



Collecting Data

Cloud Insights

NetApp

May 06, 2020

This PDF was generated from https://docs.netapp.com/us-en/cloudinsights/task_getting_started_with_cloud_insights.html on May 06, 2020. Always check docs.netapp.com for the latest.



Table of Contents

- Collecting Data 1
 - Getting started gathering data 1
 - Acquisition Unit Requirements 3
 - Configuring Acquisition Units 5
 - Configuring an Agent to Collect Data 10
 - Configuring Data Collectors 24
 - Determining data collector acquisition status 25
 - Managing configured data collectors 25
 - Researching a failed data collector 28

Collecting Data

Getting started gathering data

After you have signed up for Cloud Insights and log in to your environment for the first time, you will be guided through the following steps in order to begin collecting and managing data.

Data collectors discover information from your data sources, such as storage devices, network switches, and virtual machines. The information gathered is used for analysis, validation, monitoring and troubleshooting.

Cloud Insights utilizes three types of data collectors:

- Operating Systems
- Services
- Infrastructure

Select your first data collector from the supported vendors and models available. You can easily add additional data collectors later.

Install an Acquisition Unit

If you selected an *Infrastructure* data collector, an Acquisition Unit is required to inject data into Cloud Insights. You will need to download and install the Acquisition Unit software on a server or VM to collect data for Cloud Insights. A single Acquisition Unit can be used for multiple data collectors.




ONTAP Data
Management
Software

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?

 Linux ▼

[Linux Versions Supported](#) ⓘ [Production Best Practices](#) ⓘ

Installation Instructions

[Need Help?](#)

- 1 [Copy Installer Snippet](#)

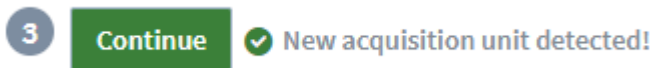
This snippet has a unique key valid for 24 hours for this Acquisition Unit only.

[+ Reveal Installer Snippet](#)

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

- 3  Waiting for Acquisition Unit to connect...

- Follow the [instructions](#) displayed to install your Acquisition Unit. Once the Acquisition Unit software is installed, the Continue button is displayed and you can proceed to the next step.



You may set up additional acquisition units later if needed. For example, you may want different Acquisition Units collecting information from data centers in different regions.

Configure the Data Collector - Infrastructure

For *Infrastructure* data collectors, you will be asked to fill out the data collector fields presented:

- Give the data collector a unique and meaningful name.
- Enter the user name and password to connect to the device, as appropriate.
- Fill in any other mandatory fields in *Configuration* and *Advanced Configuration* sections.
- Click **Test Connection** to test the connection to the device.
- Click **Add Collector** to save the data collector.

You will be able to configure additional data collectors later.

Configure the Data Collector - Operating Systems and Services

Operating System:

For *Operating System* data collectors, choose a platform (MacOS, Linux, Windows) to install a Cloud Insights Agent.

You must have at least one agent to collect data from Services.

The agent also collects data from the host itself, for use in Cloud Insights. This data is categorized as "Node" data in widgets, etc.

- Open a terminal or command window on the agent host or VM, and paste the displayed command to install the agent.
- When installation is complete, click **Complete Setup**.

Services:

For *Service* data collectors, click on a tile to open the instructions page for that service.

- Choose a platform and an Agent Access Key.
- If you don't have an agent installed on that platform, follow the instructions to install the agent.
- Click **Continue** to open the data collector instruction page.
- Follow the instructions to configure the data collector.

- When configuration is complete, click **Complete Setup**.

Add Dashboards

Depending on the type of initial data collector you selected to configure (storage, switch, etc.), one or more relevant dashboards will be imported. For example, if you configured a storage data collector, a set of storage-related dashboards will be imported, and one will be set as your Cloud Insights Home Page. You can change the home page from the **Dashboards > Show All Dashboards** list.

You can import additional dashboards later, or [create your own](#).

That's all there is to it

After you complete the initial setup process, your environment will begin to collect data.

If your initial setup process is interrupted (for example, if you close the browser window), you will need to follow the steps manually:

- Choose a Data Collector
- Install an Agent or Acquisition Unit if prompted
- Configure the Data Collector

Acquisition Unit Requirements

You must install an Acquisition Unit (AU) in order to acquire information from your data collectors. Before you install the Acquisition Unit, you should ensure that your environment meets operating system, CPU, memory, and disk space requirements.

Component	Linux Requirement	Windows Requirement
-----------	-------------------	---------------------

Operating system	<p>A computer running a licensed version of one of the following:</p> <ul style="list-style-type: none"> * CentOS 7.2 64-bit * CentOS 7.3 64-bit * CentOS 7.4 64-bit * CentOS 7.5 64-bit * CentOS 7.6 64-bit * Debian 9 64-bit * Oracle Enterprise Linux 7.5 64 bit * Red Hat Enterprise Linux 7.2 64-bit * Red Hat Enterprise Linux 7.3 64-bit * Red Hat Enterprise Linux 7.4 64-bit * Red Hat Enterprise Linux 7.5 64-bit * Red Hat Enterprise Linux 7.6 64-bit * Ubuntu Server 18.04 LTS <p>This computer should be running no other application-level software. A dedicated server is recommended.</p>	<p>A computer running a licensed version of one of the following:</p> <ul style="list-style-type: none"> * Microsoft Windows 10 64-bit * Microsoft Windows Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 <p>This computer should be running no other application-level software. A dedicated server is recommended.</p>
CPU	2 CPU cores	Same
Memory	8 GB RAM	Same
Available disk space	<p>50 GB</p> <p>For Linux, disk space should be allocated in this manner:</p> <p>/opt/netapp 25 GB</p> <p>/var/log/netapp 25 GB</p>	50 GB
Network	100 Mbps /1 Gbps Ethernet connection, static IP address, IP connectivity to all FC devices, and a required port to the Cloud Insights instance (80 or 443).	Same
Permissions	Sudo permissions on the Acquisition Unit server	Administrator permissions on the Acquisition Unit server

Virus Scan		During installation, you must completely disable all virus scanners. Following installation, the paths used by the Acquisition Unit software must be excluded from virus scanning.
------------	--	--

Configuring Acquisition Units

Cloud Insights collects device data using 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.

This topic describes how to add Acquisition Units and describes additional steps required when your environment uses a proxy.

Adding a Linux Acquisition Unit

Before you begin

- If your system is using a proxy, you must set the proxy environment variables before the acquisition unit is installed. For more information, see [Setting proxy environment variables](#).

Steps for Linux Acquisition Unit Installation


1. Log in as Administrator or Account Owner to your Cloud Insights environment.
2. Click **Admin > Data Collectors > Acquisition Units > +Acquisition Unit**

The system displays the *Install Acquisition Unit* dialog. Choose 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?

 Linux

Linux Versions Supported ⓘ Production Best Practices ⓘ

Installation Instructions

[Need Help?](#)

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. Verify that the server or VM hosting the Acquisition Unit meets the recommended system requirements.
2. Verify that the server is running a supported version of Linux. Click *OS Versions Supported (i)* for a list of supported versions.
3. Copy the Installation command snippet in the dialog into a terminal window on the server or VM that will host the Acquisition unit.
4. Paste and execute the command in the Bash shell.

After you finish

- Click **Admin > Data Collectors > Acquisition units** to check the status of Acquisition Units.
- You can access the Acquisition Unit logs at `/var/log/netapp/cloudinsights/acq/acq.log`
- Use the following script to control the Acquisition Unit:
 - `cloudinsights-service.sh` (stop, start, restart, check the status)
- Use the following script to uninstall the Acquisition Unit:
 - `cloudinsights-uninstall.sh`

Setting proxy environment variables

For environments that use a proxy, you must set the proxy environment variables before you add the Acquisition Unit. The instructions for configuring the proxy are provided on the *Add Acquisition Unit* dialog.

1. Click + in Have a Proxy Server?
2. Copy the commands to a text editor and set your proxy variables as needed.

+ Note: Restrictions on special characters in proxy username and password fields: '%' and '!' are allowed in the username field. ':', '%', and '!' are allowed in the password field.

3. Run the edited command in a terminal using the Bash shell.
4. Install the Acquisition Unit software.

Proxy Configuration

The Acquisition Unit uses 2-way/mutual authentication to connect to the Cloud Insights server. The client certificate must be passed to the Cloud Insights server to be authenticated. To accomplish this, the proxy must be set up to forward the http request to the Cloud Insights server without decrypting the data.

The Acquisition Unit uses the following two endpoints to communicate with Cloud Insights. If you have a firewall between the Acquisition Unit server and Cloud Insights, you need these endpoints when configuring firewall rules:

```
https://aulogin.<Cloud Insights Domain>  
https://<your-tenant-ID>.<Cloud Insights Domain>
```

For example:

```
https://aulogin.c01.cloudinsights.netapp.com  
https://cg0c586a-ee05-45rb-a5ac-333b5ae7718d7.c01.cloudinsights.netapp.com
```

Adding a Windows Acquisition Unit

Steps for Windows Acquisition Unit Installation


1. Log in to the Acquisition Unit server/VM as a user with Administrator permissions.
2. On that server, open a browser window and log in to your Cloud Insights environment as Administrator or Account Owner.
3. Click **Admin > Data Collectors > Acquisition Units > +Acquisition Unit**.

The system displays the *Install Acquisition Unit* dialog. Choose 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

[Need Help?](#)

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. Verify that the server or VM hosting the Acquisition Unit meets the recommended system requirements.
2. Verify that the server is running a supported version of Windows. Click *OS Versions Supported (i)* for a list of supported versions.
3. Click the **Download Installer (Windows 64-bit)** button.
4. Copy the Access Key. You will need this during the Installation.
5. On the Acquisition Unit server/VM, execute the downloaded installer.
6. Paste the Access Key into the installation wizard when prompted.
7. During installation, you will be presented with the opportunity to provide your proxy server settings.

After you finish

- Click **Admin > Data Collectors > Acquisition units** to check the status of Acquisition Units.
- You can access the Acquisition Unit log in <install dir>\Cloud Insights\Acquisition Unit\log\acq.log
- Use the following script to stop, start, restart, or check the status of the Acquisition Unit:

```
cloudinsights-service.sh
```

Proxy Configuration

The Acquisition Unit uses 2-way/mutual authentication to connect to the Cloud Insights server. The client certificate must be passed to the Cloud Insights server to be authenticated. To accomplish this, the proxy must be set up to forward the http request to the Cloud Insights server without decrypting the data.

The Acquisition Unit uses the following two endpoints to communicate with Cloud Insights. If you have a firewall between the Acquisition Unit server and Cloud Insights, you need these endpoints when configuring firewall rules:

```
https://aLOGIN.<Cloud Insights Domain>  
https://<your-tenant-ID>.<Cloud Insights Domain>
```

For example:

```
https://aLOGIN.c01.cloudinsights.netapp.com  
https://cg0c586a-ee05-45rb-a5ac-333b5ae7718d7.c01.cloudinsights.netapp.com
```

Uninstalling an Acquisition Unit

To uninstall the Acquisition Unit software, do the following:

Windows:

1. On the Acquisition Unit server/VM, open Control Panel and choose **Uninstall a Program**. Select the Cloud Insights Acquisition Unit program for removal.
2. Click Uninstall and follow the prompts.

Linux:

1. On the Acquisition Unit server/VM, run the following command:

```
sudo cloudinsights-uninstall.sh -p
```

2. For help with uninstall, run:

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

Both:

1. After uninstalling the AU software, go to **Admin > Data Collectors** and select the **Acquisition Units**

tab.

2. Click the Options button to the right of the Acquisition Unit you wish to uninstall, and select *Delete*. You can delete an Acquisition Unit only if there are no data collectors assigned to it.

Reinstalling an Acquisition Unit

To re-install an Acquisition Unit on the same server/VM, you must follow these steps:

Before you begin

You must have a temporary Acquisition Unit configured on a separate server/VM before re-installing an Acquisition Unit.

Steps

1. Log in to the Acquisition Unit server/VM and uninstall the AU software.
2. Log into your Cloud Insights environment and go to **Admin > Data Collectors**.
3. For each data collector, click the Options menu on the right and select *Edit*. Assign the data collector to the temporary Acquisition Unit and click **Save**.

You can also select multiple data collectors of the same type and click the **Bulk Actions** button. Choose *Edit* and assign the data collectors to the temporary Acquisition Unit.

4. After all of the data collectors have been moved to the temporary Acquisition Unit, go to **Admin > Data Collectors** and select the **Acquisition Units** tab.
5. Click the Options button to the right of the Acquisition Unit you wish to re-install, and select *Delete*. You can delete an Acquisition Unit only if there are no data collectors assigned to it.
6. You can now re-install the Acquisition Unit software on the original server/VM. Click **+Acquisition Unit** and follow the instructions above to install the Acquisition Unit.
7. Once the Acquisition Unit has been re-installed, assign your data collectors back to the Acquisition Unit.

Configuring an Agent to Collect Data

Cloud Insights uses [Telegraf](#) as its agent for collection of integration data. Telegraf is a plugin-driven server agent that can be used to collect and report metrics, events, and logs. Input plugins are used to collect the desired information into the agent by accessing the system/OS directly, by calling third-party APIs, or by listening to configured streams (i.e. Kafka, statsD, etc). Output plugins are used to send the collected metrics, events, and logs from the agent to Cloud Insights.

Installing an Agent

If you are installing a Service data collector and have not yet configured an Agent, you are prompted to first install an Agent for the appropriate Operating System. This topic provides instructions for installing the Telegraf agent on the following Operating Systems:

- [Windows](#)
- [RHEL and CentOS](#)
- [Ubuntu and Debian](#)
- [macOS](#)
- [Kubernetes](#)

To install an agent, regardless of the platform you are using, you must first do the following:

1. Log into the host you will use for your agent.
2. Log in to your Cloud Insights site and go to **Admin > Data Collectors**.
3. Click on **+Data Collector** and choose a data collector to install. There are several types of data collectors:
 - **Host** (Windows, Linux, macOS, etc.)
 - **Service** (integration with a wide variety of agent-collected plugins). Agents are configured and run as a service for RHEL/CentOS, Ubuntu/Debian, macOS, and Windows. For Kubernetes platforms, the agent is configured as a DaemonSet.
 - **Infrastructure** (collects from storage, switch, cloud platform, etc.). Infrastructure collection is done with an [Acquisition Unit](#) instead of an Agent.
4. Choose the appropriate platform for your host (Windows, Linux, macOS, etc.)
5. Follow the remaining steps for each platform below



Once you have installed an agent on a host, you do not need to install an agent again on that host.



Once you have installed an agent on a server/VM, Cloud Insights collects metrics from that system in addition to collecting from any data collectors you configure. These metrics are gathered as ["Node" metrics](#).

Windows

Install an Agent in your Environment

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

[Need Help?](#)

Choose Agent Access Key

Default ▼

1 Open up a PowerShell window and run the following command:

```
!$(Add-Type 'using System.Net; using System.Security.Cryptography.X509Certificates; public class TrustAllCertsPolicy : ICertificatePolicy { public bool CheckValidationResult(ServicePoint srvPoint, X509Certificate certificate, WebRequest request, int certificateProblem) {return true;}}') -and !$([System.Net.ServicePointManager]::CertificatePolicy = New-Object TrustAllCertsPolicy) -and !$( $AllProtocols = [System.Net.SecurityProtocolType]'Ssl3,Tls,Tls11,Tls12') -and !$([System.Net.ServicePointManager]::SecurityProtocol = $AllProtocols) -and !$( $pwd=(Get-Location).Path
```

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

Pre-requisites:

- PowerShell must be installed

Steps to install agent on Windows:

1. Choose an Agent Access Key.
2. Copy the command block from the agent installation dialog. You can click the clipboard icon to quickly copy the command to the clipboard.
3. Open a PowerShell window
4. Paste the command into the PowerShell window and press Enter.
5. The command will download the appropriate agent installer, install it, and set a default configuration. When finished, it will restart the agent service. The command has a unique key and is valid for 24 hours.
6. Click **Finish** or **Continue**

After the agent is installed, you can use the following commands to start/stop the service:

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

Uninstalling the Agent

To uninstall the agent on Windows, do the following in a PowerShell window:

1. Stop and delete the Telegraf service:

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

2. Delete the `C:\Program Files\telegraf` folder to remove the binary, logs, and configuration files
3. Remove the `SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf` key from the registry

Upgrading the Agent

To upgrade the telegraf agent, do the following:

- ### 1. Stop and delete the telegraf service:

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

2. Delete the `SYSTEM\CurrentControlSet\Services\EventLog\Application\telegraf` key from the registry
3. Delete `C:\Program Files\telegraf\telegraf.conf`
4. Delete `C:\Program Files\telegraf\telegraf.exe`
5. [Install the new agent.](#)

RHEL and CentOS

Install an Agent in your Environment

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

Need Help?

Choose Agent Access Key

Default

1

Open up a terminal window and run the following command in a Bash shell (requires curl, sudo, ping, and dmidecode):

```
installerName=cloudinsights-rhel_centos.sh && token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsInR5cCI6IHYZdCJpc3MiOiJvY2kiLCJleHAiOjE1NTI0OTMzMNTUsImxvZ2luIjoiaGVhZGF0eWwYyM2FjMzk1NzMtOTMlZS00Yjc2LWIzZjgtNzZlZWQ0MTkzNDdiIiwiaWF0IjoxNTUyNDA2OTU1LCJ0ZW5hbnQiOiI1ZTQ3OTk0MC0yYzg2LTQ5Y2YtOTk3OS05MjE1MDQ4NWQzOGIifQ.c1Lm1MgxsY3hbbb6F0sPgfkL_FrxvSL5j3vm4RbpZtBZPwyu_LboyKbSbnnRCM5X&& domain=mstapp.oci.cloud.netapp.com && curl -k -X GET -H "Authorization: Bearer $token" -H "X-CloudInsights-IntegrationAccessKey: 9fcd7340-92a0-4703-a9e7-dd2b0fbcb77d1" -o $installerName ht
```

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

Pre-requisites:

- The following commands must be available: curl, sudo, ping, and dmidecode

Steps to install agent on RHEL/CentOS:

1. Choose an Agent Access Key.
2. Copy the command block from the agent installation dialog. You can click the clipboard icon to quickly copy the command to the clipboard.
3. Open a Bash window
4. Paste the command into the Bash window and press Enter.
5. The command will download the appropriate agent installer, install it, and set a default configuration. When finished, it will restart the agent service. The command has a unique key and is valid for 24 hours.
6. Click **Finish** or **Continue**

After the agent is installed, you can use the following commands to start/stop the service:

If your operating system is using systemd (CentOS 7+ and RHEL 7+):

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

If your operating system is not using systemd (CentOS 7+ and RHEL 7+):

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

Uninstalling the Agent

To uninstall the agent on RHEL/CentOS, in a Bash terminal, do the following:

1. Stop the 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. Remove the Telegraf agent:

```
yum remove telegraf
```

3. Remove any configuration or log files that may be left behind:


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

Upgrading the Agent

To upgrade the telegraf agent, do the following:

1. Stop the 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. Remove the previous telegraf agent:

```
yum remove telegraf
```

- ### 3. Install the new agent.

Ubuntu and Debian

Install an Agent in your Environment

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

Need Help?

Choose Agent Access Key

Default

1

Open up a terminal window and run the following command in a Bash shell (requires curl, sudo, ping, and dmidecode):

```
installerName=cloudinsights-ubuntu_debian.sh && token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsInR5cCI6IHYwZmVudCJpc3MiOjYyZ2kiLCJleHAiOiJlNTI0OTMzMDEyImxvZ2luIjoiaW90MTUyNDQzMDEyIiwiaWF0IjoxNTUyNDQzMDEyLjEwMDQ4NWQzOGIifQ.jwoyoW7Zs2K0QBdEeb6LSAQa3Wti5ex3mAGYF_sAJLEUFyf8j4Fs86CJYo0-R8u && domain=mstapp.oc1.cloud.netapp.com && curl -k -X GET -H "Authorization: Bearer $token" -H "X-CloudInsights-IntegrationAccessKey: 9fcd7340-92a0-4703-a9e7-dd2b0fbc77d1" -o $installerName
```

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

Pre-requisites:

- The following commands must be available: curl, sudo, ping, and dmidecode

Steps to install agent on Debian or Ubuntu:

1. Choose an Agent Access Key.

2. Copy the command block from the agent installation dialog. You can click the clipboard icon to quickly copy the command to the clipboard.
3. Open a Bash window
4. Paste the command into the Bash window and press Enter.
5. The command will download the appropriate agent installer, install it, and set a default configuration. When finished, it will restart the agent service. The command has a unique key and is valid for 24 hours.
6. Click **Finish** or **Continue**

After the agent is installed, you can use the following commands to start/stop the service:

If your operating system is using systemd:

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

If your operating system is not using systemd:

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

Uninstalling the Agent

To uninstall the agent on Ubuntu/Debian, in a Bash terminal, run the following:

1. Stop the Telegraf service:

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

2. Remove the Telegraf agent:

```
dpkg -r telegraf
```

3. Remove any configuration or log files that may be left behind:

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

Upgrading the Agent

To upgrade the telegraf agent, do the following:

1. Stop the telegraf service:

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

2. Remove the previous telegraf agent:

```
dpkg -r telegraf
```

3. [Install the new agent.](#)

macOS

Install an Agent in your Environment

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

[Need Help?](#)

Choose Agent Access Key

default ▼

1 Open up a terminal window and run the following command in a Bash shell (requires curl):

```
installerName=cloudinsights-macos.sh && curl -k -X GET -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyY2xlcYI6WyJndWVzdCJdLCJpc3MiOiJvY2kiLCJleHAiOiE1NTMxMDg4NDcsImxvZ2luIjoiaidGVsZWdyYWYuM2U4MjEwYjU0MzRiYy00Y2FLLTgwZmMtYjY3NDAwYWVmZWYxIiwiaWF0IjoxNTUzMDIyNDQ3LCJ0ZW5hbnQiOiI4ZDQxOTVhNi1lYmI4LTRhZDAtYTZlZi00MTMwMjM0MGI1YyYifQ.N_B9vTgtvh0X6UsbPYeQTwi-ZWZOIxVcLFCYzIKdVbQ23kMS8L4JH6ZxJ4hFAGbs" -H "X-CloudInsights-IntegrationAccessKey: e63cf223-4e43-4831-9fde-ddacae952ca" -o $installerName
```

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

Pre-requisites:

- The "curl" command must be available

Steps to install agent on macOS:

1. Choose an Agent Access Key.
2. Copy the command block from the agent installation dialog. You can click the clipboard icon to quickly copy the command to the clipboard.
3. Open a Bash window
4. Paste the command into the Bash window and press Enter.
5. The command will download the appropriate agent installer, install it, and set a default

configuration. When finished, it will restart the agent service. The command has a unique key and is valid for 24 hours.

6. If you previously installed a Telegraf agent using Homebrew, you will be prompted to uninstall it. Once the previously installed Telegraf agent is uninstalled, re-run the command in step 5 above.
7. Click **Finish** or **Continue**

After the agent is installed, you can use the following commands to start/stop the service:

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

Uninstalling the Agent

To uninstall the agent on macOS, in a Bash terminal, run the following:

1. Stop the Telegraf service:

```
sudo launchctl stop telegraf
```

2. Uninstall the telegraf agent:

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

3. Remove any configuration or log files that may be left behind:

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

Upgrading the Agent

To upgrade the telegraf agent, do the following:

1. Stop the telegraf service:

```
sudo launchctl stop telegraf
```

2. Uninstall the previous telegraf agent:

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

3. [Install the new agent.](#)

Kubernetes

Install an Agent in your Environment

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

[Need Help?](#)

What Operating System or Platform Are You Using?

Kubernetes

Choose Agent Access Key

default

1 Open up a terminal window and run the following command in a Bash shell within (requires curl and sudo):

```
installerName=cloudinsights-kubernetes.yaml && curl -k -X GET -H "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsInR5cCI6IkpzZW50L3R1b3R5IiwiaWF0IjE1NTMxMDg5MzksImxvZ2luIjoIdGVsZWdyYWYyY2YtZjMyNS00OTg3LWE3YjMtM2RkZDg2YWE1NzAzIiwiaWF0IjoxNTUzMDIyNTM5LCJ0ZW5hbnQiOiI4ZDQxOTVhNi1lYmI4LTRhZDA0YjY0MTMwMjM0MGIlYWYifQ.OZpAwM7svQsZHKHfrRLPq-XnR2Y3YkqA2-19F7UntuSkbfK-M1V7baa0VE7wCYRH" -H "X-CloudInsights-IntegrationAccessKey: e63cf223-4e43-4831-9fde-ddacaee952ca" -o $installerName
```

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

Pre-requisites:

- The following commands must be available: curl and sudo

Steps to install agent on Kubernetes:

1. Choose an Agent Access Key.
2. Copy the command block from the agent installation dialog. You can click the clipboard icon to quickly copy the command to the clipboard.
3. Open a Bash window
4. Paste the command into the Bash window and press Enter.
5. The command will download the appropriate agent installer, install it, and set a default configuration. When finished, it will restart the agent service. The command has a unique key and is valid for 24 hours.
6. Click **Finish** or **Continue**

After the agent is installed, generate the Telegraf DaemonSet YAML and ReplicaSet YAML:

```
kubectl --namespace monitoring get ds telegraf-ds -o yaml > /tmp/telegraf-ds.yaml
kubectl --namespace monitoring get rs telegraf-rs -o yaml > /tmp/telegraf-rs.yaml
```

You can use the following commands to stop and start the Telegraf service:

```
kubectl --namespace monitoring delete ds telegraf-ds
kubectl --namespace monitoring delete rs telegraf-rs
```

```
kubectl --namespace monitoring apply -f /tmp/telegraf-ds.yaml
kubectl --namespace monitoring apply -f /tmp/telegraf-rs.yaml
```

Configuring the Agent to Collect Data from Kubernetes

For Kubernetes environments, Cloud Insights deploys the Telegraf agent as a DaemonSet and a ReplicaSet. The pods in which the agents run need to have access to the following:

- hostPath
- configMap
- secrets

These Kubernetes objects are automatically created as part of the Kubernetes agent install command provided in the Cloud Insights UI. Some variants of Kubernetes, such as OpenShift, implement an added level of security that may block access to these components. The *SecurityContextConstraint* is not created as part of the Kubernetes agent install command provided in the Cloud Insights UI, and must be created manually. Once created, restart the Telegraf pod(s).

```

apiVersion: v1
kind: SecurityContextConstraints
metadata:
  name: telegraf-hostaccess
  creationTimestamp:
  annotations:
    kubernetes.io/description: telegraf-hostaccess allows hostpath volume mounts for
restricted SAs.
  labels:
    app: ci-telegraf
priority: 10
allowPrivilegedContainer: false
defaultAddCapabilities: []
requiredDropCapabilities: []
allowedCapabilities: []
allowedFlexVolumes: []
allowHostDirVolumePlugin: true
volumes:
- hostPath
- configMap
- secret
allowHostNetwork: false
allowHostPorts: false
allowHostPID: false
allowHostIPC: false
seLinuxContext:
  type: MustRunAs
runAsUser:
  type: RunAsAny
supplementalGroups:
  type: RunAsAny
fsGroup:
  type: RunAsAny
readOnlyRootFilesystem: false
users:
- system:serviceaccount:monitoring:telegraf-user
groups: []

```

Installing the kube-state-metrics server

When you install the kube-state-metrics server you can enable collection of the following Kubernetes objects: StatefulSet, DaemonSet, Deployment, PV, PVC, ReplicaSet, Service, Namespace, Secret, ConfigMap, Pod Volume, and Ingress.

Use the following steps to install the kube-state-metrics server:

Steps

1. Create a temporary folder (for example, `/tmp/kube-state-yaml-files/`) and copy the .yaml files from <https://github.com/kubernetes/kube-state-metrics/tree/master/examples/standard> to this folder.
2. Run the following command to apply the .yaml files needed for installing kube-state-metrics:

```
kubectl apply -f /tmp/kube-state-yaml-files/
```

kube-state-metrics Counters

Use the following links to access information for the kube state metrics counters:

1. [Cronjob Metrics](#)
2. [DaemonSet Metrics](#)
3. [Deployment Metrics](#)
4. [Endpoint Metrics](#)
5. [Horizontal Pod Autoscaler Metrics](#)
6. [Ingress Metrics](#)
7. [Job Metrics](#)
8. [LimitRange Metrics](#)
9. [Namespace Metrics](#)
10. [Node Metrics](#)
11. [Persistent Volume Metrics](#)
12. [Persistent Volume Claim Metrics](#)
13. [Pod Metrics](#)
14. [Pod Disruption Budget Metrics](#)
15. [ReplicaSet metrics](#)
16. [ReplicationController Metrics](#)

Uninstalling the Agent

To uninstall the agent on Kubernetes, do the following:

1. If the monitoring namespace is being used solely for Telegraf:

```
kubectl delete ns monitoring
```

If the monitoring namespace is being used for other purposes in addition to Telegraf:

1. Stop and delete the Telegraf service:

```
kubectl --namespace monitoring delete ds telegraf-ds
kubectl --namespace monitoring delete rs telegraf-rs
```

2. Delete the Telegraf ConfigMap and ServiceAccount:

```
kubectl --namespace monitoring delete cm telegraf-conf
kubectl --namespace monitoring delete cm telegraf-conf-rs
kubectl --namespace monitoring delete sa telegraf-user
```

3. Delete the Telegraf ClusterRole and ClusterRolebinding:

```
kubectl --namespace monitoring delete clusterrole endpoint-access
kubectl --namespace monitoring delete clusterrolebinding endpoint-access
```

Upgrading the Agent

To upgrade the telegraf agent, do the following:

1. Remove the current the telegraf deployments:

```
kubectl --namespace monitoring delete ds telegraf-ds
kubectl --namespace monitoring delete rs telegraf-rs
```

2. Back up the existing configurations:

```
kubectl --namespace monitoring get cm telegraf-conf -o yaml > /tmp/telegraf-conf.yaml
kubectl --namespace monitoring get cm telegraf-conf-rs -o yaml > /tmp/telegraf-conf-rs.yaml
```

3. [Install the new agent.](#)

4. Re-apply the configurations:

```
kubectl --namespace monitoring apply -f /tmp/telegraf-conf.yaml --force
kubectl --namespace monitoring apply -f /tmp/telegraf-conf-rs.yaml --force
```

5. Restart all telegraf pods. Run the following command for each telegraf pod:

```
kubectl --namespace monitoring delete pod <Telegraf_pod>
```

Troubleshooting Agent Installation

Some things to try if you encounter problems setting up an agent:

Problem:	Try this:
I already installed an agent using Cloud Insights	If you have already installed an agent on your host/VM, you do not need to install the agent again. In this case, simply choose the appropriate Platform and Key in the Agent Installation screen, and click on Continue or Finish .
I already have an agent installed but not by using the Cloud Insights installer	Remove the previous agent and run the Cloud Insights Agent installation, to ensure proper default configuration file settings. When complete, click on Continue or Finish .

Additional information may be found from the [Support](#) page or in the [Data Collector Support Matrix](#).

Configuring Data Collectors

You configure Data Collectors in your Cloud Insights environment to collect data from devices in the data center.

Before you begin

- You must have configured an Acquisition Unit before you can start collecting data.
- You need credentials for the devices from which you are collecting Data.
- Device network addresses, account information, and passwords are required for all devices you are collecting data from.

Steps

1. From the Cloud Insights menu, click **Admin > Data Collectors**

The system displays the available Data Collectors arranged by vendor.

2. Click + **Collector** on the required vendor and select the data collector to configure.

In the dialog box you can configure the data collector and add an Acquisition Unit.

3. Enter a name for the data collector.

Names can contain can contain letters (a-z), numbers (0-9), dashes (-), underscores (_), apostrophes

('), and periods (.).

4. Enter the Acquisition Unit to associate with this data collector.
5. Enter the required fields in the Configuration screen.
6. Click **Advanced Configuration** to add additional configuration fields. (Not all data collectors require advanced configuration.)
7. Click **Test Configuration** to verify that the data collector is properly configured.
8. Click **Add Collector** to save the configuration and add the data collector to your Cloud Insights tenant.

After adding a new data collector, Cloud Insights initiates three polls:

- 1st inventory poll: immediately
- 1st performance data poll to establish a baseline: immediately after inventory poll
- 2nd performance poll: within 15 seconds after completion of 1st performance poll

Polling then proceeds according to the configured inventory and performance poll intervals.

Determining data collector acquisition status

Because data collectors are the primary source of information for Cloud Insights, it is imperative that you ensure that they remain in a running state.

Data collector status is displayed in the upper right corner of any asset page as the message "Acquired N minutes ago", where N indicates the most recent acquisition time of the asset's data collector(s). The acquisition time/date is also displayed.

Clicking on the message displays a table with data collector name, status, and last successful acquisition time. If you are signed in as an Administrator, clicking on the data collector name link in the table takes you to detail page for that data collector.

Managing configured data collectors

The Installed Data Collectors page provides access to the data collectors that have been configured for Cloud Insights. You can use this page to modify existing data collectors.

Steps

1. In the Cloud Insights menu, click **Admin > Data Collectors**

The Available Data Collectors screen is displayed.

2. Click **Installed Data Collectors**

A list of all of the installed Data Collectors is displayed. The list provides collector name, status, the IP address the collector is accessing, and when data was last acquired from the a device. Action that can be performed on this screen include:

- Control polling
- Change data collector credentials
- Clone data collectors

Controlling Data Collector polling

After making a change to a data collector, you might want it to poll immediately to check your changes, or you might want to postpone the data collection on a data collector for one, three, or five days while you work on a problem.

Steps

1. In the Cloud Insights menu, click **Admin > Data Collectors**
2. Click **Installed Data Collectors**
3. Select the check box to the left of the Data Collector you want to change
4. Click **Bulk Actions** and select the polling action you want to take.

Bulk actions can be performed simultaneously on multiple Data Collectors. Select the data collectors, and chose the action to perform from the **Bulk Action** menu.

Editing data collector information

You can edit existing data collector setup information.

To edit a single data collector:

1. In the Cloud Insights menu, click **Admin > Data Collectors** to open the list of installed Data Collectors.
2. In the options menu to the right of the data collector you want to modify, click **Edit**.

The Edit Collector dialog is opened.

3. Enter the changes and click **Test Configuration** to test the new configuration or click **Save** to save the configuration.

You can also edit multiple data collectors:

1. Select the check box to the left of each data collector you want to change.
2. Click the **Bulk Actions** button and choose **Edit** to open the Edit data Collector dialog.

3. Modify the fields as above.



The data collectors selected must be the same vendor and model, and reside on the same Acquisition Unit.

When editing multiple data collectors, the Data Collector Name field shows “Mixed” and cannot be edited. Other fields such as user name and password show “Mixed” and can be edited. Fields that share the same value across the selected data collectors show the current values and can be edited.

When editing multiple data collectors, the **Test Configuration** button is not available.

Cloning data collectors

Using the clone facility, you can quickly add a data source that has the same credentials and attributes as another data source. Cloning allows you to easily configure multiple instances of the same device type.

Steps

1. In the Cloud Insights menu, click **Admin > Data Collectors**.
2. Click **Installed Data Collectors**.
3. Click the check box to the left of the data collector you want to copy.
4. In the options menu to the right of the selected data collector, click **Clone**.

The Clone Data Collector dialog is displayed.

5. Enter new information in the required fields.
6. Click **Save**.

After you finish

The clone operation copies all other attributes and settings to create the new data collector.

Performing bulk actions on data collectors

You can simultaneously edit some information for multiple data collectors. This feature allows you to initiate a poll, postpone polling, and resume polling on multiple data collectors. In addition, you can delete multiple data collectors.

Steps

1. In the Cloud Insights menu, click **Admin > Data Collectors**
2. Click **Installed Data Collectors**
3. Click the check box to the left of the data collectors you want to modify.
4. In the options menu to the right, click the option you want to perform.

After you finish

The operation you selected is performed on the data collectors. When you chose to delete data collectors, a dialog is displayed requiring you to conform the action.

Researching a failed data collector

If a data collector has failure message and a High or Medium Impact, you need to research this problem using the data collector summary page with its linked information.

Use the following steps to determine the cause of failed data collectors. Data collector failure messages are displayed on the **Admin** menu and on the **Installed Data Collectors** page.

Steps

1. Click **Admin > Data Collectors > Installed Data Collectors**.
2. Click the linked Name of the failing data collector to open the Summary page.
3. On the Summary page, check the Comments area to read any notes that might have been left by another engineer who might also be investigating this failure.
4. Note any performance messages.
5. Move your mouse pointer over the segments of the Event Timeline graph to display additional information.
6. Select an error message for a Device and displayed below the Event Timeline and click the Error details icon that displays to the right of the message.

The Error details include the text of the error message, most likely causes, information in use, and suggestions of what can be tried to correct the problem.

7. In the Devices Reported By This Data Collector area, you might filter the list to display only devices of interest, and you can click the linked **Name** of a device to display the asset page for that device.
8. When you return to the data collector summary page, check the **Show Recent Changes** area at the bottom of the page to see if recent changes could have caused the problem.

:leveloffset: -1

Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.