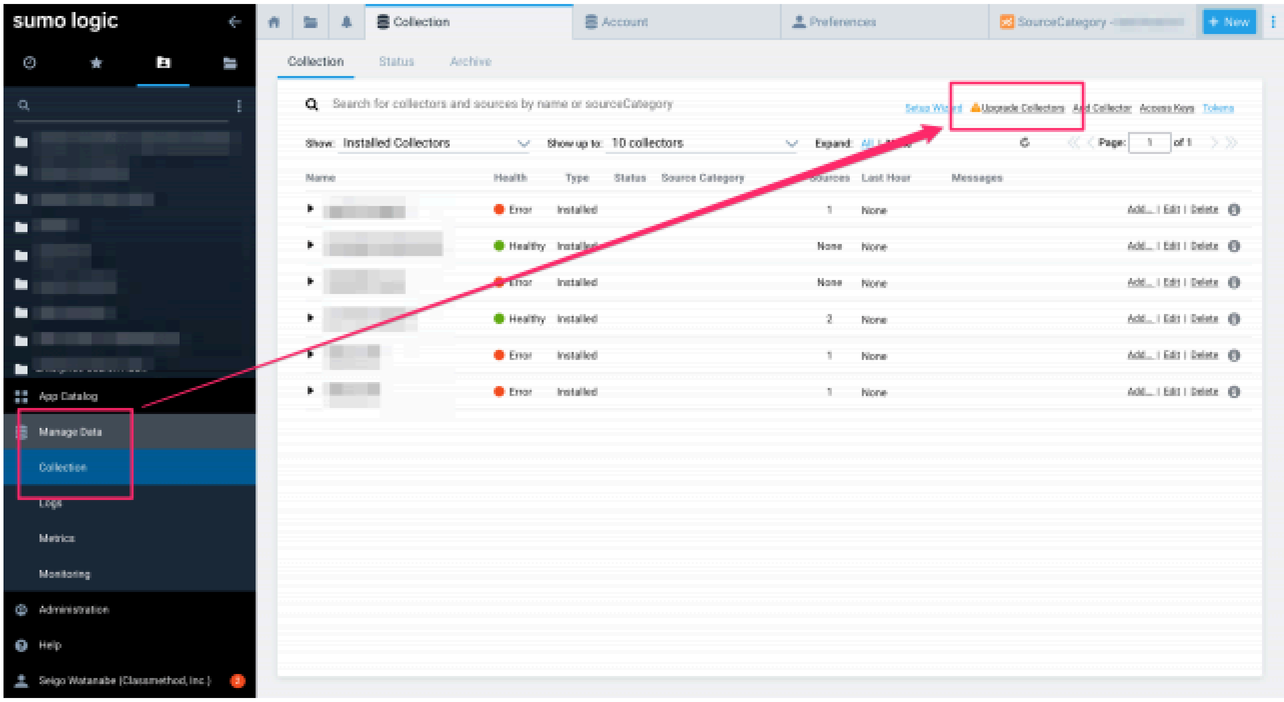
Remotely upgrade an installed collector #sumologic

dev.classmethod.jp/articles/202112-sumologic-installed-collector-remote-upgrade

渡辺聖剛

December 12, 2021



Name	Health	Type	Status	Source Category	Sources	Last Hour	Messages	
[redacted]	Error	Installed			1	None		Add... | Edit | Delete
[redacted]	Healthy	Installed			None	None		Add... | Edit | Delete
[redacted]	Error	Installed			None	None		Add... | Edit | Delete
[redacted]	Healthy	Installed			2	None		Add... | Edit | Delete
[redacted]	Error	Installed			1	None		Add... | Edit | Delete
[redacted]	Error	Installed			1	None		Add... | Edit | Delete

*Additional information about the impact was added on December 14, 2021

You may have heard the news that a zero-day vulnerability has been discovered in log4j2, a widely used Java logging framework.

Our DevelopersIO blog also has several related articles.

- AWS WAF adds "Log4JRCE" managed rules to address Log4j vulnerabilities | DevelopersIO
- Verifying SpringBoot Applications for Log4j2 Vulnerability Issues | DevelopersIO

Sumo Logic's Installed Collector is also written in Java and uses log4j as its logging framework.
On December 11th local time, a version of the collector that addresses this vulnerability was released.

> December 11, 2021 (19.361-12)
> Log4j upgraded to 2.15.0 to fix the zero-day exploit affecting the popular Apache Log4j utility (CVE-2021-44228).

Installed Collectors can be remotely upgraded, so be sure to keep them up to date with the latest version.

Before we get started: Impact on Installed Collectors

Sumo Logic has not made any announcements online, but as of December 11th, they have sent emails to user accounts explaining the impact.
According to the emails, Collector version 19.227-15 (released October 2018) is no longer affected by this vulnerability. However, they recommend using the latest version of the Installed Collector to minimize risk.

By the way, the official Sumo Logic blog has an article on how to use Sumo Logic to search logs for traces of attacks exploiting this vulnerability.

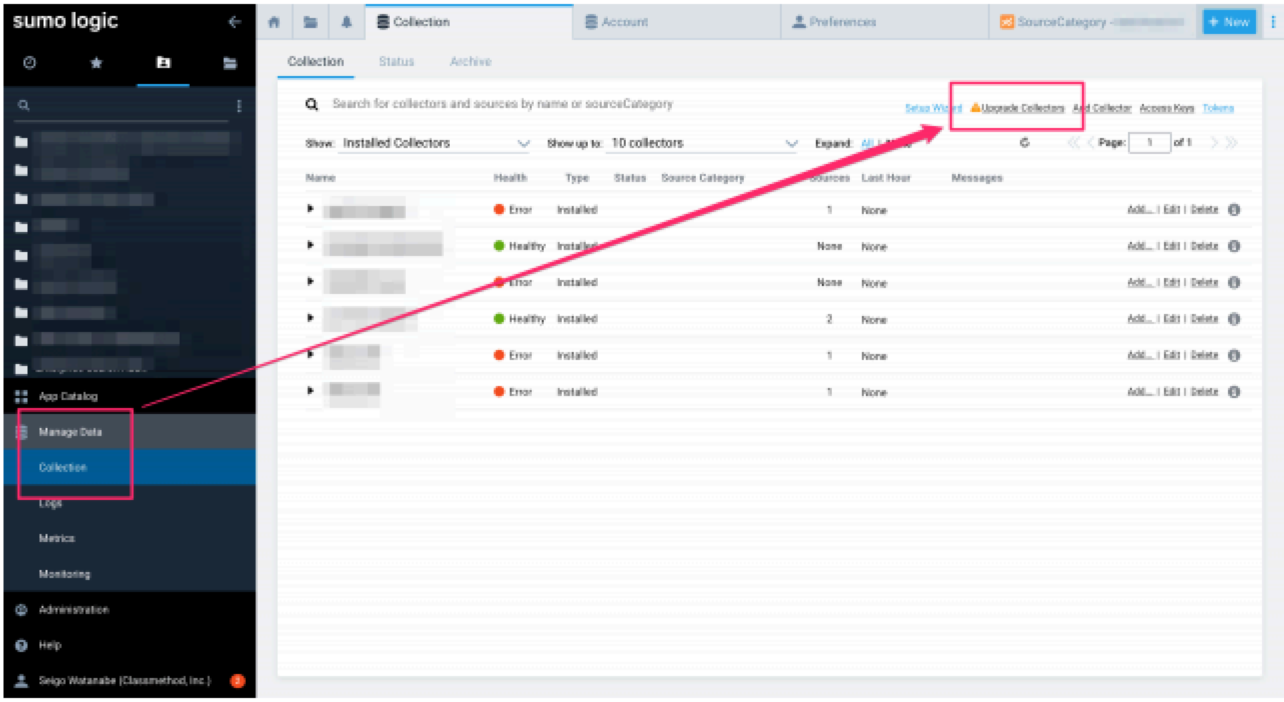
Give it a try

You can upgrade an Installed Collector in three ways:

- From the Sumo Logic web console (Japanese / English)
- Connect to a running server using SSH (Japanese / English)
- Use the Collector Management API (English only)

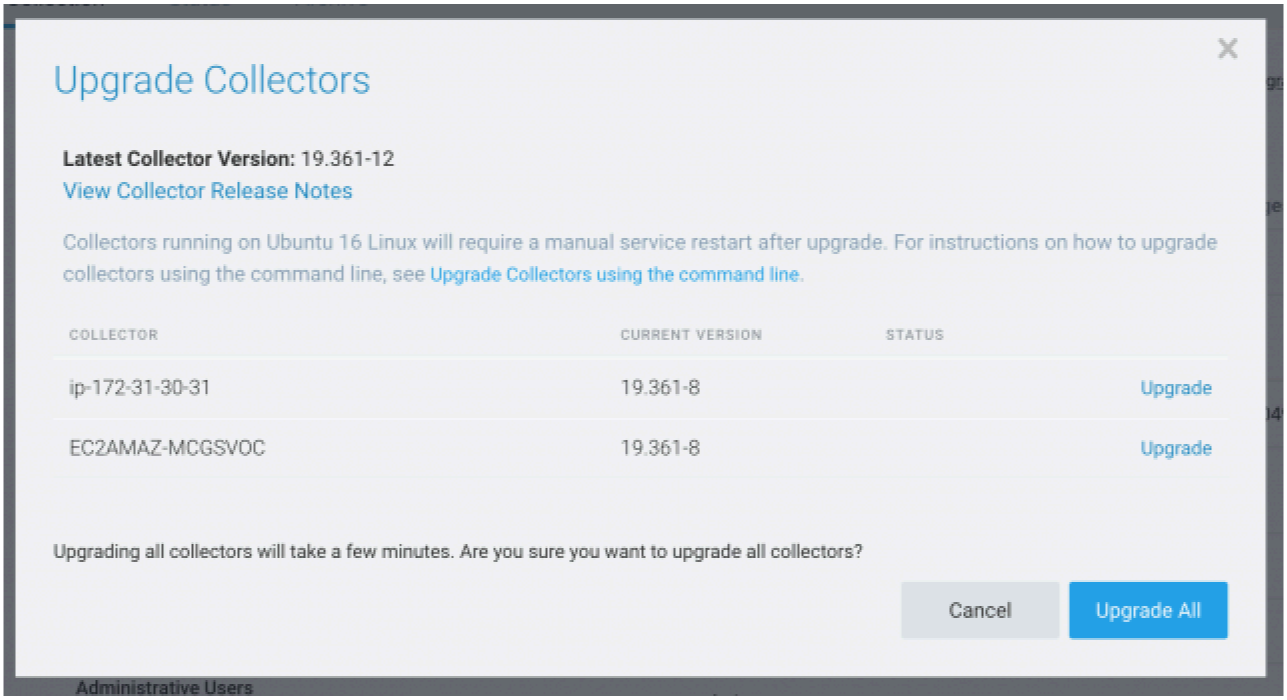
If you haven't already done so, please read the Sumo Logic best practices.
Here, we'll follow those best practices and implement them from the web console.

Log in to the Sumo Logic web console and click `Manage Data`--> . You will see a warning icon in front of "Upgrade Collection" in the top right corner of the tab.`CollectionCollection`



Name	Health	Type	Status	Source Category	Sources	Last Hour	Messages	
[redacted]	Error	Installed			1	None		Add... | Edit | Delete
[redacted]	Healthy	Installed			None	None		Add... | Edit | Delete
[redacted]	Error	Installed			None	None		Add... | Edit | Delete
[redacted]	Healthy	Installed			2	None		Add... | Edit | Delete
[redacted]	Error	Installed			1	None		Add... | Edit | Delete
[redacted]	Error	Installed			1	None		Add... | Edit | Delete

When I opened it, I saw that two Installed Collectors were listed as being eligible for upgrade.



Upgrade Collectors

Latest Collector Version: 19.361-12

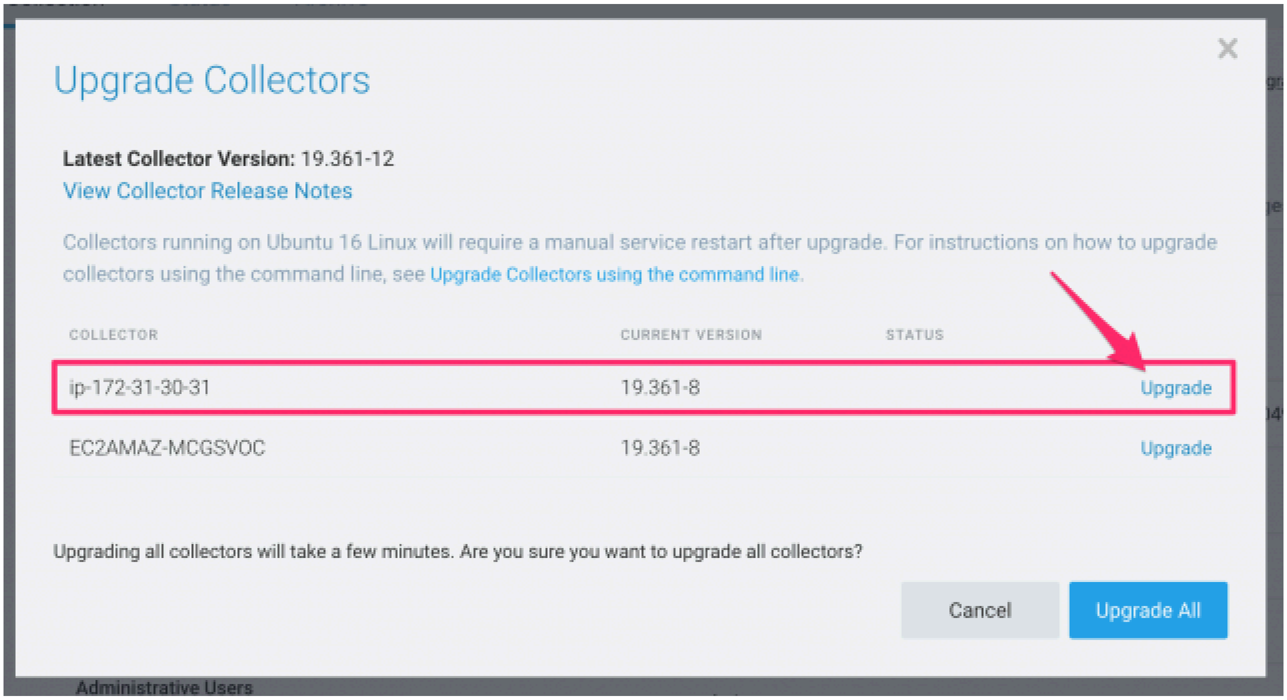
View Collector Release Notes

Collectors running on Ubuntu 16 Linux will require a manual service restart after upgrade. For instructions on how to upgrade collectors using the command line, see Upgrade Collectors using the command line.

COLLECTOR	CURRENT VERSION	STATUS	
ip-172-31-30-31	19.361-8		Upgrade
EC2AMAZ-MCGSVOC	19.361-8		Upgrade

Upgrading all collectors will take a few minutes. Are you sure you want to upgrade all collectors?

`ip-172-31-30-31`First, let's try upgrading the collector running on Amazon Linux 2. `Upgrade`Click on the right side to start the upgrade.



Upgrade Collectors

Latest Collector Version: 19.361-12

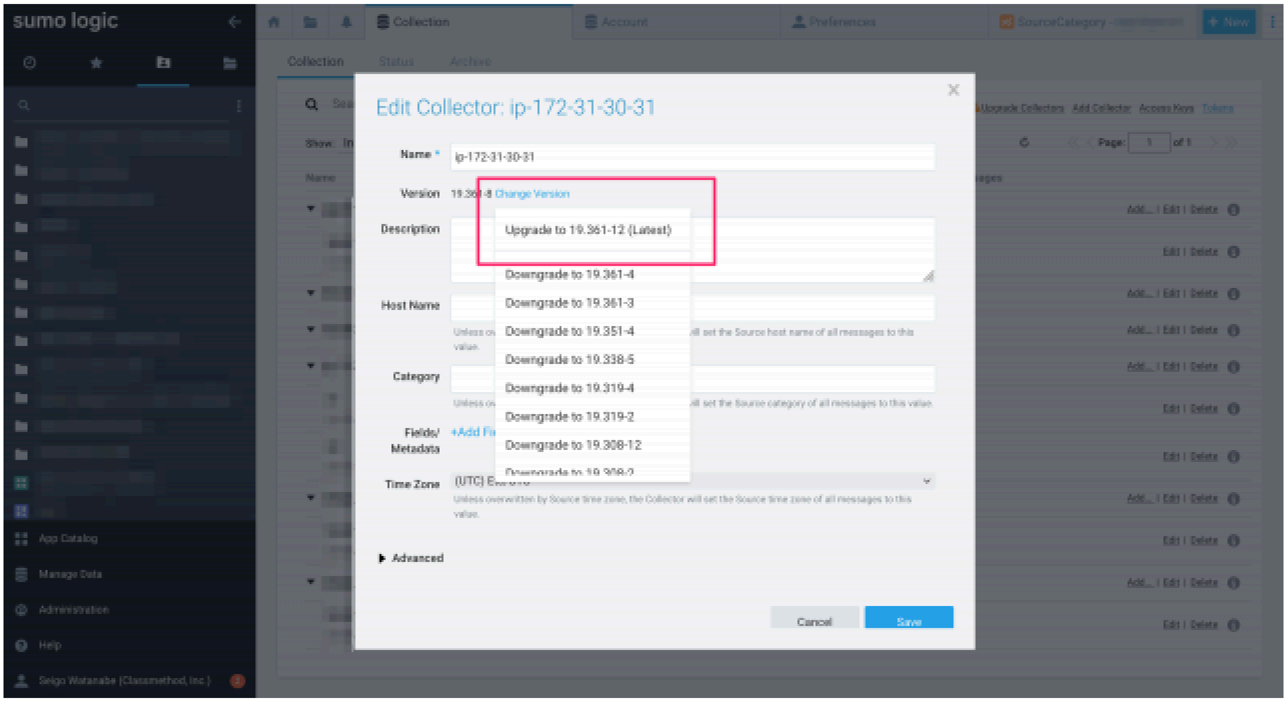
View Collector Release Notes

Collectors running on Ubuntu 16 Linux will require a manual service restart after upgrade. For instructions on how to upgrade collectors using the command line, see Upgrade Collectors using the command line.

COLLECTOR	CURRENT VERSION	STATUS	
ip-172-31-30-31	19.361-8		Upgrade
EC2AMAZ-MCGSVOC	19.361-8		Upgrade

Upgrading all collectors will take a few minutes. Are you sure you want to upgrade all collectors?

By the way, although it was not relevant this time, you can also upgrade by opening the details of the target collector (host) from the collector management screen.



Edit Collector: ip-172-31-30-31

Name * ip-172-31-30-31

Version 19.361-8 Change Version

- Upgrade to 19.361-12 (Latest)
- Downgrade to 19.361-4
- Downgrade to 19.361-3
- Downgrade to 19.351-4
- Downgrade to 19.338-5
- Downgrade to 19.319-4
- Downgrade to 19.319-2
- Downgrade to 19.308-12
- Downgrade to 19.308-2

Description

Host Name

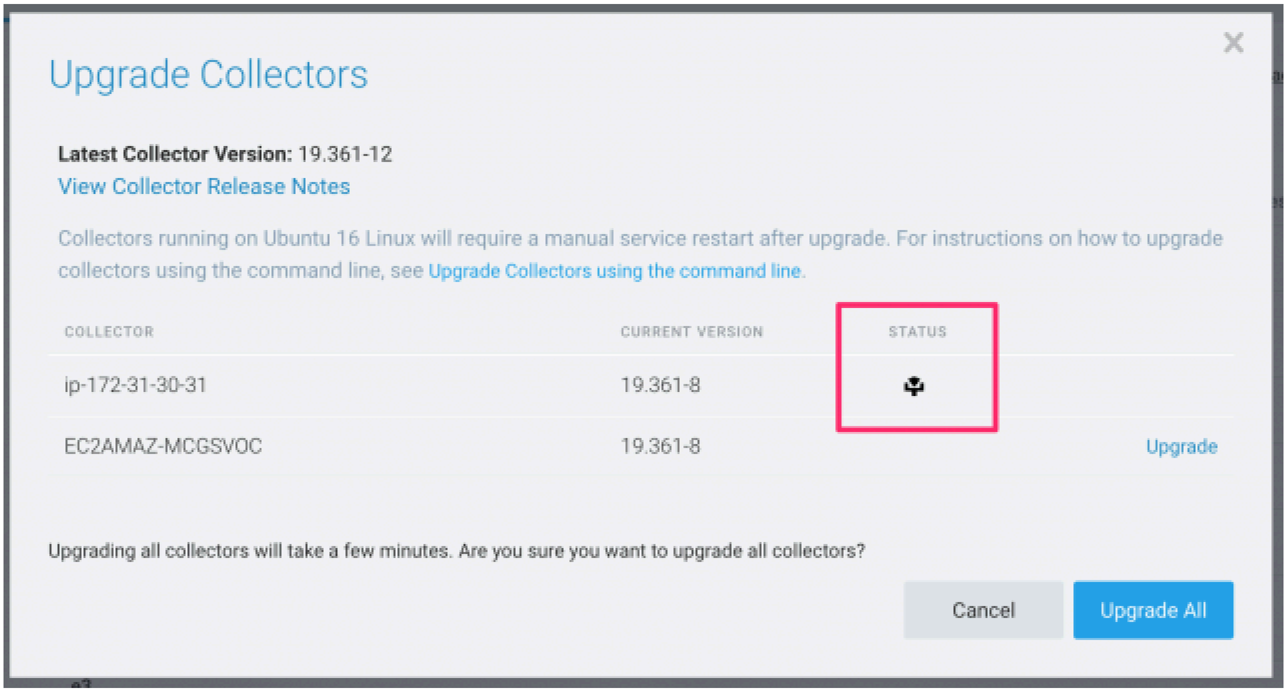
Category

Fields/ Metadata +Add Fi

Time Zone (UTC) Etc/UTC

Unless overwritten by Source time zone, the Collector will set the Source time zone of all messages to this value.

This time it took about 5 minutes to complete.



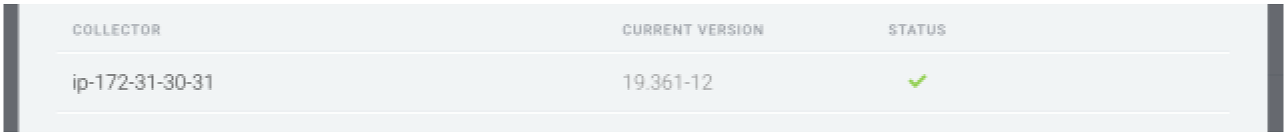
Upgrade Collectors

Latest Collector Version: 19.361-12
View Collector Release Notes

Collectors running on Ubuntu 16 Linux will require a manual service restart after upgrade. For instructions on how to upgrade collectors using the command line, see Upgrade Collectors using the command line.

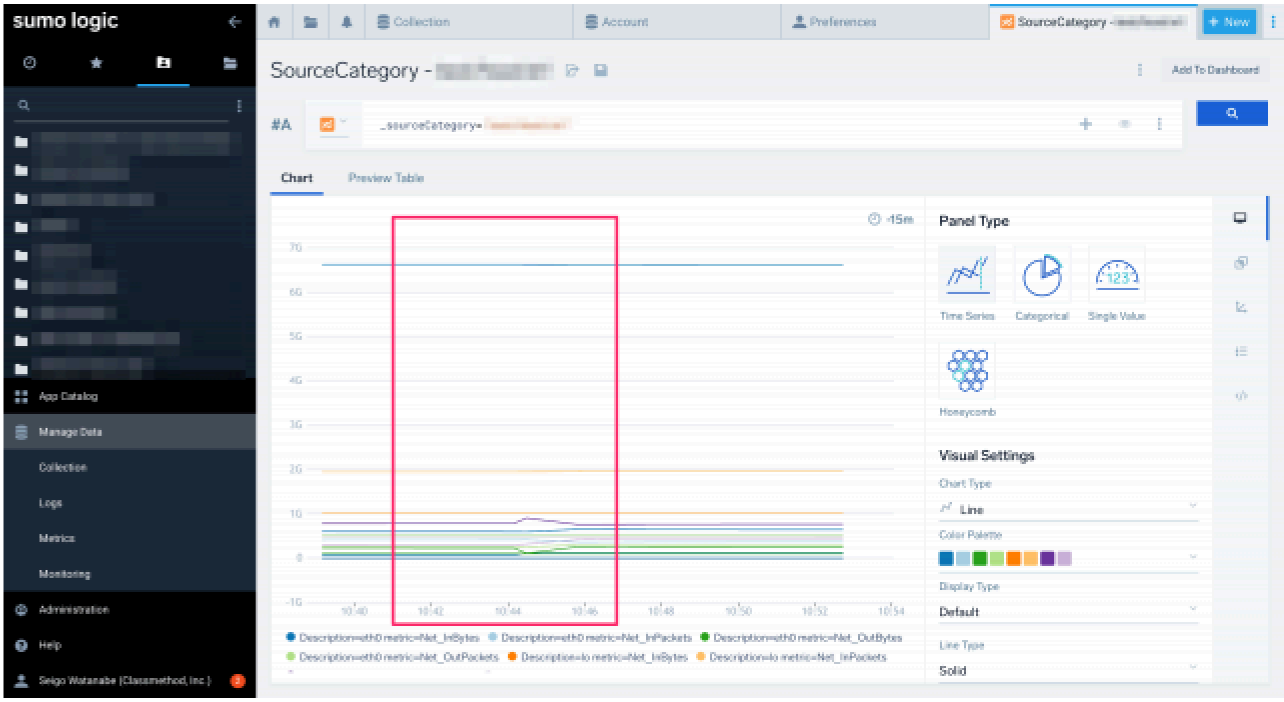
COLLECTOR	CURRENT VERSION	STATUS
ip-172-31-30-31	19.361-8	
EC2AMAZ-MCGSVOC	19.361-8	Upgrade

Upgrading all collectors will take a few minutes. Are you sure you want to upgrade all collectors?



COLLECTOR	CURRENT VERSION	STATUS
ip-172-31-30-31	19.361-12	✓

As the documentation states, it will not stop during the upgrade (it will only stop for the moment when the process is finally restarted).

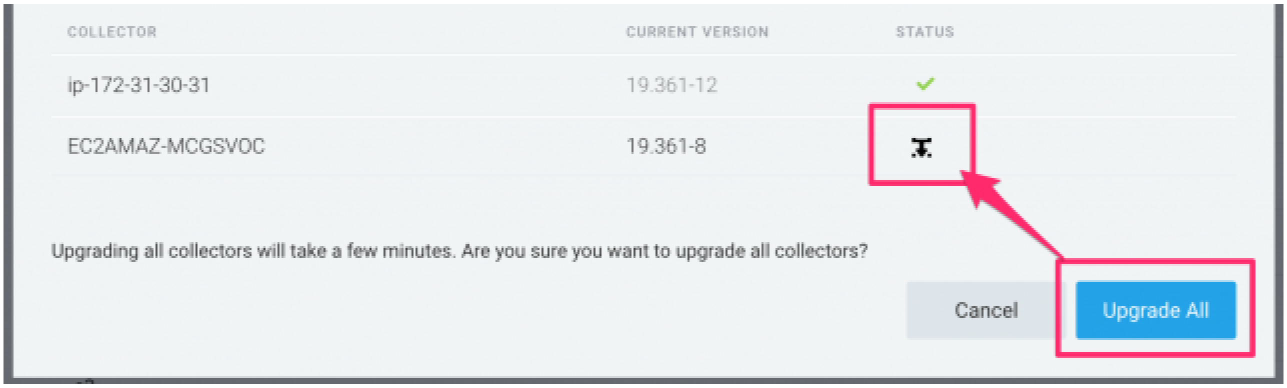


SourceCategory - [redacted]

#A _sourceCategory=[redacted]

Chart Type: Line
Display Type: Default
Line Type: Solid

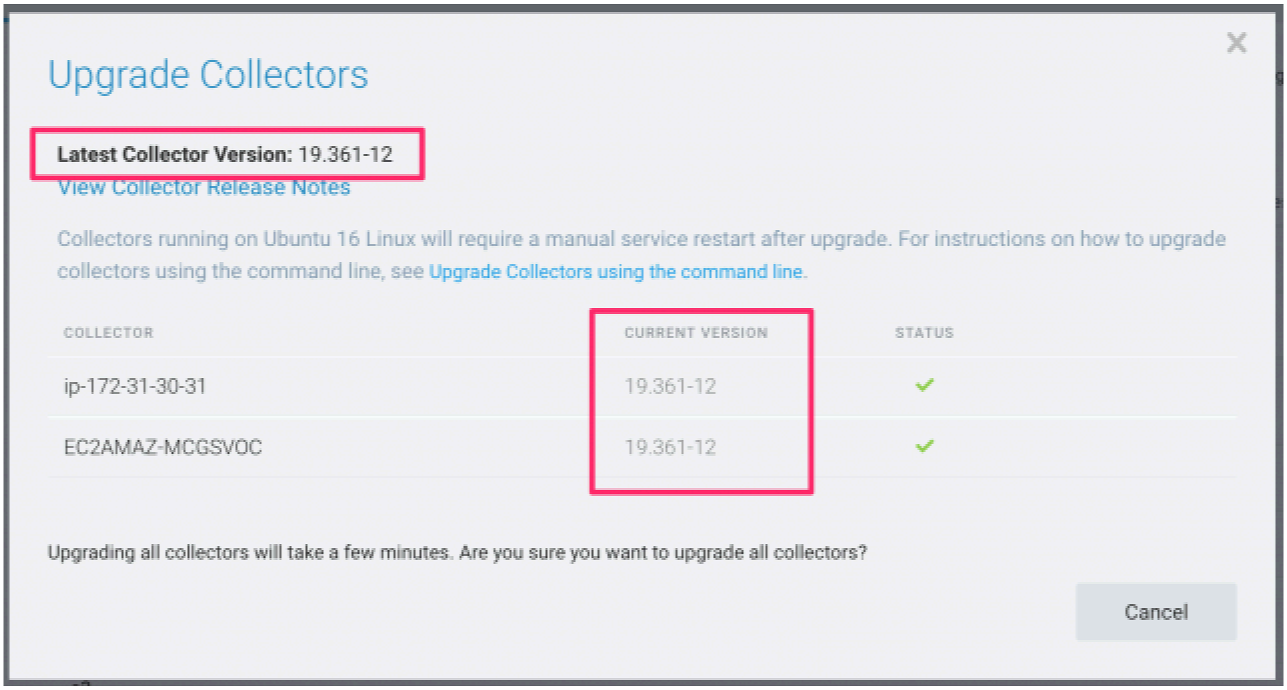
Next, `EC2AMAZ-MCGSVOC`I tried it on the Windows host. Since there was only one left, `Upgrade All`I tried the button.
The upgrade process started on this host as well (if there were multiple hosts left, it would start all at once).



COLLECTOR	CURRENT VERSION	STATUS
ip-172-31-30-31	19.361-12	✓
EC2AMAZ-MCGSVOC	19.361-8	⧗

Upgrading all collectors will take a few minutes. Are you sure you want to upgrade all collectors?

This was also completed in about 5 minutes!



Upgrade Collectors

Latest Collector Version: 19.361-12
View Collector Release Notes

Collectors running on Ubuntu 16 Linux will require a manual service restart after upgrade. For instructions on how to upgrade collectors using the command line, see Upgrade Collectors using the command line.

COLLECTOR	CURRENT VERSION	STATUS
ip-172-31-30-31	19.361-12	✓
EC2AMAZ-MCGSVOC	19.361-12	✓

Upgrading all collectors will take a few minutes. Are you sure you want to upgrade all collectors?

Precautions

As stated in the Upgrade Collection dialog, if the target host is running Ubuntu 16, please upgrade from the command line.

> Collectors running on Ubuntu 16 Linux will require a manual service restart after upgrade.

There may be cases where the update fails, but the old collector will continue to run even in that case.
This may be a timing issue, so please retry, or log in to the server in question and try upgrading from the command line .

The documentation lists the following common causes of failure:

- Insufficient available disk space
- A permissions error has blocked access to Sumo Logic (e.g. file access)
- A network error occurred during the upgrade

Collector Upgrade Best Practices

Sumo Logic's help documentation provides best practices for upgrading Collectors.

The key points are:

- Use the latest
- Upgrade using the Sumo Logic User Interface
- Test the new Collector in a staging environment

It also contains check items, so please use it as a reference for the upgrade process.