash).ToLower() -eq "INSTALLER_CHECKSUM ") {  
&$installerName -download -verify -install } else { Write-Host "Install  
script checksum does not match"})"  
* Nur zum Herunterladen:
```

```
!$(installerName=".\\cloudinsights-windows.ps1") ... -and $(if(((Get-  
FileHash $installerName).Hash).ToLower() -eq "INSTALLER_CHECKSUM ") {  
&$installerName -download -verify } else { Write-Host "Install script  
checksum does not match"})"
```

Der Nur-Download-Befehl lädt alle erforderlichen Artefakte von Data Infrastructure Insights in das Arbeitsverzeichnis herunter. Zu den Artefakten zählen unter anderem:

- ein Installationsskript
- eine Umgebungsdatei
- eine Telegraf-Binärdatei
- eine Signatur für die Telegraf-Binärdatei
- ein öffentliches Zertifikat zur Überprüfung der Binärsignatur

Das von DII heruntergeladene und kopierte Installations-Snippet führt automatisch eine Prüfsumme des Installationsskripts aus und die Signatur der Telegraf-Binärdatei wird durch das Installationsskript überprüft.

Prüfsummenwert überprüfen

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

- RHEL/Ubuntu:

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

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

Installieren Sie das heruntergeladene Paket

Sobald alle Artefakte zufriedenstellend überprüft wurden, kann die Agenteninstallation durch Ausführen des folgenden Befehls gestartet werden:

Nicht-Windows:

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

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

Erstellen und Verwenden von API-Zugriffstoken

Um ein API-Zugriffstoken für die Telegraf-Datenaufnahme zu erstellen, führen Sie bitte einen der folgenden Schritte aus:

Erstellen über die Data Collector-Installationsseite

1. Navigieren Sie zur Data Collector-Installationsseite für die Plattform, die Sie verwenden möchten (Windows, Linux).
2. Erstellen Sie ein Token mit der Schaltfläche + API-Zugriffstoken.

3. Geben Sie einen Namen ein und klicken Sie auf „Speichern“.
4. Der Tokenname sollte jetzt im Dropdown-Menü ausgewählt werden und wird bei der Installation des Collectors verwendet.

Manuelles Erstellen eines API-Zugriffstokens

1. Navigieren Sie zu Admin > API-Zugriff.
2. Klicken Sie auf + API-Zugriffstoken.
3. Geben Sie einen Namen und optional eine Beschreibung ein.
4. Wählen Sie unter „Für Aufrufe welcher API-Typen wird dieses Token verwendet?“ nur „Datenaufnahme“ aus und deaktivieren Sie dann „Erfassungseinheit“.
5. Wählen Sie unter „Berechtigungen“ Lesen/Schreiben aus.
6. Deaktivieren Sie „Token für Kubernetes automatisch rotieren“.

Um Ihr neu erstelltes API-Zugriffstoken zu verwenden, wählen Sie es aus der Dropdown-Liste „Vorhandenes API-Zugriffstoken auswählen oder neues erstellen“ auf der Installationsseite aus. Bitte beachten Sie, dass nur Token mit den folgenden Eigenschaften verwendet werden können:

- API-Typ: Nur „Datenaufnahme“
- Berechtigungen: Lesen/Schreiben
- Automatische Kubernetes-Rotation: Aus

Fehlerbehebung

Wenn beim Einrichten eines Agenten Probleme auftreten, können Sie Folgendes versuchen:

Problem:	Versuchen Sie Folgendes:
<p>Nach der Konfiguration eines neuen Plug-Ins und dem Neustart von Telegraf kann Telegraf nicht gestartet werden. Die Protokolle zeigen einen Fehler ähnlich dem folgenden an: „[telegraf] Fehler beim Ausführen des Agenten: Fehler beim Laden der Konfigurationsdatei /etc/telegraf/telegraf.d/cloudinsights-default.conf: Plugin-Ausgaben.http: Zeile <Zeilennummer>: In der Konfiguration wurden die Felder ["use_system_proxy"] angegeben, aber sie wurden nicht verwendet.“</p>	<p>Die installierte Telegraf-Version ist veraltet. Befolgen Sie die Schritte auf dieser Seite, um den Agenten für Ihre entsprechende Plattform zu aktualisieren.</p>
<p>Ich habe das Installationsskript auf einer alten Installation ausgeführt und jetzt sendet der Agent keine Daten</p>	<p>Deinstallieren Sie den Telegraf-Agenten und führen Sie das Installationsskript erneut aus. Befolgen Sie die Schritte zum Aktualisieren des Agenten auf dieser Seite für Ihre entsprechende Plattform.</p>
<p>Ich habe bereits einen Agenten mit Data Infrastructure Insights installiert</p>	<p>Wenn Sie bereits einen Agenten auf Ihrem Host/Ihrer VM installiert haben, müssen Sie den Agenten nicht erneut installieren. Wählen Sie in diesem Fall einfach die entsprechende Plattform und den entsprechenden Schlüssel im Bildschirm „Agent-Installation“ aus und klicken Sie auf „Weiter“ oder „Fertig stellen“.</p>

Problem:	Versuchen Sie Folgendes:
<p>Ich habe bereits einen Agenten installiert, aber nicht mithilfe des Data Infrastructure Insights -Installationsprogramms</p>	<p>Entfernen Sie den vorherigen Agenten und führen Sie die Installation des Data Infrastructure Insights Agenten aus, um die richtigen Standardeinstellungen der Konfigurationsdatei sicherzustellen. Wenn Sie fertig sind, klicken Sie auf Weiter oder Fertig.</p>

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

Konfigurieren von Datenkollektoren

Sie konfigurieren Datenkollektoren in Ihrer Data Infrastructure Insights Umgebung, um Daten von Geräten im Rechenzentrum zu erfassen.

Bevor Sie beginnen

- Sie müssen eine Erfassungseinheit konfiguriert haben, bevor Sie mit der Datenerfassung beginnen können.
- Sie benötigen Anmeldeinformationen für die Geräte, von denen Sie Daten erfassen.
- Für alle Geräte, von denen Sie Daten erfassen, sind Gerätenetzwerkadressen, Kontoinformationen und Passwörter erforderlich.

Schritte

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Observability > Collectors**

Das System zeigt die verfügbaren Datensammler nach Anbieter sortiert an.

2. Klicken Sie auf **+ Collector** 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.
4. Klicken Sie auf **Erweiterte Konfiguration**, um zusätzliche Konfigurationsfelder hinzuzufügen. (Nicht alle Datensammler erfordern eine erweiterte Konfiguration.)
5. Klicken Sie auf **Konfiguration testen**, um zu überprüfen, ob der Datensammler richtig konfiguriert ist.
6. Klicken Sie auf **Collector hinzufügen**, um die Konfiguration zu speichern und den Datensammler zu Ihrem Data Infrastructure Insights Mandanten hinzuzufügen.

Es kann bis zu zwei Abfrageperioden dauern, bis Daten des Dienstes in Dashboards angezeigt werden oder für Abfragen verfügbar sind.

- 1. Bestandsaufnahme: sofort
- 1. Leistungsdatenabfrage zur Ermittlung einer Baseline: unmittelbar nach der Bestandsabfrage
- 2. Leistungsumfrage: innerhalb von 15 Sekunden nach Abschluss der 1. Leistungsumfrage

Die Abfrage erfolgt dann gemäß den konfigurierten Bestands- und Leistungsabfrageintervallen.

Ermitteln des Erfassungsstatus des Datensammlers

Da Datensammler die primäre Informationsquelle für Data Infrastructure Insights sind, müssen Sie unbedingt sicherstellen, dass sie in einem laufenden Zustand bleiben.

Der Status des Datensammlers wird in der oberen rechten Ecke jeder Asset-Seite als Meldung „Vor N Minuten erfasst“ angezeigt, wobei N den aktuellsten Erfassungszeitpunkt des/der Datensammlers/Datensammler des Assets angibt. Außerdem werden Uhrzeit und Datum der Erfassung angezeigt.

Wenn Sie auf die Nachricht klicken, wird eine Tabelle mit dem Namen, dem Status und der letzten erfolgreichen Erfassungszeit des Datensammlers angezeigt. Wenn Sie als Administrator angemeldet sind, gelangen Sie durch Klicken auf den Link mit dem Namen des Datensammlers in der Tabelle zur Detailseite dieses Datensammlers.

Verwalten konfigurierter Datenkollektoren

Die Seite „Installierte Datensammler“ bietet Zugriff auf die Datensammler, die für Data Infrastructure Insights konfiguriert wurden. Auf dieser Seite können Sie vorhandene Datensammler ändern.

Schritte

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Observability > Collectors**

Der Bildschirm „Verfügbare Datensammler“ wird angezeigt.

2. Klicken Sie auf **Installierte Datensammler**

Es wird eine Liste aller installierten Datensammler angezeigt. Die Liste enthält den Namen und Status des Collectors, die IP-Adresse, auf die der Collector zugreift, und das Datum, an dem zuletzt Daten von einem Gerät abgerufen wurden. Auf diesem Bildschirm können unter anderem folgende Aktionen ausgeführt werden:

- Kontrollabfragen
- Ändern der Anmeldeinformationen des Datensammlers
- Klonen von Datensammlern

Steuern der Datensammlerabfrage

Nachdem Sie eine Änderung an einem Datensammler vorgenommen haben, möchten Sie möglicherweise, dass dieser sofort eine Abfrage durchführt, um Ihre Änderungen zu überprüfen. Oder Sie möchten die Datenerfassung auf einem Datensammler um einen, drei oder fünf Tage verschieben, während Sie an einem Problem arbeiten.

Schritte

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Observability > Collectors**
2. Klicken Sie auf **Installierte Datensammler**
3. Aktivieren Sie das Kontrollkästchen links neben dem Datensammler, den Sie ändern möchten
4. Klicken Sie auf **Massenaktionen** und wählen Sie die gewünschte Umfrageaktion aus.

Massenaktionen können gleichzeitig auf mehreren Datensammlern ausgeführt werden. Wählen Sie die

Datensammler aus und wählen Sie die auszuführende Aktion aus dem Menü **Massenaktion**.

Bearbeiten von Datenkollektorinformationen

Sie können vorhandene Einrichtungsinformationen des Datensammlers bearbeiten.

So bearbeiten Sie einen einzelnen Datensammler:

1. Klicken Sie im Menü „Data Infrastructure 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**.

Der Dialog „Collector bearbeiten“ wird geöffnet.

3. Geben Sie die Änderungen ein und klicken Sie auf **Konfiguration testen**, 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 neben jedem Datensammler, den Sie ändern möchten.
2. Klicken Sie auf die Schaltfläche **Massenaktionen** und wählen Sie **Bearbeiten**, um das Dialogfeld „Datensammler bearbeiten“ zu öffnen.
3. Ändern Sie die Felder wie oben.



Die ausgewählten Datensammler müssen vom selben Anbieter und Modell sein und sich auf derselben Erfassungseinheit befinden.

Beim Bearbeiten mehrerer Datensammler wird im Feld „Name des Datensammlers“ „Gemischt“ angezeigt und kann nicht bearbeitet werden. Andere Felder wie Benutzername und Passwort zeigen „Gemischt“ an und können bearbeitet werden. Felder, die in allen ausgewählten Datensammlern denselben Wert aufweisen, zeigen die aktuellen Werte an und können bearbeitet werden.

Beim Bearbeiten mehrerer Datensammler ist die Schaltfläche **Konfiguration testen** nicht verfügbar.

Klonen von Datenkollektoren

Mithilfe der Klonfunktion können Sie schnell eine Datenquelle hinzufügen, die über dieselben Anmeldeinformationen und Attribute wie eine andere Datenquelle verfügt. Durch Klonen können Sie problemlos mehrere Instanzen desselben Gerätetyps konfigurieren.

Schritte

1. Klicken Sie im Menü „Data Infrastructure Insights“ auf **Observability > Collectors**.
2. Klicken Sie auf **Installierte Datensammler**.
3. Klicken Sie auf das Kontrollkästchen links neben dem Datensammler, den Sie kopieren möchten.
4. Klicken Sie im Optionsmenü rechts neben dem ausgewählten Datensammler auf **Klonen**.

Das Dialogfeld „Datensammler klonen“ wird angezeigt.

5. Geben Sie in den erforderlichen Feldern neue Informationen ein.
6. Klicken Sie auf **Speichern**.

Nach Abschluss

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

Durchführen von Massenaktionen auf Datensammlern

Sie können einige Informationen für mehrere Datensammler gleichzeitig bearbeiten. Mit dieser Funktion können Sie eine Umfrage starten, die Umfrage verschieben und die Umfrage auf mehreren Datensammlern fortsetzen. Darüber hinaus können Sie mehrere Datensammler löschen.

Schritte

1. Klicken Sie im Menü „Data Infrastructure 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 Option, die Sie ausführen möchten.

Nach Abschluss

Der von Ihnen ausgewählte Vorgang wird auf den Datensammlern ausgeführt. Wenn Sie sich für das Löschen von Datensammlern entscheiden, wird ein Dialogfeld angezeigt, in dem Sie aufgefordert werden, die Aktion zu bestätigen.

Untersuchung eines gescheiterten Datensammlers

Wenn ein Datensammler eine Fehlermeldung und eine hohe oder mittlere Auswirkung aufweist, müssen Sie dieses Problem mithilfe der Übersichtsseite des Datensammlers und der darin verknüpften Informationen untersuchen.

Führen Sie die folgenden Schritte aus, um die Ursache für fehlgeschlagene Datensammler zu ermitteln. Fehlermeldungen zum 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 fehlerhaften Datensammlers, um die Seite „Zusammenfassung“ zu öffnen.
3. Überprüfen Sie auf der Seite „Zusammenfassung“ den Bereich „Kommentare“, um alle Notizen zu lesen, die möglicherweise von einem anderen Techniker hinterlassen wurden, der diesen Fehler möglicherweise ebenfalls untersucht.
4. Beachten Sie alle Leistungsmeldungen.
5. Bewegen Sie den Mauszeiger über die Segmente des Ereigniszeitleistendiagramms, um zusätzliche Informationen anzuzeigen.
6. Wählen Sie eine Fehlermeldung für ein Gerät aus, die unterhalb der Ereigniszeitleiste angezeigt wird, und klicken Sie auf das Symbol „Fehlerdetails“, das rechts neben der Meldung angezeigt wird.

Die Fehlerdetails umfassen den Text der Fehlermeldung, die wahrscheinlichsten Ursachen, verwendete Informationen und Vorschläge, was zur Behebung des Problems versucht werden kann.

7. Im Bereich „Von diesem Datensammler gemeldete Geräte“ können Sie die Liste filtern, um nur die Geräte anzuzeigen, die Sie interessieren, und Sie können auf den verknüpften **Namen** eines Geräts klicken, um die Asset-Seite für dieses Gerät anzuzeigen.

8. Wenn Sie zur Übersichtsseite des Datensammlers zurückkehren, überprüfen Sie den Bereich **Letzte Änderungen anzeigen** unten auf der Seite, um festzustellen, ob das Problem durch kürzliche Änderungen verursacht worden sein könnte.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.