Qualys Policy Compliance Scanning Connector for Jenkins

User Guide

Version 1.0.2

October 15, 2020

Copyright 2018-2020 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 Policy Compliance Scanning Connector to see your Qualys PC 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 Policy Compliance Scanning Connector for Jenkins

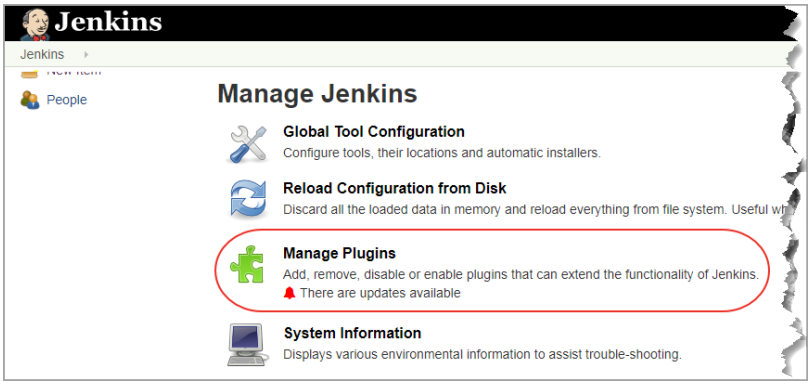
The Qualys Policy Compliance Scanning Connector empowers to automate the PC scanning of host and cloud instance from Jenkins. By integrating scans in this manner, Host or cloud instance security testing is accomplished to discover and eliminate security flaws.

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

Install the Plugin

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

Next, click **Manage Plugins**.



If you are installing Qualys Policy Compliance Scanning Connector for the first time, click the **Available** tab and search for Qualys Policy Compliance 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 Policy Compliance Scanning Connector, go to the **Updates** tab, search for the plugin and click **Download now and Install after restart**.

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

Pre-requisites for Configuring the Plugin

1. You must have a subscription to Qualys Policy Compliance and your Qualys Policy compliance account that you want to use for scanning the target host must have permission to access PC API.

2. In your Qualys PC account, create an option profile with a name starting with 'Jenkins_' and add policies to this option profile for the Policy Compliance scan. In the Option Profile configuration section, the plugin will list only the option profiles that have a name starting with "Jenkins_".

3. Note that for selected option profiles, you need to select at least one policy for a successful scan launch.

4. An authentication record for the target asset is required for the PC scan. If you already have an authentication record created for the host, the Scan API will use this record for scanning the host else you can use the plugin to create a new authentication record for the host. See Configure Scan Options in the guide.

5. For the EC2 Instance scan, ensure your target instance is in the 'Running' state. Both the scanner appliance and EC2 connector that you have selected should be of the same account id (Users can see the account id in the drop-down field for EC2 connector and scanner on Qualys PC Scanning connector's configuration form)

Good to Know

· When the Jenkins Job with Qualys Policy Compliance Scanning connector stage is built for the first time, the Qualys Policy Compliance Scanning connector will -

1. Add a target asset (Host IP/EC2 Instance) into your Qualys subscription if not already present.

2. The connector will then create an asset group with a name starting with 'Jenkins_AG_<Jenkins_project_name>'.

3. On successful creation of the asset group, the connector will then add the target asset into this newly created asset group

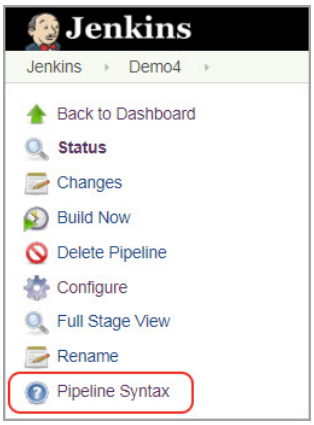
4. The Qualys PC Scanning connector will attempt to create an authentication record using credentials selected by the user if no authentication record is found and the user have selected respective setting in Qualys PC Scanning connector's configuration.

5. The connector will also add policies selected by the user in the configuration to the asset group created in the job.

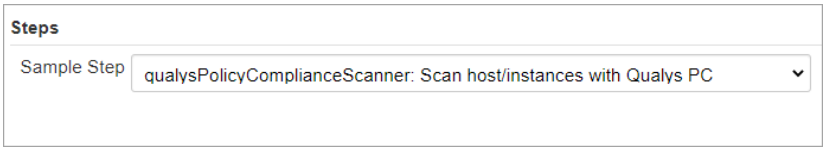
- On the subsequent run, Qualys Policy Compliance Scanning Connector will check if the asset group is present or not. If the asset group already exists, the plugin will simply overwrite the target asset and policies in it if at all they are changed in the connector configuration.

Configure the Plugin for Pipeline projects

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



Select "**qualysPolicyComplianceScanner:Scan Host/Instances with Qualys PC**" from the **Steps** drop-down menu.



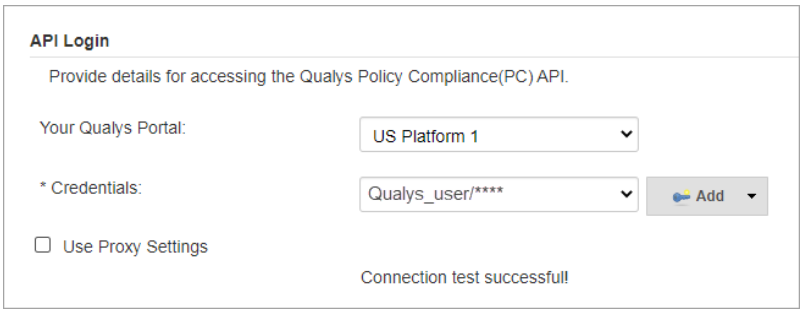
Configure API Login

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 Policy Compliance (PC) API. You'll need valid account credentials for an active Qualys PC 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 PC 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.

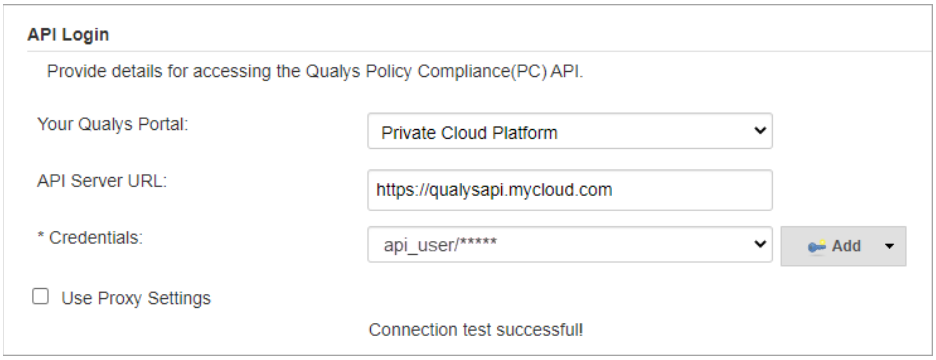
Note that what you select here depends on the Qualys platform your organization is using. Learn more.

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.



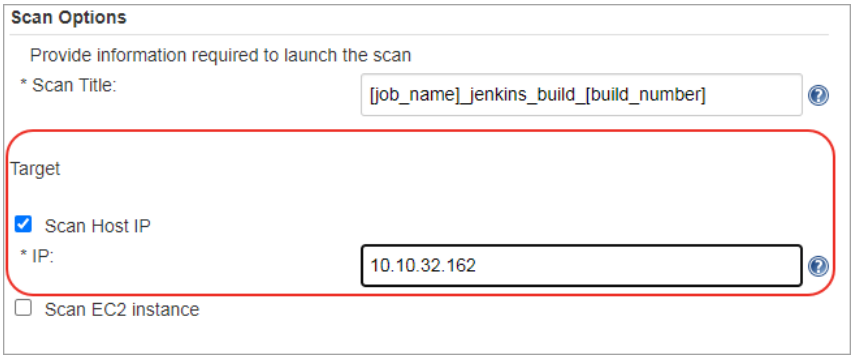
Click the "Test Connection" button. Assuming you have entered the correct API server URL for your subscription and the credentials are valid, you will see the message "Connection test successful!".

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

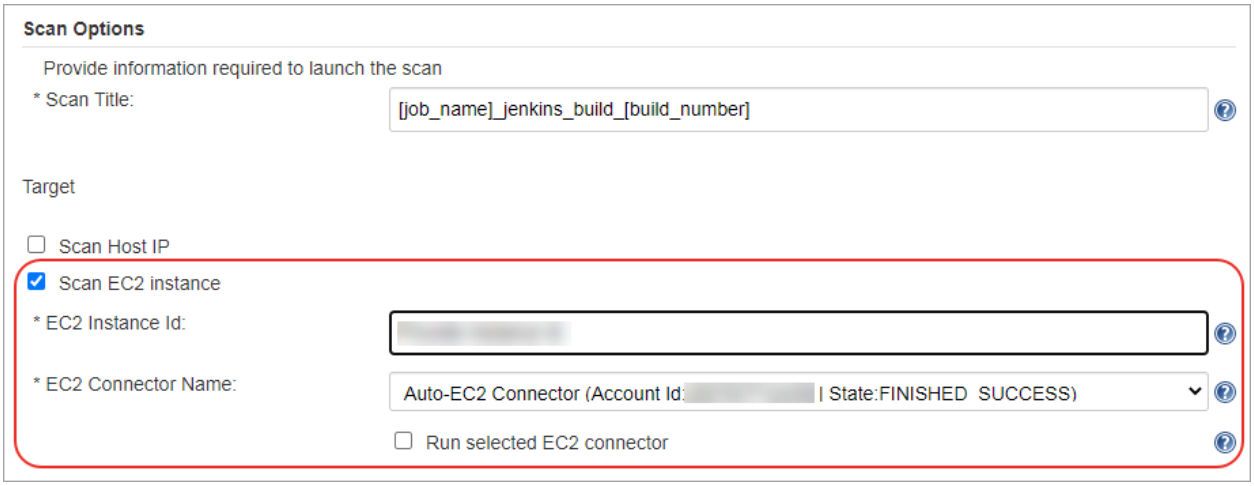
Next, either enter the host IP in your Qualys PC account or AWS EC2 Cloud Instance information that you wish to scan. You can also specify an environment variable for the Host IP and EC2 ID. Note that we currently support scanning only single IP or EC2 instance.



By default, the PC 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.

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 PC scan, 2) select the connector name for the instance.



When you select the “Run selected EC2 connector” check box, we run the EC2 connector to get the updated information about the instance only if the configured EC2 instace ID state is returned as 'Unknown' by Qualys hostasset APIs. Post running the connector, scan launch attempt will be made only if the EC2 instance state is known.

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

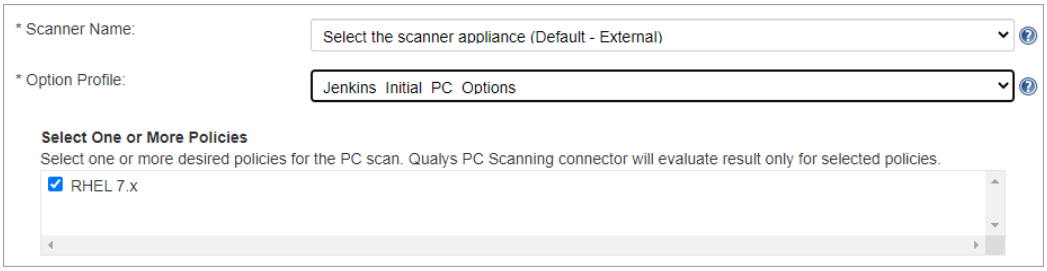
The Create Authentication Record step is optional. If you already have an authentication record for the host in your account, we will use that authentication record to authenticate to the host.

In case the authentication record is not present for the host in your account, select Create Authentication Record and then select Windows or Unix platform. Click the Add button to add your host credentials, then select the credentials from the Credentials drop-down field.

When the plugin will run, we will create an authentication record with the name Jenkins_windows_[Job Name] for windows or Jenkins_unix_[Job Name] for Unix based on the platform selection.

Note that new authentication record creation from the plugin will fail if an authentication record for the target host already exists in your account. You need to delete the host authentication record from your account to create the new authentication record from the plugin.

Next, configure scan parameters.



Scanner Name – Select the scanner appliance name from the drop-down that PC will use to scan your host assets on your network or on an EC2 instance to check the compliance of your systems against your policies. The default value is the “External” scanner if you do not select a scanner from the Scanner drop-down.

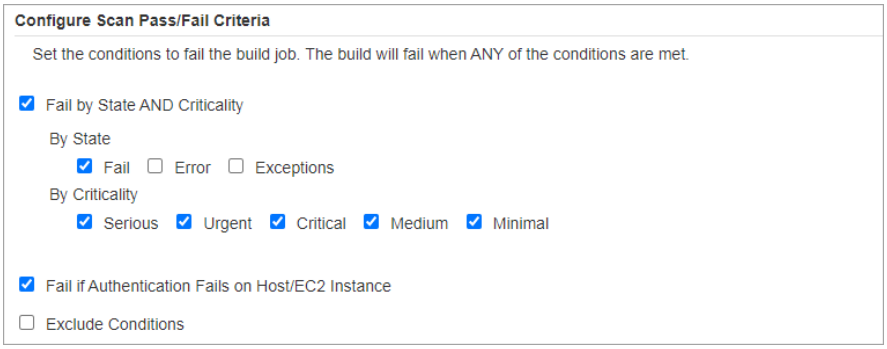
Selecting the Host IP option will show you all the scanners including the scanners configured for scanning EC2 instances. When you select Cloud Instance (AWS EC2) option, we will show you only those scanners that are configured to scan EC2 instances. Select the appropriate scanner that is configured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

Option Profile – The option profile contains the settings used for a compliance scan. Select the option profile and one or more policies for the PC scan. We show only the policies for the selected option profile. The plugin will evaluate the results for selected policies only.

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. You can set any or all of the three conditions to fail the build. The three conditions are:



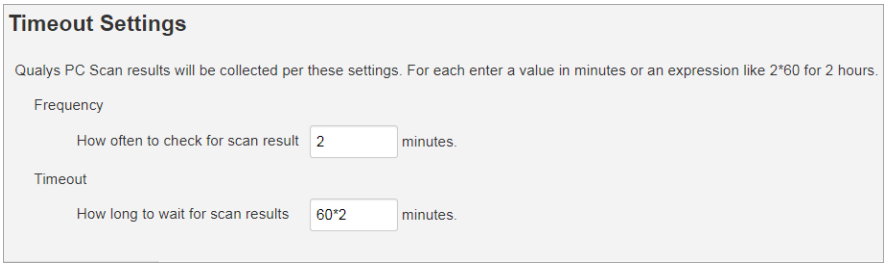
Fail by State AND Criticality – This criterion lets you choose the states and the corresponding criticality to fail a build. The build will fail if both the state and the criticality condition is fulfilled. The build can be failed for all or any of these states for the controls you are evaluating: Fail, Error and Exceptions, and any or all of these criticalities: Serious, Urgent, Critical, Medium, and Minimal.

Fail if Authentication Fails on Host/EC2 Instance – This criteria if selected will fail the build if the plugin fails to authenticate to the host IP or EC2 Instance using the authentication record. If this option is not selected and yet the authentication fails, we will pass the build but no reports will be generated.

Exclude Condition - You can use the Exclude Conditions option to ignore specified CIDs or Control IDs while evaluating the policy for failure conditions. For example, we will not fail a build if an excluded CID is detected for a policy in the scan even if that CID meets the specified failure condition. We evaluate the Exclude conditions first and remove the CIDs that match the exclude conditions before evaluating the Failure Conditions.

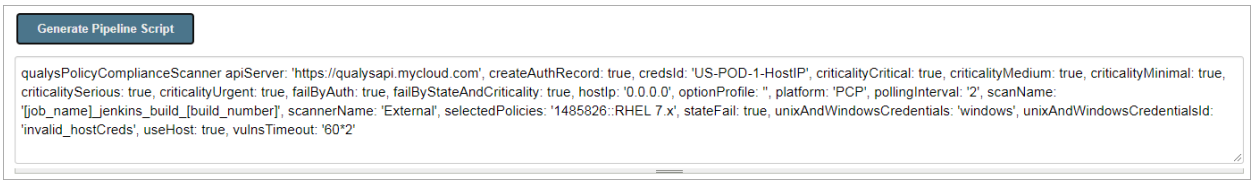
Timeout Settings

scan status polling frequency and timeout duration for the scan.



In the Timeout settings, specify the polling frequency in minutes for collecting the PC 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 PC scan.

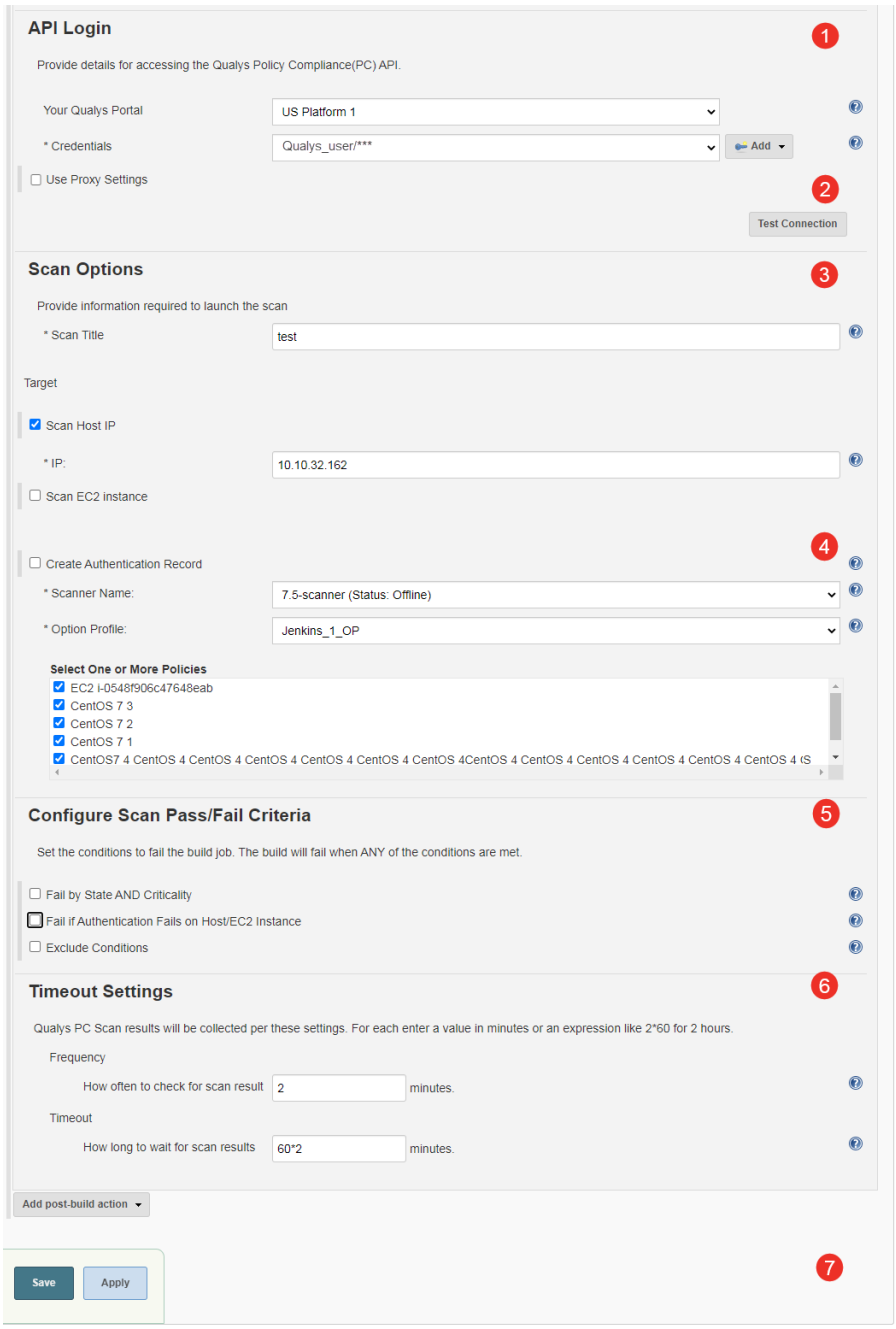


The pipeline snippet is now ready to be plugged into your pipeline script.

Configure the Plugin for Freestyle Projects

As the configuration settings are 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 PC** 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 PC 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 PC 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 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) For PC plugin, only authentication record creation is optional. Scanner and Option profile with at least one policy are required parameters.

5) Configure scan Pass/fail criteria. You can fail a build by state and criticality of the control and authentication result.

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

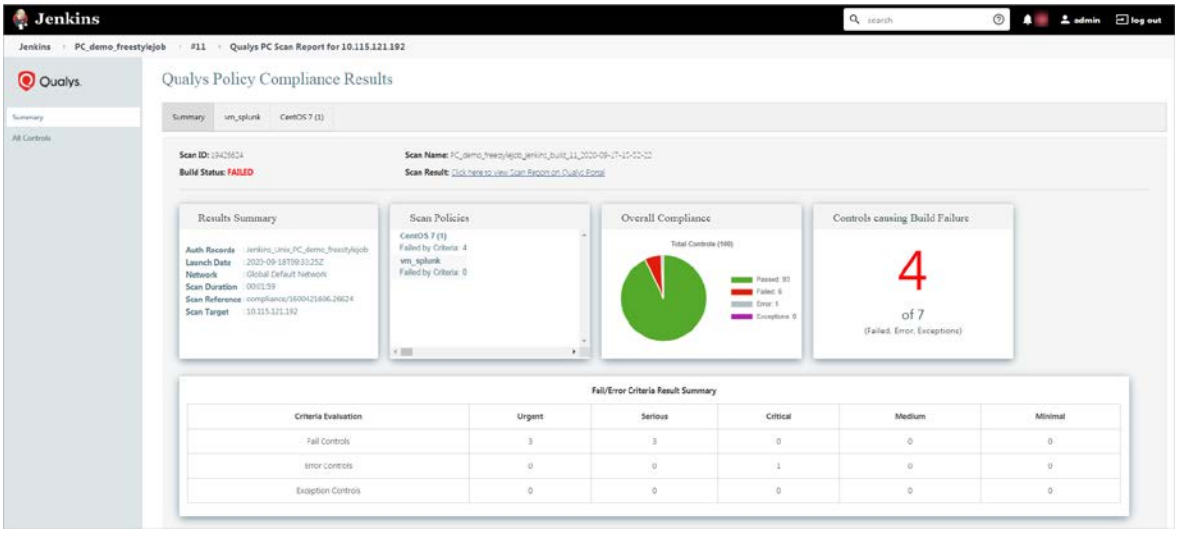
7) Finally, click Save.

Qualys PC Scan Status

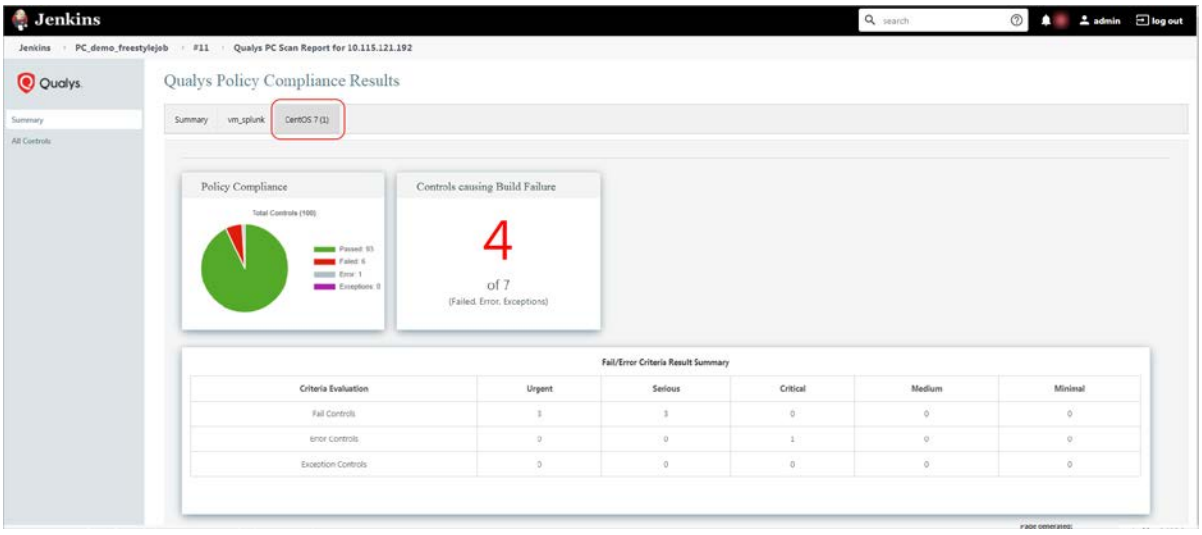
Upon successful PC scan, Qualys PC Scanning connector will generate the scan report for the respective Jenkins build with link name 'Qualys PC Scan Report for <target_asset_ip>'. After the scan completes, go to Qualys PC Scan Results. Click the Summary tab. The report has four sections: Results Summary, Scan Policies, Overall Compliance, Controls Causing Build Failure.

The header of the result shows the scan's ID, name, and the link to view the scan result in the PC module. The sections give you information on the total number of controls scanned for the selected policies along with the graphical break up of the number of controls with status as passed, failed, error, and exceptions. We also show the total number of controls that met the failure conditions, which caused the build to fail.

The "Pass/Fail Criteria Results Summary section" shows in a matrix the count of failed, error, and exceptions controls found in the policy scan by their criticalities.

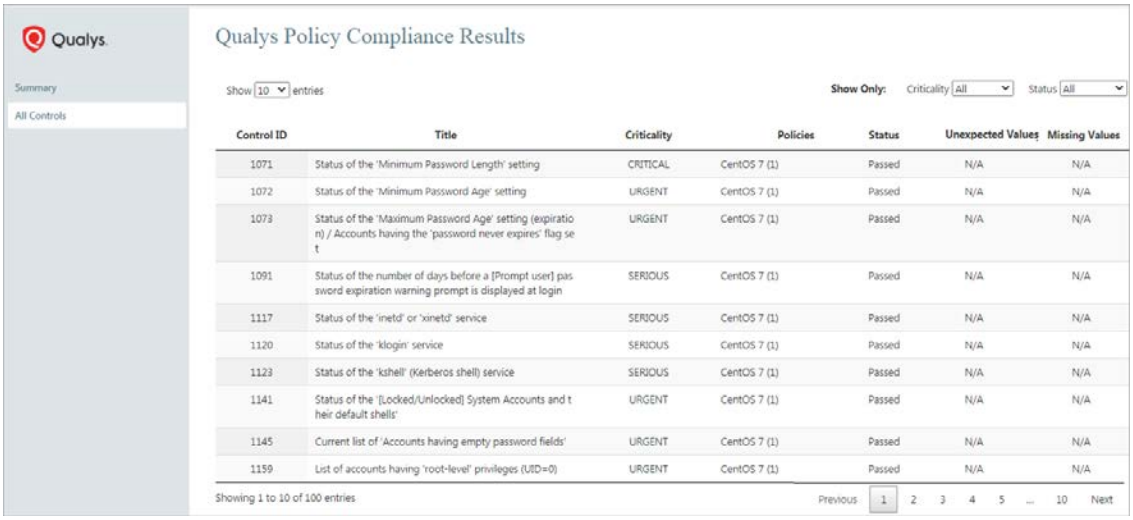


In the Summary tab, when you click a policy name in the "Scan Policies" section to view its details in a separate policy tab. In the policy tab, you will see the scan result for the selected policy.



Similarly, in the Summary tab when you click the count in the “Controls using build failures” section, we show you details of these controls in the “All Controls” tab.

The “All Controls” tab gives the details of the scanned controls such as control’s ID, title, criticality, policy name, status, and unexpected values. You can filter the controls by their criticality and status.



Troubleshooting

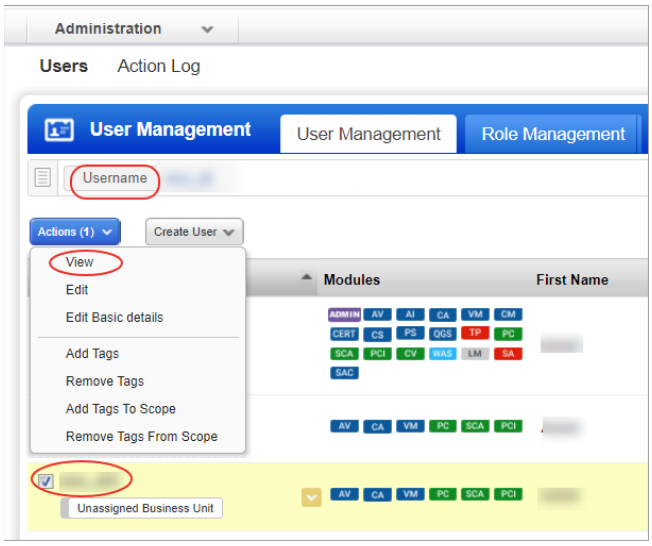
Test connection is successful but the Scanner, Option Profile, EC2 Connector drop-down fields on configuration are empty.

This issue happens because your Qualys user account that you used to connect to the API server does not have permissions to access the PC APIs. To check the user's privileges:

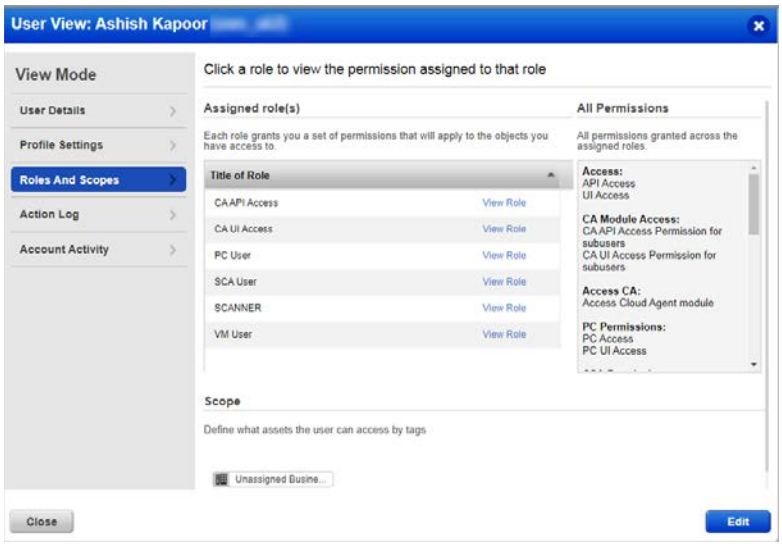
1. Log in to the Qualys Platform using your account credentials and from the module picker, select the Administration module.

2. On the User Management tab, search for the user by username.

3. Select the user, and then select Actions > View to go to the User View screen.



4. Go to the Roles and Scopes tab and check if the user has access to PC APIs.



Jenkins Build console logs displays - "Data not found for policy "policy_name" and host <asset_ip>"

The PC Scan API server returns this message in response to the API calls made by the Qualys PC Scanning Connector to fetch the PC scan data for the host asset. During the scan, if the Scan API discovers that the technology specified in the policy is not present on the target host, then no scan data is generated by the API for this policy after the scan. Hence, the message no data found for policy.

For API to scan the host for the selected policy, ensure the technology that you have added to the policy is also present on the host

Frequently Asked Questions (FAQ)

What are the possible causes of a 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 Policy Compliance 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 that Qualys Policy Compliance 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.