Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift

Installation Guide

November 22, 2022

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

Table of Contents

Preface ... 4

About Qualys ... 4
Contact Qualys Support ... 4

Get Started ... 5

Qualys Cloud Agent Introduction ... 5
Cloud Agent Platform Availability for CoreOS ... 5
A few things to consider... ... 5
- Cloud Agent requirements ... 5
- What are the installation steps? ... 5
- Need help with troubleshooting? ... 5

Installation ... 6

Tips and best practices ... 6
How to download Agent Installer ... 7
Installation steps ... 8
- What you'll need ... 8
- Steps to install Agents ... 9
- What happens next? ... 14

Proxy Configuration ... 14

On Demand Scan ... 16

Best Practices ... 18

Upgrading Cloud Agent ... 18
Uninstalling Cloud Agent ... 18

Proxy Configuration Encryption Utility ... 20

Preface

Welcome to Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift. 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 Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift. We'll tell you about Requirements, Installation Steps, Proxy Configuration, 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 - server, virtual machine, laptop, desktop or cloud instance.

Get informed quickly on Qualys Cloud Agent (CA).

Video Tutorials

Cloud Agent Platform Introduction (2m 10s)

Getting Started Tutorial (6m 34s)

Cloud Agent Platform Availability for CoreOS

For the most current list of supported cloud agents with versions and modules on the Qualys Cloud Platform, please refer to the following article: Cloud Agent Platform Availability Matrix

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.

What are the installation steps?

Our Cloud Agent UI walks you through the steps to install agents on your hosts. You might want to configure proxy settings for our agent to communicate with our cloud platform.

Need help with troubleshooting?

We recommend you inspect the agent's log file located here:

/var/log/qualys/qualys-cloud-agent.log

Installation

It’s easy to install Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift. We’ll walk you through the steps quickly.

Qualys provides installers and packages for each supported operating system that are coded for each Qualys platform. It's not possible to connect an agent coded for one platform to another platform. Organizations can use their existing software distribution tools (SCCM, BigFix, rpm, Casper, etc.) to install the agent into target machines.

The platform supports detection of duplicate agent IDs and automatically re-provisions the duplicate agents.

Customers using software distribution tools must package the Qualys-provided installer along with the specific Activation Key and Customer ID strings to install properly. Do not package up the artifacts that are installed by the agent into your own installer as the installation environment is keyed for that specific machine when the agent is installed; doing so will create duplicates that the platform may not be able to easily de-duplicate.

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 Installer

Installation steps

Proxy Configuration

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 using elevated privileges.

Be sure to activate agents to provision agents for modules - Vulnerability Management (VM). 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.

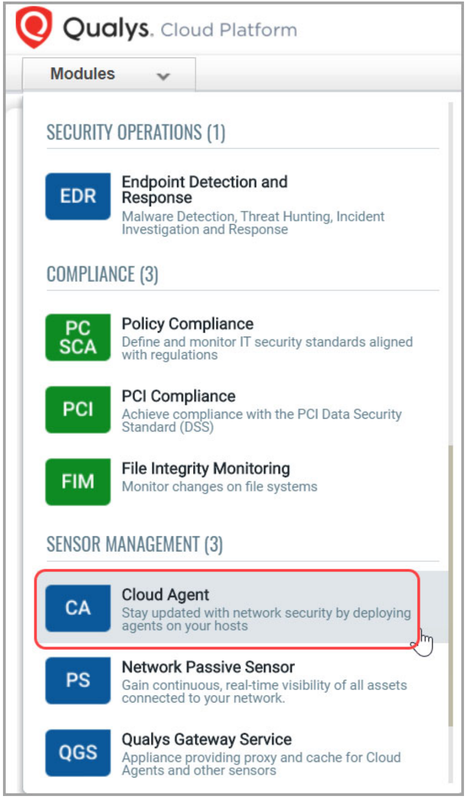
How many agents can I install? You can install any number of agents but can activate an agent only if you have a license. The Agents tab in the Cloud Agent UI tells you about your installed agents.

Check to be sure agents are connected Once installed agents connect to the Qualys Cloud Platform and provision 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.

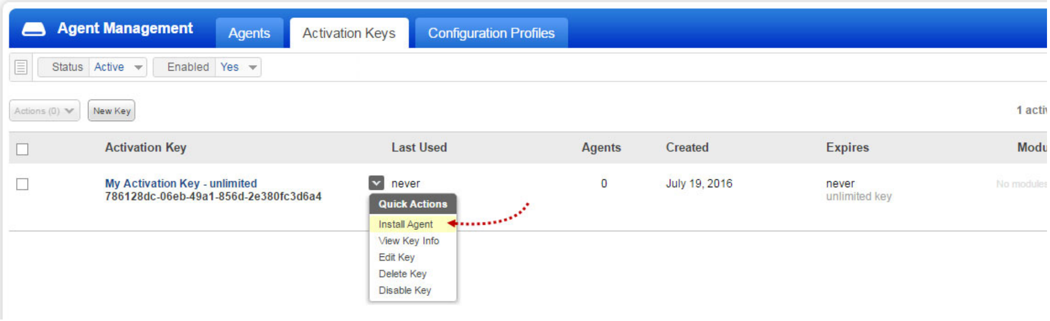
How to download Agent Installer

Here's how to download an installer 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.

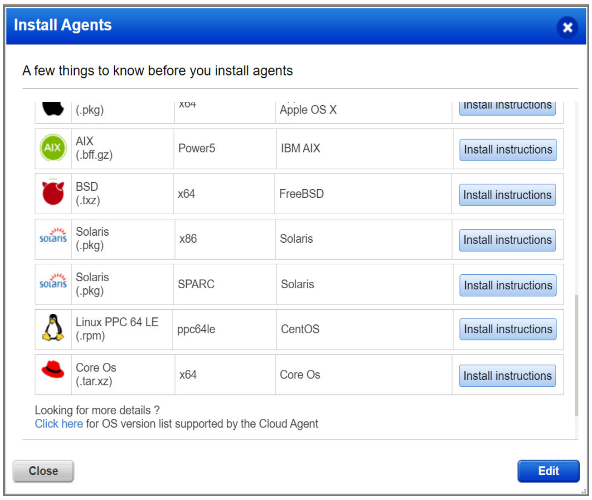

Qualys. Cloud Platform
Modules
SECURITY OPERATIONS (1)
EDR
Endpoint Detection and Response
Malware Detection, Threat Hunting, Incident Investigation and Response
COMPLIANCE (3)
PC SCA
Policy Compliance
Define and monitor IT security standards aligned with regulations
PCI
PCI Compliance
Achieve compliance with the PCI Data Security Standard (DSS)
FIM
File Integrity Monitoring
Monitor changes on file systems
SENSOR MANAGEMENT (3)
CA
Cloud Agent
Stay updated with network security by deploying agents on your hosts
PS
Network Passive Sensor
Gain continuous, real-time visibility of all assets connected to your network.
QGS
Qualys Gateway Service
Appliance providing proxy and cache for Cloud Agents and other sensors

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



□	Activation Key	Last Used	Agents	Created	Expires	Modu
□	My Activation Key - unlimited 786128dc-06eb-49a1-856d-2e380fc3d6a4	never	0	July 19, 2016	never unlimited key	No modules

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



A few things to know before you install agents

	(.pkg)	x64	Apple OS X	Install instructions
AIX	AIX (.bff.gz)	Power5	IBM AIX	Install instructions
	BSD (.txz)	x64	FreeBSD	Install instructions
solaris	Solaris (.pkg)	x86	Solaris	Install instructions
solaris	Solaris (.pkg)	SPARC	Solaris	Install instructions
	Linux PPC 64 LE (.rpm)	ppc64le	CentOS	Install instructions
	Core Os (.tar.xz)	x64	Core Os	Install instructions

Looking for more details ?
Click here for OS version list supported by the Cloud Agent

What happens? The Agent installer 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 installer 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 Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift (.tar.xz) to get everything you need.

Prerequisites:

- OpenShift Cluster with versions 4.6, 4.7, 4.8, 4.9 or 4.10

- Cluster configured with Registry for Master and Worker Nodes

Steps to install Agents

Use one of the following methods to install agents:

Method 1: For registry support

1. Download the Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift Container image tar file from Qualys Cloud Platform.

2. After downloading the file, untar the Qualys Cloud agent package using this command:

```
sudo tar -xvf QualysCloudAgent.tar.xz
```

3.Perform the following steps to load the images in different environment:

a-1. To load the images in Docker Runtime environment: Push the Qualys Cloud Agent image to a repository common to all nodes in the Kubernetes cluster using these commands:

```
sudo docker load -i QualysCloudAgent.tar
sudo docker tag <IMAGE NAME/ID> <URL to push image to the
repository>
sudo docker push <URL to push image to the repository>
```

For example:

```
sudo docker load -i QualysCloudAgent.tar
sudo docker tag c3fa63a818df mycloudregistry.com/linux-cloud-
agent:3.5.0.20
sudo docker push mycloudregistry.com/linux-cloud-agent:3.5.0.20
```

Note: Do not use these examples as is. Replace the registry/image path with your own.

a-2. To load the images in Container Runtime environment: Push the Qualys Cloud Agent image to a repository common to all nodes in the Kubernetes cluster using these commands:

```
ctr -n=k8s.io images import QualysCloudAgent.tar
ctr images tag <IMAGE NAME/ID> <URL to push image to the
repository>
ctr images push <URL to push image to the repository>
```

For example:

```
ctr -n=k8s.io images import QualysCloudAgent.tar
ctr images tag c3fa63a818df mycloudregistry.com/linux-cloud-
agent:3.5.0.20
ctr images push mycloudregistry.com/linux-cloud-agent:3.5.0.20
```

Note: Do not use these examples as is. Replace the registry/image path with your own.

a-3 To load the images in OpenShift CRI-O Runtime environment: Push the Qualys Cloud Agent image to a repository common to all nodes in the OpenShift cluster using these commands:

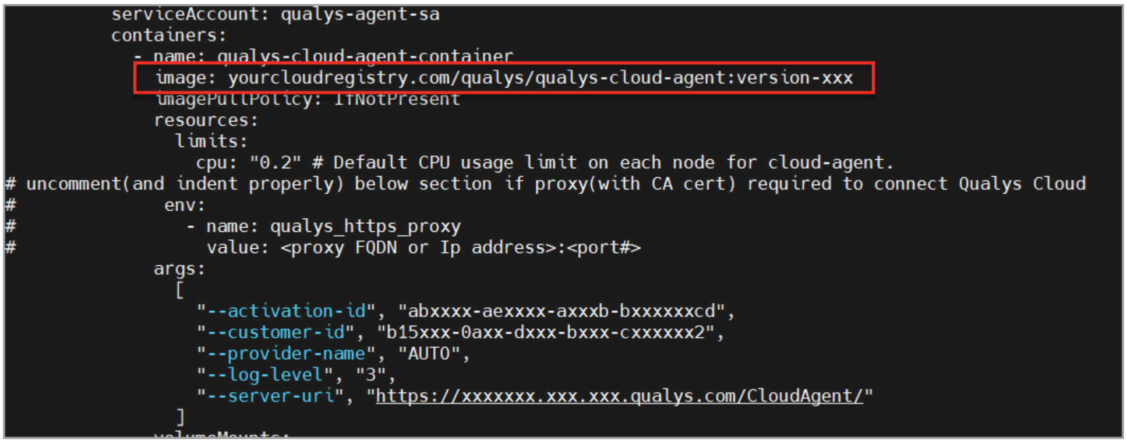
```
podman load -i QualysCloudAgent.tar
podman tag <IMAGE NAME/ID> <URL to push image to the repository>
podman push <URL to push image to the repository>
```

For example:

```
podman load -i QualysCloudAgent.tar
podman tag c3fa63a818df mycloudregistry.com/linux-cloud-
agent:3.5.0.20
podman push mycloudregistry.com/linux-cloud-agent:3.5.0.20
```

Note: Do not use these examples as is. Replace the registry/image path with your own.

b. Modify parameters in the lxa-openshift-crio-ds.yml file for your registry path <registry path>



```
          serviceAccount: qualys-agent-sa
          containers:
            - name: qualys-cloud-agent-container
              image: yourcloudregistry.com/qualys/qualys-cloud-agent:version-xxx
              imagePullPolicy: IfNotPresent
              resources:
                limits:
                  cpu: "0.2" # Default CPU usage limit on each node for cloud-agent.
# uncomment(and indent properly) below section if proxy(with CA cert) required to connect Qualys Cloud
#              env:
#                - name: qualys_https_proxy
#                  value: <proxy FQDN or Ip address>:<port#>
              args:
                [
                  "--activation-id", "abxxxx-aexxxx-axxxb-bxxxxxxcd",
                  "--customer-id", "b15xxx-0axx-dxxx-bxxx-cxxxxxx2",
                  "--provider-name", "AUTO",
                  "--log-level", "3",
                  "--server-uri", "https://xxxxxxx.xxx.xxx.qualys.com/CloudAgent/"
                ]
              volumeMounts:
```

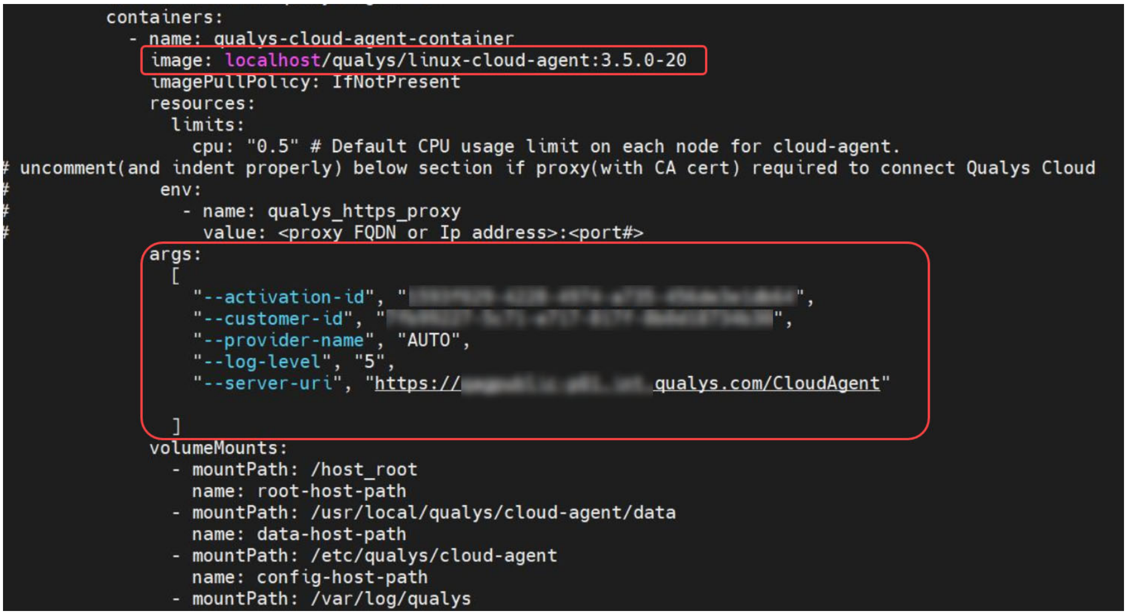
Important: The field alignment in the .yml file is very important. Ensure that you follow the formatting provided in the template.

4. Configure the following parameters in YML:

Parameter	Description
image	(Optional) path of image (localhost path or shared repository path). By default, it is a local directory.
cpu	(Optional) CPU usage limit in percentage for Cloud Agent. A valid range is 0-100 and the default value is 0.2
proxy	IPv4 address or FQDN of the proxy server
activation-id	Activation Id for the Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift, auto-generated based on your subscription.

Parameter	Description
customer-id	Qualys subscription's customerId, auto-generated based on your subscription.
provider-name	The value for this parameter can be AWS, AZURE, GCP, IBM, ALIBABA, ORACLE, NONE or AUTO. If you provide 'NONE' value, it does check for provider name. If you provide 'AUTO' value, it will auto check the provider.
log-level	Configuration to set the logging level for Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift. Valid values are to 5 and the default is 3.

Sample YML Configurations:



```
          containers:
            - name: qualys-cloud-agent-container
              image: localhost/qualys/linux-cloud-agent:3.5.0-20
              imagePullPolicy: IfNotPresent
              resources:
                limits:
                  cpu: "0.5" # Default CPU usage limit on each node for cloud-agent.
# uncomment(and indent properly) below section if proxy(with CA cert) required to connect Qualys Cloud
#              env:
#                - name: qualys_https_proxy
#                  value: <proxy FQDN or Ip address>:<port#>
              args:
                [
                  "--activation-id", "[redacted]",
                  "--customer-id", "[redacted]",
                  "--provider-name", "AUTO",
                  "--log-level", "5",
                  "--server-uri", "https://[redacted]qualys.com/CloudAgent"

                ]
              volumeMounts:
                - mountPath: /host_root
                  name: root-host-path
                - mountPath: /usr/local/qualys/cloud-agent/data
                  name: data-host-path
                - mountPath: /etc/qualys/cloud-agent
                  name: config-host-path
                - mountPath: /var/log/qualys
```

Note: If CPU set to more than 0.5 or 0.7 using YML file, agent won't be installed on all nodes in the cluster.

5. Once you have modified the lxa-openshift-crio-ds.yml file, run the following command on OpenShift master to create a DaemonSet:

```
# oc apply -f lxa-openshift-crio-ds.yml
```

6. Verify the container running under qualys name space using following command:

```
$oc get pods -n qualys-agent
NAME READY STATUS RESTARTS AGE
qualys-cloud-agent-4lcnb 1/1  Running 0 42m
qualys-cloud-agent-4nxjr 0/1  Running 0 42m
qualys-cloud-agent-bdhh9 1/1  Running 0 42m
qualys-cloud-agent-grcm7 0/1  Running 0 42m
```

```
qualys-cloud-agent-hw959 0/1  Running0 42m
qualys-cloud-agent-krxjc 0/1  Running 0 42m
```

Method 2

1. Download the Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift Container image tar file from Qualys Cloud Platform.

2. Upload the downloaded Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift Container image tar in one of the locations below, where we can access OpenShift cluster via OpenShift nodes login.

a. into private repository

b. into the master or worker nodes, that is, the nodes, where you want the Cloud Agent to run.

Untar package file (for example: package_name in the commands) file and load on master or worker node using following commands:

```
# tar -xJf <package_name.tar.xz>
# sudo podman load -i <package_name.tar>
```

Note: The command above is applicable only when the option b is followed.

3. Verify that the following files are present:

- lxa-openshift-crio-ds.yml

- version-info

- image-id

- qualys-cloud-agent-md5

- qualys-cloud-agent-sha

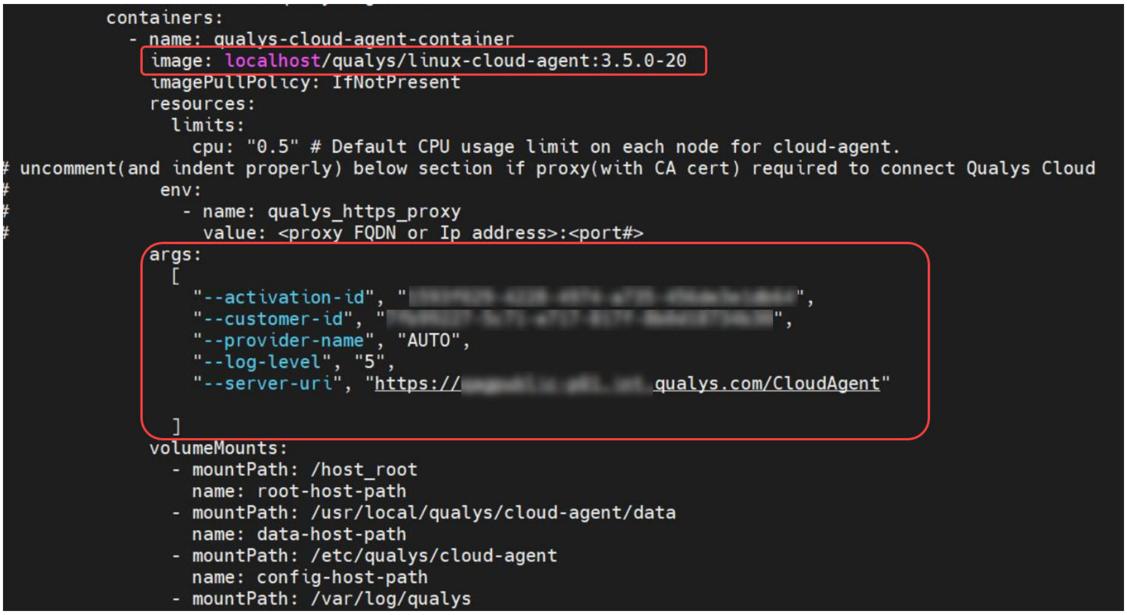
- qualys-cloud-agent.tar

4. Configure the following parameters in YML:

Parameter	Description
image	(Optiona) path of image (localhost path or shared repository path). By default, it is a local directory.
cpu	(Optional) CPU usage limit in percentage for Cloud Agent. A valid range is 0-100 and the default value is 0.2
proxy	IPv4 address or FQDN of the proxy server
activation-id	Activation Id for the Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift, auto-generated based on your subscription.
customer-id	Qualys subscription’s customerId, auto-generated based on your subscription.

Parameter	**Description**
provider-name	The value for this parameter can be AWS, AZURE, GCP, IBM, ALIBABA, ORACLE, NONE or AUTO. If you provide 'NONE' value, it does check for provider name. If you provide 'AUTO' value, it will auto check the provider.
log-level	Configuration to set the logging level for Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift. Valid values are to 5 and the default is 3.

Sample YML Configurations:



```
         containers:
           - name: qualys-cloud-agent-container
             image: localhost/qualys/linux-cloud-agent:3.5.0-20
             imagePullPolicy: IfNotPresent
             resources:
               limits:
                 cpu: "0.5" # Default CPU usage limit on each node for cloud-agent.
# uncomment(and indent properly) below section if proxy(with CA cert) required to connect Qualys Cloud
#             env:
#               - name: qualys_https_proxy
#                 value: <proxy FQDN or Ip address>:<port#>
             args:
               [
                 "--activation-id", "[redacted]",
                 "--customer-id", "[redacted]",
                 "--provider-name", "AUTO",
                 "--log-level", "5",
                 "--server-uri", "https://[redacted]qualys.com/CloudAgent"

               ]
             volumeMounts:
               - mountPath: /host_root
                 name: root-host-path
               - mountPath: /usr/local/qualys/cloud-agent/data
                 name: data-host-path
               - mountPath: /etc/qualys/cloud-agent
                 name: config-host-path
               - mountPath: /var/log/qualys
```

Note: If CPU set to more than 0.5 or 0.7 using YML file, agent won't be installed on all nodes in the cluster.

5. Once you have modified the lxa-openshift-crio-ds.yml file, run the following command on OpenShift master to create a DaemonSet:

```
# oc apply -f lxa-openshift-crio-ds.yml
```

6. Verify the container running under qualys name space using following command:

```
$oc get pods -n qualys-agent
NAME READY STATUS RESTARTS AGE
qualys-cloud-agent-4lcnb 1/1  Running 0 42m
qualys-cloud-agent-4nxjr 0/1  Running 0 42m
qualys-cloud-agent-bdhh9 1/1  Running 0 42m
qualys-cloud-agent-grcm7 0/1  Running 0 42m
qualys-cloud-agent-hw959 0/1  Running0 42m
qualys-cloud-agent-krxjc 0/1  Running 0 42m
```

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

What happens next?

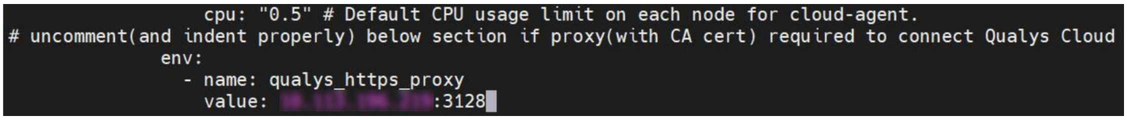
We'll start syncing asset data to the cloud!

Once installed an agent connects to the Qualys Cloud Platform and provisions 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.

What happens next?

Proxy Configuration

You can configure proxy in YML file. Following snippet shows sample proxy configuration.



```
         cpu: "0.5" # Default CPU usage limit on each node for cloud-agent.
# uncomment(and indent properly) below section if proxy(with CA cert) required to connect Qualys Cloud
       env:
        - name: qualys_https_proxy
         value: [redacted]:3128
```

Following parameters are optional while configuring proxy.

Parameter	Description
proxy	IPv4 address or FQDN of the proxy server
value	<proxy FQDN or IP address>:<port#>
ProxyCertFile	Proxy certificate file path. ProxyCertFile is applicable only if Proxy has valid certificate file. If this option is not provided, then Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift would try to connect to the server with given https Proxy settings only. If only ProxyCertFile is provided without Proxy then Qualys Cloud Agent for Red Hat Enterprise Linux CoreOS in Red Hat OpenShift would simply ignore the ProxyCertFile and it would try to connect to the server without any https proxy settings.

Steps to deploy the Cloud Agent in OpenShift cluster:

1. Login to Bastion (jump) host or master command to deploy linux-cloud-agent on OpenShift Cluster:

Note: OC login required to apply lxa-openshift-crio-ds.yml

2. Once you have modified the lxa-openshift-crio-ds.yml file, run the following command on OpenShift cluster to create a DaemonSet:

```
oc apply -f lxa-openshift-crio-ds.yml
```

3. Verify the container running under qualys name space using following command:

```
$ oc get pods -n qualys-agent
NAME                       READY   STATUS    RESTARTS   AGE
qualys-cloud-agent-9rl54   1/1     Running   0          3h27m
qualys-cloud-agent-c9dml   1/1     Running   0          3h27m
qualys-cloud-agent-gb7b5   1/1     Running   0          3h27m
qualys-cloud-agent-gttl7   1/1     Running   0          3h27m
qualys-cloud-agent-hfb5m   1/1     Running   0          3h27m
qualys-cloud-agent-pbrjg   1/1     Running   0          3h27m
```

When the instance is started, it will activate the Qualys Cloud Agent which will provision itself and continue to function as expected.

On Demand Scan

You can run an On Demand Scan to instruct the agent to immediately scan as long as the agent is not already scanning. The On Demand Scan runs independently of the interval scan that you configure in the Configuration Profile and will reset the scan interval on the local agent after a successful scan.

Prerequisite: The agent must be activated for that specific Qualys application for which you are running the On Demand Scan. When activated, the Agent downloads manifests for that application from the Qualys platform; if the manifest is not present for that type, On Demand Scan will not execute.

Use the cloudagentctl.sh script to run the OnDemand Scan. You'll find this script at /usr/local/qualys/cloud-agent/bin/. Run following command on Master node:

```
>_# oc -n qualys-agent exec -it <container_id> -- bash
/usr/local/qualys/cloud-agent/bin/cloudagentctl.sh action=demand
type=inv cputhrottle={0-1000}
```

Where action and type are mandatory parameters.

action is "demand", meaning an On Demand Scan.

type is the application for which you want to run the scan (the agent must be activated for the respective application first).

cputhrottle is 1-1000. Default is 0, which is no throttling.

For example, to initiate an On Demand Scan for the Vulnerability Management application (VM) with no throttling:

```
>_# oc -n qualys-agent exec -it <container_id> -- bash
/usr/local/qualys/cloud-agent/bin/cloudagentctl.sh action=demand
action=demand type=vm
```

The script calls the agent to run asynchronously in the background and returns to the shell prompt. The script prints a ControlId that you can track in the log file. The ControlId is the timestamp of the script initiation, e.g. On-Demand-Request ControlId: 20200427151136.0

The On Demand Scan logs to the same log file as the agent at /var/log/qualys/qualys-cloud-agent.log. You can find the logging for the scan initiation and completion in the log file.

```
2020-04-27 15:11:36.474 [qualys-cloud-
agent][9710]:[Information]:[140048573286144]:OnDemandRequest Params:
ControlID=20200427151136.0, Action=OnDemand, Type=VM, CPUThrottle=0"
```

If the agent is currently performing an interval scan for the same type, the On Demand Scan will delay waiting for the currently running scan to finish. The script will print a log line with this status.

```
2020-04-27 15:11:36.474 [qualys-cloud-
agent][9710]:[Information]:[140048573286144]:Interval Event of same type
```

```
is in progress with state INTERVAL_EVENT_SCAN
2020-04-27 15:11:36.474 [qualys-cloud-
agent][9710]:[Information]:[140048573286144]:OnDemand request for
Control ID : 20200427151136.0 will be delayed.
```

If the script errors due to the manifest file not being present, check whether the Cloud Agent is activated for that particular application. If agent is activated but you still get manifest related errors while running the On Demand Scan command, the agent may not have downloaded the manifest for that application. You can manually force a manifest download by deactivating then reactivating the agent for that application from the Cloud Agent user interface module. If that doesn't correct the issue, contact Qualys Support.

Once an On Demand Scan is completed, the results are logged in the log file located at /var/log/qualys/qualys-cloud-agent.log.

Best Practices

Here are some best practices for managing your cloud agents. Refer to the Cloud Agent Technical Whitepaper for additional documentation and best practices.

Upgrading Cloud Agent

1. Login in to the OpenShift via Bastion (jump) host OR Master node using OpenShift Container login.

Note: Use the same host you have used while installing Qualys Cloud Agent.

2. Upload new image in OpenShift cluster and update the image name in the yml file: Set your registry path <registry path>: OR Set to localhost/qualys/linux-cloud-agent: latest

3. Run the command to delete and recreate the Qualys Cloud Agent on CoreOS:

```
# oc delete -f lxa-openshift-crio-ds.yml
# oc apply -f lxa-openshift-crio-ds.yml
```

Note: Auto upgrade is not supported and manual intervention is required.

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.

Note: Self revoke is not supported. If revoke request sent from UI or API, agent will be halted but won't uninstall itself, and manual intervention is required.

Uninstalling the agent from Container

1. Login in to the OpenShift via Bastion (jump) host or Master node using OpenShift Container login.

Note: Use the same host you have used while installing Qualys Cloud Agent.

2. Run the following command to remove the Qualys Cloud Agent

```
# oc delete -f lxa-openshift-crio-ds.yml
```

3. Remove Qualys Cloud Agent Config, Data, and Log Directories manually on all masters and workers

```
# sudo rm -rf /usr/local/qualys/cloud-agent/data
# sudo rm -rf /etc/qualys/cloud-agent
# sudo rm -rf /var/log/qualys
```

Proxy Configuration Encryption Utility

You can use the Proxy Configuration Encryption utility to encrypt the user name and/or password (as needed) that you provide to the proxy environment variable qualys_https_proxy or https_proxy.

The **string-util** utility is included in the Cloud Agent installation package. Install or extract the Cloud Agent installation package to get the utility.

The string-util utility is to be used once on any system where it's installed to encrypt the values that will be used on all systems running Cloud Agent that have the same credentials. It is not required to run the utility on each system running Cloud Agent.

Provide the encrypted user name and password to your proxy environment variable in YML file.

```
qualys_https_proxy=https://[<#encrypted_username>:<#encrypted_password>@
]<host>[:<port>]
```

The # delimiter indicates to the Cloud Agent that the user name and password are encrypted. Not including the # indicates that the user name and password are in plain text format.

For example (only encrypting password):

```
qualys_https_proxy=https://sys_account:#sRpSHQP582a1+gaJwHOm3g==@proxy.m
yco.com:8080
```

For example (encrypting username and password):

```
qualys_https_proxy=https://#uWpsHMSY932b2+fdcH723d==:#sRpSHQP582a1+gaJwH
Om3g==@proxy.myco.com:8080
```