Cloud Agent for AWS Bottlerocket Container Host

Installation Guide

March 11, 2024

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 AWS Bottlerocket Container host. This installation guide describes how to install Qualys 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 requirements, installation steps, proxy configuration, updating, and uninstallation of Qualys Cloud Agent for AWS Bottlerocket Container host.

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 is 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 AWS Bottlerocket Container Host

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

A few things to consider...

Check the following steps, before installing Qualys Cloud Agent on AWS Bottlerocket Container host.

Cloud Agent requirements

- Your agent hosts must be able to reach Qualys Cloud Platform (or the Qualys Private Cloud Platform) over HTTPS port 443. Login to the Qualys Cloud Platform and go to **Help > About** to see the URL your hosts need to access.

What are the installation steps?

Qualys Cloud Agent UI walks you through the steps to install Qualys Cloud Agents on your hosts. You might want to configure proxy settings for a Cloud Agent to communicate with Qualys Cloud Platform.

Need help with troubleshooting?

We recommend you inspect the Cloud Agent log files located in AWS Bottlerocket Container host.

In Admin container, Cloud Agent logs are available at:

```
/.bottlerocket/rootfs/var/log/qualys
```

In AWS Bottlerocket Container host, Cloud Agent logs are available at:

```
/var/log/qualys
```

Installation

This chapter explains the installation steps for Qualys Cloud Agent on AWS Bottlerocket Container host. The scope of the document includes prerequisites, Cloud Agent download procedure, installation steps, proxy configuration, updating Cloud Agent, and uninstalling Cloud Agent.

Qualys provides installers and packages for each supported operating system that are coded for each Qualys platform. It is not possible to connect a Cloud Agent coded for one platform to another platform. Organizations can also use the Puppet automation tool to install the Qualys Cloud Agent on AWS Bottlerocket Container host.

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

Customers using software distribution tools like Puppet, must package the Qualys-provided installer along with the associated Activation Key and Customer ID 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 re-provision.

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 need an agent activation key to install Qualys Cloud Agent. 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 is automatically assigned to agent hosts. This helps you manage your agents and report on agent hosts.

Running the agent installer You have 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 applications - Vulnerability Management (VM). Activating an agent for a application consumes an agent activation key. You can setup auto activation by defining applications for activation keys, or do it manually in the Qualys Cloud Agent UI.

What happens if you skip activation? Cloud Agents syncs only inventory information to the cloud platform (IP address, OS, DNS and NetBIOS names, MAC address) and host assessments is not performed.

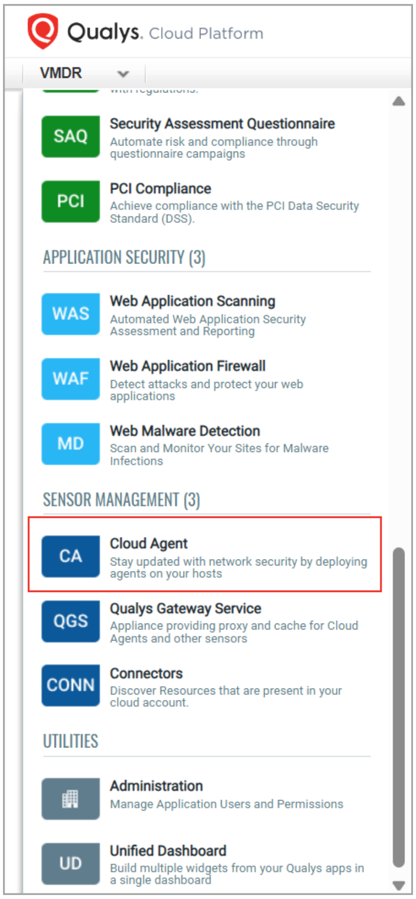
How many agents can I install? You can install any number of agents but can activate an agent only if you have an activation key. The **Agents** tab in the Cloud Agent UI shows your installed agents.

Check to be sure agents are connected Once installed agents connect to the Qualys Cloud Platform and provisions themselves. You can see agent status on the **Agents** tab in Cloud Agent UI- this is updated continuously. If your Cloud Agent does not have a status, this means that your agent is not successfully connected to the Qualys Cloud Platform and you need to troubleshoot.

How to Download Agent Installer

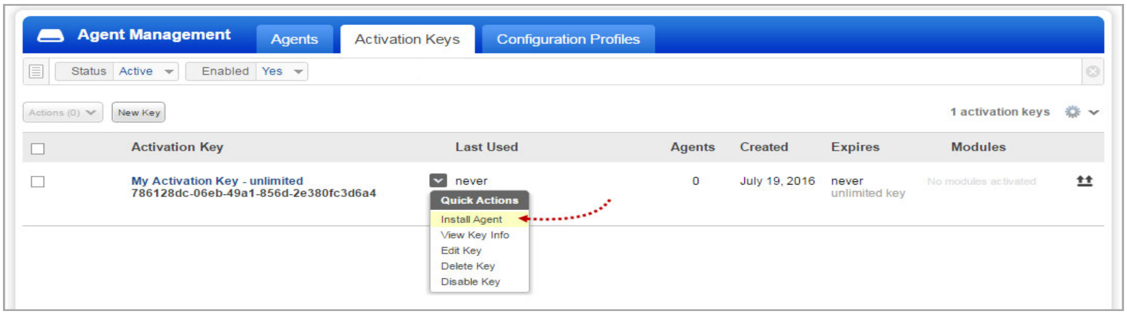
This section describes how to download a Qualys Cloud Agent installer from the Qualys Cloud Platform and get the associated Activation ID and Customer ID.

Login to the Qualys Cloud Platform and click **Cloud Agent** from application list to open Cloud Agent application.


Qualys. Cloud Platform
VMDR
SAQ
Security Assessment Questionnaire
Automate risk and compliance through questionnaire campaigns
PCI
PCI Compliance
Achieve compliance with the PCI Data Security Standard (DSS).
APPLICATION SECURITY (3)
WAS
Web Application Scanning
Automated Web Application Security Assessment and Reporting
WAF
Web Application Firewall
Detect attacks and protect your web applications
MD
Web Malware Detection
Scan and Monitor Your Sites for Malware Infections
SENSOR MANAGEMENT (3)
CA
Cloud Agent
Stay updated with network security by deploying agents on your hosts
QGS
Qualys Gateway Service
Appliance providing proxy and cache for Cloud Agents and other sensors
CONN
Connectors
Discover Resources that are present in your cloud account.
UTILITIES
Administration
Manage Application Users and Permissions
UD
Unified Dashboard
Build multiple widgets from your Qualys apps in a single dashboard

On Cloud Agent UI, click **Agent Management** > **Activation Keys**.

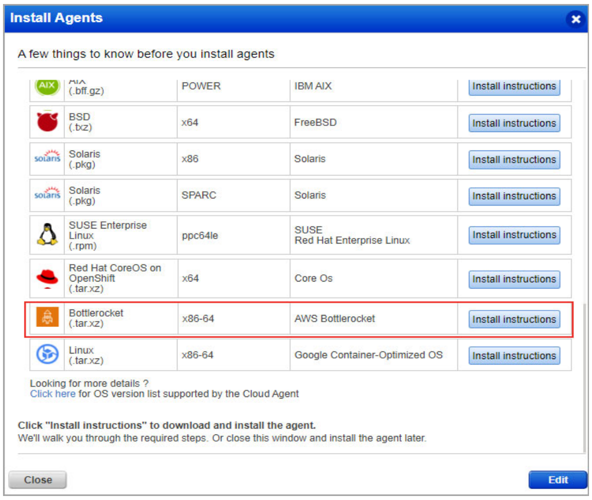
Select an activation key and in **Quick Actions** menu of the key, click **Install Agent**.



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

Note: If no activation key is available, then create new key using the **New Key** option available on **Activation Keys** tab in Cloud Agent UI.

On **Install Agents** window, click **Install Instruction** for the Bottlerocket OS.



A few things to know before you install agents

AIX (.bff.gz)	POWER	IBM AIX	Install instructions
BSD (.txz)	x64	FreeBSD	Install instructions
Solaris (.pkg)	x86	Solaris	Install instructions
Solaris (.pkg)	SPARC	Solaris	Install instructions
SUSE Enterprise Linux (.rpm)	ppc64le	SUSE Red Hat Enterprise Linux	Install instructions
Red Hat CoreOS on OpenShift (.tar.xz)	x64	Core Os	Install instructions
Bottlerocket (.tar.xz)	x86-64	AWS Bottlerocket	Install instructions
Linux (.tar.xz)	x86-64	Google Container-Optimized OS	Install instructions

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

Click "Install instructions" to download and install the agent.
We'll walk you through the required steps. Or close this window and install the agent later.

What happens? The Agent installer is downloaded to your local system, and the Cloud Agent UI gives the associated Activation key ID and Customer ID - copy and paste these details to a safe place, as you have to provide these details to complete the installation.

Installation steps

What is Needed for Installation

To install cloud agents, you have to download the Qualys Cloud Agent installer and get the associated ActivationID and CustomerID. To get the Cloud Agent installer, login to the Qualys Cloud Platform, go to the Cloud Agent (CA) application, and follow the installation steps for Qualys Cloud Agent for AWS Bottlerocket Container host (.tar.xz) to get everything you need.

Note: The Qualys Cloud Agent for AWS Bottlerocket Container host is supported only on Intel architecture; do not install these cloud agents on other architectures or platforms.

Prerequisites

To install Qualys Cloud Agent on AWS Bottlerocket Container host, you need a host system (jump host) which can communicate with AWS Cluster and has the following tools:

- AWS Account with AWS CLI and Amazon Elastic Kubernetes Service (EKS) access.

- Amazon Elastic Container Registry (Amazon ECR) to upload Qualys Cloud Agent installer.

- Kubectl for communicating with Kuberenetes control plane. It allows you to perform every Kubernetes operation.

- Docker Application

- eksctl a simple CLI, for creating and managing clusters on EKS.

Note: You can use any repository supported by AWS EKS to push the Qualys Cloud Agent image. The installation process for Qualys Cloud Agent on AWS Bottlerocket Container host is same.

For example, AWS ECR repository, Docker hub, Oracle Cloud Infrastructure Registry, and so on.

Steps to Install Agents

Use the following steps to install Qualys Cloud Agent on your AWS Bottlerocket container host:

1. Download the Qualys Cloud Agent installer (tar.xz) for AWS Bottlerocket container host from Qualys Cloud Platform. Refer to How to Download Agent Installer.

2. Extract the downloaded Qualys Cloud Agent file on your jump host, using the following command:

```
tar -xvf <qualys-cloud-agent-installer>
```

For example,

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

3. Load the extracted Cloud Agent image to the jump host using following command.

```
docker load -i <qualys-cloud-agent-image>
```

For example,

```
docker load -i QualysCloudAgent.tar
```

4. Login to the ECR repository using following command.

```
aws ecr get-login-password --region <region> docker login --
username AWS --password-stdin <ECR repository url>
```

For example,

```
aws ecr get-login-password --region us-east-1 | docker login --
username AWS --password-stdin 123456789012.dkr.ecr.us-east-
1.amazonaws.com
```

5. Tag the extracted Qualys Cloud Agent image to ECR repository using the following command.

```
docker tag <Image Name/ID>: <Tag Name> <ECR repository url>/<repo
name>: <Tag Name>
```

For example,

```
docker tag qualys/linux-cloud-agent:1.2.123-4
123456789012.dkr.ecr.us-east-1.amazonaws.com/<local repo>:1.2.123-
4
```

6. Push the Cloud Agent image to ECR repository using the following command.

```
docker push <ECR repository url> <repo name>: <Tag Name>
```

For example,

```
docker push 123456789012.dkr.ecr.us-east-1.amazonaws.com/<local
repo>:1.2.123-4
```

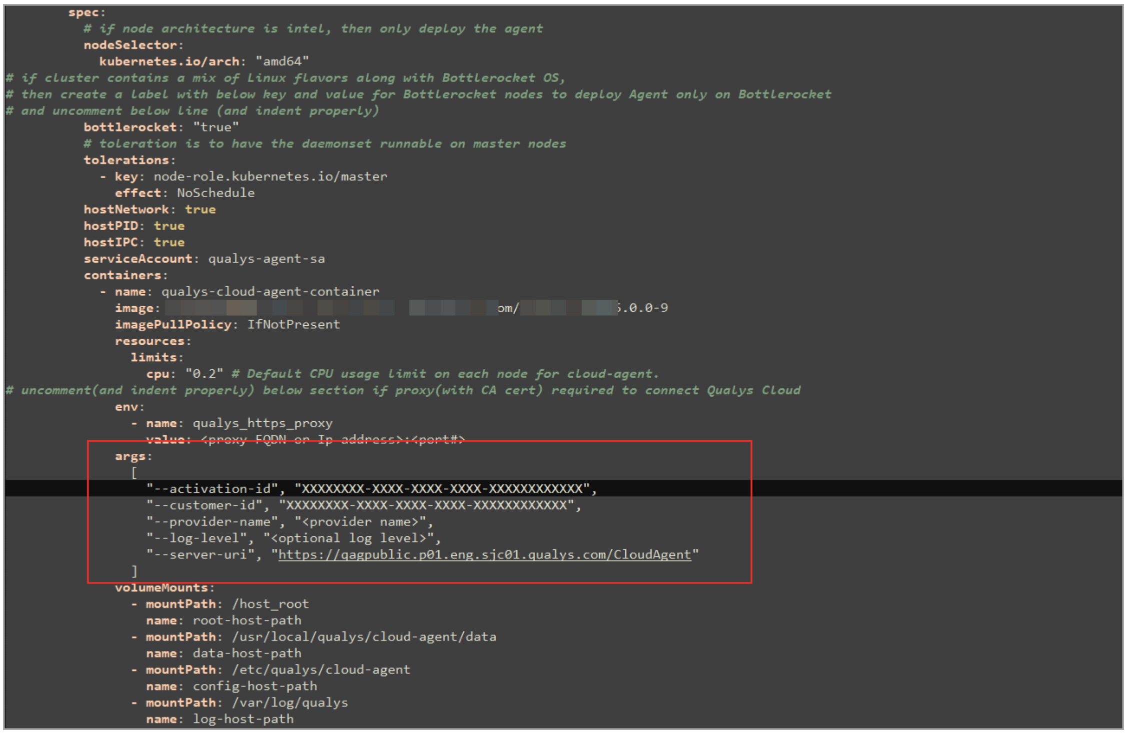
7.Open the `.yml` file in jump host and update with the following parameters:

Parameter	**Description**
activation-id	activation-id for the Qualys Cloud Agent for AWS Bottlerocket container host, auto-generated based on your subscription.
customer-id	Qualys subscription’s customer -id, auto-generated based on your subscription.
server-uri	https://qagpublic.qg1.apps.qualys.com/CloudAgent This server uri is associated with the activation key for your Cloud Agent installer.

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, the host does not check for the provider. If you provide 'AUTO' value, the host auto checks the provider.
log-level	Configuration to set the logging level for Qualys Cloud Agent for Linux AWS Bottlerocket. Default value for this parameter is 3. You can set the log level value up to 5.
image	The path for your Qualys Cloud Agent image on ECR repository.
Proxy (Optional)	IPv4 address or FQDN of the proxy server.
CPU (Optional)	(Optional) CPU usage limit in percentage for Cloud Agent. A valid range is 0-100 and the default value is 0.2.

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

Sample `.yml` configuration:



```
    spec:
     # if node architecture is intel, then only deploy the agent
     nodeSelector:
      kubernetes.io/arch: "amd64"
# if cluster contains a mix of Linux flavors along with Bottlerocket OS,
# then create a label with below key and value for Bottlerocket nodes to deploy Agent only on Bottlerocket
# and uncomment below line (and indent properly)
     bottlerocket: "true"
     # toleration is to have the daemonset runnable on master nodes
     tolerations:
      - key: node-role.kubernetes.io/master
       effect: NoSchedule
     hostNetwork: true
     hostPID: true
     hostIPC: true
     serviceAccount: qualys-agent-sa
     containers:
      - name: qualys-cloud-agent-container
       image: [redacted]om/[redacted].0.0-9
       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", "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
         "--customer-id", "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
         "--provider-name", "<provider name>",
         "--log-level", "<optional log level>",
         "--server-uri", "https://qagpublic.p01.eng.sjc01.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
         name: log-host-path
```

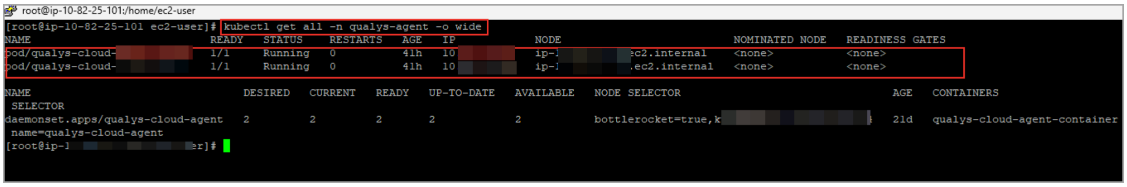
8. Deploy the updated `.yml` file using following command to install the Qualys Cloud Agent on AWS Bottlerocket container host.

```
kubectl apply -f qualys-cloud-agent-deploy.yml
```

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

```
kubectl get all -n qualys-agent -o wide
```

The Cloud Agent running status is displayed on the screen.



root@ip-10-82-25-101:/home/ec2-user

```
[root@ip-10-82-25-101 ec2-user]# kubectl get all -n qualys-agent -o wide
NAME                              READY   STATUS    RESTARTS   AGE   IP            NODE                              NOMINATED NODE   READINESS GATES
pod/qualys-cloud-[redacted]       1/1     Running   0          41h   10[redacted]  ip-1[redacted]ec2.internal        <none>           <none>
pod/qualys-cloud-[redacted]       1/1     Running   0          41h   10[redacted]  ip-1[redacted].ec2.internal       <none>           <none>

NAME                                DESIRED   CURRENT   READY   UP-TO-DATE   AVAILABLE   NODE SELECTOR                   AGE   CONTAINERS
 SELECTOR
daemonset.apps/qualys-cloud-agent   2         2         2       2            2           bottlerocket=true,k[redacted]   21d   qualys-cloud-agent-container
 name=qualys-cloud-agent
[root@ip-1[redacted]er]#
```

When the Cloud Agent instance is started, it activates the Qualys Cloud Agent which provisions itself and start functioning as expected.

What happens next?

Qualys Cloud Agent start syncing asset data to the Qualys Cloud Platform!

Once installed, the Qualys Cloud Agent connects to the Qualys Cloud Platform and provisions itself. You can see your first asset discovery results within a few minutes. The first assessment scan in the Qualys Cloud Platform takes some time, after that scans complete as soon as new host metadata is uploaded to the Qualys Cloud Platform.

Install Cloud Agent in Multi-OS Environment

Qualys Cloud Agent for AWS Bottlerocket Container host is currently supported only on Intel platform. Perform the following steps to install the Cloud Agent in a cluster where multiple OS/architecture nodes are present along with AWS Bottlerocket Intel node.

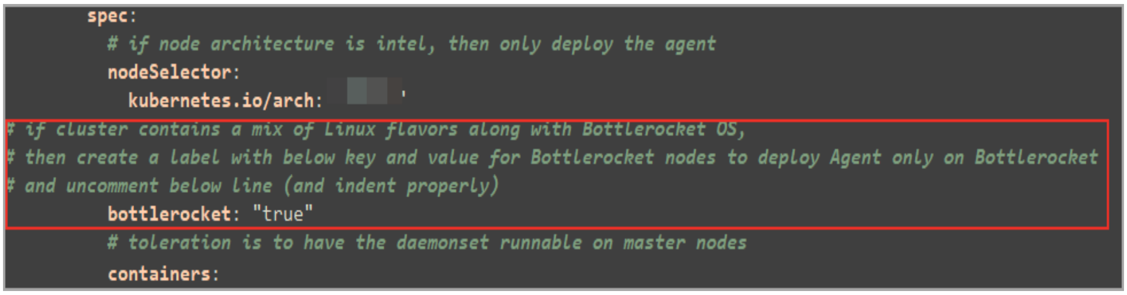
1. Add the label to the AWS Bottlerocket node with the Intel arechitecture using the following command.

```
kubectl label nodes <node-name1> <node-name2> <node-name3>
<label-name>=<label-value>
```

For example,

```
kubectl label nodes ip-12-34-56-78.ec2.internal ip-87-65-43-
21.ec2.internal bottlerocket=true
```

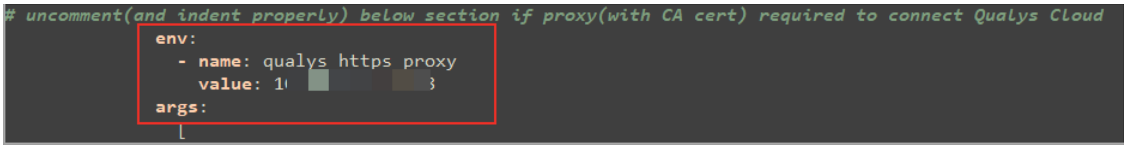
2. Access the `.yml` file associated with the Qualys Cloud Agent you want install and uncomment the label name and label value line. Refer to the following snippet.



```
        spec:
          # if node architecture is intel, then only deploy the agent
          nodeSelector:
            kubernetes.io/arch: [redacted]
# if cluster contains a mix of Linux flavors along with Bottlerocket OS,
# then create a label with below key and value for Bottlerocket nodes to deploy Agent only on Bottlerocket
# and uncomment below line (and indent properly)
          bottlerocket: "true"
          # toleration is to have the daemonset runnable on master nodes
          containers:
```

Proxy Configuration

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



```
# uncomment(and indent properly) below section if proxy(with CA cert) required to connect Qualys Cloud
              env:
                - name: qualys_https_proxy
                  value: [redacted]
              args:
                [
```

Provide the proxy name and proxy value for your network.

Following parameters are optional for proxy configuration.

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 AWS Bottlerocket Container host tries to connect to the server with given https Proxy settings only. If only ProxyCertFile is provided without proxy, then Qualys Cloud Agent for AWS Bottlerocket container host ignores the ProxyCertFile and it tries to connect to the server without any https proxy settings.

Multiple Proxy Server Support in Proxy URL

The Cloud Agent has support for multiple proxy servers defined in the Proxy URL. You can have up to five proxy servers included in the proxy URL.

Each time the Cloud Agent connects to the Qualys Cloud Platform, it always uses the first proxy server in the ordered list.

If the connection using the first proxy server fails, the Cloud Agent tries to the next configured proxy in case of http failures. If the connections using all the configured proxies fail, the Cloud Agent attempts a direct connection to the Qualys Cloud Platform.

You can use a configuration tool to the set the proxy order to be sequential or random. The Cloud Agent does not maintain a history of last proxy server used.

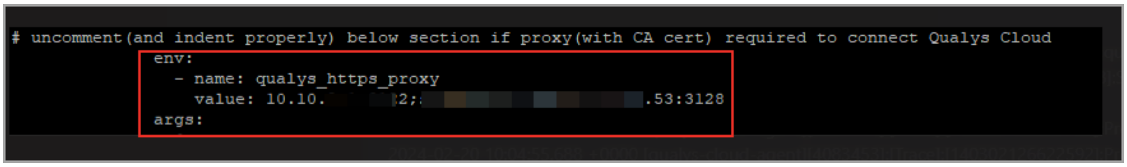
This proxy configuration can be used with the Qualys Gateway Service or third-party proxy servers. There is no requirement that the failover proxy servers need to be on the same subnet as the first proxy server as long as the Cloud Agent can connect to other proxy servers even on other subnets.

Multiple proxies can be configured with `qualys_https_proxy` or `https_proxy` environment variables. It is recommended that you provide multiple proxies in the `qualys_https_proxy` environment variable.

The following example shows how to set multiple proxies:

```
qualys_https_proxy=”https://[<username>:<password>@]<host1>:<port>;
https://[<username>:<password>@]<host2>:<port>;
https://[<username>:<password>@]<host3>:<port>”
```

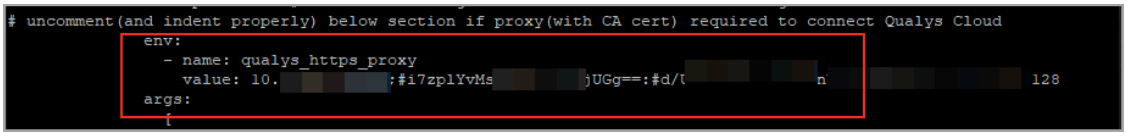
The following snippet shows the multiple proxies without encryption.



```
# uncomment(and indent properly) below section if proxy(with CA cert) required to connect Qualys Cloud
            env:
              - name: qualys_https_proxy
                value: 10.10.[redacted]2;[redacted].53:3128
            args:
```

The list of proxies must be given in double quotes (“...”) and separated by a semi-colon (;). If semicolon (;) is embedded in username/password, you must url-encode it. You can use the Proxy Configuration Encryption Utility to encrypt the user name and/or password that you provide to the proxy environment variable.

The following snippet shows the multiple proxies with encryption.



```
# uncomment(and indent properly) below section if proxy(with CA cert) required to connect Qualys Cloud
            env:
              - name: qualys_https_proxy
                value: 10.[redacted];#i7zplYvMs[redacted]jUGg==:#d/U[redacted]n[redacted]128
            args:
              [
```

You can combine multiple proxy certificates into a single file, and place it at same location as earlier `/etc/qualys/cloud-agent/cert/ca-bundle.crt`. Ensure that all certificates are valid, else you might get SSL/certificate errors.

Note: If you update the proxy settings, Cloud Agent must be restarted.

On Demand Scan

On Demand scan feature launch the immediate scan on agent host, if the agent host is not performing any scan on the same application. The On Demand Scan runs independently of the interval scan that you configure in the Configuration Profile and resets the scan interval on the agent after a successful scan.

Prerequisite: The Cloud Agent must be activated for the application for which you want to launch the On Demand Scan. When activated, the Agent downloads manifests for that application from the Qualys Cloud Platform. If the manifest for the application is not available, then Cloud Agent does not launch the scan.

Use the `cloudagentctl.sh` script to run the On Demand Scan. You can find this script at `/usr/local/qualys/cloud-agent/bin/`.

Following are the steps to run the On Demand Scan:

1. Get the list of instances running on the AWS Bottlerocket container host:

```
kubectl get all -n qualys-agent -o wide
```

2. Login to the AWS Bottlerocket container host and run the following command:

```
kubectl exec -it qualys-cloud-agent-<instance id> -n qualys-agent
-- /bin/bash
```

3. Run the following command to start the On Demand scan:

```
/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 the amount of CPU used for Cloud Agent execution. The higher the CPU throttle value less CPU is used at the expense of higher execution time. The range for CPU throttle is 0-1000. Default value is set at 0, which means no throttling.

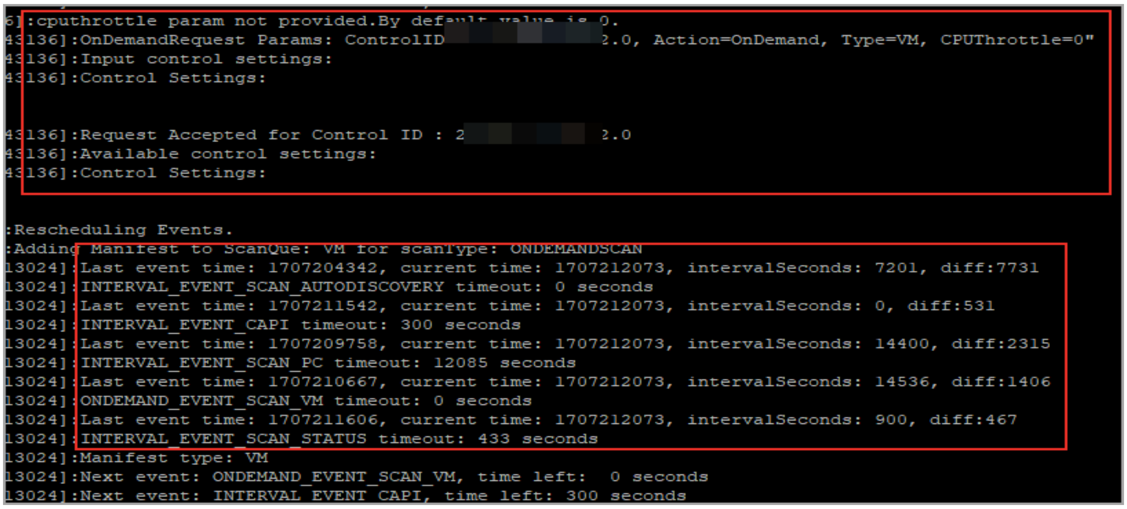
For example, to initiate an On Demand Scan for the Vulnerability Management application (VM) with no throttling:

```
/usr/local/qualys/cloud-agent/bin/cloudagentctl.sh action=demand
type=vm cputhrottle=0
```

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. For example, On-Demand-Request ControlId: 20240228164415.0.

The scan logs for On Demand Scans and Interval Scans are stored at same location. `/var/log/qualys/qualys-cloud-agent.log`

You can find the On-Demand Scan information in the following log file.



```
6]:cputhrottle param not provided.By default value is 0.
43136]:OnDemandRequest Params: ControlID[redacted]2.0, Action=OnDemand, Type=VM, CPUThrottle=0"
43136]:Input control settings:
43136]:Control Settings:


43136]:Request Accepted for Control ID : 2[redacted]2.0
43136]:Available control settings:
43136]:Control Settings:


:Rescheduling Events.
:Adding Manifest to ScanQue: VM for scanType: ONDEMANDSCAN
13024]:Last event time: 1707204342, current time: 1707212073, intervalSeconds: 7201, diff:7731
13024]:INTERVAL_EVENT_SCAN_AUTODISCOVERY timeout: 0 seconds
13024]:Last event time: 1707211542, current time: 1707212073, intervalSeconds: 0, diff:531
13024]:INTERVAL_EVENT_CAPI timeout: 300 seconds
13024]:Last event time: 1707209758, current time: 1707212073, intervalSeconds: 14400, diff:2315
13024]:INTERVAL_EVENT_SCAN_PC timeout: 12085 seconds
13024]:Last event time: 1707210667, current time: 1707212073, intervalSeconds: 14536, diff:1406
13024]:ONDEMAND_EVENT_SCAN_VM timeout: 0 seconds
13024]:Last event time: 1707211606, current time: 1707212073, intervalSeconds: 900, diff:467
13024]:INTERVAL_EVENT_SCAN_STATUS timeout: 433 seconds
13024]:Manifest type: VM
13024]:Next event: ONDEMAND_EVENT_SCAN_VM, time left:  0 seconds
13024]:Next event: INTERVAL_EVENT_CAPI, time left: 300 seconds
```

If the agent is currently performing an interval scan for the same application, the On Demand Scan waits for the currently running scan to finish. The script prints a log line with following status.

```
2024-02-28 15:11:36.474 [qualys-cloud-agent][9710]:[Information]:[123456789123456]:Interval Event of same type is in progress with state INTERVAL_EVENT_SCAN
2024-02-28 15:11:36.474 [qualys-cloud-agent][9710]:[Information]:[123456789123456]:OnDemand request for Control ID: 20240427151136.0 will be delayed.
```

If the script shows error that manifest file is not present, then check whether the Cloud Agent is activated for that particular application. If agent is activated but you still get manifest related errors , the agent may not have downloaded the manifest for that application. You can manually force a manifest download by deactivating and then reactivating the agent for that application from the Cloud Agent UI. If that does not 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 Qualys Cloud Agent Technical Whitepaper for additional documentation and best practices.

Updating Cloud Agent

1. Login in to the jump host.

2. Upload new Qualys Cloud Agent image in ECR repository and update the image download url in the `.yml` file.

3. Run the following command to delete a Cloud Agent using the old `.yml` file:

```
kubectl delete -f qualys-cloud-agent-deploy.yml
```

4. Apply the new `.yml` file to deploy updated Qualys Cloud Agent on AWS Bottlerocket container host.

```
kubectl apply -f qualys-cloud-agent-deploy.yml
```

Note: Qualys Cloud Agent for AWS Bottlerocket container host does not support the auto upgrading to the latest versions.

Uninstalling Cloud Agent

Uninstalling Cloud Agent from Cloud Agent UI or API

You can uninstall the Qualys Cloud Agent using the Cloud Agent UI or Cloud Agent API. When you uninstall a agent using UI or API, the Cloud Agent stops working but data and logs files associated with that Cloud Agent are not removed. Hence, you have to remove the data and log files associated with the Cloud Agent manually. Following are the steps to uninstall the cloud agent from AWS Bottlerocket Container host.

1. Login in to the jump host.

2. Run the following command to uninstall the Qualys Cloud Agent:

```
kubectl delete -f qualys-cloud-agent-deploy.yml
```

3. Login to the AWS Bottlerocket Container host.

4. Remove the Qualys Cloud Agent data and logs from AWS Bottlerocket container host available at following locations:

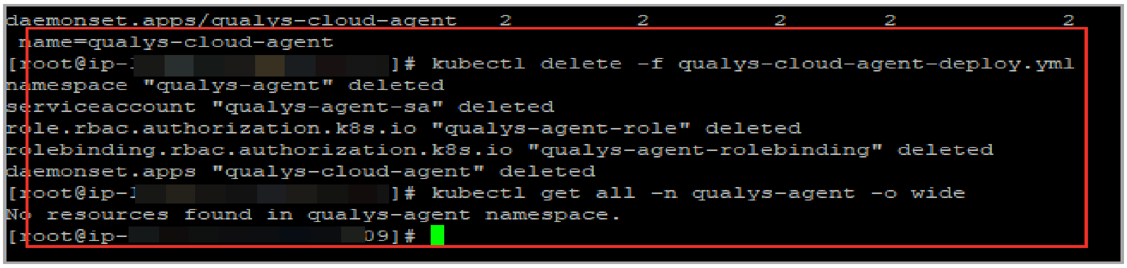
In Admin container, Cloud Agent logs are available at:

```
/.bottlerocket/rootfs/var/log/qualys
```

In AWS Bottlerocket Container host, Cloud Agent logs are available at:

```
/var/log/qualys
```

The following image shows the Cloud Agent status after uninstallation.



```
daemonset.apps/qualys-cloud-agent   2         2          2        2            2
 name=qualys-cloud-agent
[root@ip-[redacted]]# kubectl delete -f qualys-cloud-agent-deploy.yml
namespace "qualys-agent" deleted
serviceaccount "qualys-agent-sa" deleted
role.rbac.authorization.k8s.io "qualys-agent-role" deleted
rolebinding.rbac.authorization.k8s.io "qualys-agent-rolebinding" deleted
daemonset.apps "qualys-cloud-agent" deleted
[root@ip-[redacted]]# kubectl get all -n qualys-agent -o wide
No resources found in qualys-agent namespace.
[root@ip-[redacted]09]#
```

Proxy Configuration Encryption Utility

You can use the Proxy Configuration Encryption utility to encrypt the user name and/or password 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 this utility.

If you encrypt the credentials for a system using **string-util**, the encryption setting is applied to all the systems using same credentials.

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

```
qualys_https_proxy=https://[<#encrypted_username>:<#encrypted_pass
word>@]<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 (Encrypting password):

```
qualys_https_proxy=https://sys_account:#sRpSHQP582a1+gaJwHOm3g==@p
roxy.myco.com:8080
```

For example (Encrypting username and password):

```
qualys_https_proxy=https://#uWpsHMSY932b2+fdcH723d==:#sRpSHQP582a1
+gaJwHOm3g==@proxy.myco.com:8080
```