



# Cloud Agent for Linux Installation Guide

Agent Version 1.5 - 1.6, 2.0.2

December 22, 2017

Copyright 2016-2017 by Qualys, Inc. All Rights Reserved.

Qualys, the Qualys logo and QualysGuard are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.  
919 E Hillsdale Blvd  
4th Floor  
Foster City, CA 94404  
1 (650) 801 6100

# CONTENTS

---

## **Preface**

### **Chapter 1 Get Started**

|   |   |
|---|---|
| Qualys Cloud Agent Introduction .....             | 5 |
| Cloud Agent Platform Availability for Linux ..... | 6 |
| A few things to consider.....                     | 7 |
| Cloud Agent requirements .....                    | 7 |
| What are the installation steps?.....             | 7 |
| Run as user and user's default group.....         | 7 |
| Need help with troubleshooting? .....             | 8 |
| Credentials - what are my options? .....          | 8 |

### **Chapter 2 Installation**

|   |    |
|---|----|
| Tips and best practices .....                     | 11 |
| How to download Agent image.....                  | 12 |
| Installation steps .....                          | 13 |
| What you'll need .....                            | 13 |
| Steps to install Agents.....                      | 13 |
| Steps to install Agents in AWS.....               | 13 |
| What happens next?.....                           | 14 |
| Troubleshooting.....                              | 14 |
| Proxy configuration.....                          | 16 |
| Anti-Virus and HIPS Exclusion / Whitelisting..... | 18 |

### **Chapter 3 Configuration Tool**

|  |    |
|--|----|
| Command line options .....             | 20 |
| Use cases .....                        | 22 |
| Example 1 – Provision Agent .....      | 22 |
| Example 2 – Use non-root account ..... | 22 |
| Example 3 – Raise logging level .....  | 22 |

### **Chapter 4 Best Practices**

|  |    |
|--|----|
| Uninstalling Cloud Agent .....           | 23 |
| Agentless Tracking and Cloud Agents..... | 24 |

### **Appendix A Certificate Support on RHEL 5.4**

### **Appendix B Certificate Support on SUSE Linux Enterprise 11**

---

# Preface

Welcome to Qualys Cloud Agent for Linux. This user guide describes how to install cloud agents on hosts in your network.

## About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions with over 9,300 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Fujitsu, HCL Comnet, HPE, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the [Cloud Security Alliance \(CSA\)](#). For more information, please visit [www.qualys.com](http://www.qualys.com).

## Contact Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at [www.qualys.com/support/](http://www.qualys.com/support/).

# CHAPTER 1

---

## Get Started

Thank you for your interest in Qualys Cloud Agent!

This document tells you all about installing Qualys Cloud Agent for Linux. We'll tell you about Requirements, Installation Steps, Proxy Configuration, Anti-Virus and HIPS Exclusion / Whitelisting, how to use our Agent Configuration Tool, Best Practices and more.

## Qualys Cloud Agent Introduction

Qualys Cloud Platform gives you everything you need to continuously secure all of your global IT assets. Now with Qualys Cloud Agent, there's a revolutionary new way to help secure your network by installing lightweight cloud agents in minutes, on any host anywhere - such as laptop, desktop or virtual machine.

**Watch the overview** for an introduction.

### Videos from the Qualys Community

[Cloud Agent Platform Introduction \(2m 10s\)](#)

[Getting Started Tutorial \(4m 58s\)](#)

**Get informed quickly** about Qualys Cloud Agent (CA)..

### Learn more from the Qualys Community

[CA Platform Announcement](#)

[Getting Started Guide](#)

# Cloud Agent Platform Availability for Linux

Current Release: 1.6.0.61, 2.0.2.79\*

End-of-Support versions: 1.3.3.23, 1.3.1.16

\*Current release for customers with FIM enabled

| Supported Platforms |                               |        |           | Supported Qualys Modules/Agent Versions |                             |                             |                      |                      |
|---------------------|-------------------------------|--------|-----------|---|-----------------------------|-----------------------------|----------------------|----------------------|
| Vendor              | Operating System              | Arch   | Installer | Inventory                               | VM                          | PC                          | FIM                  | IOC                  |
| Red Hat             | Red Hat Enterprise Linux 5.4x | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61, 2.0.2.79             | 1.5.0.61-1.6.0.61, 2.0.2.79 | 1.5.0.61-1.6.0.61, 2.0.2.79 | 2.0.2.79             | <i>not available</i> |
| Red Hat             | Red Hat Enterprise Linux 6, 7 | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61, 2.0.2.79             | 1.5.0.61-1.6.0.61, 2.0.2.79 | 1.5.0.61-1.6.0.61, 2.0.2.79 | 2.0.2.79             | <i>not available</i> |
| Red Hat             | CentOS 5.4+                   | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61, 2.0.2.79             | 1.5.0.61-1.6.0.61, 2.0.2.79 | 1.5.0.61-1.6.0.61, 2.0.2.79 | 2.0.2.79             | <i>not available</i> |
| Red Hat             | CentOS 6, 7                   | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61, 2.0.2.79             | 1.5.0.61-1.6.0.61, 2.0.2.79 | 1.5.0.61-1.6.0.61, 2.0.2.79 | 2.0.2.79             | <i>not available</i> |
| Red Hat             | Fedora 22, 23, 24             | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61                       | 1.5.0.61-1.6.0.61           | <i>not available</i>        | <i>not available</i> | <i>not available</i> |
| SUSE                | SUSE Linux Enterprise 11, 12  | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61                       | 1.5.0.61-1.6.0.61           | 1.5.0.61-1.6.0.61           | <i>not available</i> | <i>not available</i> |
| SUSE                | OpenSUSE 12                   | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61                       | 1.5.0.61-1.6.0.61           | <i>not available</i>        | <i>not available</i> | <i>not available</i> |
| SUSE                | OpenSUSE 13                   | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61                       | 1.5.0.61-1.6.0.61           | 1.5.0.61-1.6.0.61           | <i>not available</i> | <i>not available</i> |
| SUSE                | OpenSUSE Leap 42.1            | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61                       | 1.5.0.61-1.6.0.61           | <i>not available</i>        | <i>not available</i> | <i>not available</i> |
| Amazon              | Amazon Linux 2015.09          | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61                       | 1.5.0.61-1.6.0.61           | <i>not available</i>        | <i>not available</i> | <i>not available</i> |
| Amazon              | Amazon Linux 2016.09          | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61                       | 1.5.0.61-1.6.0.61           | 1.5.0.61-1.6.0.61           | <i>not available</i> | <i>not available</i> |
| Amazon              | Amazon Linux 2017.03          | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61                       | 1.5.0.61-1.6.0.61           | 1.5.0.61-1.6.0.61           | <i>not available</i> | <i>not available</i> |
| Oracle              | Oracle Enterprise Linux 5.11  | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61                       | 1.5.0.61-1.6.0.61, 2.0.2.79 | 1.5.0.61-1.6.0.61, 2.0.2.79 | 2.0.2.79             | <i>not available</i> |
| Oracle              | Oracle Enterprise Linux 6, 7  | x86_64 | (.rpm)    | 1.5.0.61-1.6.0.61, 2.0.2.79             | 1.5.0.61-1.6.0.61, 2.0.2.79 | 1.5.0.61-1.6.0.61, 2.0.2.79 | 2.0.2.79             | <i>not available</i> |

| Vendor | Supported Platforms |        |           | Supported Qualys Modules/Agent Versions |                                    |                                    |                          |                          |
|--------|---------------------|--------|-----------|---|------------------------------------|------------------------------------|--------------------------|--------------------------|
|        | Operating System    | Arch   | Installer | Inventory                               | VM                                 | PC                                 | FIM                      | IOC                      |
| Debian | Debian 7.x, 8.x     | x86_64 | (.deb)    | 1.5.0.61-<br>1.6.0.61                   | 1.5.0.61-<br>1.6.0.61              | 1.5.0.61-<br>1.6.0.61              | <i>not<br/>available</i> | <i>not<br/>available</i> |
| Ubuntu | Ubuntu 12.x         | x86_64 | (.deb)    | 1.5.0.61-<br>1.6.0.61,<br>2.0.2.79      | 1.5.0.61-<br>1.6.0.61,<br>2.0.2.79 | 1.5.0.61-<br>1.6.0.61,<br>2.0.2.79 | 2.0.2.79                 | <i>not<br/>available</i> |
| Ubuntu | Ubuntu 14.x         | x86_64 | (.deb)    | 1.5.0.61-<br>1.6.0.61,<br>2.0.2.79      | 1.5.0.61-<br>1.6.0.61,<br>2.0.2.79 | 1.5.0.61-<br>1.6.0.61,<br>2.0.2.79 | 2.0.2.79                 | <i>not<br/>available</i> |
| Ubuntu | Ubuntu 15.x         | x86_64 | (.deb)    | 1.5.0.61-<br>1.6.0.61                   | 1.5.0.61-<br>1.6.0.61              | <i>not<br/>available</i>           | <i>not<br/>available</i> | <i>not<br/>available</i> |
| Ubuntu | Ubuntu 16.04        | x86_64 | (.deb)    | 1.5.0.61-<br>1.6.0.61,<br>2.0.2.79      | 1.5.0.61-<br>1.6.0.61,<br>2.0.2.79 | <i>not<br/>available</i>           | 2.0.2.79                 | <i>not<br/>available</i> |

## A few things to consider...

### Cloud Agent requirements

- Your hosts must be able to reach your Qualys Cloud Platform (or the Qualys Private Cloud Platform) over HTTPS port 443. Log into the Qualys Cloud Platform and go to Help > About to see the URL your hosts need to access.
- To install Cloud Agent for Linux, you must have root privileges, non-root with Sudo root delegation, or non-root with sufficient privileges (VM license only). Proxy configuration is supported. [Learn more](#)

### What are the installation 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 using our configuration tool. This ability limits the level of access of the 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`

You'll also find helpful information in Qualys online help.

### Qualys Help

[Troubleshooting](#)

[Error messages](#)

## Credentials - what are my options?

### Use an account with root privileges

This is recommended as it gives the Cloud Agent for Linux 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 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 Qualys Community**

[Sudo command list](#)

## Installation

It's easy to install Cloud Agent for Linux. We'll walk you through the steps quickly.

Keep in mind - Depending on your environment, you might need to take steps to support communications between agent hosts on your network and the Qualys Cloud Platform.

[Tips and best practices](#)

[How to download Agent image](#)

[Installation steps](#)

[Proxy configuration](#)

[Anti-Virus and HIPS Exclusion / Whitelisting](#)

## Tips and best practices

**What is an activation key?** You'll need an agent activation key to install agents. This provides a way to group agents and bind them to your subscription with Qualys Cloud Platform. You can create different keys for various business functions and users.

**Benefits of adding asset tags to an activation key** Tags assigned to your activation key will be automatically assigned to agent hosts. This helps you manage your agents and report on agent hosts.

**Running the agent installer** You'll need to run the installer from an elevated command prompt, or use a systems management tool.

**Be sure to activate agents** to provision agents for modules - Vulnerability Management (VM), Policy Compliance (PC), or both. Activating an agent for a module consumes an agent license. You can set up auto activation by defining modules for activation keys, or do it manually in the Cloud Agent UI.

What happens if I skip activation? Agents will sync inventory information only to the cloud platform (IP address, OS, DNS and NetBIOS names, MAC address), host assessments will not be performed.

**How many agents can I install?** You can install any number of agents but can activate an agent only if you have a license. The Agents tab in the Cloud Agent UI tells you about your installed agents.

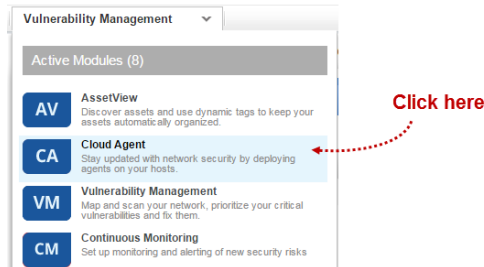
**Check to be sure agents are connected** Once installed agents immediately connect to the Qualys Cloud Platform and register themselves. You can see agent status on the Agents tab - this is updated continuously. If your agent doesn't have a status, it has not successfully connected to the cloud platform and you need to [troubleshoot](#).

# How to download Agent image

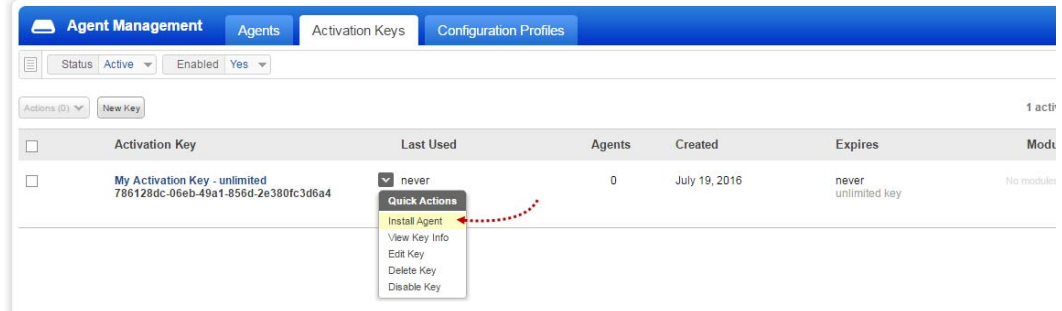
## Download an image of Qualys Cloud Agent for Linux

Here's how to download an image from the Qualys Cloud Platform and get the associated Activation ID and Subscription ID.

Log into the Qualys Cloud Platform and select **CA** for the Cloud Agent module.



Choose an activation key (create one if needed) and select **Install Agent** from the Quick Actions menu.



Click **Install instructions** for the target host.



What happens? The Agent image is downloaded to your local system, and in the UI you'll see the associated Activation key ID and Subscription ID - copy and paste this to a safe place, you'll need it to complete the installation.

# Installation steps

## What you'll need

To install cloud agents, you'll need to download the Cloud Agent image and get the associated ActivationID and CustomerID. Just log into the Qualys Cloud Platform, go to the Cloud Agent (CA) module, and follow the installation steps for Linux (.rpm) or Linux (.deb) to get everything you need.

[Cloud Agent requirements](#)

[Have AWS? Click here](#)

## Steps to install Agents

1. Copy the Qualys Cloud Agent image onto the target host.
2. Install the Qualys Cloud Agent using the following commands:

### Linux (.rpm)

```
> sudo rpm -ivh qualys-cloud-agent.x86_64.rpm
> sudo /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh
ActivationId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx
CustomerId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx
```

### Linux (.deb)

```
> sudo dpkg --install qualys-cloud-agent.x86_64.deb
> sudo /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh
ActivationId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx
CustomerId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx
```

## Steps to install Agents in AWS

These steps are similar to installing on Linux (.rpm) hosts, with an extra step to restart the Qualys Cloud Agent service and AMI instance.

1. Spin up an AMI instance.
2. Copy the Qualys Cloud Agent RPM onto the instance.
3. Install the Qualys Cloud Agent RPM using the following command:

```
> sudo rpm -ivh qualys-cloud-agent.x86_64.rpm
```

4. Stop Qualys Cloud Agent service:

```
> sudo service qualys-cloud-agent stop
```

5. Run the Qualys Cloud Agent installation command:

```
> sudo /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh  
ActivationId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx  
CustomerId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

6. Stop the instance and create an image out of the instance. This completes the bake-in process.

When the instance is started it will activate the Cloud Agent which will provision itself and continue functioning as expected.

## What happens next?

### We'll start syncing asset data to the cloud!

Once installed an agent immediately connects to the Qualys Cloud Platform and registers itself. We would expect you to see your first asset discovery results within a few minutes. The first assessment scan in the cloud takes some time, after that scans complete as soon as new host metadata is uploaded to the cloud platform.

## Troubleshooting

You'll find helpful information in Qualys online help.

### Qualys Help

[Troubleshooting](#)

[Error messages](#)

Cloud agents installed on RHEL 5.4 may throw SSL communication errors while trying to communicate with the Qualys Platform. This happens when the certificate files are not present on the host asset. The solution to fix the issue is provided in [Appendix A](#).

Cloud agents installed on SUSE Linux Enterprise 11 may throw a file not found error for the certificate ca-bundle.crt when trying to communicate with the Qualys Platform. This happens when the certificate files are not present on the host asset. The solution to fix the issue is provided in [Appendix B](#).

## You might also be interested in...

[Proxy configuration](#)

## Anti-Virus and HIPS Exclusion / Whitelisting

# Proxy configuration

## How to enable a proxy

**Good to Know** By default the Cloud Agent for Linux will operate in non-proxy mode. The agent can be configured to use an HTTPS proxy for internet access.

## What are my options?

The agent can be configured in one of these ways:

- 1) /etc/sysconfig/qualys-cloud-agent - applies to Cloud Agent for Linux (.rpm)
- 2) /etc/default/qualys-cloud-agent - applies to Cloud Agent for Linux (.deb)
- 3) /etc/environment - applies to Cloud Agent for Linux (.rpm) and (.deb)

Tip - Option 3) is a better choice if the systemwide proxy will be used by the agent.

## Tell me the steps

Here are the steps to enable the Linux agent to use a proxy for communication with our cloud platform:

- 1) if /etc/sysconfig/qualys-cloud-agent file doesn't exist create it
- 2) add 1 of the following lines to the file (1 line only):

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

4) restart qualys-cloud-agent service using the following command:

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

# Anti-Virus and HIPS Exclusion / Whitelisting

Have Anti-Virus or HIPS software installed? It's required that the following files, directories, and processes are excluded or whitelisted in all security software installed on the system in order to prevent conflicts with the Cloud Agent.

## Directory list used by Cloud Agent installation

```
/etc
/etc/init.d
/etc/qualys
/etc/qualys/cloud-agent
/etc/qualys/cloud-agent/.centos
/etc/qualys/cloud-agent/cert
/etc/qualys/cloud-agent/.suse
/etc/qualys/cloud-agent/.systemd
/usr/local
/usr/local/qualys
/usr/local/qualys/cloud-agent
/usr/local/qualys/cloud-agent/bin
/usr/local/qualys/cloud-agent/lib
/usr/share/doc
/usr/share/doc/qualys-cloud-agent-<version>
```

## Agent daemon process “qualys-cloud-agent”

The agent runs as daemon process “qualys-cloud-agent”.

The agent runs various read-only commands during the scanning process. These are the same commands run by a scan using a scanner appliance. Learn more

<https://community.qualys.com/message/16520>

## Some transient files are created during agent execution

```
/usr/local/qualys/cloud-agent/Config.db
- this is the current agent configuration

/usr/local/qualys/cloud-agent/manifests/*.db
- this contains manifests used during agent based scans
```

## Configuration Tool

Our easy to use tool gives you many options for configuring Cloud Agent for Linux. You'll find this tool at `/usr/local/qualys/cloud-agent/qualys-cloud-agent.sh`. This tool is available with Linux Agent 1.3 and later.

Our configuration tool allows you 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.

## Command line options

qualys-cloud-agent.sh supports these command line options.

| Configuration option | Description   |
|----------------------|---|
| 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).  |
| LogFileDir           | 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  |
| LogDestType          | (Available using Linux Agent 1.3.3 and later) The destination of log lines generated by Linux Agent. Set to <b>file</b> or <b>syslog</b> . If set to <b>file</b> specify the location of the log file. By default the destination is a log file:<br>/var/log/qualys/qualys-cloud-agent.log  |
| ServerUri            | Use this option to migrate the agent from one Qualys shared Pod or PCP to another.<br>ServerUri takes the URL of the Qualys shared Pod or PCP you want to migrate the Agent to, in the following format:<br>ServerUri=<http_url>/CloudAgent<br>where <http_url> is the URL of the Qualys shared Pod or PCP.<br>Use this option along with ActivationId and CustomerId in order to move the agent to another Qualys shared Pod or PCP. |

| <b>Configuration option</b> | <b>Description</b>   |
|-----------------------------|--|
| CmdMaxTimeOut               | Execution of a command is dropped if the time taken to execute is more than the specified value. Default timeout is 1800 seconds (30 minutes).   |
| ProcessPriority             | Specify the Linux niceness scale between -20 to 19 to set a priority for the Qualys cloud agent process. The lower the number the more priority the agent process gets. Default value is zero. |

## Use cases

### 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

Here's best practices for managing your cloud agents.

### Uninstalling Cloud Agent

#### Uninstalling the agent from the Cloud Agent module UI or API

When you uninstall a cloud agent using the Cloud Agent module user interface or Cloud Agent API, the agent and license is removed from the Qualys subscription. We'll also purge the associated agent host record and scan results for any licensed modules, i.e. Vulnerability Management, Policy Compliance.

#### Uninstalling the agent from the host itself

When you uninstall a cloud agent the agent from the host itself using the uninstall utility, the agent, its license usage, and scan results are still present in the Qualys subscription. In order to remove the agent's host record, license, and scan results use the Cloud Agent module user interface or Cloud Agent API to uninstall the agent.

##### Linux RPM based system

```
sudo rpm -e qualys-cloud-agent
```

##### Linux Debian based system

```
sudo dpkg --purge qualys-cloud-agent
```

## Agentless Tracking and Cloud Agents

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 hosts using Linux Agent 1.3.3 and later.). This is recommended best practice if you are interested in using Linux Agent and Agentless Tracking to evaluate the same host.

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.

### 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? Log into the Qualys Cloud Platform, go to Help > Contact Support and search for **Agentless Tracking**.

#### 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 you can 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/hostid

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

2) Uninstall duplicate agents not communicating

Click [here](#) for instructions.

# APPENDIX A

---

## Certificate Support on RHEL 5.4

Cloud agent installed on RHEL 5.4 may throw this error while trying to communicate with the Qualys Platform. This happens when the certificate files are not present on the host asset.

```
Http request failed: Peer certificate cannot be authenticated with
given CA certificates: SSL certificate problem: unable to get
local issuer certificate
```

To fix this issue, you must manually create the certificate files, and place them in the appropriate location on the host asset.

Create the two cert files: `cert1.crt` and `cert2.crt`. Paste the contents in a text editor, and then save the file with the extension “.crt”.

Use the following commands to append the contents of `cert1.crt` and `cert2.crt` at the end of `/etc/pki/tls/certs/ca-bundle.crt`

```
cat cert1.crt >> /etc/pki/tls/certs/ca-bundle.crt
cat cert2.crt >> /etc/pki/tls/certs/ca-bundle.crt
```

Now restart the QAgent Service.

### **cert1.crt**

```
subject= /C=US/O=Symantec Corporation/OU=Symantec Trust
Network/CN=Symantec Class 3 Secure Server CA - G4
```

```
issuer= /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign,
Inc. - For authorized use only/CN=VeriSign Class 3 Public Primary Certification
Authority - G5
```

```
serial=513FB9743870B73440418D30930699FF
```



```
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCB
yJELMAkGALUEBhMCVVMxVzAVBgNVBAoTDlZlcm1TaWduLlCBJmMuMR8wHQYDVQQL
ExZWZlZjU2LnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJp
U2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkiHVzZSBvbm55MUUwQwYDVQQDEzxW
ZXJpU2lnbiBDbGFzcyAzIFB1YmVzYyBQcm1tYXJ5IENlcnRpb24gQXV0aG9yaXR5
IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2MjMjMTU5WjCBByJELMAkGAL
UEBhMCVVMxVzAVBgNVBAoTDlZlcm1TaWduLlCBJmMuMR8wHQYDVQQLExZWZlZjU2
LnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJpU2lnbiwgSW5j
LiAtIEZvciBhdXRob3JpemVkiHVzZSBvbm55MUUwQwYDVQQDEzxWZXJpU2lnbiBDb
GFzcyAzIFB1YmVzYyBQcm1tYXJ5IENlcnRpb24gQXV0aG9yaXR5IC0gRzUwggEiMA
0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvJAgIKXo1nmAMqudL007cfLw8RRy7K
+D+KQL5VwiZiUVj/XxrcgxiV0i6CqqpkKzj/i5Vbext0uz/o9+B1fs70PbZmIVYc9g
DaTY3vjgw2IIPVQT60nKWVSfJuUrjxuf6/WhkcIzSdhDY2pSS9KP6HBRtdGJaXvHc
Paz3BJ023tdS1bTlr8Vd6Gw9KI18q8ckmcY5fQGB0+QueQA5N06tRn/Arr0PO7gi+s3i
+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/
Fla4OndTRQ8Bnc+MUCH71P59zuDMKz10/NIEwiu5T6CUVAgMBAAAgjgbIwga8wDwYD
VR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWz
BZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGGUj+XTGoasjY5rw8+AatRIGCx7GS4
wJRYjaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVROBBYEFH/
TZafC3ey78DAJ80M5+gKvMzEzMA0GCSqGSIb3DQEBBQUAA4IBAQCTJEowX2LP2BqYLz3q3
JktvXf2pXkiOOzE p6B4Eq1iDkVwZMXnl2YtmAl+X6/WzChl8gGqCBpH3vn5fJJJaCGkg
Ddk+bW48DW7Y5gaRQBis+MHT39tBquCWIMnNZBU4gcmU7qKEKQsTb47bDN01AtukixlE0k
F6BWlKWE9gyn6CagsCqiUXObXbf+eEZSqVir2G3l6BFoMtEMze/aiCKm0oHw0LxOXnGiYZ
4fQRbxCl1fznQgUy286dUV4otp6F01vvpX1FQHK0tw5rDgb7MzVICbidJ4vEZV8N
hnaCRHr21Vz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7WNq
-----END CERTIFICATE-----
```



## Certificate Support on SUSE Linux Enterprise 11

Cloud agent installed on SUSE Linux Enterprise 11 may throw the following error for the certificate `ca-bundle.crt` when trying to communicate with the Qualys Platform. This happens when the certificate files are not present on the host asset.

```
[qualys-cloud-agent][8056]:[Error]:Http request failed:Problem with the SSL CA cert (path? access rights?): error setting certificate verify locations: CAfile: /etc/ssl/ca-bundle.crt CApath: none
```

To fix this issue, you must manually install the certificate files in the appropriate location on the host asset. You can either use the certificate files from your existing RHEL or CentOS assets or download the certificate files from the following location:

<https://curl.haxx.se/docs/caextract.html>

Copy the certificate files (`ca-bundle.pem`) at the following default location on SUSE Linux Enterprise 11:

```
/etc/ssl/
```

If you want to use a non default location, ensure that the directory path is added in the `/etc/qualys/cloud-agent/qagent.config` file in the following manner:

```
{
  "os": "Suse",
  "cafile": "<CustomizedPath>"
}
```

Now restart the QAgent Service.