How To - CI/CD with Qualys

What does Qualys offer?

Qualys is an award-winning cloud security and compliance solution. It helps businesses simplify IT security operations and lower the cost of compliance by delivering critical security intelligence on demand and automates the full spectrum of auditing, compliance and protection for Internet perimeter systems, internal networks, and web applications.

The Qualys Cloud Platform and its integrated suite of security and compliance solutions provides organizations of all sizes with a global view of their security and compliance solutions, while drastically reducing their total cost of ownership. Qualys solutions include: continuous monitoring, vulnerability management, policy compliance, PCI compliance, security assessment questionnaire, web application scanning, web application firewall, and more.

What is Vulnerability Management?

Qualys VM is a cloud service that gives you immediate, global visibility into where your IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps you to continuously secure your IT infrastructure and comply with internal policies and external regulations. Qualys VM checks your servers, computers and other devices for vulnerabilities and helps you identify the patches you need to download to fix them. It keeps track of the security problems it finds for each system, and provides graphical reports that tell you which patches to use on which systems so that you can get the most improvement in security for the least effort.

What is Vulnerability Assessment?

Vulnerability Assessment (VA) is an integral component of vulnerability management. VA is the process of identifying network and device vulnerabilities before hackers can exploit them.

What is Continuous Monitoring?

Qualys Continuous Monitoring (CM) is a next-generation cloud service that gives you the ability to identify threats and unexpected changes in your Internet perimeter before they turn into breaches with realtime scanning. With CM you can track what happens within Internet-facing devices throughout your DMZs and cloud environments – anywhere in the world. It detects changes in your perimeter that could be exploited and immediately notifies the IT staff responsible for the affected assets so they can take appropriate action. It lets you easily configure rules and alerts so you can know and react as soon as something changes on your network.

What is Web Application Scanning?

Qualys Web Application Scanning (WAS) is a cloud service that provides automated crawling and testing of custom web applications to identify vulnerabilities including cross-site scripting (XSS) and SQL injection. The automated service enables regular testing that produces consistent results, reduces false positives, and easily scales to secure large number of websites. Proactively scans websites for malware infections, sending alerts to website owners to help prevent black listing and brand reputation damage.

What is Policy Compliance?

Qualys Policy compliance (PC) is a cloud service that performs automated security configuration assessments on IT systems throughout your network. It helps you to reduce risk and continuously comply with internal policies and external regulations by providing proof of compliance demanded by auditors across multiple compliance initiatives. Qualys Policy Compliance automates the collection of technical controls from information assets within the enterprise; and provides compliance reporting by leveraging a comprehensive knowledgebase that is mapped to prevalent security regulations, industry standards and compliance frameworks.

What is PCI?

Qualys PCI Compliance (PCI) provides businesses, online merchants and Member Service Providers the easiest, most cost-effective and highly-automated way to achieve compliance with the Payment Card Industry Data Security Standard. Known as PCI DSS, the standard provides organizations the guidance they need to ensure that credit cardholder information is kept secure from possible security breaches.

Is Qualys a software product or a service?

Qualys' Software-as-a-Service (SaaS) delivery model, allows users to access Qualys from any Web browser. This unique SaaS platform enables organizations to assess and manage its security exposures freeing them from the substantial cost, resource and deployment issues associated with traditional software products. Qualys is capable of managing Internet exposed vulnerabilities as well as vulnerabilities found on hosts that are not directly accessible from the Internet.

For those entities that want an on-premise solution, Qualys offers MSSPs, enterprises and government agencies our award-winning security and compliance solutions as a private cloud from your own data center where you retain full control of all the underlying security data. The Private

Cloud Platform combines the virtualized Qualys software with a self-contained, internally-redundant cloud appliance. The platform comes pre-configured for your environment, for fast deployment. Because it runs in the cloud, we can scale Qualys as your needs grow. We just add more capacity to meet the scanning, analysis and reporting needs of your business.

Is Qualys host-based or network-based?

Qualys is a cloud-based solution that detects vulnerabilities on all networked assets, including servers, network devices (e.g. routers, switches, firewalls, etc.), peripherals (such as IP-based printers or fax machines) and workstations. Qualys can assess any device that has an IP address. Qualys works both from the Internet to assess perimeter devices as well as from the inside of your network, to assess risk from an internal perspective, using secure, hardened Qualys Scanner Appliances.

My company already deployed firewalls, Intrusion Detection Systems (IDS), and other security solutions. Why do we need vulnerability management?

Qualys complements your firewalls, intrusion detection, antivirus, and other security solutions by providing a proactive, preventive approach to network security. Firewalls often permit threats and vulnerabilities, such as worms and viruses, to traverse un-trusted networks, such as the Internet, to your internal network. As worms get more intelligent, we will continue to see firewalls become an antiquated defense. Intrusion detection systems have already been deemed "yesterday's security tool," as they are reactive, "after the fact" technologies, much like antivirus solutions.

Qualys is a proactive solution, which informs you of known vulnerabilities in your infrastructure. Qualys can even tell you if you are vulnerable to a new exposure before you perform a scan!

My company recently performed an annual security audit with the help of a consulting firm. Why do I need Qualys?

In the past, scanning your networks once a year or once a quarter was sufficient. However, with the average time between vulnerability detection and exploitation diminishing each year, annual audits are no longer frequent enough. With Qualys you can fully automate security assessments and reduce the time between audits from yearly or quarterly, to monthly, weekly or, even daily. You can decide how often a vulnerability assessment is required; varying from device to device, from network to network. Scans can be scheduled or performed on demand. Also, with the Qualys subscription, customers are entitled to an unlimited number of scans. Most customers schedule weekly scans and conduct on demand scans after a security policy change, or on a new device before it is deployed into a production environment.

How often is the vulnerability database updated?

Qualys updates its vulnerability database with multiple vulnerability checks each day, as new vulnerabilities emerge. An average of 20 new signature updates are delivered each week. We maintain the industry's largest, most comprehensive and up-to-date Vulnerability Knowledge Base. Our CVE-compliant Knowledge Base contains more than 35,000 checks.

How do I know that the vulnerability database is up-to-date?

Qualys engineers develop vulnerability signatures every day in response to emerging threats. As soon as these signatures pass rigorous testing in the Qualys Quality Assurance Lab they are automatically made available to you for your next scheduled or on demand scan. No user action is required. In addition, as a part of the Qualys service, you can sign up to receive daily or weekly vulnerability signature update emails, detailing the new vulnerabilities Qualys is capable of detecting.

What is the service availability for Qualys?

Qualys is available 24x7x365 and can be accessed anytime from anywhere through a Web browser. Qualys consistently maintains 99% availability. The service is constantly updated transparently, without any interruption to users, and is only taken off-line once a quarter for maintenance and updates. This process usually lasts a few hours in duration.

What does Qualys do to protect my data?

Stored data is kept in an encrypted format. Qualys encrypts each users' data uniquely, so that only the user who created the data can access it. Qualys has no insight into customer data. In fact, Qualys does not have access to the encryption key, so Qualys has no ability to decrypt the stored data.

The Qualys Cloud Platform resides behind network-based, redundant, highly-available firewalls and intrusion monitoring solutions. In addition, each host runs a localized firewall on top of the customized, hardened Linux distribution, which is unique to Qualys.

The Qualys Cloud Platform is hosted in a data center that is subject to at least an annual SSAE 16 or industry standard alternative audit by an internationally-recognized accounting firm. All Qualys devices are located in physically secure, dedicated, locked cabinets protected by multiple-factor authentication, including biometrics.

More information

Our company is expanding internationally. Is Qualys restricted to the U.S. only?

Qualys is a global company and our users are capable of assessing any network or system anywhere in the world. If the device resides on the Internet, Qualys uses the Security Operations Center (SOC) that is geographically closest to the device, in order to minimize latency and congestion. Organizations can choose to deploy secure, hardened Qualys scanner appliances throughout their enterprise in any country in the world. We currently support 3 SOCs – in the United States and Europe.

Additionally, Qualys has support staff in the U.S., EMEA, India and Japan as well as sales staff around the world to help service global enterprises 24x7x365.

What happens if my network experiences rapid growth, for example through an acquisition?

Qualys scales virtually infinitely with an organization's network growth. You can easily add or remove IP addresses to your account by contacting your account manager or Qualys Support.

What type of company is typically in need of Qualys?

Qualys, via its unique Software-as-a-Service (SaaS) model, addresses the security scanning needs of customers across multiple segments, including the majority of the Fortune 500 and Forbes Global 2000 as well as, small to medium businesses, consultants and managed service providers. Regardless of the environment, the scalable, secure end-to-end solution is unchanged.

Can I use Qualys and pay as I go?

Yes. There are "pay per scan" packages available for Qualys. It is recommended, however, that any organization that is setting out to secure their enterprise choose the annual subscription service.

Where can I find product documentation and release notes?

Both are available online: product documentation and release notes.

Subscriptions

Small businesses	Mid-sized businesses	Enterprise
See all your security and compliance needs in one place.	Powerful and scalable cloud-based solution for security and compliance.	Powerful, globally scalable, and highly customizable.
Learn more	Learn more	Learn more
≤ 256 IPs for scans	≤ 5,120 IPs for scans	Unlimited IPs for scans
≤ 25 web apps for scans	≤ 200 web apps for scans	Unlimited web apps for scans
≤ 2 scanners	≤ 5 scanners	Unlimited scanners
≤ 3 users	Unlimited users	Unlimited users
	Remediation ticketing & tracking	Remediation ticketing & tracking
	Integration with public clouds	Integration with public clouds

Plugins installed to achieve CI/CD with Qualys

Please download the container security plugin from Qualys website (link below) and upload it using Jenkins.

https://qualysguard.qg1.apps.qualys.in/cs/#/configurations/integrations

☑	Qualys API Security Plugin Provides a build step to run static Assessment on API using the Qualys API Security service.	1.0.0
☑	Qualys Container Security Plugin This Plugin allows you to get the security posture for the docker images built in Jenkins and visualize it.	1.6.0.1
☑	Qualys VM Plugin Provides a post-deploy step to run a vulnerability scan using the Qualys Vulnerability Management (VM) service.	1.0.0
☑	Qualys WAS Plugin Provides a post-deploy step to run a vulnerability scan using the Qualys Web Application Scanning (WAS) service.	2.0.4

List of All Qualys Developed Integrations

Product	Documentation	GA Supported Modules
splunk>	User Guide Splunkbase Apps	Vulnerability Management (VM) Policy Compliance (PC) Web Application Scanning (WAS) Container Security (CS)
servicenow	User Guide Community Guide ServiceNow App Store	Qualys Asset Inventory CMDB Sync (New) Qualys CMDB Sync App (Legacy)
Jenkins	WAS Integration Guide CS Integration Guide VM - Please contact your TAM	Web Application Scanning (WAS) Container Security (CS) Vulnerability Management (VM) - Beta Release
Bamboo	User Guide	Container Security (CS)
Radar	User Guide App Exchange	Vulnerability Management (VM)
CI/CD Shell Script	Github & Tutorial	Container Security (CS)
BURPSUITE PROFESSIONAL	User Tutorial Blog Post	Web Application Scanning (WAS)
Qualys Browser Recorder	User Guide Download	Web Application Scanning (WAS)
bugcrowd	Qualys User Guide Bugcrowd User Guide Integration Video Integration Data Sheet	Web Application Scanning (WAS)
amazon web services	User Guide AWS Marketplace Marketing Overview	Vulnerability Management (VM) Qualys Cloud Agents (QCA) Policy Compliance (PC) Security Configuration Assessment (SCA) Web Application Scanning (WAS) Web Application Firewall (WAF)
Azure	User Guide Marketing Overview	Vulnerability Management (VM) Qualys Cloud Agents (QCA)
Google Cloud Platform	User Guide Marketing Overview	Vulnerability Management (VM) Qualys Cloud Agents (QCA)

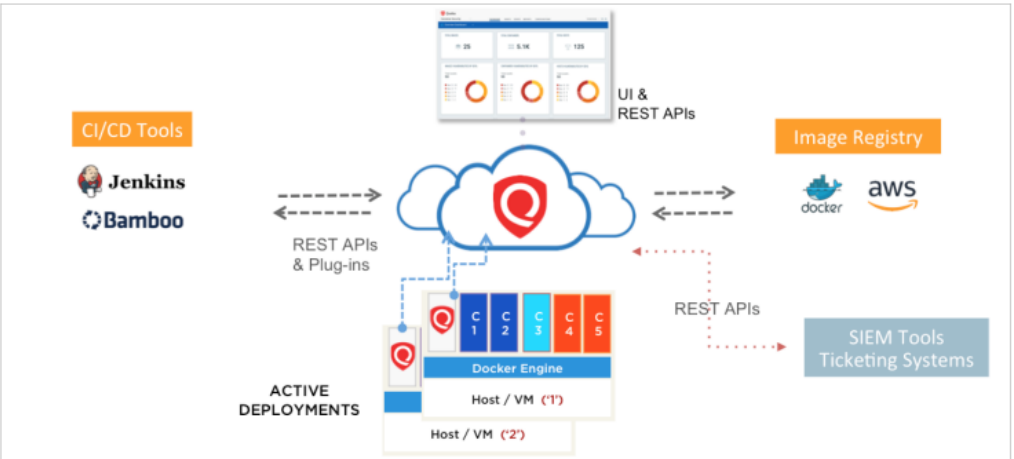
Qualys Vulnerability Analysis with Jenkins (Using Jenkins plugins provided by Qualys)

Using this Jenkins plugin, we can achieve

1. Container Security.
2. Discovery and Vulnerability Security Scanning.
3. Web Application Security Scanning.

Container Security Overview

Qualys Container Security provides discovery, tracking, and continuously protecting container environments. This addresses vulnerability management for images and containers in their DevOps pipeline and deployments across cloud and on-premise environments.



With this version, Qualys Container Security supports

- Discovery, inventory, and near-real time tracking of container environments

- Vulnerability analysis for images and containers

- Vulnerability analysis for registries

- Integration with CI/CD pipeline using APIs (DevOps flow)

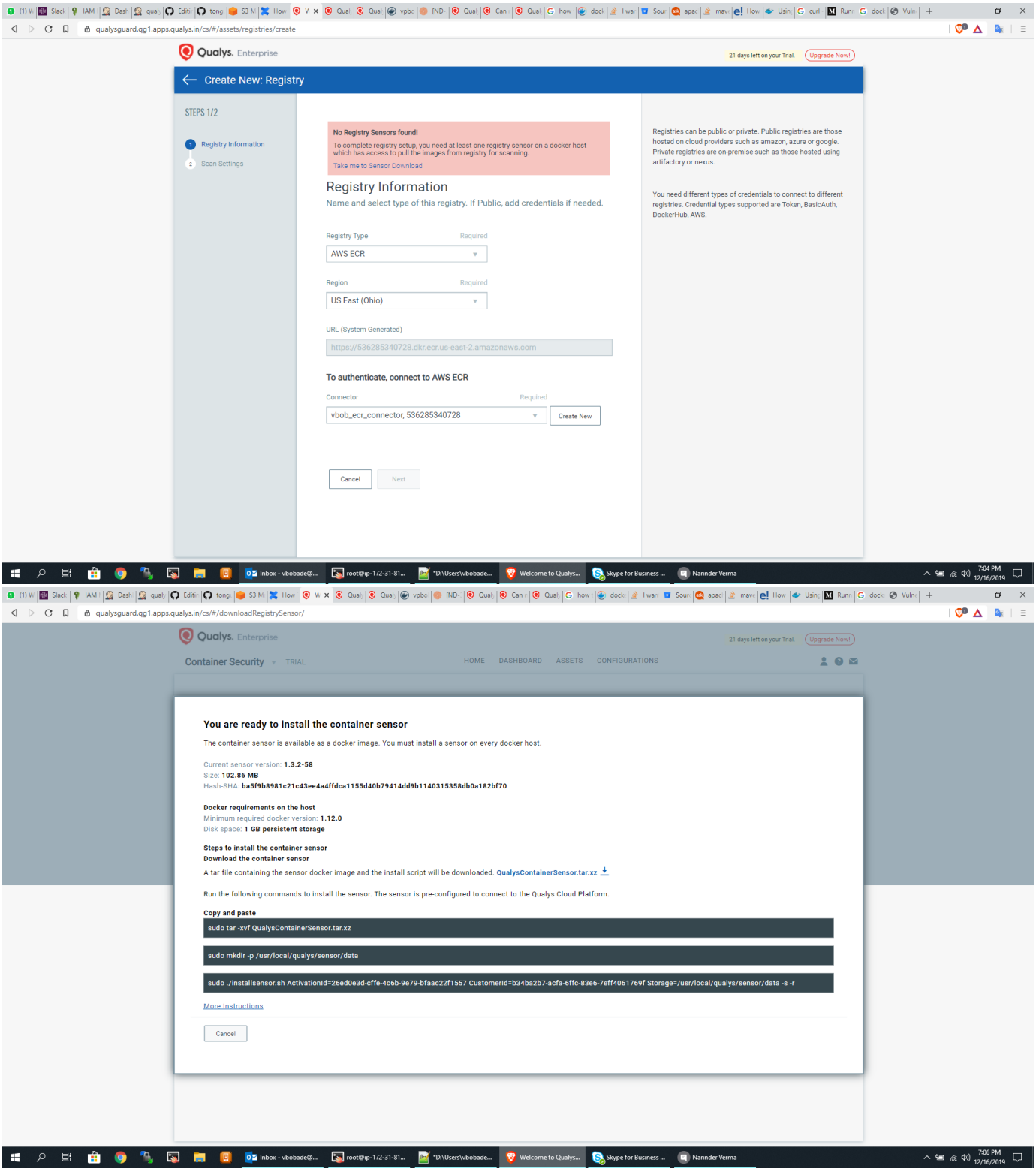
- Uses new 'Container Sensor' – providing native container support, distributed as docker image

Upon installation, the sensor does automatic discovery of Images and Containers on the deployed host, provides a vulnerability analysis of them, and additionally it monitors and reports on the docker related events on the host. The sensor lists and scans registries for vulnerable images. The sensor container runs in non-privileged mode. It requires a persistent storage for storing and caching files.

Currently, the sensor only scans Images and Containers. For getting a vulnerability posture on the Host, you would require Qualys Cloud Agents or a scan through Qualys Virtual Scanner Appliance.

Registry scanning -

To enable registry scanning for vulnerabities it is mandatory to install the Qualys agent on the docker host - below snapshot is occurred when we tried to create registry.



For more details on how to achieve continuous integration using Qualys please refer to the below document.

https://www.qualys.com/docs/qualys-vulnerability-analysis-jenkins-plugin-guide.pdf

CI & CD Approach 1

We are able to build our application using maven build tool > building its docker image > pushing that image to ECR. However since we are using containerized Jenkins here we are unable to install Qualys agent on (docker) host using our Jenkinsfile so its blocking here. To create registry to scan docker images in ECR - it is mandatory to install this Qualys agent on the docker host.The initial draft of Jenkinsfile for this approach is

mentioned below:

```
pipeline {
     agent any
     stages {
   stage ("git checkout") {
            steps {
                git ('https://github.com/vpbobade/demo-java')
            }
        }

        stage ("Checkout to different branch") {
            steps {
                sh "git branch -r"
                sh "git checkout master"
            }
        }

        stage ("package stage") {
            steps {
    sh "${tool name: 'maven', type:'maven'}/bin/mvn package"
    sh "bin/build"

     //def dockerHome = tool 'myDocker'
     //env.PATH = "${dockerHome}/bin:${env.PATH}"
     //docker build -t vpbobade/mydemojava:1.0.0 .
            }
        }
  stage ("Deploying Qualys sensor on docker host") {
   steps {
    script {
     sshagent(['ssh_vbob']) {
      sh 'chmod -R 775 qualys_install.sh'
      sh 'sh qualys_install.sh'
       }
                }
            }
        }

        stage ("Building docker image") {
//Build the docker image with a tag (qualys:sample in this case)
   steps {
    script {
     docker.withTool('myDocker') {

docker.withRegistry('https://536285340728.dkr.ecr.us-east-1.amazonaws.co
m','ecr:us-east-1:vbob_aws') {
       //docker.build("${config.ImageName}:${config.ImageVersion}",
"$WORKSPACE/first-stash")
       docker.build('vbob_qualys')
```

```
//docker.image("${config.ImageName}:${config.ImageVersion}").push()
        docker.image('vbob_qualys').push('latest')
     sh "echo 'further work in progress......'"

     }
    }
   }
  }
 }

       //sh "docker build -f Dockerfile -t vpbobade/mydemojava:1.0.0 . >
docker_out"
    //sh "./make_docker_image.sh"
    //docker.build registry


/*
  stage ('Push Docker image to DockerHub') {
   steps {
    withCredentials([usernamePassword(credentialsId: 'mydocker',
passwordVariable: 'pass', usernameVariable: 'user')]) {
          sh "docker login -u ${user} -p ${pass}"
    }
                sh 'docker push vpbobade/mydemojava:1.0.0'
            }
        }


  stage ('Get Image id') {
//Use the same repo:tag (qualys:sample in this case) combination with
the grep command to get the same image id and save the image id in an
environment variable
   steps {
    script {
     //def IMAGE_ID = sh(script: "docker images | grep -E
'^vbob_qualys/mydemojava:*' | head -1  | awk '{print \$3}'",
returnStdout:true).trim()
     //env.IMAGE_ID = IMAGE_ID
     //def IMAGE_ID = sh ()
    }
   }
     }
*/

//Start Using the Plugin
//Define docker image Ids

  stage ('Get ImageVulns - Qualys Plugin') {
//Use the same environment variable(env.IMAGE_ID) as an input to Qualys
```

```
Plugin's step
   steps {
    getImageVulnsFromQualys useGlobalConfig:true, imageIds: env.IMAGE_ID
   }
  }


  stage ('Performing Discovery Security Scanning') {
   steps {
    qualysWASScan authRecord: 'useDefault', cancelOptions: 'none',
credsId: 'Qualys_Alti', optionProfile: 'useDefault', platform:
'INDIA_PLATFORM', pollingInterval: '5', scanName:
'[job_name]_jenkins_build_[build_number]', scanType: 'DISCOVERY',
vulnsTimeout: '60*24', webAppId: '3919083'
   }
  }

  stage ('Performing Vulnerability Security Scanning') {
   steps {
    qualysWASScan authRecord: 'useDefault', cancelOptions: 'none',
credsId: 'Qualys_Alti', optionProfile: 'useDefault', platform:
'INDIA_PLATFORM', pollingInterval: '5', scanName:
'[job_name]_jenkins_build_[build_number]', scanType: 'VULNERABILITY' ,
vulnsTimeout: '60*24', webAppId: '3919083'
   }
  }

  stage ('Deploy to Dev') {
   steps {
    script {
     def dockerRun = 'docker run -d  vpbobade/mydemojava:1.0.0'
      sshagent(['deploy_to_docker']) {
      sh "ssh -o StrictHostKeyChecking=no ec2-user@172.31.81.65
${dockerRun}"
        }
    }
   }
```

```
  }
 }
}
```

CI & CD Approach 2

We are able to achieve CI & CD using the static Jenkins server where we are using docker hub as our registry server building and pushing built docker images into it also we are providing the image IDs to the Qualys Jenkins plugin and kicking the desired scan thereafter. The initial draft of Jenkinsfile for this approach is mentioned below:

```
pipeline {

//   environment {
//    registry = "mydocker/vpbobade"
//    registryCredential = 'mydocker'
//}

     agent any
     stages {
  stage ("git checkout") {
           steps {
               git ('https://github.com/vpbobade/demo-java')
           }
       }

       stage ("Checkout to different branch") {
           steps {
               sh "git branch -r"
               sh "git checkout master"
           }
       }

       stage ("package stage") {
           steps {
               sh 'bin/build'
           }
       }

       stage ("Building docker image") {
//Build the docker image with a tag (qualys:sample in this case)
   steps {
       sh "docker build -f Dockerfile -t vpbobade/mydemojava:1.0.0 . >
docker_out"
    //sh "./make_docker_image.sh"
    //docker.build registry
   }
     }

  stage ('Push Docker image to DockerHub') {
```

```
   steps {
    withCredentials([usernamePassword(credentialsId: 'mydocker',
passwordVariable: 'pass', usernameVariable: 'user')]) {
          sh "docker login -u ${user} -p ${pass}"
    }
                sh 'docker push vpbobade/mydemojava:1.0.0'
            }
        }


  stage ('Get Image id') {
//Use the same repo:tag (qualys:sample in this case) combination with
the grep command to get the same image id and save the image id in an
environment variable
   steps {
    script {
     def IMAGE_ID = sh(script: "docker images | grep -E
'^vpbobade/mydemojava:*' | head -1  | awk '{print \$3}'",
returnStdout:true).trim()
      env.IMAGE_ID = IMAGE_ID
    }
   }
     }

//Start Using the Plugin
//Define docker image Ids

  stage ('Get ImageVulns - Qualys Plugin') {
//Use the same environment variable(env.IMAGE_ID) as an input to Qualys
Plugin's step
   steps {
     getImageVulnsFromQualys useGlobalConfig:true, imageIds:
env.IMAGE_ID
   }
  }
/*
  stage ('Performing Vulnerability Security Scanning') {
   steps {
     qualysWASScan authRecord: 'useDefault', cancelOptions: 'none',
credsId: 'Qualys_Alti', optionProfile: 'useDefault', platform:
'INDIA_PLATFORM', pollingInterval: '5', scanName:
'[job_name]_jenkins_build_[build_number]', scanType: 'VULNERABILITY' ,
vulnsTimeout: '60*24', webAppId: '3919083'
   }
  }
*/
  stage ('Performing Discovery Security Scanning') {
   steps {
     qualysWASScan authRecord: 'useDefault', cancelOptions: 'none',
credsId: 'Qualys_Alti', optionProfile: 'useDefault', platform:
```

```
'INDIA_PLATFORM', pollingInterval: '5', scanName:
'[job_name]_jenkins_build_[build_number]', scanType: 'DISCOVERY',
vulnsTimeout: '60*24', webAppId: '3919083'
   }
  }

  stage ('Deploy to Dev') {
   steps {
    script {
     def dockerRun = 'docker run -d  vpbobade/mydemojava:1.0.0'
      sshagent(['deploy_to_docker']) {
      sh "ssh -o StrictHostKeyChecking=no
centos@ec2-35-175-208-250.compute-1.amazonaws.com ${dockerRun}"

     }
    }
   }
```

```
    }
      }
}
```

For more details on this tasks please have a look at my github project here

https://github.com/vpbobade/demo-java

References links and docs:

Please refer to this link for cloud agent installation for Linux.

https://www.qualys.com/docs/qualys-cloud-agent-linux-install-guide.pdf

Please refer to this link for more idea on Qualys API.

https://www.qualys.com/docs/qualys-api-quick-reference.pdf

https://www.qualys.com/docs/qualys-was-api-user-guide.pdf

Please refer this link for more details on Container security and sensor deployment.

https://www.qualys.com/docs/qualys-container-security-user-guide.pdf

https://www.qualys.com/docs/qualys-container-sensor-deployment-guide.pdf

Some links which can be helpful to sort out with issues

https://discussions.qualys.com/thread/17914-scan-taking-too-long-time-limit-reached

Important link for scanning registries

https://qualysguard.qg2.apps.qualys.com/cs/help/vuln_scans/vulnerability_scanning_of_registries.htm

https://discussions.qualys.com/docs/DOC-6637-getting-started-with-container-security-solution-from-aws-marketplace

https://qualysguard.qg1.apps.qualys.in/portal-front/