



# Qualys Host Scanning Connector for Jenkins

User Guide

Version 1.1.3

July 26, 2021

Copyright 2018-2021 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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](http://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/](http://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 instances from Jenkins. By integrating scans in this manner, Host or cloud instance security testing is accomplished to discover and eliminate security flaws.

**Note:** Qualys Host Scanning Connector supports Jenkins version 2.204.1 or greater.

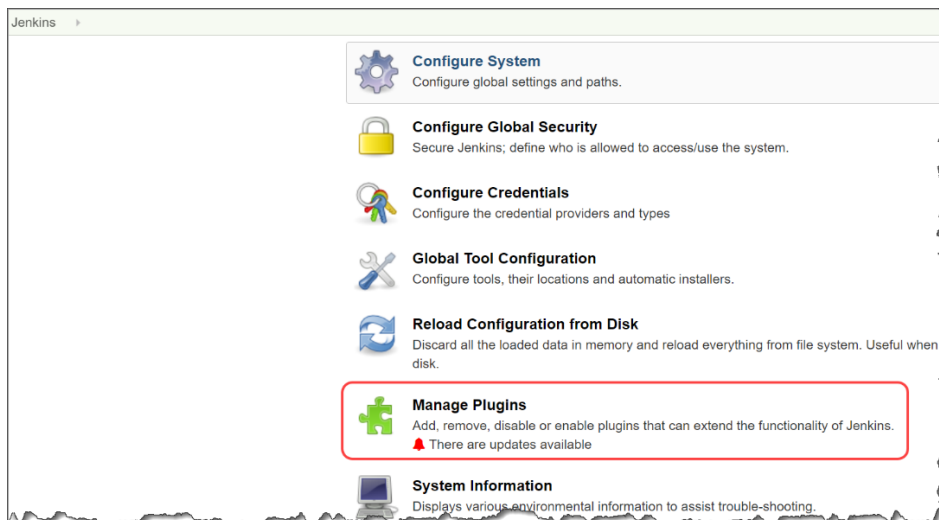
We'll help you: [Install the Plugin](#) | [Configure the Plugin](#)

## 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 the restart. Only after the plugin is installed, it is listed in the Installation tab.

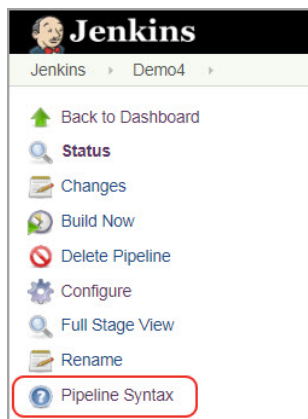
If the plugin is already installed in Jenkins and you want to update the Qualys Host Scanning Connector, go to the Updates tab, search for the plugin and click **Download now and Install after restart**.

**Note:** The plugin is also listed in the plugin store at <https://plugins.jenkins.io/>.

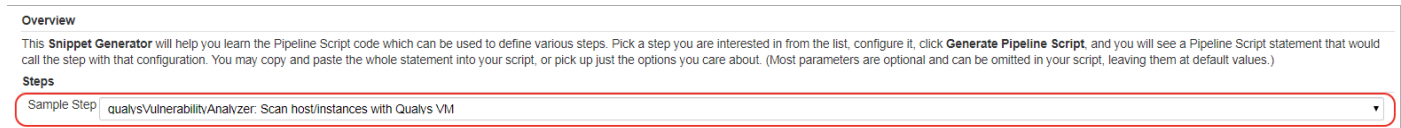
That's it! The installation is now complete. Read on to learn about configuring the plugin.

## 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 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 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:** The options to select credentials are based on the Qualys platform used by your organization [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.

Test connection is used to check API server connectivity from the Jenkins instance.

The screenshot shows the 'API Login' form for the Qualys VM API. The title is 'API Login' and the subtitle is 'Provide details for accessing the Qualys VM API.' There are two main input fields: 'Your Qualys Portal' with a dropdown menu showing 'US Platform 3', and '\* Credentials' with a dropdown menu showing 'Qualys\_user/\*\*\*\*'. To the right of the credentials dropdown is an 'Add' button with a plus icon. Below these fields, there is a status message 'Connection test successful!' and a 'Test Connection' button.

Once you have entered the correct API server URL and valid credentials, you get a "Connection test successful!" message.

**Note:** 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.

The screenshot shows the 'API Login' form for the Qualys WAS API. The title is 'API Login' and the subtitle is 'Provide details for accessing the Qualys WAS API.' There are three main input fields: 'Your Qualys Portal' with a dropdown menu showing 'Private Cloud Platform', 'API Server URL:' with a text input field containing 'https://qualysapi.mycloud.com', and 'Credentials' with a dropdown menu showing 'Qualys\_user/\*\*\*\*'. To the right of the credentials dropdown is an 'Add' button with a plus icon. Below these fields, there is a checkbox labeled 'Use Proxy Settings' which is currently unchecked. At the bottom right, there is a 'Test Connection' button.

## 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:** We currently support scanning only single IP or EC2 instances.



The screenshot shows the 'Target' section of a configuration form. It has two main options: 'Host IP' (selected with a checked checkbox) and 'Cloud Instance (AWS EC2)' (unselected). Under 'Host IP', there is a text field for '\* IP:' containing '1' followed by a blurred IP address, and a dropdown menu for 'Network:' showing 'VM IP Network'. Both fields have a blue help icon to their right. The 'Cloud Instance (AWS EC2)' option is also accompanied by a blue help icon.

By default, the VM scan name is:

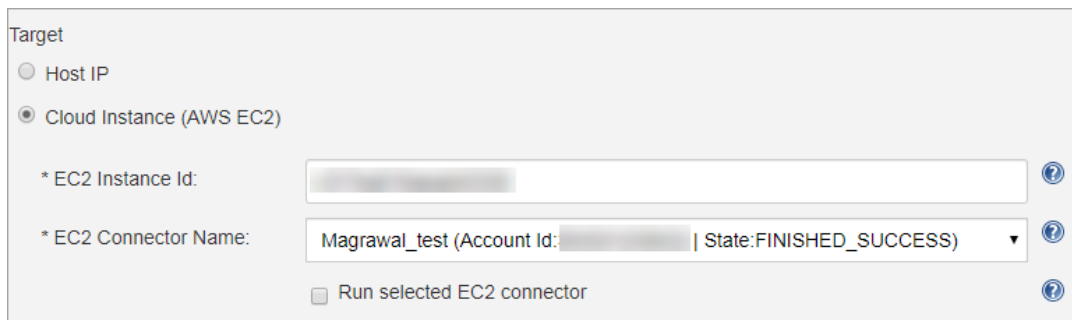
```
[job_name]_jenkins_build_[build_number] + timestamp
```

You can edit the scan name, but the timestamp is automatically appended.

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

**Note:** Networks may not populate if the custom network list option is not enabled for your subscription or if there are no networks assigned to you. See [FAQs](#).

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



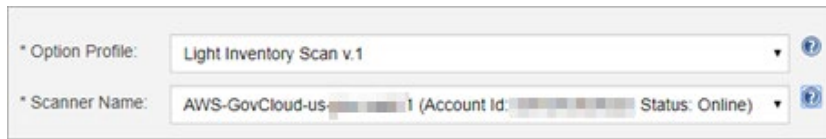
The screenshot shows the 'Target' section of a configuration form with 'Cloud Instance (AWS EC2)' selected. It includes a text field for '\* EC2 Instance Id:' with a blurred ID and a blue help icon. Below it is a dropdown for '\* EC2 Connector Name:' showing 'Magrawal\_test (Account Id: [blurred] | State: FINISHED\_SUCCESS)' with a blue help icon. At the bottom, there is a checkbox for 'Run selected EC2 connector' which is checked, also with a blue help icon.

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, the connector run is executed to fetch the updated information about the instance. A scan is launched if the instance status is not known. If the instance status information is known, then the connector run is not executed, instead, the scan is directly launched. By default, this check box is selected.

We call the **hostasset** API with ID and accountId of the EC2 instance to get the region/endpoint details.

Next, configure scan parameters.



The image shows a configuration window with two dropdown menus. The first dropdown, labeled '\* Option Profile:', has 'Light Inventory Scan v.1' selected. The second dropdown, labeled '\* Scanner Name:', has 'AWS-GovCloud-us-1 (Account Id: [redacted] Status: Online)' selected. Both dropdowns have a blue question mark icon to their right.

**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. The 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 an EC2 instance for vulnerabilities. The default value is External scanner. Selecting the Host IP and Network shows you all the scanners that are in your network. Select the **All Scanners in Network** option if you do not want to select a particular scanner and let the backend decide to launch the scan using any of the available scanners in the network. Select this option if you want to reuse the saved plugin configuration and are not sure that the scanner that you have selected for the current scan will be available for the next scan.

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

**Note:** The option profiles and scanners may take a bit longer to populate after the 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.

**Configure Scan Pass/Fail Criteria**

Set the conditions to fail the build job. The build will fail when ANY of conditions are met.

**Failure Conditions**

By Vulnerability Severity

☒ Fail with Severity **5** or above.

By QID

☒ Fail with any of these QIDs: **150001,150124,150179-150181**

By CVE

☒ Fail with any of these CVEs: **CVE-2010-0422**

By CVSS score

☒ Fail with: **CVSSv2** BASE score **2.0** or above.

By PCI Vulnerability Detections

☒ Fail if any PCI Vulnerabilities are identified

☐ Apply above fail conditions to potential vulnerabilities as well

☒ Exclude Conditions

**CVEs** **CVE-2010-0414**

### 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 the scan has severity equal to or greater than 2, that is 2,3,4 and 5.

**Note:** 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 condition 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 match the exclude conditions before starting to evaluate the Failure Conditions.

## Timeout Settings

**Timeout Settings**  
Qualys VM Scan results will be collected per these settings. For each enter a value in minutes or an expression like 2\*60 for 2 hours.

Frequency

How often to check for data

2

minutes.

?

Timeout

How long to wait for scan results

60\*2

minutes.

?

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.

**Generate Pipeline Script**

```
qualysVulnerabilityAnalyzer apiServer: 'https://qualysapi.qualys.com', byCvss: 'cvss_base', bySev: 5, cveList: 'CVE-2010-0422', cvssBase: '2.0', doExclude: true, excludeBy: 'cve_id', excludeList: 'CVE-2010-0414', failByCvss: true, failByCvss: true, failByPoi: true, failByQids: true, hostIp: '0.0.0.0', isSev: true, optionProfile: 'Initial Options', pollingInterval: '2', qidList: '150001,150124,150179-150181', scanName: '[job_name]_jenkins_build_[build_number]', scannerName: 'External', useHost: true, vulnsTimeout: '60*2'
```

**Note:** If the custom network feature is not enabled in your subscription, you get Network selected as **Enable the custom network list option for your subscription**. For this scan, a predefined network will be used.

\* IP:

0.0.0.0

?

Network:

Enable the custom network list option for your subscription. For this scan, a predefined network will be used

?

When you generate the Pipeline Script, the value for the network field in the script is ACCESS FORBIDDEN.

**Note:** Access forbidden is not an error. The plugin gets this response for an API call, as the custom network feature for your subscription is not enabled. The plugin launches the scan with the global default network. It is recommended to not make any changes in the pipeline script generated by the Qualys host scanning connector.

**Generate Pipeline Script**

```
qualysVulnerabilityAnalyzer bySev: 5, credsId: '1-150001', failBySev: true, hostIp: '0.0.0.0', network: 'ACCESS FORBIDDEN', optionProfile: 'Initial Options', platform: 'US_PLATFORM_2', pollingInterval: '2', proxyCredentialsId: '', proxyPort: 3143, proxyServer: '192.168.1.4', scanName: '[job_name]_jenkins_build_[build_number]', scannerName: 'External', useHost: true, useProxy: true, vulnsTimeout: '60*2'
```

**1 API Login**  
Provide details for accessing the Qualys VM API.

Your Qualys Portal:

\* Credentials:

☒ Use Proxy Settings

\* Proxy Server:   
Examples: 10.15.201.155, corp.proxyserver.company.com

\* Proxy Port:

\* Credentials:

**2 Test Connection**

**3 Scan Options**  
Provide information required to launch the scan

\* Scan Title:

Target

☒ Host IP

\* IP:

Network:

☐ Cloud Instance (AWS EC2)

**4 Initial Options**

\* Option Profile:

\* Scanner Name:   
Note: Wait till the scanner list gets completely populated after selecting the network.

**5 Configure Scan Pass/Fail Criteria**  
Set the conditions to fail the build job. The build will fail when ANY of the conditions are met.

**Failure Conditions**

By Vulnerability Severity

☒ Fail with Severity:  or above.

By QID

☒ Fail with any of these QIDs:

By CVE

☒ Fail with any of these CVEs:

By CVSS score

☐ Fail with: CVSSv2  or above.

By PCI Vulnerability Detections

☒ Fail if any PCI Vulnerabilities are identified

☒ Apply above fail conditions to potential vulnerabilities as well

☐ Exclude Conditions

**6 Timeout Settings**  
Qualys VM Scan results will be collected per these settings. For each enter a value in minutes or an expression like 2\*60 for 2 hours.

Frequency

How often to check for data:  minutes.

Timeout

How long to wait for scan results:  minutes.

**Advanced Settings**

☒ Delete workspace when build is done

**7 Save**

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

## Configure the Plugin for Freestyle Projects

As the configuration settings are the 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 and Network 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 the Host IP field should be `env.hostIp`.

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

4) Provide parameters: Option profile and Scanner name to launch the scan.

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.

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

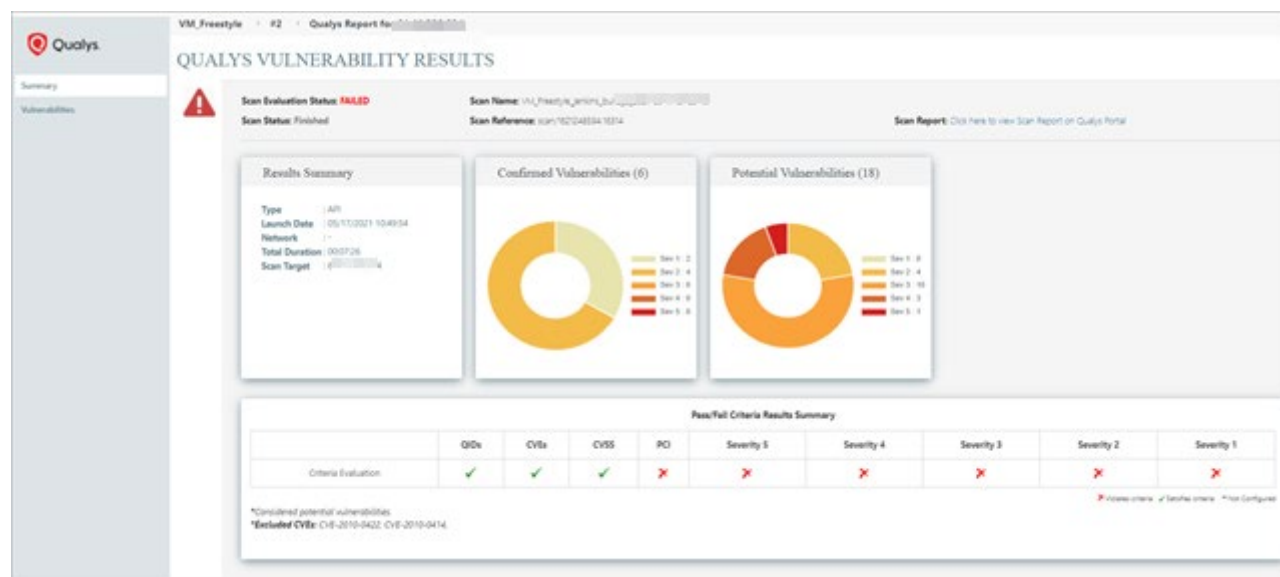
7) Finally, click **Save**.

## Qualys VM Scan Status

After the scan completes, go to Qualys VM Scan Results. Click the **Summary** tab. The 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 scan evaluation pass/fail status based on the scan results and evaluation criteria configured, scan completion status and scan report link for viewing the report on the Qualys Portal. 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 lists the vulnerabilities that are found in the VM scan and their details. We will show you the vulnerability details include QIDs, vulnerability titles, CVE ID, severity, type, bug traq id, and whether a vulnerability is a PCI vulnerability or not.

You can use the filters at the top to find the vulnerabilities by severity, type (potential, confirmed). The PCI Vuln filter allows you to find PCI-related vulnerabilities.

The **Exploitable** and **Associated Malware** filters when selected list the vulnerabilities for which exploitability and associated malware information is present in Qualys knowledgebase.

Jenkins

search

VM 113 - Freestyle - HostIP

#8

Qualys Report for

Qualys

Summary

Vulnerabilities

QUALYS VULNERABILITY RESULTS

Show10entries

Show Only:SeverityAllPCI VulnAllVuln TypeAllExploitableAssociated MalwareReset Filters

QID	Title	CVE ID	Severity	Category	PCI Vuln?	Type	Bug Traq Id
82003	ICMP Timestamp Request	CVE-1999-0524	1	TCP/IP	no	Confirmed	-
66040	Statd Format Bug Vulnerability	CVE-2000-0666 + 1 more	5	RPC	yes	Potential	1480
11	Hidden RPC Services	-	5	RPC	yes	Confirmed	-
38560	OpenSSH Signal Handling Vulnerability	CVE-2006-5051 + 4 more	4	General remote services	yes	Potential	20216, 20241, 20245, 20418
42413	OpenSSH LoginGraceTime Denial of Service Vulnerability	CVE-2010-5107	3	General remote services	no	Potential	58162, 58162
42428	OpenSSH "child_set_env()" Security Bypass Issue	CVE-2014-2532	2	General remote services	yes	Potential	66355
38623	OpenSSH Xauth Command Injection Vulnerability	CVE-2016-3115	3	General remote services	yes	Potential	84314
38679	OpenSSH Multiple Vulnerabilities	CVE-2015-5600 + 2 more	4	General remote services	yes	Potential	75990, 91787, 92012, 76317
38692	OpenSSH 7.4 Not Installed Multiple Vulnerabilities	CVE-2016-10009 + 4 more	4	General remote services	yes	Potential	84312, 94968, 94972, 94977, 94975, 93776
38788	OpenSSH Information Disclosure Vulnerability	CVE-2011-4327	2	General remote services	no	Potential	-

Showing 1 to 10 of 34 entries

Previous1234Next

Each row when expanded shows CVSS v2 and v3 Base and Temporal scores and the corresponding CVE IDs for the vulnerability.

Qualys

Summary

Vulnerabilities

VM 113 - Freestyle - HostIP

#8

Qualys Report for

QUALYS VULNERABILITY RESULTS

Show10▼entries

Show Only:

SeverityAll▼

PCI VulnAll▼

Vuln TypeAll▼

☐ Exploitable

☐ Associated Malware

Reset Filters

QID	Title	CVE ID	Severity	Category	PCI Vuln?	Type	Bug Traq Id
<div><div></div><div>02003</div></div>	ICMP Timestamp Request	CVE-1999-0524	1	TCP/IP	no	Confirmed	-
<div>CVSS Base Score: 0.0 (AV:L/AC:L/Au:N/CN:N/IN:AIN)</div> <div>CVSS Temporal Score: 0.0 (E:F/RL:W/RCC)</div> <div>CVSS3 Base Score: -</div> <div>CVSS3 Temporal Score: -</div> <div>CVE ids</div> <div>CVE-1999-0524</div> <div>Result</div> <div>Timestamp of host (network byte ordering): 05:37:12 GMT</div>							
<div><div></div><div>66040</div></div>	Statd Format Bug Vulnerability	CVE-2000-0666 + 1 more	5	RPC	yes	Potential	1480
<div><div></div><div>11</div></div>	Hidden RPC Services	-	5	RPC	yes	Confirmed	-
<div><div></div><div>38560</div></div>	OpenSSH Signal Handling Vulnerability	CVE-2006-5051 + 4 more	4	General remote services	yes	Potential	20216, 20241, 20245, 20418
<div><div></div><div>42413</div></div>	OpenSSH LoginGraceTime Denial of Service Vulnerability	CVE-2010-5107	3	General remote services	no	Potential	58162, 58162
<div><div></div><div>42428</div></div>	OpenSSH "child_set_env()" Security Bypass Issue	CVE-2014-2532	2	General remote services	yes	Potential	66355
<div><div></div><div>38623</div></div>	OpenSSH Xauth Command Injection Vulnerability	CVE-2016-3115	3	General remote services	yes	Potential	84314
<div><div></div><div>38679</div></div>	OpenSSH Multiple Vulnerabilities	CVE-2015-5600 + 2 more	4	General remote services	yes	Potential	75990, 91787, 92012, 76317
<div><div></div><div>38692</div></div>	OpenSSH 7.4 Not Installed Multiple Vulnerabilities	CVE-2016-10009 + 4 more	4	General remote services	yes	Potential	84312, 94968, 94972, 94977, 94975, 93776
<div><div></div><div>38788</div></div>	OpenSSH Information Disclosure Vulnerability	CVE-2011-4327	2	General remote services	no	Potential	-

Showing 1 to 10 of 34 entries

Previous

1

2

3

4

Next

## Frequently Asked Questions (FAQ)

### What are the possible causes of the 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 an 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 an 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:** The 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.

### Why do I see this message when I click the Network drop-down field "Enable the custom network list option for your subscription. For this scan, a predefined network will be used."?

This message is shown if the custom network list option is not enabled for you in the subscription. This message does not mean that you cannot launch the scan. The plugin will use a predefined network to launch the VM scan. If you want to launch the scan with a custom network, contact your Account Administrator to enable the custom network support option for your user.

### Why do I see this message when I click the Network drop-down field "There are currently no networks assigned to you. Contact your System Administrator to assign custom networks."?

This message is shown when your user is not assigned a business unit or asset group in the VM module. When you see this message, contact your System Administrator to add your user to the business unit or the asset group that has the host asset on which you want to launch the scan. Depending on whether you are added to a business unit or an asset group, you will see the networks of BU or asset group.

Here are the steps to assign networks:

1. Click the VMDR module from the module picker and go to the **Users** tab.
2. Select the user you want to assign a network.
3. From the Quick Actions menu, click **Edit**.
4. On the Edit User page, go to the User Role and select a business unit that has the asset in one of the asset groups or go to the Assets Groups and select the asset group that has the asset.

**Under pipeline syntax > Sample step dropdown, when I toggle between sample steps provided by Qualys Integration plugin, then API Server URL field is shown even when the PCP option is not selected in the Qualys Portal**

This is a known issue and currently, we do not have a fix for this issue. We suggest you reload the page to fix this issue.

## **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 1.1.3

- With this release, we will use the upgraded third-party library for rendering graphical charts that are used for displaying vulnerability results in the Jenkins scan report section.
- On the Qualys Vulnerability Results page, in the Vulnerabilities tab, we have added 2 new filters: Exploitable and Associated Malware to help you find vulnerabilities that have exploitable and associated malware information in the Qualys KnowledgeBase. We have removed the CVSS columns from the vulnerability table. You will see this information when you expand a QID row.

### Improvements in 1.1.2

- We replaced the **Scan Build Status** field in the Header section of the Scan Report page with **Scan Evaluation Status**. This field denotes the scan evaluation pass/fail status based on scan results and evaluation criteria configured.
- With this release, we will now support AE Platform (Dubai). If your VM account resides on this platform, then select this platform from the Your Qualys Portal drop-down field in the API Login section on the plugin configuration page.

### Improvements in 1.1.1

#### Added a new option “All Scanners in Network” in the Scanner Name drop-down field

You will now see a new option All Scanners in Network in the Scanner Name drop-down field when selecting a scanner name. When you select this option, the backend will launch a scan using any of the scanners that are currently available in your network. Select this option if you are not sure that the scanner that you have selected for the scan will be available for the next scan.

#### Report to show a link to view the scan report on the Qualys Portal

The Scan Results page will show a link in the Scan Report field that will allow you to view the vulnerability scan report on the Qualys Portal.

### Improvements in 1.1.0

#### Added a new field on the configuration page to choose a network

You can now launch a scan from your custom network. We added a new field Network on the configuration page. When you select a Network, we will the system shows you all the scanners in the selected network. You can select one of these scanners to launch the scan. Ensure the customer network support option is enabled for your subscription.



## 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 the 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 calls made through the plugin.