Collecting Data

Cloud Insights

NetApp
June 25, 2024

Table of Contents

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.

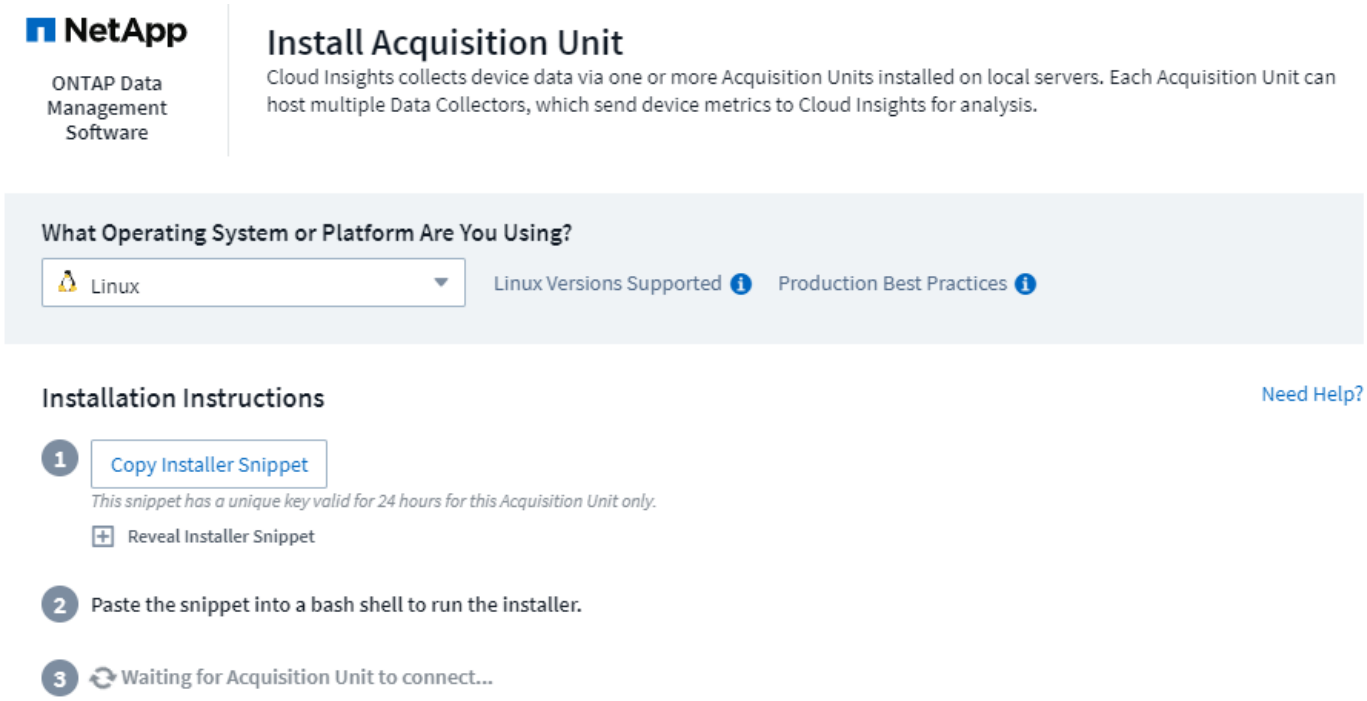
Cloud Insights has available three types of data collectors:

- Infrastructure (storage devices, network switches, compute infrastructure)
- Operating Systems (such as VMware or Windows)
- Services (such as Kafka)

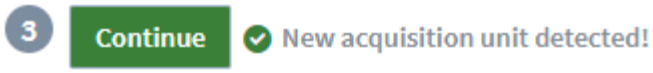
Select your first data collector from the supported vendors and models available. You can easily add additional data collectors later.

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 on the data center from which you will be collecting. A single Acquisition Unit can be used for multiple data collectors.



- 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 credentials (user name and password) to connect to the device, as appropriate.
- Fill in any other mandatory fields in *Configuration* and *Advanced Configuration* sections.
- 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 (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

Useful definitions

The following definitions may be useful when talking about Cloud Insights data collectors or features:

- Collector life cycle: A collector will belong to one of the following states in its life cycle:
  - **Preview**: Available in a limited capacity or to a limited audience. Preview features and data collectors are expected to become GA following the preview period. Preview periods vary based on audience or functionality.
  - **GA**: A feature or data collector that is Generally Available to all customers, based on Edition or feature set.
  - **Deprecated**: Applies to data collectors that are, or are expected to become, no longer functionally sustainable. Deprecated data collectors are often replaced with newer, functionally-updated data collectors.
  - **Deleted**: A data collector that has been removed and is no longer available.
- Acquisition Unit: a computer dedicated to hosting data collectors, typically a Virtual Machine. This computer is typically located in the same data center / VPC as the monitored items.
- Data Source: a module for communicating with a hardware or software stack. It consists of a configuration and code that runs on the AU computer to communicate with the device.

Acquisition Unit Requirements

You must install an Acquisition Unit (AU) in order to acquire information from your infrastructure data collectors (storage, VM, port, EC2, etc.). Before you install the Acquisition Unit, you should ensure that your environment meets operating system, CPU, memory, and disk space requirements.

Requirements

Component	Linux Requirement	Windows Requirement

Operating system	A computer running a licensed version of one of the following: * Centos (64-bit): 7.2 through 7.9, 8.1 through 8.4, Stream 8, Stream 9 * AlmaLinux 9.3 and 9.4 * Debian (64-bit): 9 and 10 * OpenSUSE Leap 15.1 through 15.5 * Oracle Enterprise Linux (64-bit): 7.5 through 7.9, 8.1 through 8.8 * Red Hat Enterprise Linux (64-bit): 7.2 through 7.9, 8.1 through 8.10, 9.1 through 9.4 * Rocky 9.0 through 9.4 * SUSE Enterprise Linux Server 15, 15 SP2 through 15 SP5 * Ubuntu Server: 18.04, 20.04, 22.04 LTS * SELinux on the above platforms This computer should be running no other application-level software. A dedicated server is recommended. If you are running with SELinux, it is recommended to execute the following commands on the acquisition unit system: sudo semanage fcontext -a -t usr_t "/opt/netapp/cloudinsights(/.*)?" sudo restorecon -R /opt/netapp/cloudinsights	A computer running a licensed version of one of the following: * Microsoft Windows 10 64-bit * Microsoft Windows Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows 11 This computer should be running no other application-level software. A dedicated server is recommended.
CPU	2 CPU cores	Same
Memory	8 GB RAM	Same
Available disk space	50 GB (100 GB recommended) For Linux, disk space should be allocated in this manner: /opt/netapp 10 GB (20 GB for large environments) /var/log/netapp 40 GB (80 GB for large environments) /tmp at least 1 GB available during installation	50 GB

Network	100 Mbps/1 Gbps Ethernet connection, static IP address, and port 80 or 443 connectivity from Acquisition Unit to *.cloudinsights.netapp.com or your Cloud Insights environment (i.e. https://<environment_id>.c01.cloudinsights.netapp.com) is required. For requirements between Acquisition Unit and each Data Collector, please refer to instructions for the Data Collector. If your organization requires proxy usage for internet access, you may need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. For example, does your organization block access by default, and only allow access to specific web sites/domains by exception? If so, you will need to get the following domain added to the exception list: *.cloudinsights.netapp.com For more information, read about Proxies here (Linux) or here (Windows).	Same
Permissions	Sudo permissions on the Acquisition Unit server. /tmp must be mounted with exec capabilities.	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.

Additional recommendations

- For accurate audit and data reporting, it is strongly recommended to synchronize the time on the Acquisition Unit machine using **Network Time Protocol (NTP)** or **Simple Network Time Protocol (SNTP)**.

Regarding Sizing

You can get started with a Cloud Insights Acquisition Unit with just 8GB memory and 50GB of disk space, however, for larger environments you should ask yourself the following questions:

Do you expect to:

- Discover more than 2500 virtual machines or 10 large (> 2 node) ONTAP clusters, Symmetrix, or HDS/HPE VSP/XP arrays on this Acquisition Unit?
- Deploy 75 or more total data collectors on this Acquisition Unit?

For each "Yes" answer above, it is recommend to add 8 GB of memory and 50 GB of disk space to the AU. So for example if you answered "Yes" to both, you should deploy a 24GB memory system with 150GB or more of disk space. On Linux, the disk space to be added to the log location.

For additional sizing questions, contact NetApp Support.

Additional Federal Edition requirement

- For Acquisition Unit installations in Cloud Insights Federal Edition clusters, the underlying operating system must have a good source of entropy. On Linux systems this is typically done by installing *rng-tools* or by using hardware random number generation (RNG). It is the customer's responsibility to ensure this requirement is met on the Acquisition Unit machine.

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.

For accurate audit and data reporting, it is strongly recommended to synchronize the time on the Acquisition Unit machine using **Network Time Protocol (NTP)** or **Simple Network Time Protocol (SNTP)**.

Read about Cloud Insights security here.

Adding a Linux Acquisition Unit

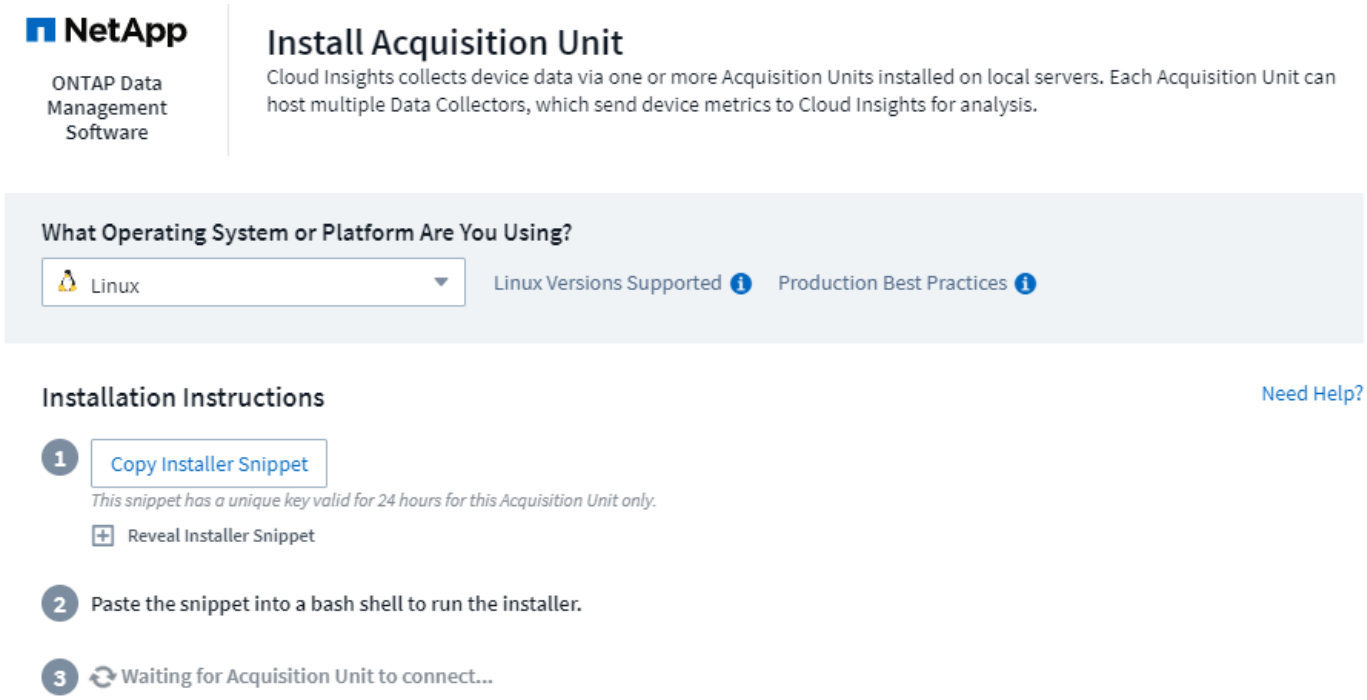
Before you begin

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

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



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 **Observability > 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: Be aware of 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 https request to the Cloud Insights server without decrypting the data.

The simplest way to do this is to specify wildcard configuration in your proxy/firewall to communicate with Cloud Insights, for example:

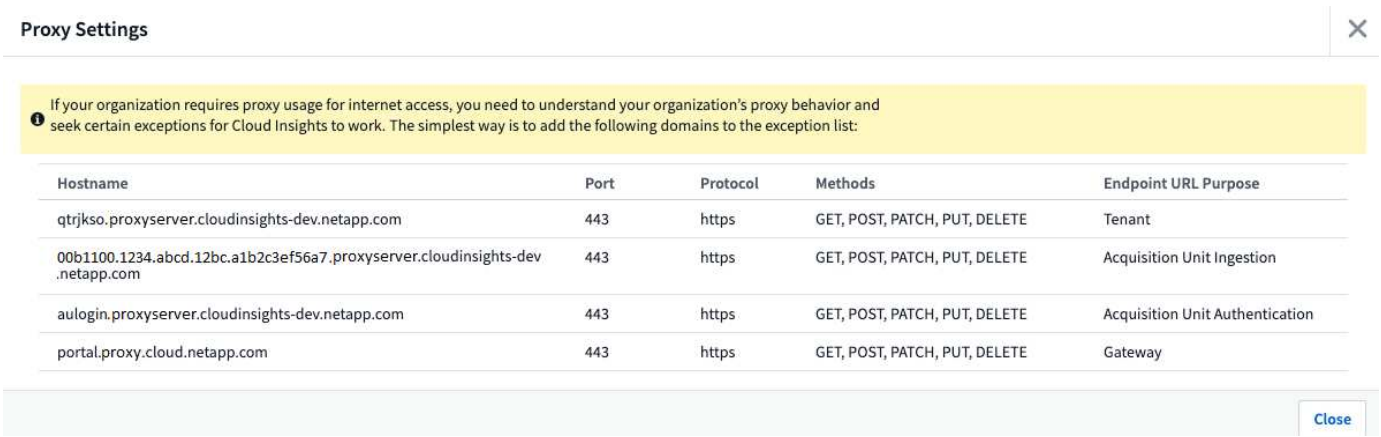
```
*.cloudinsights.netapp.com
```

The use of an asterisk (*) for wildcard is common, but your proxy/firewall configuration may use a different format. Check with your proxy documentation to ensure correct wildcard specification in your environment.

More information on proxy configuration can be found in the NetApp Knowledgbase.

Viewing Proxy URLs

You can view your proxy endpoint URLs by clicking the **Proxy Settings** link when choosing a data collector during onboarding, or the link under *Proxy Settings* on the **Help > Support** page. A table like the following is displayed.



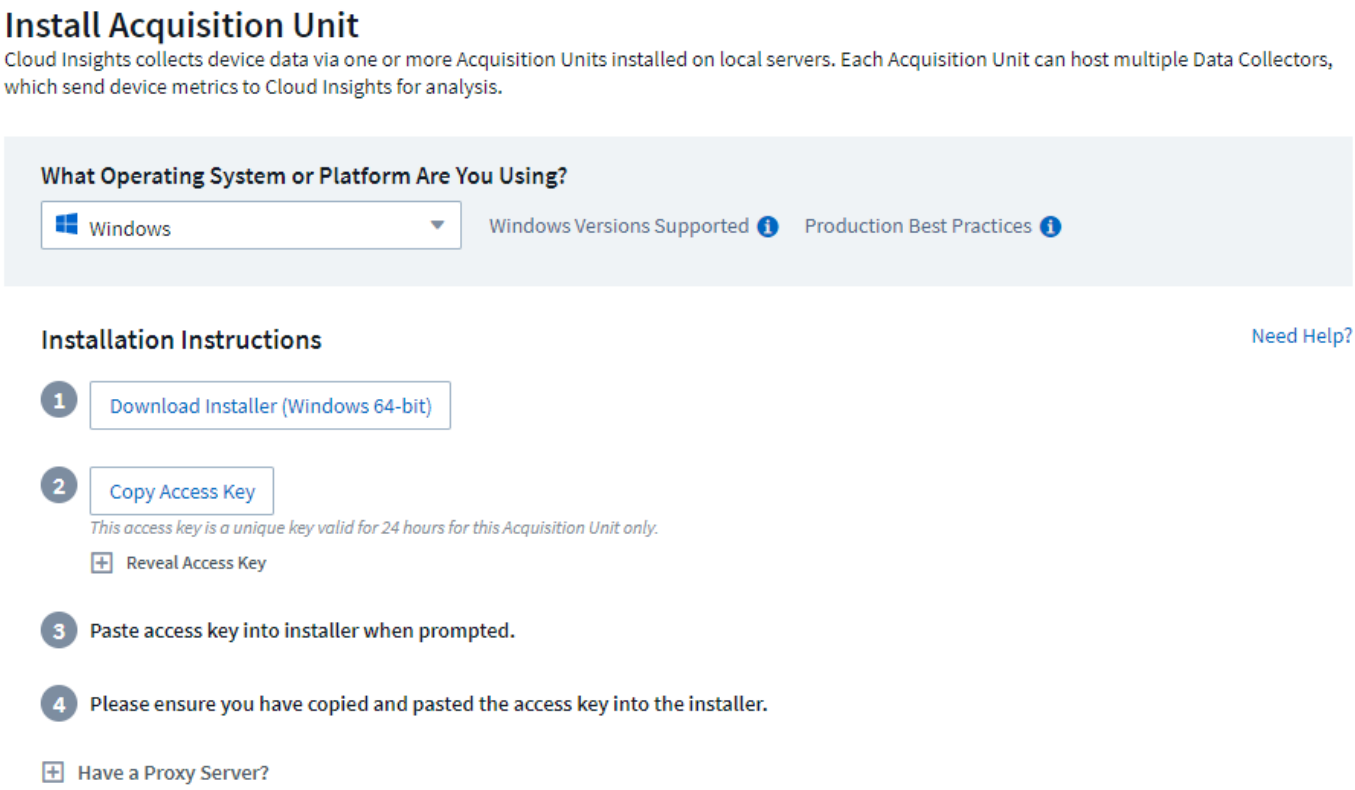
If you have Workload Security in your environment, the configured endpoint URLs will also be displayed in this list.

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

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



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 * > Observability > 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 https request to the Cloud Insights server without decrypting the data.

The simplest way to do this is to specify wildcard configuration in your proxy/firewall to communicate with Cloud Insights, for example:

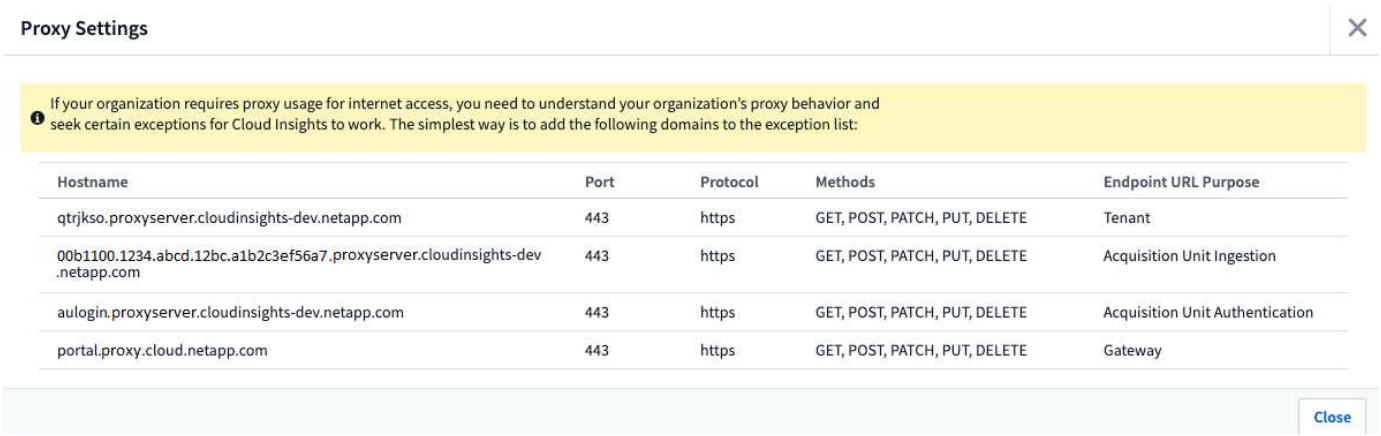
```
*.cloudinsights.netapp.com
```

The use of an asterisk (*) for wildcard is common, but your proxy/firewall configuration may use a different format. Check with your proxy documentation to ensure correct wildcard specification in your environment.

More information on proxy configuration can be found in the NetApp Knowledgbase.

Viewing Proxy URLs

You can view your proxy endpoint URLs by clicking the **Proxy Settings** link when choosing a data collector during onboarding, or the link under *Proxy Settings* on the **Help > Support** page. A table like the following is displayed.



If you have Workload Security in your environment, the configured endpoint URLs will also be displayed in this list.

Uninstalling an Acquisition Unit

To uninstall the Acquisition Unit software, do the following:

Windows:

If you are uninstalling a **Windows** acquisition unit:

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:

If you are uninstalling a **Linux** acquisition unit:

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
```

Windows and Linux:

After uninstalling the AU:

1. In Cloud Insights, go to **Observability > 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.

> You cannot delete an Acquisition Unit (AU) that has data collectors connected to it. Move all of the AU's data collectors to another AU (edit the collector and simply select a different AU) before deleting the original AU.

An Acquisition unit with a star next to it is being used for device resolution. Before removing this AU, you must select another AU to use for Device Resolution. Hover over a different AU and open the "three dots" menu to select "Use for Device Resolution".

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 **Observability > 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.

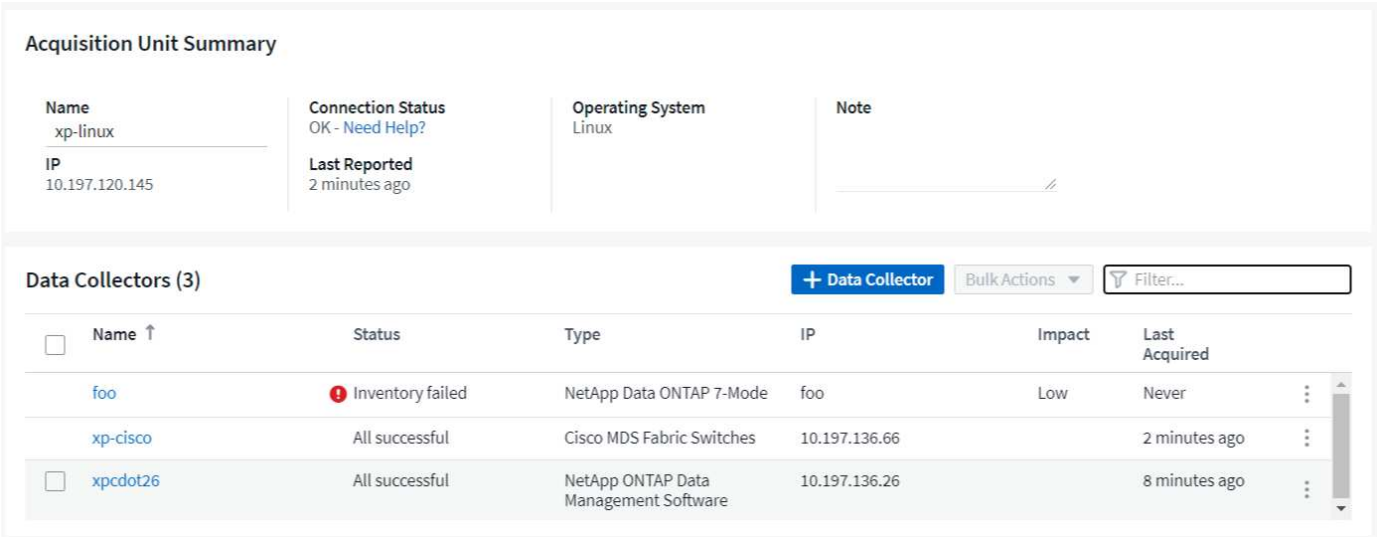
4. After all of the data collectors have been moved to the temporary Acquisition Unit, go to **Observability > Collectors** and select the **Acquisition Units** tab.

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.

Viewing AU Details

The Acquisition Unit (AU) detail page provides useful detail for an AU as well as information to help with troubleshooting. The AU detail page contains the following sections:

- A **summary** section showing the following:
  - **Name** and **IP** of the Acquisition Unit
  - Current connection **Status** of the AU
  - **Last Reported** successful data collector poll time
  - The **Operating System** of the AU machine
  - Any current **Note** for the AU. Use this field to enter a comment for the AU. The field displays the most recently added note.
- A table of the AU's **Data Collectors** showing, for each data collector:
  - **Name** - Click this link to drill down into the data collector's detail page with additional information
  - **Status** - Success or error information
  - **Type** - Vendor/model
  - **IP** address of the data collector
  - Current **Impact** level
  - **Last Acquired** time - when the data collector was last successfully polled



For each data collector, you can click on the "three dots" menu to Clone, Edit, Poll, or Delete the data collector. You can also select multiple data collectors in this list to perform bulk actions on them.

To restart the Acquisition Unit, click the **Restart** button at the top of the page. Drop down this button to attempt to **Restore Connection** to the AU in the event of a connection problem.

Configuring an Agent to Collect Data (Windows/Linux)

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.

The current Telegraf version for Cloud Insights is **1.24.0**.

For information on installing on Kubernetes, see the NetApp Kubernetes Monitoring Operator page.

For accurate audit and data reporting, it is strongly recommended to synchronize the time on the Agent machine using **Network Time Protocol (NTP)** or **Simple Network Time Protocol (SNTP)**.

If you want to verify the installation files before instaling the Agent, see the section below on Verifying Checksums.

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

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 environment and navigate to **Observability > Collectors**.
3. Click on **+Data Collector** and choose a data collector to install.
4. Choose the appropriate platform for your host (Windows, Linux)
5. Follow the remaining steps for each platform.

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.

If you are using a proxy, read the proxy instructions for your platform before installing the Telegraf agent.

Log Locations

Telegraf log messages are redirected from stdout to the following log files be default:

- RHEL/CentOS: /var/log/telegraf/telegraf.log
- Ubuntu/Debian: /var/log/telegraf/telegraf.log
- Windows: C:\Program Files\telegraf\telegraf.log

Windows

Pre-requisites:

- PowerShell must be installed
- If you are behind a proxy, you must follow the instructions in the **Configuring Proxy Support for Windows** section.

Configuring Proxy Support for Windows

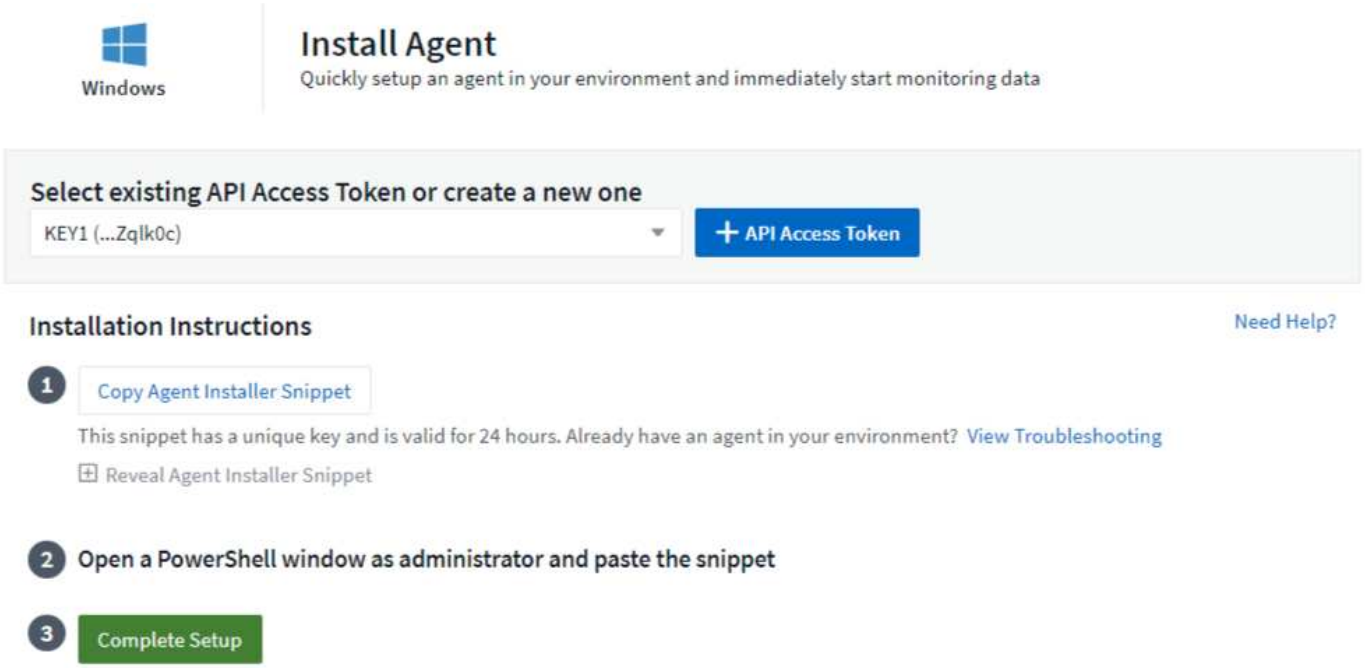
If your environment uses a proxy, read this section before you install.

The steps below outline the actions needed to set the *http_proxy/https_proxy* environment variables. For some proxy environments, users may also need to set the *no_proxy environment* variable.

For systems residing behind a proxy, perform the following to set the *https_proxy* and/or *http_proxy* environment variable(s) **PRIOR** to installing the Telegraf agent:

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

Installing the agent



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. Remove the certificate from the trustore:

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

3. Delete the *C:\Program Files\telegraf* folder to remove the binary, logs, and configuration files
4. 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

Pre-requisites:

- The following commands must be available: curl, sudo, ping, sha256sum, openssl, and dmidecode
- If you are behind a proxy, you must follow the instructions in the **Configuring Proxy Support for RHEL/CentOS** section.

Configuring Proxy Support for RHEL/CentOS

If your environment uses a proxy, read this section before you install.

The steps below outline the actions needed to set the *http_proxy/https_proxy* environment variables. For some proxy environments, users may also need to set the *no_proxy environment* variable.

For systems residing behind a proxy, perform the following steps **PRIOR** to installing the Telegraf agent:

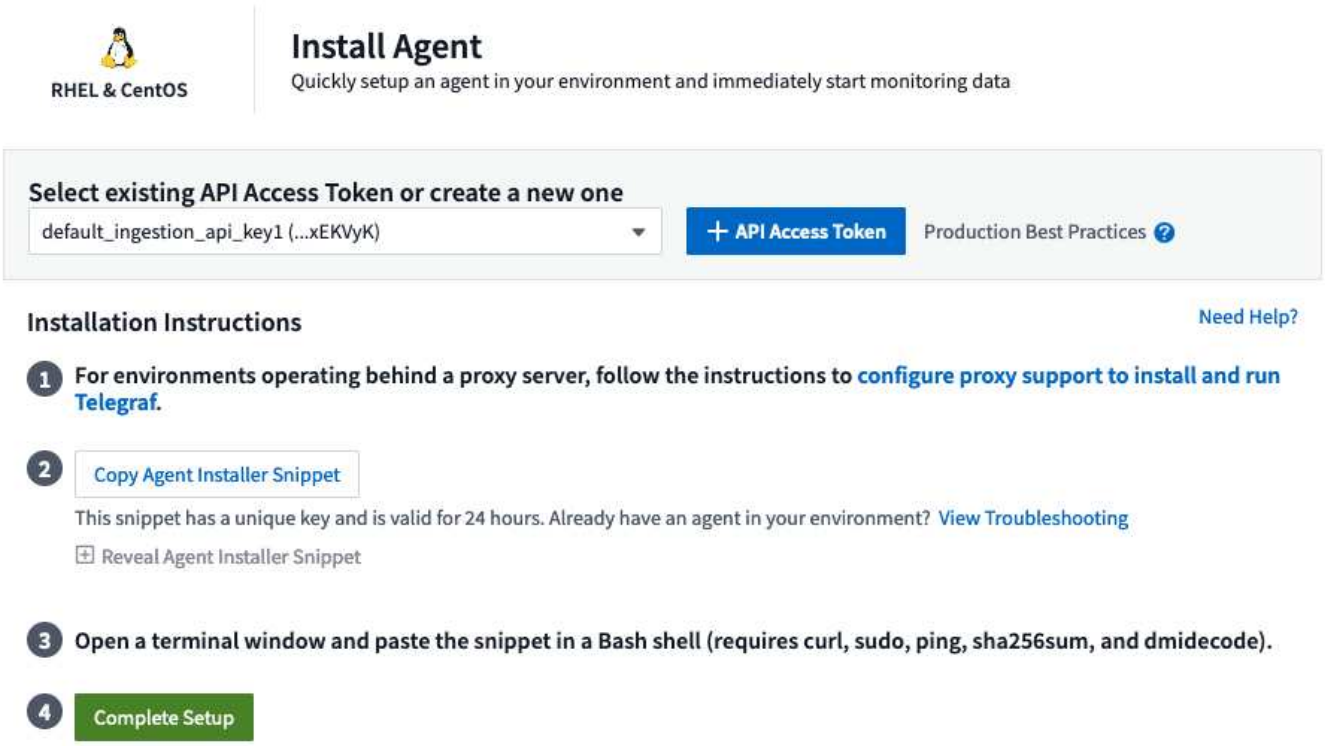
1. Set the *https_proxy* and/or *http_proxy* environment variable(s) for the current user:

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

2. Create */etc/default/telegraf*, and insert definitions for the *https_proxy* and/or *http_proxy* variable(s):

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

Installing the agent



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

Pre-requisites:

- The following commands must be available: curl, sudo, ping, sha256sum, openssl, and dmidecode
- If you are behind a proxy, you must follow the instructions in the **Configuring Proxy Support for Ubuntu/Debian** section.

Configuring Proxy Support for Ubuntu/Debian

If your environment uses a proxy, read this section before you install.

The steps below outline the actions needed to set the *http_proxy/https_proxy* environment variables. For some proxy environments, users may also need to set the *no_proxy environment* variable.

For systems residing behind a proxy, perform the following steps **PRIOR** to installing the Telegraf agent:

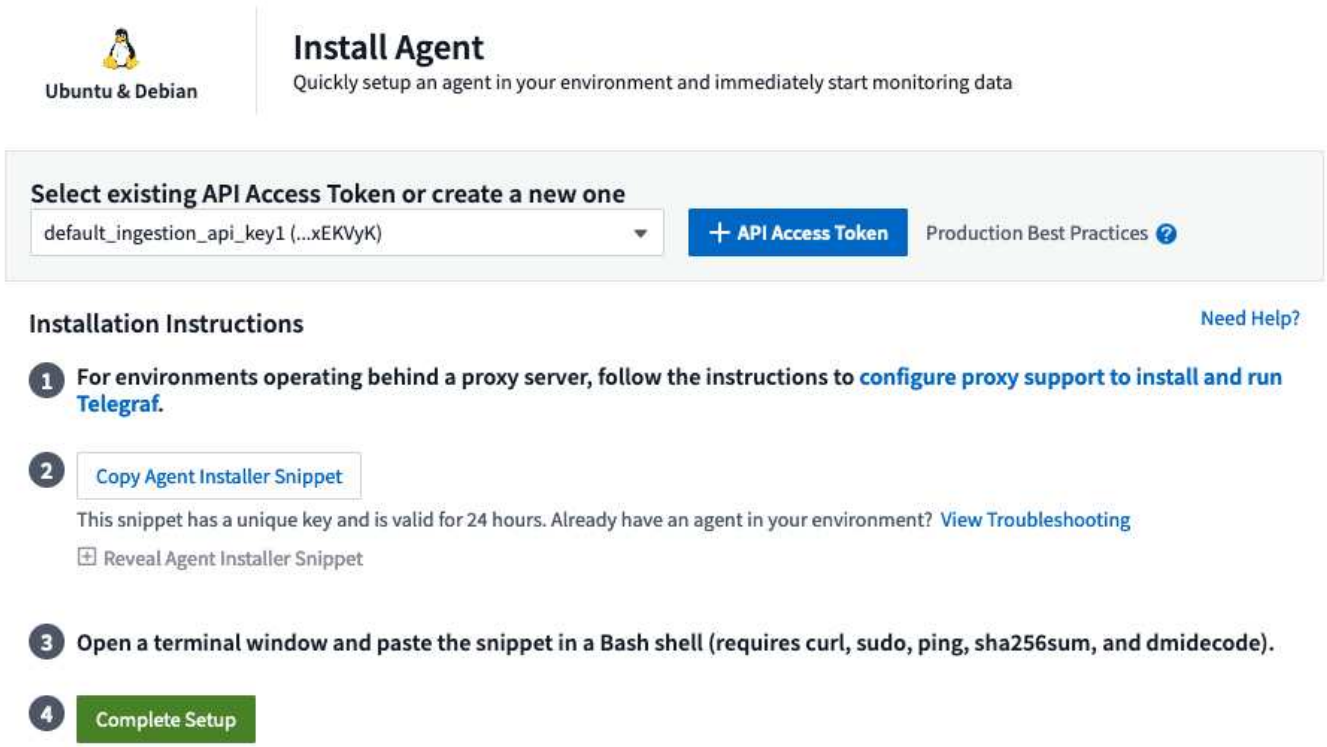
1. Set the *https_proxy* and/or *http_proxy* environment variable(s) for the current user:

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

2. Create /etc/default/telegraf, and insert definitions for the *https_proxy* and/or *http_proxy* variable(s):

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

Installing the agent



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.

Verifying Checksums

The Cloud Insights agent installer performs integrity checks, but some users may want to perform their own verifications before installing or applying downloaded artifacts. This can be done by downloading the installer and generating a checksum for the downloaded package, then comparing the checksum to the value shown in the install instructions.

Download the installer package without installing

To perform a download-only operation (as opposed to the default download-and-install), users can edit the agent installation command obtained from the UI and remove the trailing “install” option.

Follow these steps:

1. Copy the Agent Installer snippet as directed.
2. Instead of pasting the snippet into a command window, paste it into a text editor.
3. Remove the trailing “--install” (Linux) or “-install” (Windows) from the command.
4. Copy the entire command from the text editor.
5. Now paste it into your command window (in a working directory) and run it.

Non-Windows (these examples are for Kubernetes; actual script names may vary):

- Download and install (default):

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

- Download-only:

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

Windows:

- Download and install (default):

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

- Download-only:

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

The download-only command will download all required artifacts from Cloud Insights to the working directory. The artifacts include, but may not be limited to:

- an installation script
- an environment file
- YAML files
- a checksum file (ending in sha256.signed or sha256.ps1)

The installation script, environment file, and YAML files can be verified using visual inspection.

Generate checksum value

To generate the checksum value, perform the following command for your appropriate platform:

- RHEL/Ubuntu:

```
sha256sum <package_name>
```

- Windows:

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

Verify checksum

Extract the expected checksum from the checksum file

- Non-Windows:

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

- Windows:

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

Install the downloaded package

Once all of the artifacts have been satisfactorily verified, the agent installation can be initiated by running:

Non-Windows:

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

Windows:

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

Troubleshooting

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

Problem:	Try this:
After configuring a new plugin and restarting Telegraf, Telegraf fails to start up. The logs indicate that an error resembling the following: "[telegraf] Error running agent: Error loading config file /etc/telegraf/telegraf.d/cloudinsights-default.conf: plugin outputs.http: line <linenumber>: configuration specified the fields ["use_system_proxy"], but they weren't used"	The installed Telegraf version is outdated. Follow the steps on this page to **Upgrade the Agent** for your appropriate platform.
I ran the installer script on an old installation and now the agent isn't sending data	Uninstall the telegraf agent and then re-run the installation script. Follow the **Upgrade the Agent** steps on this page for your appropriate platform.
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**.

Problem:	Try this:
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 **Observability > Collectors**

   The system displays the available Data Collectors arranged by vendor.

2. Click **+ Collector** 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.

<<<<<<< HEAD
. Click **Advanced Configuration** to add additional configuration fields. (Not all data collectors require advanced configuration.)
. Click **Test Configuration** to verify that the data collector is properly configured.
. Click **Add Collector** to save the configuration and add the data collector to your Cloud Insights tenant.

It may take up to two poll periods before data from the service is displayed in dashboards or available for querying.
>>>>>>> b8087143154c7dd9f5d1d3f33ee1bbdf97a7c9d1

- 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
:toc: macro
:hardbreaks:
:toclevels: 2
:icons: font
:linkattrs:
:relative_path: ./
:imagesdir: /tmp/d20240625-801275-1wyx0zx/source/./../media/

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
:toc: macro
:hardbreaks:
:toclevels: 1
:icons: font
:linkattrs:
:relative_path: ./
:imagesdir: /tmp/d20240625-801275-1wyx0zx/source/./../media/

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 **Observability > 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 **Observability > 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 **Observability > 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 **Observability > 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 **Observability > 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
:toc: macro
:hardbreaks:
:toclevels: 1
:icons: font
:linkattrs:
:relative_path: ./
:imagesdir: /tmp/d20240625-801275-1wyx0zx/source/./media/

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.