Cloud Agent

Linux / Mac Agent Deployment

Thank you for your interest in Qualys Cloud Agent! This document gives you tips and best practices for setting up your Linux and Mac Agents. We'll tell you about Credentials, Proxy Configuration, how to use our Agent Configuration Tool, and Best Practices.

A few things to consider…

What Linux versions are supported?

- Linux (.rpm) - Red Hat Linux 5.0 +, CentOS 5.11+, Fedora, openSUSE 11, 12, SUSE 11, 12, Amazon Linux 2015.09 and above
- Linux (.deb) - Debian 7, 8 and Ubuntu 12 , 14, 15

What MacOS versions are supported?

- MacOS X Yosemite (version 10.10)
- MacOS X El Capitan (version 10.11)

What are the steps?

Our Cloud Agent UI walks you through the steps to install agents on your hosts. Once the agent is installed you will need to provision it using our agent configuration tool. You might want to configure proxy settings for our agent to communicate with our cloud platform.

Run as user and user's default group

Typically the agent installation requires root level access on the system (for example in order to access the RPM database). After the Cloud Agent has been installed it can be configured to run in a specific user and group context. This ability limits the level of access of our Cloud Agent. Learn more

Need help with troubleshooting?

We recommend you inspect the agent's log file located here:
/var/log/qualys/qualys-cloud-agent.log

Credentials - what are my options?

Use an account with root privileges

This is recommended as it gives the Cloud Agent enough privileges to gather necessary information for the host system's evaluation.

Use a non-root account with Sudo root delegation

Either the non-root user needs to have sudo privileges directly or through a group membership. Be sure NOPASSWD option is configured.

Here is an example of agentuser entry in sudoers file (where “agentuser” is the user name for the account you’ll use to install the Linux Agent):
%agentuser ALL=(ALL)   NOPASSWD: ALL

Use non-root account with sufficient privileges (VM agent only)

The specific privileges needed are:
1) execute "rpm" for automatic update
2) commands required for data collection (see Sudo command list at the Community)

From the Community
Sudo Command List

Proxy Configuration

Linux Agent - Good to Know By default the Linux Agent will operate in non-proxy mode. The agent can be configured to use an HTTPS proxy for internet access in one of the following ways:
1) /etc/sysconfig/qualys-cloud-agent – applicable for Cloud Agent on Linux (.rpm)
2) /etc/default/qualys-cloud-agent – applicable for Cloud Agent on Linux (.deb)
3) /etc/environment – applicable for Cloud Agent on Linux (.deb) and (.rpm)
(*Tip* This is a better option if the systemwide proxy will be used by the agent)

Mac Agent - Good to Know The MacOS agent will consult the system settings for HTTPS proxy specification. If HTTPS proxy is not specified the agent will operate without a proxy. The proxy is set for system-wide proxy through System_Preference/Network. Only proxies set for the following options are honored: Web Proxy (HTTP), Secure Web Proxy (HTTPS)Web Proxy (HTTP)

Tell me the steps

1) If a proxy configuration file doesn’t exist create it.
Linux (.rpm): /etc/sysconfig/qualys-cloud-agent
Linux (.deb): /etc/default/qualys-cloud-agent
MacOS: /etc/qualys/cloud-agent/proxy

2) Add one of the following lines to the file:

```
https_proxy=https://[<username>:<password>@]<host>[:<port>]
```

or:

```
qualys_https_proxy=https://[<username>:<password>@]<host>[:<port>]
```

where <username> and <password> are specified if the https proxy uses authentication. If special characters are embedded in the username or password (e.g. @, :, $) they need to be url-encoded. where <host> is the proxy server's IPv4 address or FQDN. where <port> is the proxy's port number.

If the proxy is specified with the https_proxy environment variable, it will be used for all commands performed by the Cloud Agent. If the proxy is specified with the qualys_https_proxy environment variable, it will only be used by the Cloud Agent to communicate with our cloud platform.

3) Change the permissions using these commands:

Linux (.rpm):

```
chown root /etc/sysconfig/qualys-cloud-agent
chmod 644 /etc/sysconfig/qualys-cloud-agent
```

Linux (.deb):

```
chown root /etc/default/qualys-cloud-agent
chmod 644 /etc/default/qualys-cloud-agent
```

MacOS:

```
chown root /etc/qualys/cloud-agent/proxy
chmod 644 /etc/qualys/cloud-agent/proxy
```

4) Linux Agent only: Restart qualys-cloud-agent service using the following command:

```
service qualys-cloud-agent restart
```

Agent Configuration Tool

Our easy to use tool gives you many options for configuring the agent. You'll find this tool at /usr/local/qualys/cloud-agent/qualys-cloud-agent.sh. This is available with Linux Agent 1.3 and Mac Agent (any version).

Using this tool you have the option to:
- Provision agents
- Configure logging - set a custom log level and log file path
- Enable sudo to run all data collection commands
- Configure the daemon to run as a specific user and/or group

The Agent will automatically pick up changes made through the configuration tool so there is no need to restart the agent or reboot the agent host.

Configuration options

ActivationId	A valid activation key ID (UUID). This value is obtained from the Cloud Agent UI (go to Activation Keys, select a key then View Key Info). This parameter is required to provision an agent.
CustomerId	A valid customer ID (UUID). This value is obtained from the Cloud Agent UI (go to Activation Keys, select a key then Install Agent). This parameter is required to provision an agent.
LogLevel	A log level (0-5). A higher value corresponds to more verbosity. Default is to report only errors (0).
LogFilePath	A full path to the log file. By default the path is /var/log/qualys/
UseSudo	Set to 1 to run all data collection commands using the sudo escalation method. By default sudo is not used (0).
SudoCommand	A command for privilege escalation such as SudoCommand pbrun. If the command has spaces it must be double quoted.

User	A valid username if you want the daemon to run as a certain user. The daemon will start as root but will drop to the specified user, and continue running as the specified user.
Group	A valid group name if you want the daemon to run as a certain group. The daemon will switch to the specified group (if any).
HostIdSearchDir	(Available using Linux Agent 1.3.3 and later) The directory where the host ID file is located. This file contains a host ID tag assigned to the system by Qualys. By default the directory is /etc/ and the location of the host ID file is /etc/qualys/hostid Using Agentless Tracking with your VM/PC license? The location of the host ID file should match the location in your Unix authentication record. Learn more
LogDestType	(Available using Linux Agent 1.3.3 and later) The destination of log lines generated by Linux Agent. Set to **file** or **syslog**. If set to **file** specify the location of the log file. By default the destination is a log file: /var/log/qualys/qualys-cloud-agent.log

Example 1 – provision agent

The following example shows how to provision Qualys Cloud Agent. Please note that this method of activation will assume that root user should be used by the agent.

```
$ /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh
ActivationId="022224c8-31c7-11e5-b4f7-0021ccba987e"
CustomerId="146556fa-31c7-11e5-87b6-0021ccba987e"
```

Example 2 – use non-root account

The following example shows how to configure Qualys Cloud Agent to use a non-root account for running data collection commands.

```
$ /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh
ActivationId="022224c8-31c7-11e5-b4f7-0021ccba987e"
CustomerId="146556fa-31c7-11e5-87b6-0021ccba987e" UseSudo=1 User=scanuser
Group=wheel
```

Keep in mind - A new group needs to exist when the configuration command runs. The expectation is that the non-root user will be added to the specified group to allow it to access binary and temporary files that comprise Qualys Cloud Agent. In order to perform unattended data collection the non-root user needs to have sudo privilege without a password.

Example 3 – raise logging level

It is also possible to instruct Qualys Cloud Agent to log events at a higher than normal logging level using the following command:

```
$ /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh LogLevel=4
```

Note we’ve omitted the ActivationID and CustomerID parameters to illustrate the configuration tool can be used to adjust the log level after provisioning.

Best Practices

How to Uninstall Agent from the command line

Linux RPM based systems -To uninstall use:
sudo rpm -e qualys-cloud-agent

Linux Debian based systems - To uninstall use:
sudo dpkg --purge qualys-cloud-agent

Mac OSX based systems - To uninstall use:
sudo /usr/local/qualys/cloud-agent/bin/qagent_uninstall.sh

Linux/Mac Agent and Agentless Tracking

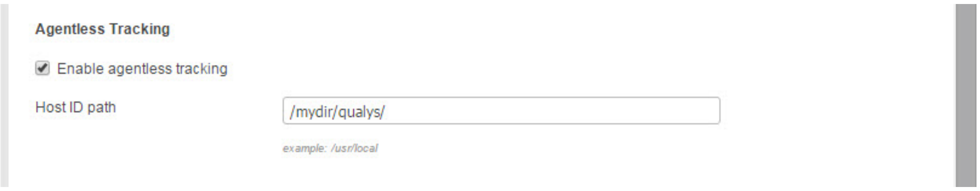
Say you’re already using Agentless Tracking on hosts and now you’re ready to install Cloud Agent on the same hosts. You’ll want to use the same host ID tag installed on the host. This will help you to avoid duplicate assets for the same host in your account.

You can configure the location of the host ID file installed on your Linux/Mac hosts. Once configured, the same file with the same host ID tag is accessed by our service when the host is evaluated using 1) Agentless Tracking AND 2) Cloud Agent. This is recommended best practice if you are interested in using Linux /Mac Agent and Agentless Tracking to evaluate the same host. (Supported using Linux Agent 1.3.3 and later, any version of Mac Agent.)

What are the steps?

1) Check your Unix authentication record
This is the record you’re using to access the system using Agentless Tracking. You’ll see the location of the host ID file configured for the authentication record.

Want help with Agentless Tracking? Go to Help > Online Help and search for **Agentless Tracking**.



Agentless Tracking

☑ Enable agentless tracking

Host ID path /mydir/qualys/

example: /usr/local

2) Install the Agent
Use the agent configuration tool (qualys-cloud-agent.sh) and the HostIdSearchDir option to install the Linux Agent and configure the location of the host ID file. Be sure this location matches the location defined in your authentication record. By default HostIdSearchDir is set to /etc/. To stay consistent with the Agentless Tracking location Qualys appends “/qualys/hostid” to the path provided.

Example - Install as root user and set host ID file to /mydir/qualys/hosted

```
$ /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh ActivationId="022224c8-
31c7-11e5-b4f7-0021ccba987e" CustomerId="146556fa-31c7-11e5-87b6-0021ccba987e"
HostIdSearchDir="/mydir/"
```

Did you already install Linux Agent 1.3.2 or earlier?

If yes and you’ve also been using Agentless Tracking on the same hosts, you’ll end up with duplicate agents for the same IP in your account. One of the duplicates will take over and continue communicating properly and the other will stop communicating to our cloud platform.

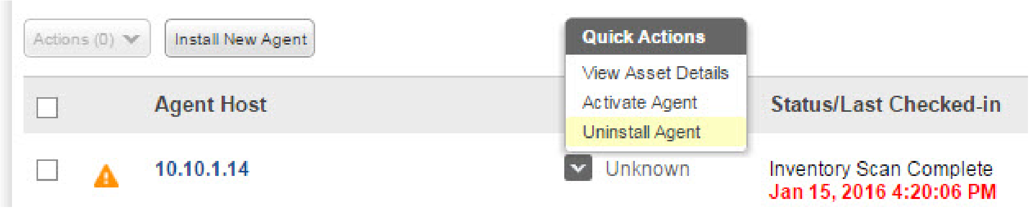
How to resolve this

1) Configure HostIdSearchDir for your agent
Configure the location of the host ID file using the agent configuration tool (qualys-cloud-agent.sh) and the HostIdSearchDir option.

Example - Install as root user and set host ID file to /mydir/qualys/hosted

```
$ /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh
HostIdSearchDir="/mydir/"
```

2) Uninstall duplicate agents not communicating
Use the Cloud Agent UI and select the Uninstall Agent option from the Quick Actions menu.



□		Agent Host		Status/Last Checked-in
□	⚠	10.10.1.14	Unknown	Inventory Scan Complete Jan 15, 2016 4:20:06 PM