

Icinga 2

Overview

This page covers how to add and configure the Icinga 2 connector using GroundWork Cloud Hub. The connection requires a unique set of parameters (e.g., endpoint, credentials). You will need your GroundWork server and virtual environment connector parameters handy.

CONTENTS

RELATED RESOURCES

- [About GroundWork Hubs](#)
- icinga.com

WAS THIS PAGE HELPFUL?

- [Leave Feedback](#)

Prerequisites

Enable the API

The Icinga 2 system you run needs to have the API feature enabled. By default, it is not in the current version of Icinga 2 (2.5.4). It is installed, however, and it is a relatively simple matter to set it up. Please see the relevant documentation at <http://docs.icinga.org>.

1. Assuming you have Icinga 2 installed properly, and the API is not enabled, the commands will guide you through the basics:

```
# icinga2 api setup
# service icinga2 restart
```

2. The data you will need to connect to the API will be in the file:

```
/etc/icinga2/conf.d/api-users.conf
```

3. It will look something like this:

```
object ApiUser "root" {
    password = "3393c21c662f1b42"
    // client_cn = ""
    permissions = [ "*" ]
}
```

4. This defines a user (root) and password for connecting to the API, and technically this is all you really need. You can test with a curl command, like this:

```
# curl -k -s -u root:3393c21c662f1b42 'https://{icinga2 server name here}:5665/v1/status'
```

5. That should return some XML to the command line with a lot of metrics embedded in it. Note, however, that the data is retrieved over HTTPS, so an SSL certificate has been generated.
6. If you want to simply trust this certificate, you can choose to do so in the connector. If you wish to import the certificate and not simply blindly trust it (which is a good idea), you will need to do a few more steps.

Copy and import the certificate

1. On the Icinga 2 server, suitable responsive to a curl command with username and password over HTTPS as illustrated above, find the **ca.crt** file and securely copy it to the GroundWork server. It is located here by default on the Icinga 2 server:

```
/etc/icinga2/pki/ca.crt
```

2. On the GroundWork server, create a new, empty directory in a secure location on the disk, accessible to user nagios. For example, as **root**, type:

```
# mkdir /usr/local/groundwork/config/cloudhub/icinga2/
# chown nagios.nagios /usr/local/groundwork/config/cloudhub/icinga2/
# cd /usr/local/groundwork/config/cloudhub/icinga2/
```

3. Copy the **ca.crt** file to that directory, and change directory to that location. Then type issue the following commands as **root**:

```
# source /usr/local/groundwork/scripts/setenv.sh
# keytool -genkeypair -alias private -keyalg RSA -keysize 2048 -dname "CN=Unknown, OU=Unknown,
O=Unknown, L=Unknown, ST=Unknown, C=Unknown" -keypass {password one} -keystore
icinga2-keystore.jks -storepass {password two}
```

4. Replace the password strings in the above command with passwords you maintain for this. Make sure they are unique, and that you record them securely.

```
# keytool -importcert -trustcacerts -noprompt -alias root -file ca.crt -keystore
icinga2-keystore.jks -storepass {password two}
```

5. Then test that the certificate is in place with:

```
# keytool -list -keystore icinga2-keystore.jks -storepass {password two}
```

1.0 Adding a New Connection

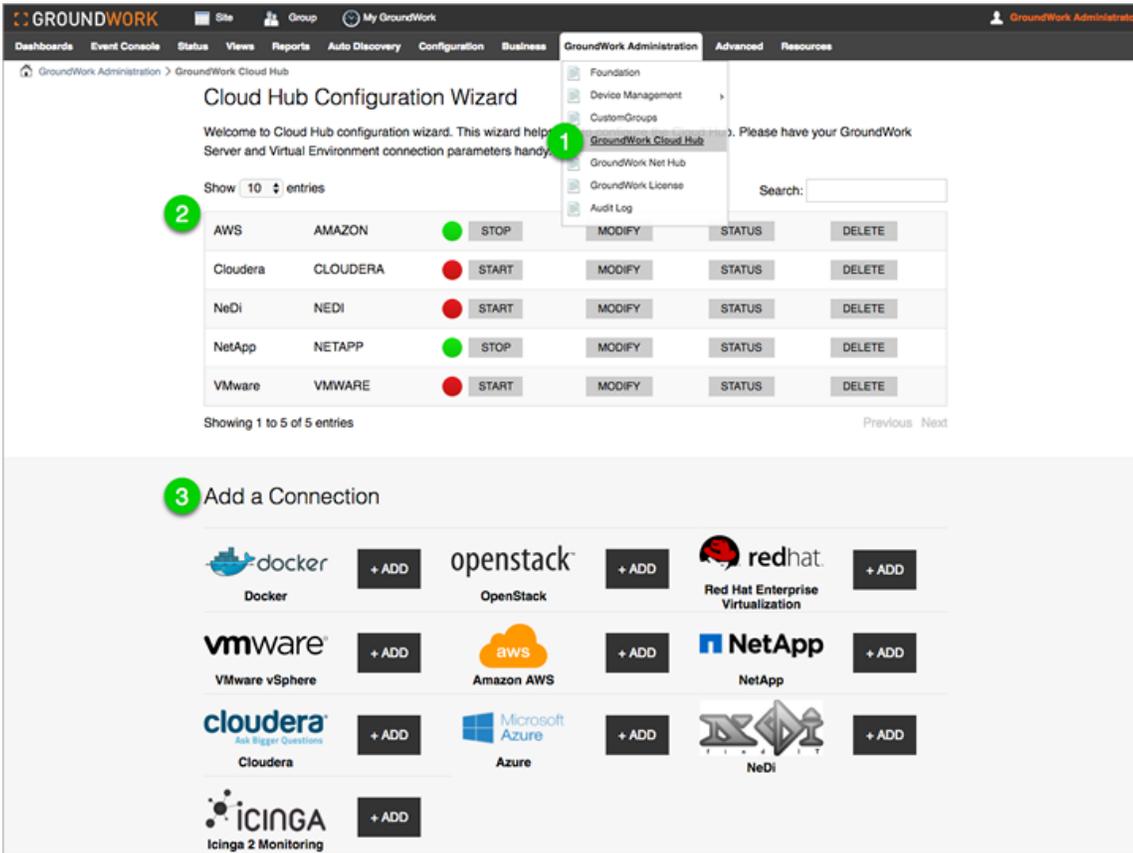
To access Cloud Hub, log in to GroundWork Monitor as an *Administrator* and select **(1) GroundWork Administration > GroundWork Cloud Hub**.

The initial Cloud Hub screen is used to **(2) Add new**, or **Start, Stop, Modify**, obtain **Status** for, or **Delete** configured connectors.

The **Start** option enables a configured connector to begin the discovery and data collection process. If you decide you do not want to monitor a particular region, simply select **Stop** for the corresponding connector, the connectors configuration will be maintained for a subsequent start. **Modify** opens the Configuration page with a link to the Metrics screen. **Status** provides connection status information including error details. If a configured connector fails to connect, a connector-specific service will be updated to a Warning state, or Critical if you run out of retries (hosts will still become Unreachable and services Unknown if retries are exhausted). To stop and completely **Delete** a connection, see [How to delete hosts](#). To keep a Cloud Hub connector configuration and temporarily suspend its monitoring, see [Black List](#).

To **(3) add a new connection click +Add** corresponding to the *Icinga 2* connector icon. You will need to create a new connection in this way for each region to be monitored.

Figure: Adding a connection



Next, in the configuration page (shown below) you will need to enter both the GroundWork server and remote server parameters. The data the GroundWork server receives comes from the remote virtualization server. The information is pulled from the API on a periodic basis based on the check interval that is set.

The (1) **Groundwork Server** is where Cloud Hub will store Icinga 2 metrics. Often, this is the same server as where Cloud Hub is running. However, Cloud Hub can also be run in a distributed environment, on its own node in a GroundWork cluster. Here we enter the GroundWork server parameters, each described in the first table below.

Next enter values for the remote (2) **Icinga 2 Server**, shown below and described in the second table.

Validate both server configurations by selecting the (3) **Test** button which will check if the connections are accessible with the given credentials. A dialog will be displayed with either a success message or, if the server cannot be contacted, an error message will be displayed with information describing why the connection failed.

And after the remote server parameters have been entered and verified, click (4) **Save** to save and write the entries to an XML file in the GroundWork server `/usr/local/groundwork/config/cloudhub` directory. The Cloud Hub connector is assigned an agent ID and that in turn becomes a record locator in Foundation when you begin monitoring.

Figure: Icinga 2 connector

Table: GroundWork server values

GroundWork Server Version	Indicates the minimum GroundWork Monitor version needed. In other words, a version below the indicated value is incompatible.
Display Name	This is the configuration's name displayed in the list of Cloud Hub connectors on the Cloud Hub home page.
GroundWork Server Name	The host name or IP address where a Groundwork server is running. A port number should not be entered here. If Groundwork is running on the same server, you can enter <i>localhost</i> .
Is SSL enabled on GroundWork Server?	Check the SSL checkbox if your GroundWork server is provisioned with a secure HTTPS transport.
GroundWork Web Services Username	The provisioned Username granted API access on the GroundWork server.  For all systems, make sure the Web Services Username and Password match with the entries in the <i>ws_client.properties</i> file.
GroundWork Web Services Password	The corresponding API Token (password) for the given Username on the GroundWork server, see GroundWork Administration > GroundWork License > Webservices API Account Info Token (encrypted).  For all systems, make sure the Web Services Username and Password match with the entries in the <i>ws_client.properties</i> file.
Merge hosts on GroundWork Server?	If checked, this option combines all metrics of same named hosts under one host. For example, if there is a Nagios configured host named <i>demo1</i> and a Cloud Hub discovered host named <i>demo1</i> , the services for both configured and discovered hosts will be combined under the hostname <i>demo1</i> (case-sensitive).

Table: Icinga 2 server values

Icinga 2 Server	This is the URL for the Icinga 2 virtualization server (e.g., <i>icinga2host.yourdomain.com</i>).
Icinga 2 API Port	This is the API port, 5665 is the default.

Icinga 2 API Username and Password	This is your username for the API on the Icinga 2 server which is stored in this file <i>/etc/icinga2/conf.d/api-users.conf</i> .
Icinga 2 API Username and Password	This is your password for the API on the Icinga 2 server which is stored in this file <i>/etc/icinga2/conf.d/api-users.conf</i> .
Trust SSL Certificate on Icinga 2 Server?	Check this box if the Icinga 2 server is configured for secure HTTPS.
Icinga 2 Server SSL CA Certificate	If SSL, this is the <i>ca.crt</i> location.
Icinga 2 Server SSL CA Certificate Keystore	If SSL, this is the <i>icinga2-keystore.jks</i> location.
Icinga 2 Server SSL CA Certificate Keystore Password	If SSL, this is the keystore password.
Graph Icinga 2 Service Metrics?	Select to include Icinga 2 service metrics.
Sync Interval (in mins)	This is the polling interval for collecting monitoring data from the virtual instance and sending it to the GroundWork server. The value is in minutes.
Connection Retries (-1 infinite)	This entry is the number of retries for the connection and sets a limit on how many attempts are made after a failure. If you set this to -1, the retrying goes on forever. The number set indicates how many connections are attempted before the connection is left inactive (until you restart it).

2.0 Determining Metrics To Be Monitored

The metrics are configured within Icinga 2 and not within the GroundWork Monitoring Cloud Hub interface.