Cloud Agent for Linux

Installation Guide

Agent Version 1.5 - 1.7, 2.0.2, 2.1

October 10, 2018

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

Table of Contents

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. The Qualys Cloud Platform and its integrated apps help businesses 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, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, 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.

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/.

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.

Get informed quickly on Qualys Cloud Agent (CA).

Video Tutorials

Cloud Agent Platform Introduction (2m 10s)

Getting Started Tutorial (4m 58s)

Cloud Agent Platform Availability for Linux

Current Release: 1.71.37, 2.1.0.91

End-of-Support versions: 1.3.3.23, 1.3.1.16

Next End-of-Support versions: 1.5.0.70, 1.5.0.61

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)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	*not available*	*not available*
Red Hat	Red Hat Enterprise Linux 6	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	2.1.0.91 (RHEL 6.5+)	*not available*
Red Hat	Red Hat Enterprise Linux 7 7.1, 7.2, 7.3, 7.4, 7.5	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	2.1.0.91	*not available*
Red Hat	CentOS 5.4+	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	*not available*	*not available*
Red Hat	CentOS 6	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	2.1.0.91 (CentOS 6.5+)	*not available*
Red Hat	CentOS 7 7.1, 7.2, 7.3, 7.4, 7.5	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	2.1.0.91	*not available*

Supported Platforms				Supported Qualys Modules/Agent Versions				
Vendor	**Operating System**	**Arch**	**Installer**	**Inventory**	**VM**	**PC**	**FIM**	**IOC**
Red Hat	Fedora 22, 23, 24	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	*not available*	*not available*	*not available*
SUSE	SUSE Linux Enterprise Server (SLES) 11, 12	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	2.1.0.91	*not available*
SUSE	OpenSUSE 12	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	*not available*	*not available*	*not available*
SUSE	OpenSUSE 13	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	*not available*	*not available*
SUSE	OpenSUSE Leap 42.1	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	*not available*	*not available*	*not available*
Amazon	Amazon Linux 2015.09	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	*not available*	*not available*	*not available*
Amazon	Amazon Linux 2016.09	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	*not available*	*not available*
Amazon	Amazon Linux 2017.03	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	2.1.0.91	*not available*
Amazon	Amazon Linux 2017.09	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	2.1.0.91	*not available*
Amazon	Amazon Linux 2018.03	x86_64	(.rpm)	2.1.0.91	2.1.0.91	2.1.0.91	2.1.0.91	*not available*
Amazon	Amazon Linux 2	x86_64	(.rpm)	1.7.1.37-2.1.0.91	1.7.1.37-2.1.0.91	1.7.1.37-2.1.0.91	2.1.0.91	*not available*
Oracle	Oracle Enterprise Linux 5.11	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	*not available*	*not available*
Oracle	Oracle Enterprise Linux 6	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	2.1.0.91	*not available*
Oracle	Oracle Enterprise Linux 7 7.1, 7.2, 7.3, 7.4, 7.5	x86_64	(.rpm)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	2.1.0.91	*not available*
Debian	Debian 7.x (Vendor EOL May 2018)	x86_64	(.deb)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	*not available*	*not available*
Debian	Debian 8.x, 9.x	x86_64	(.deb)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	*not available*	*not available*
Ubuntu	Ubuntu 12.04 LTS	x86_64	(.deb)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	*not available*	*not available*
Ubuntu	Ubuntu 14.04 LTS	x86_64	(.deb)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	2.1.0.91	*not available*
Ubuntu	Ubuntu 15.x	x86_64	(.deb)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	*not available*	*not available*	*not available*
Ubuntu	Ubuntu 16.04 LTS	x86_64	(.deb)	1.6.0.61-2.1.0.91	1.6.0.61-2.1.0.91	not *available*	2.1.0.91	*not available*
Ubuntu	Ubuntu 18.04 LTS	x86_64	(.deb)	1.7.1.37-2.1.0.91	1.7.1.37-2.1.0.91	not *available*	*not available*	*not available*

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

Learn more

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 - review 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

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.

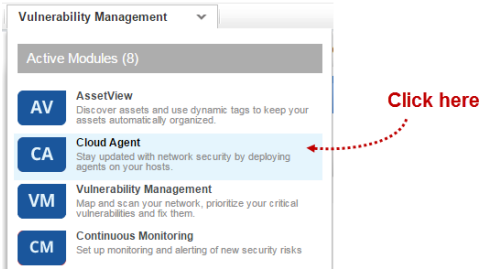
net-tools package You may need to install the net-tools package on agent endpoints, if not already present, in order to run network commands. This is required on systems running Red Hat Enterprise Linux, Oracle Enterprise Linux and CentOS version 7.1 since some commands like netstat, /sbin/ifconfig, route are deprecated.

How to download Agent image

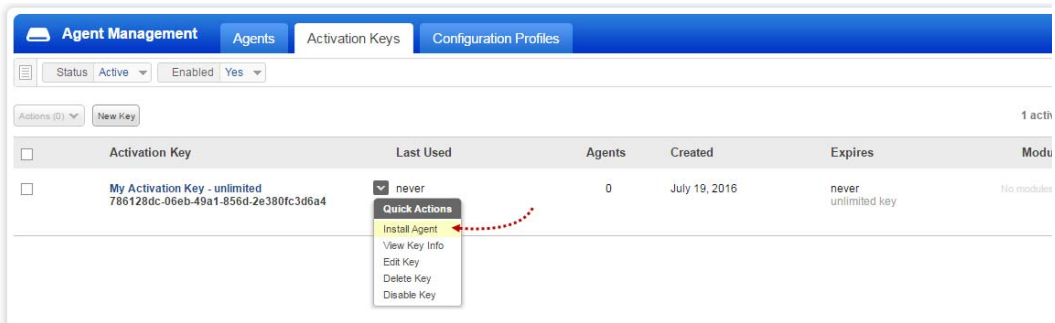
Download an image of Qualys Cloud Agent for Linux

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.

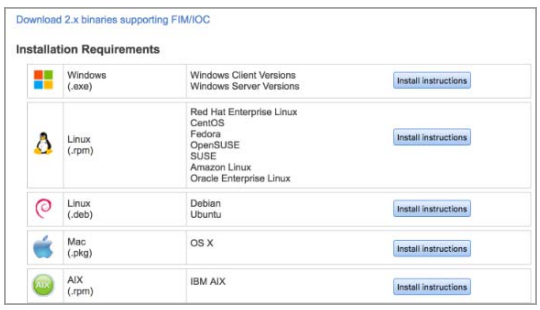


Choose an activation key (create one if needed) and select **Install Agent** from the Quick Actions menu.



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

Note: Agent installer for FIM/IOC is different than those used for other modules. Click **Download 2.x binaries supporting FIM/IOC**, and then click Install instructions next to the target host, to get the agent installer for FIM/IOC.



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-xxxxxxxxxxxx
CustomerId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

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-xxxxxxxxxxxx
CustomerId=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

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.

Learn more

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. Click here for solution to fix the issue.

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. Click here for solution to fix the issue.

You might also be interested in...

Proxy configuration

Anti-Virus and HIPS Exclusion / Whitelisting

Proxy configuration

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 to use an HTTPS proxy 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 <cloud_agent_user> /etc/sysconfig/qualys-cloud-agent
chmod 600 /etc/sysconfig/qualys-cloud-agent
```

Linux (.deb)

```
chown <cloud_agent_user> /etc/default/qualys-cloud-agent
chmod 600 /etc/default/qualys-cloud-agent
```

Where `<cloud_agent_user>` is a user configured through the Configuration Tool.

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). Limitations of using UseSudo=1
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).

Configuration option	Description
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 usin gLinux 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
ServerUri	Use this option to migrate the agent from one Qualys shared Pod or PCP to another. ServerUri takes the URL of the Qualys shared Pod or PCP you want to migrate the Agent to, in the following format: `ServerUri=<http_url>/CloudAgent` where <http_url> is the URL of the Qualys shared Pod or PCP. Use this option along with ActivationId and CustomerId in order to move the agent to another Qualys shared Pod or PCP.
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.
UseAuditDispatcher	Set UseAuditDispatcher to 1 if you want to run FIM along with auditd enabled. Agent version 2.0.2 required auditd to be disabled on the host. These agents when upgraded to 2.1 through selfpatch retain this setting where UseAuditDispatcher is set to 0. Agents with 1.x version are set with UseAuditDispatcher=1 on selfpatch to 2.1. Fresh installation of 2.1 agent comes with UseAuditDispatcher=1 (by default) where you can run FIM along with auditd enabled.

Limitations of using UseSudo=1

If you configure the cloud agent for **UseSudo=1** to run commands using the sudo escalation method, you may face any of the following issues:

- Commands run by the cloud agent or any script added in the cloud agent manifest, fail to get the custom path set in the PATH environment.

- Scan results show empty values for service_list, bios_info, and service_info, when the agents fails to find related path in the PATH environment.

This happens because when you set UseSudo=1, the agent tries to find the custom path in the **secure_path** parameter located in the /etc/sudoers file. If this parameter is not set, the agent then tries to find the custom path in the path that is used when you run **sudo sh**.

To resolve this issue, add your custom path or the path used by the agent while scanning for service_list, bios_info, and service_info, to the secure_path parameter. If you have disabled secure_path parameter, add the respective paths to the path that is used when you run sudo sh.

Alternatively, you can configure the agent for UseSudo=0.

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.

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 **cer1.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 SHA256 SSL CA

issuer= /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2008 VeriSign, Inc. - For authorized use only/CN=VeriSign Universal Root Certification Authority

serial=69879419D9E36270749DBBE59DC6685E

```
-----BEGIN CERTIFICATE-----
MIIFSTCCBDGgAwIBAgIQaYeUGdnjYnB0nbvlncZoXjANBgkqhkiG9w0BAQsFADCB
vTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwOCBWZXJp
U2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5MTgwNgYDVQQDEy9W
ZXJpU2lnbiBVbml2ZXJzYWwgUm9vdCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAe
Fw0xMzA0MDkwMDAwMDBaFw0yMzA0MDgyMzU5NTlaMIGEMQswCQYDVQQGEwJVUzEd
MBsGA1UEChMUU3ltYW50ZWMgQ29ycG9yYXRpb24xHzAdBgNVBAsTFlN5bWFudGVj
IFRydXN0IE5ldHdvcmsxNTAzBgNVBAMTLFN5bWFudGVjIENsYXNzIDMgU2VjdXJl
IFNlcnZlciBTSEEyNTYgU1NMIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvjgWUYuA2+oOTezoP1zEfKJd7TuvpdaeEDUs48XlqN6Mhhcm5t4LUUos
0PvRFFpy98nduIMcxkaMMSWRDlkXo9ATjJLBr4FUTrxiAp6qpxpX2MqmmXpwVk+Y
By5LltBMOVO5YS87dnyOBZ6ZRNEDVHcpK1YqqmHkhC8SFTy914roCR5W8bUUrIqE
zq54omAKU34TTBpAcA5SWf9aaC5MRhM7OQmCeAI1SSAIgrOxbIkPbh41JbAsJIPj
xVAsukaQRYcNcv9dETjFkXbFLPsFKoKVoVlj49AmWM1nVjq633zS0jvY3hp6d+QM
jAvrK8IisL1Vutm5VdEiesYCTj/DNQIDAQABo4IBejCCAXYwEgYDVR0TAQH/BAgw
```

```
BgEB/wIBADA+BgNVHR8ENzA1MDOgMaAvhi1odHRwOi8vY3JsLndzLnN5bWFudGVj
LmNvbS91bml2ZXJzYWwtcm9vdC5jcmwwDgYDVR0PAQH/BAQDAgEGMDcGCCsGAQUF
BwEBBCswKTAnBggrBgEFBQcwAYYbaHR0cDovL29jc3Aud3Muc3ltYW50ZWMuY29t
MGsGA1UdIARkMGIwYAYKYIZIAYb4RQEHNjBSMCYGCCsGAQUFBwIBFhpodHRwOi8v
d3d3LnN5bWF1dGguY29tL2NwczAoBggrBgEFBQcCAjAcGhpodHRwOi8vd3d3LnN5
bWF1dGguY29tL3JwYTAqBgNVHREEIzAhpB8wHTEbMBkGA1UEAxMSVmVyaVNpZ25N
UEtJLTItMzczMB0GA1UdDgQWBBTbYiD7fQKJfNI7b8fkMmwFUh2tsTAfBgNVHSME
GDAWgBS2d/ppSEefUxLVwuoHMnYH0ZcHGTANBgkqhkiG9w0BAQsFAAOCAQEAGcyV
4i97SdBIkFP0B7EgRDVwFNVENzHv73DRLUzpLbBTkQFMVOd9m9o6/7fLFK0wD2ka
KvC8zTXrSNy5h/3PsVr2Bdo8ZOYr5txzXprYDJvSl7Po+oeVU+GZrYjo+rwJTaLE
ahsoOy3DIRXuFPqdmBDrnz7mJCRfehwFu5oxI1h5TOxtGBlNUR8IYb2RBQxanCb8
C6UgJb9qGyv3AglyaYMyFMNgW379mjL6tJUOGvk7CaRUR5oMzjKv0SHMf9IG72AO
Ym9vgRoXncjLKMziX24serTLR3x0aHtIcQKcIwnzWq5fQi5fK1ktUojljQuzqGH5
S5tV1tqxkju/w5v5LA==
-----END CERTIFICATE-----
```

cert2.crt

subject= /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2008 VeriSign, Inc. - For authorized use only/CN=VeriSign Universal Root Certification Authority

issuer= /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2008 VeriSign, Inc. - For authorized use only/CN=VeriSign Universal Root Certification Authority

serial=401AC46421B31321030EBBE4121AC51D

```
-----BEGIN CERTIFICATE-----
MIIEuTCCA6GgAwIBAgIQQBrEZCGzEyEDDrvkEhrFHTANBgkqhkiG9w0BAQsFADCB
vTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwOCBWZXJp
U2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5MTgwNgYDVQQDEy9W
ZXJpU2lnbiBVbml2ZXJzYWwgUm9vdCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAe
Fw0wODA0MDIwMDAwMDBaFw0zNzEyMDEyMzU5NTlaMIG9MQswCQYDVQQGEwJVUzEX
MBUGA1UEChMOVmVyaVNpZ24sIEluYy4xHzAdBgNVBAsTFlZlcmlTaWduIFRydXN0
IE5ldHdvcmsxOjA4BgNVBAsTMShjKSAyMDA4IFZlcmlTaWduLCBJbmMuIC0gRm9y
IGF1dGhvcml6ZWQgdXNlIG9ubHkxODA2BgNVBAMTL1ZlcmlTaWduIFVuaXZlcnNh
bCBSb290IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAx2E3XrEBNNti1xWb/1hajCMj1mCOkdeQmIN65lgZOIzF
9uVkhbSicfvtvbnazU0AtMgtc6XHaXGVHzk8skQHnOgO+k1KxCHfKWGPMiJhgsWH
H26MfF8WIFFE0XBPV+rjHOPMee5Y2A7Cs0WTwCznmhcrewA3ekEzeOEz4vMQGn+H
LL729fdC4uW/h2KJXwBL38Xd5HVEMkE6HnFuacsLdUYI0crSK5XQz/u5QGtkjFdN
/BMReYTtXlT2NJ8IAfMQJQYXStrxHXpma5hgZqTZ79IugvHw7wnqRMkVauIDbjPT
rJ9VAMf2CGqUuV/c4DPxhGD5WycRtPwW8rtWaoAljQIDAQABo4GyMIGvMA8GA1Ud
EwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMG0GCCsGAQUFBwEMBGEwX6FdoFsw
WTBXMFUWCWltYWdlL2dpZjAhMB8wBwYFKw4DAhoEFI/l0xqGrI2Oa8PPgGrUSBgs
exkuMCUWI2h0dHA6Ly9sb2dvLnZlcmlzaWduLmNvbS92c2xvZ28uZ2lmMB0GA1Ud
DgQWBBS2d/ppSEefUxLVwuoHMnYH0ZcHGTANBgkqhkiG9w0BAQsFAAOCAQEASvj4
```

```
sAPmLGd75JR3Y8xuTPl9Dg3cyLk1uXBPY/ok+myDjEedO2Pzmvl2MpWRsXe8rJq+
seQxIcaBlVZaDrHC1LGmWazxY8u4TB1ZkErvkBYoH1quEPuBUDgMbMzxPcP1Y+Oz
4yHJJDnp/RVmRvQbEdBNc6N9Rvk97ahfYtTxP/jgdFcrGJ2BtMQo2pSXpXDrrB2+
BxHw1dvd5Yzw1TKwg+ZX4o+/vqGqvz0dtdQ46tewXDpPaj+PwGZsY6rp2aQW9IHR
lRQOfc2VNNnSj3BzgXucfr2YYdhFh5iQxeuGMMY1v/D/w1WIg0vvBZIGcfK4mJO3
7M2CYfE45k+XmCpajQ==
-----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.