Qualys Host Scanning Connector for Jenkins

User Guide

Version 1.0.6

August 31, 2020

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

Preface

Welcome to Qualys Cloud Platform! In this guide, we'll show you how to install and use the Qualys Host Scanning Connector to see your Qualys VM scan data in Jenkins.

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

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/

Introduction to Qualys Host Scanning Connector for Jenkins

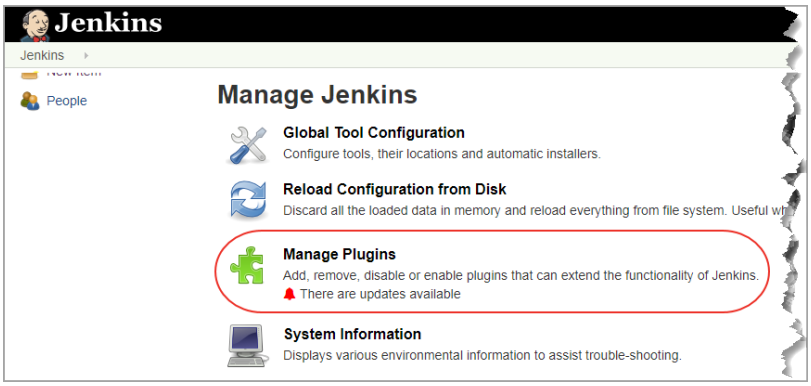
The Qualys Host Scanning Connector empowers to automate the VM scanning of host and cloud instance from Jenkins. By integrating scans in this manner, Host or cloud instance security testing is accomplished to discover and eliminate security flaws.

We'll help you: Install the Plugin | Configure the Plugin

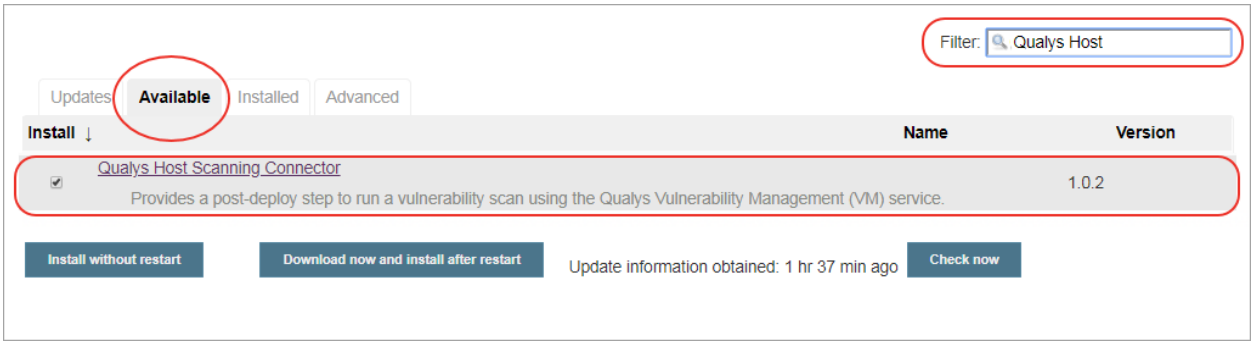
Install the Plugin

You can install the Qualys Host Scanning Connector from Jenkins. To install the Qualys Host Scanning Connector, log into your instance of Jenkins and click Manage Jenkins.

Next, click Manage Plugins.



If you are installing Qualys Host Scanning Connector for the first time, click the "Available" tab and search for Qualys Host Scanning Connector using the Filter bar. Select the plugin and click either Install without restart or Download now and Install after restart. After the plugin is installed, it will be listed in the Installed tab.



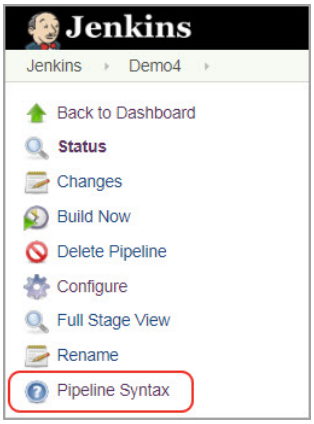
If the plugin is already installed in Jenkins and you want to update the Qualys Host Scanning Connector, go to the Updates tab, search for the plugin and click “Download now and Install after restart”.

Note that the plugin is also listed in the plugin store at https://plugins.jenkins.io/.

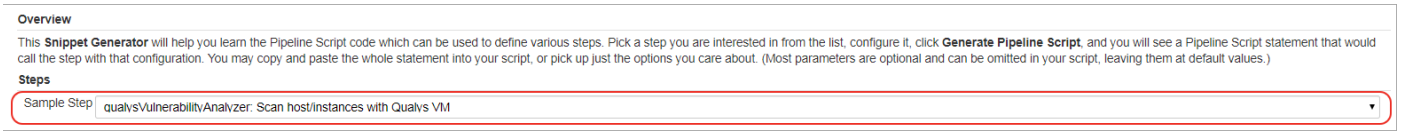
That’s it! The installation is now complete. Read on to learn about configuring the plugin.

Configure the Plugin for Pipeline projects

Open your application’s pipeline project and click "Pipeline Syntax" to enter the Snippet Generator.



Select "qualysVulnerabilityAnalyzer: Scan host/instances with Qualys VM" from the drop-down menu.



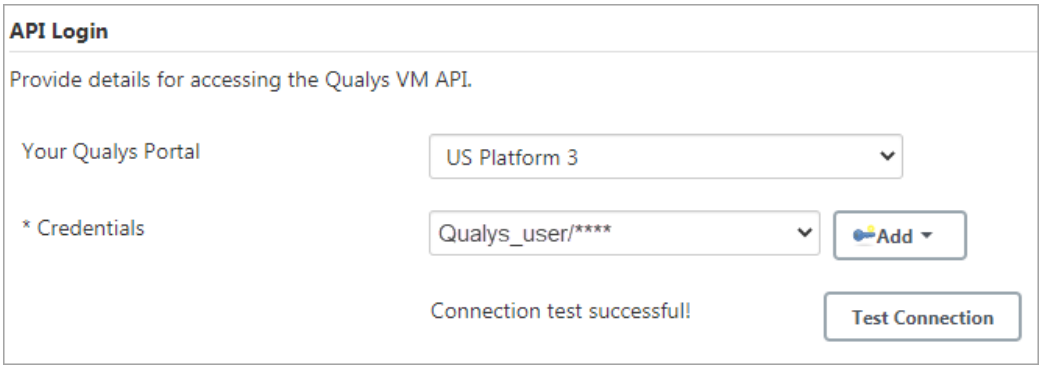
Configure API Login

Now you are ready to configure the plugin. The first step is to confirm that Jenkins can communicate to the Qualys Cloud Platform via the Qualys VM API. You'll need valid account credentials for an active Qualys VM subscription. The account must have API access enabled as well as a role assigned with all necessary permissions. Qualys recommends using a service account restricted to API access only (no UI access) and having the least privileges possible.

Select the Qualys platform/portal where your Qualys account resides and your account credentials for authenticating to the to the VM API server. Use the Add button to add account credentials in the Jenkins store for the new user. Once added, the credential is listed in the "Credentials" drop-down.

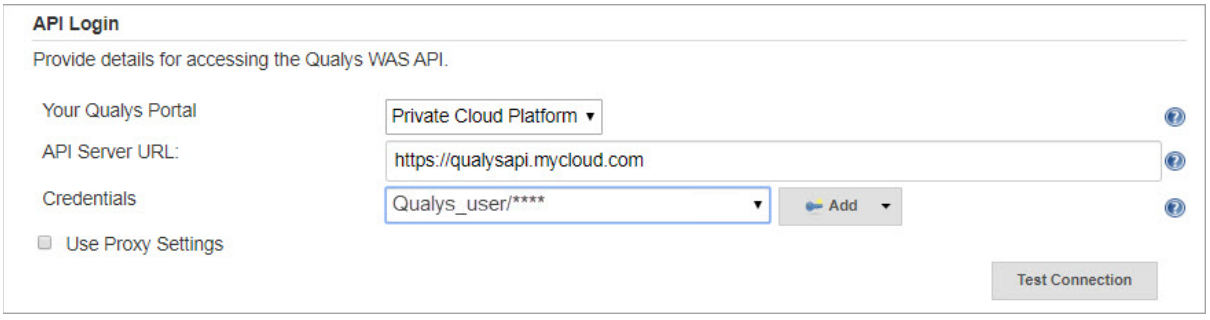
Note that what you select here depends on the Qualys platform your organization is using. Learn more.

If your Jenkins instance does not have direct Internet access and a proxy is required, click the "Use Proxy Settings" checkbox and enter the required information.



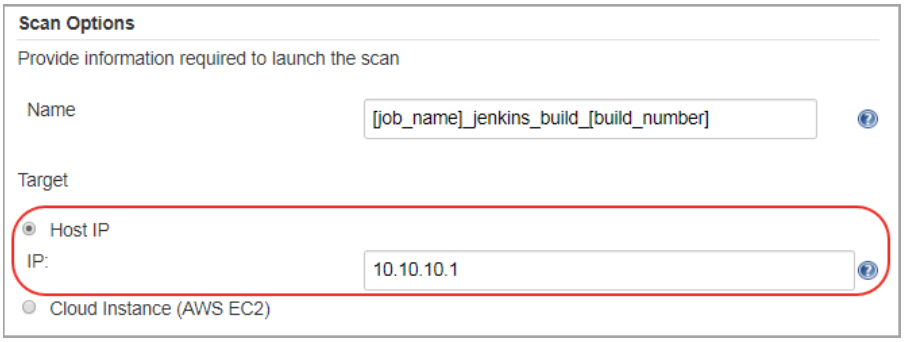
Click the "Test Connection" button. Assuming you have entered the correct API server URL for your subscription and the credentials are valid, you will see the message "Connection test successful!".

Note that if your Qualys account resides on a private cloud platform, select "Private Cloud Platform" as your Qualys cloud platform, specify the API server URL and your account credentials to access the API.



Configure Scan Options

Next, either enter the host IP in your Qualys VM account or AWS EC2 Cloud Instance information that you wish to scan. Note that we currently support scanning only single IP or EC2 instance.

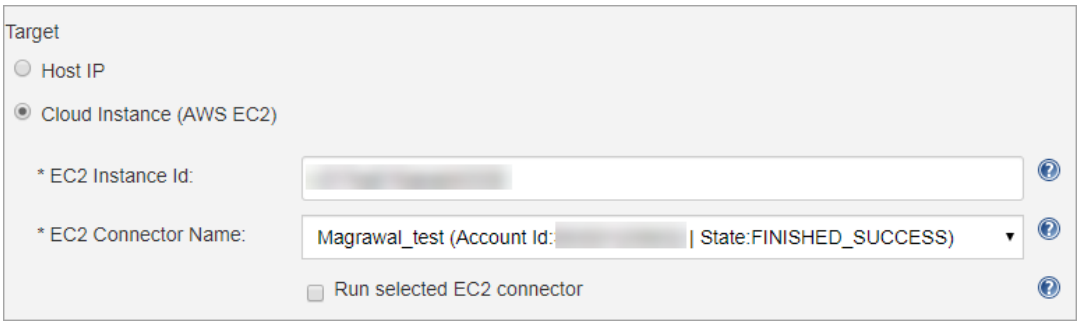


By default, the VM scan name will be:
`[job_name]_jenkins_build_[build_number] + timestamp`

You can edit the scan name, but a timestamp will automatically be appended regardless.

Provide the Host/Asset IP. You can also specify an environment variable for the Host IP.

Optionally, to scan your assets residing on an EC2 cloud instance: 1) Provide ID of Amazon EC2 Instance on which you want to launch the VM scan, 2) select the connector name for the instance.

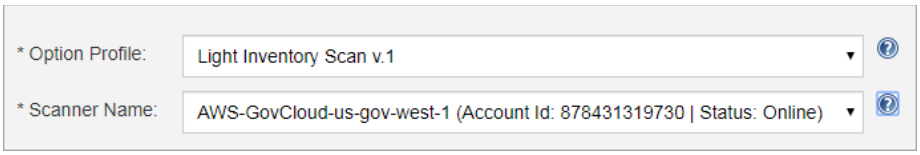


Currently, we support scanning a single Instance ID. You can also specify an environment variable for the EC2 ID.

When you select the “Run selected EC2 connector” check box, we run the connector to get the updated information about the instance and then launch the scan if the instance status is not known. If we have the instance status information, we do not run the connector and directly launch the scan. By default, this check box is selected.

We call the “hostasset” API with the “Id” and “accountId” of the ec2 instance to get the region/endpoint details.

Next, configure scan parameters.



Option Profile – The option profile contains the various scan settings such as the vulnerability types that should be tested (detection scope), scan intensity, error thresholds, etc. This is the recommended setting; however, you can also select the Other option and choose a specific option profile ID if desired. Default value is Initial Options.

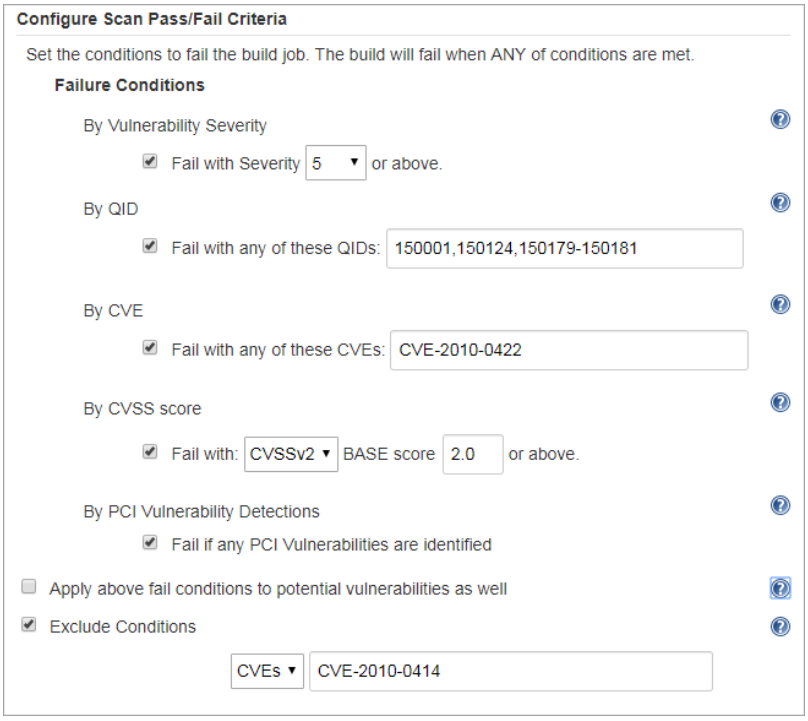
Scanner Name – Select the scanner appliance name from the drop-down that VM will use to scan your host assets on your network or on an EC2 instance for vulnerabilities. Default value is External scanner. Selecting the Host IP option will show you all the scanners including the scanners configured for scanning EC2 instances.

When you select Cloud Instance (AWS EC2) option, we will show you only those scanners that are configured to scan EC2 instances. Select the appropriate scanner that is configured to scan your ec2 instance.

Note that option profiles and scanners may take a bit longer to populate after connection to the API server is successful.

Configure Scan Pass/Fail Criteria

Next, configure the pass/fail criteria for a build, scan status polling frequency and timeout duration for the scan.



Failure Conditions

You can set conditions to fail a build by vulnerability severity, Qualys Vulnerability Identifiers (QIDs), CVE IDs, CVSSv2 or V3 with a specific base score and PCI vulnerability detections. A build

will fail if the scan results contain vulnerabilities that match any of the specified failure conditions.

The failure condition by a vulnerability severity fails a build if a vulnerability with a specified or higher severity is found. For example, if you set vulnerability severity to 2 then a build will fail if a vulnerability found in scan has severity equal to or greater than 2, that is 2,3,4 and 5.

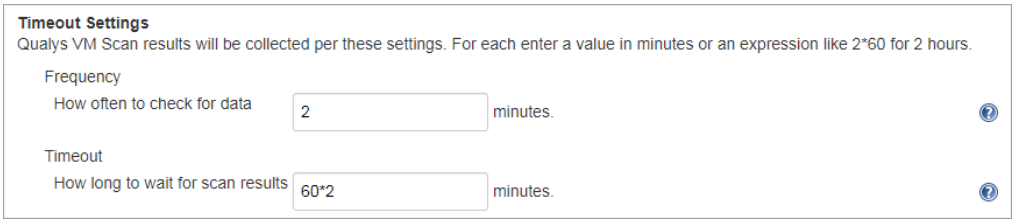
Note that a Qualys severity “5” rating is the most dangerous vulnerability while severity “1” is the least.

You also have the option to fail the build if the scan contains potential vulnerabilities. By default, failure conditions configured will be applicable only to “Confirmed” vulnerabilities. If you want to apply the conditions to Potential vulnerabilities as well, enable this option. A build will fail if the scan results contain potential vulnerabilities that match the conditions specified in the failure conditions. When you select this option, at least one failure conditions must be set.

Exclude Conditions

You can use the Exclude Conditions option to ignore specified CVE IDs or QIDs while evaluating the vulnerabilities for failure conditions. For example, we will not fail a build if an excluded QID is detected for a vulnerability in the scan even if that vulnerability meets the failure condition such as vulnerability severity. We evaluate the Exclude conditions first and remove the vulnerabilities that matches the exclude conditions before starting to evaluate the Failure Conditions.

Timeout Settings



In the Timeout settings, specify the polling frequency in minutes for collecting the VM scan status data and the timeout duration for a running Jenkins build. The default value for polling frequency is 2 minutes and 120 minutes is the default timeout duration.

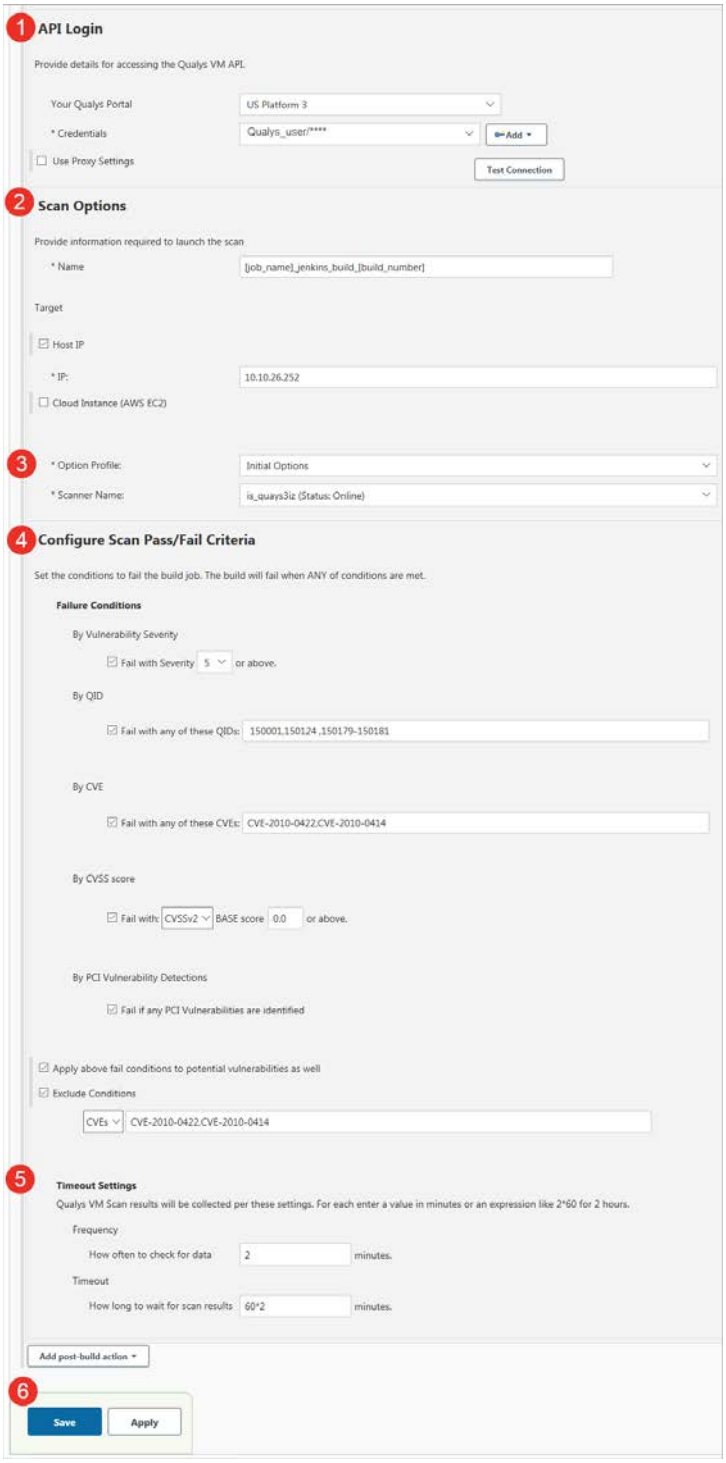
Next, click "Generate Pipeline Script". This is your pipeline snippet for launching a VM scan.

The pipeline snippet is now ready to be plugged into your pipeline script.

Configure the Plugin for Freestyle Projects

As the configuration settings are same as Pipeline Project, see “Configure the Plugin Pipeline Project” for detailed configuration.

To create a Freestyle Project, click the Post-build Actions tab and Go to the Post-build Actions section. Select the "Scan host/instances with Qualys VM" option from the “Add post -build action” drop-down menu and then provide the following configuration details:



1) Provide your login account credentials to access the Qualys VM API server on the Qualys cloud platform. Select Use Proxy Settings to provide proxy information if your Jenkins server is behind a firewall.

2) Click Test Connection to verify that the plugin can connect to the Qualys VM API server.

3) Provide parameters: scan name, target host IPs or AWS EC2 information required to call the launch scan API.

For Host/AssetIP and EC2 Instance ID, you can also specify an environment variable in this format:
`env.{variable name}`

For example:

If your environment variable name for Host IP is "hostIp" then the input for Host IP field should be env.hostIp.

If your environment variable name for EC2 Instance ID is "ec2Id" then the input for EC2 ID field should be env.ec2Id.

4) Optional parameters that you can pass to launch scan API. 5) Build fail conditions by vulnerabilities detected for severity types and by QIDs CVE IDs, CVSSv2 or V3 with a specific base score and PCI and potential vulnerability detections.

5) Provide data collection frequency and timeout duration for the running scan.

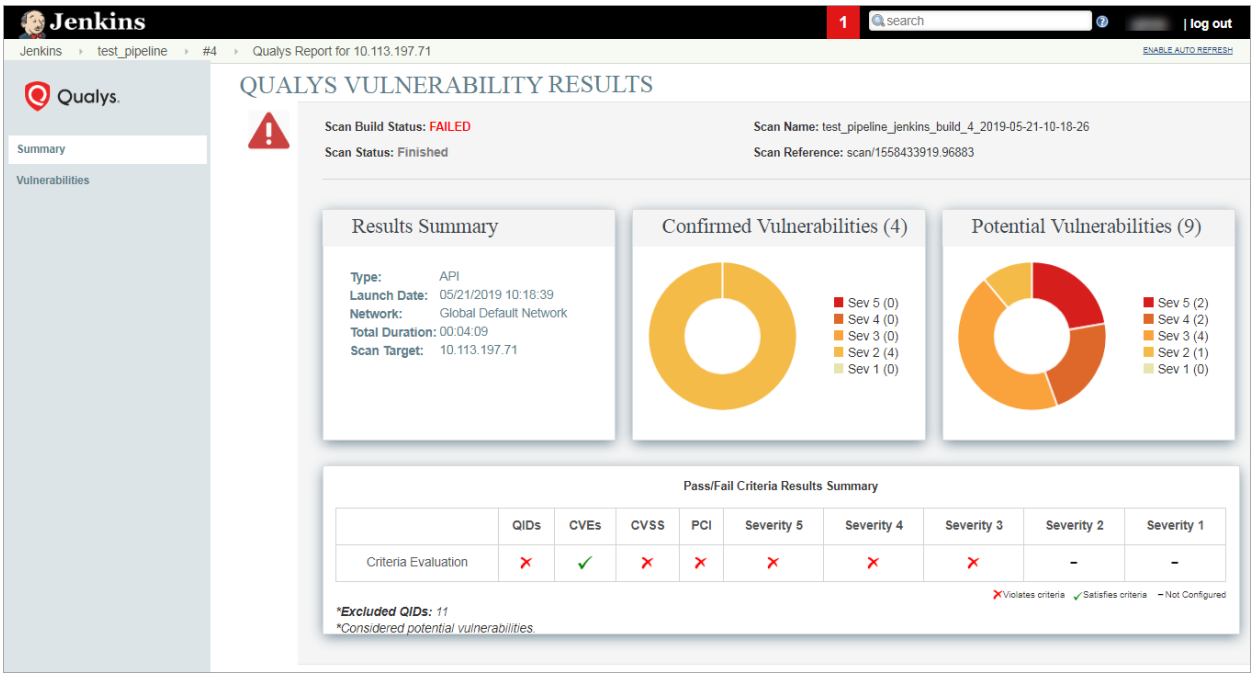
6) Finally, click Save.

Qualys VM Scan Status

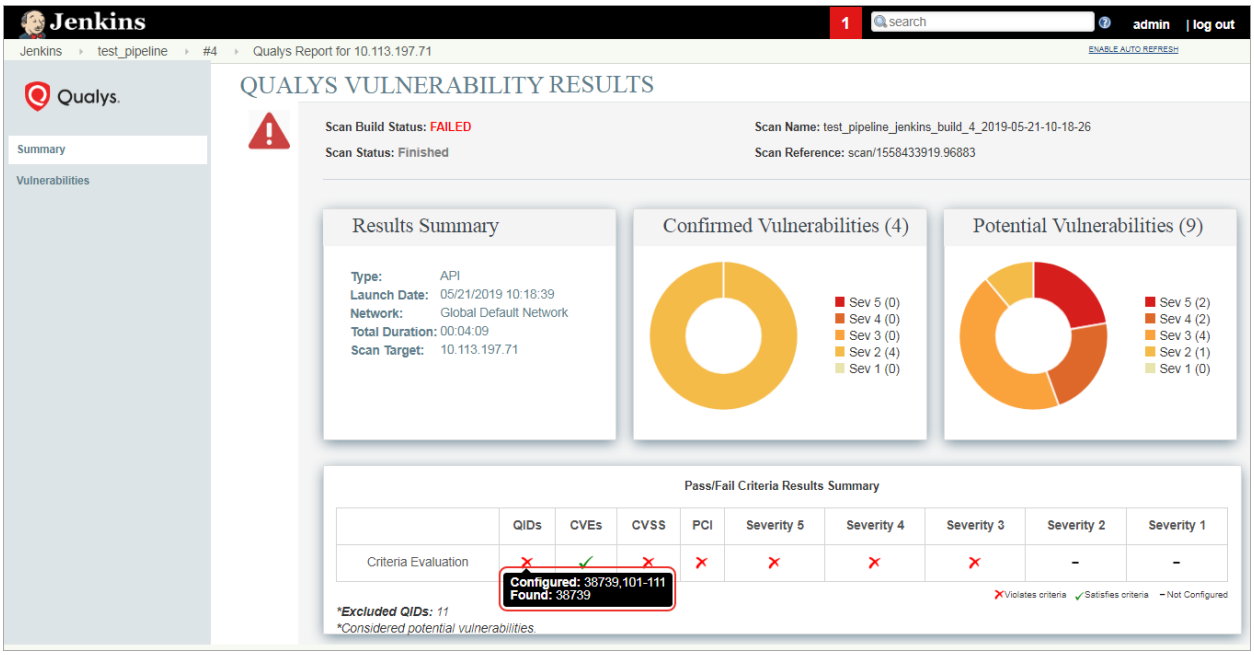
After the scan completes, go to Qualys VM Scan Results. Click the Summary tab. Report has a header and four sections: Results Summary, Confirmed Vulnerabilities, Potential Vulnerabilities and Pass/Fail Criteria Results Summary.

The Header shows along with other information build pass/fail status based on the scan results and scan completion status. Results Summary shows the scan launch date, duration and other details. Confirmed and Potential Vulnerabilities show graphical break up of confirmed and potential vulnerabilities by vulnerability severity type. Move your mouse over the graphical chart to view the number of vulnerabilities for each category of severity.

The Pass/Fail Criteria Results Summary section shows the pass/fail criteria and whether they are violated or satisfied. When the criteria are violated, the ✗ icon is shown while for satisfied criteria, the ✓ icon is shown.



Move the mouse over the ✗ and ✓ icons to view the value that you have configured for the criteria, and the actual value obtained after the scan.



The Vulnerabilities tab is available to provide you the details of vulnerabilities, such as QIDs, vulnerability titles, CVE ID, vulnerability severity, CVSS V2 and/or V3 scores, vulnerability type.

Frequently Asked Questions (FAQ)

What are the possible causes of scan not getting launched resulting in build failure?

Cause	Build Status
EC2 instance not found	We will not launch the scan and abort the build with appropriate error message.
No host Alive	Qualys Host Scanning Connector will try to launch the scan, but the build will fail as no alive hosts are found.
Disabled Connector	We will not launch the scan and abort the build with appropriate error message. We recommend that you check the connector state and the scanner appliance status while configuring them.

What happens if the "Run selected EC2 connector" check box is selected?

We will run the connector if the EC2 instance state is unknown and then launch the scan. Note that Qualys Host Scanning Connector won't be able to run the connector if the connector is disabled.

What happens if the "Run selected EC2 connector" check box is not selected?

We directly run the scan if we have the instance information.

URL to the Qualys API Server

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL.

What's New

Improvements in 1.0.5

Drop-down provided to Select Qualys platform

- We now provide a drop-down that you can use to select your Qualys platform that has your account in the API login section for accessing the Qualys VM API.

Support environment variable for Host IP and EC2 instance Id

- Qualys Host Scanning Connector will now also support environment variable input for Host IP and EC2 instance Id for Freestyle project. The format for specifying the environment variable is "`env.{variable name}`" For example: env.hostIp for Host IP where hostIp is the variable name or env.ec2Id for EC2 instance Id, where ec2Id is the variable name.

See the Qualys Host Scanning Connector for Jenkins guide for more information on improvements.

Fixed Issue

- Qualys Host Scanning Connector will now retry API calls if encountered by the 'concurrent API limit reached' error. Retries will take place every 2 seconds for 2 minutes or until plugin receives 200 responses.

Improvements in 1.0.6

Fixed Issue

We added a fix that will allow the plugin to correctly interpret special characters in the connector names and option profile names so that valid data is passed in API call made through plugin.