Qualys IaC Security Integration with Bamboo

In the existing Continuous Integration and Continuous Deployment (CICD) environment, the security scans are conducted on cloud resources after deployment. As a result, you secure your cloud resources post-deployment to respective Cloud accounts.

With an introduction of the Infrastructure as Code (IaC) security feature by Qualys CloudView, you can now secure your IaC templates before the cloud resources are deployed in your cloud environments. The IaC Security feature will help you shift cloud security and compliance posture to the left, allowing evaluation of cloud resources for misconfigurations much early during the development phase.

CloudView offers integration with Bamboo to scan and secure your IaC templates using the Bamboo plans. It continuously verifies security misconfigurations against CloudView controls and displays the misconfigurations for each run. With a continuous visibility of the security posture of your IaC Templates at Bamboo, you can plan for remediation to stay secure post deployment.

Scanning IaC Templates at Bamboo

The Bamboo integration allows you to perform IaC scans using plans. We provide you with plans and options that you can configure to run based on various triggers.

You can perform an IaC scan on either of the following:
- the entire git repository.
- only the templates that were newly added / updates to the branch.

The results are generated on the build console that provides you with proactive visibility into the security of your IaC templates residing in Git repositories.

Pre-requisite
- Install Java 8 with version less than 255.
- Ensure you have the latest version of Bamboo installed.
- To auto-trigger a Bamboo plan, ensure that you install a specific Source Code Management (SCM) plugin, e.g., Bitbucket plugin, Bitbucket Server Integration.
- Ensure that you have a valid Qualys CloudView Security Assessment app subscription.

Let us see the quick workflow:

Configure the Plan
Add Task
Run IaC Scan
View Scan Output
Configure the Plan

Before running a scan, we have to create a new plan on your Bamboo dashboard.

1. On the Bamboo dashboard, go to Create > Create Plan.

2. On the plan configuration screen, select an existing or new project.
3. Enter plan name, key and description. Click Create.
4. Next, you can either link a git repository with your plan to scan templates in your repository or continue configuring the plan to scan local template files.

5) To continue without linking a repository, select ‘None’ and click **Save**.

**To Link a Repository**

a) Select ‘Link new repository’

b) Select repository source (Git, BitBucket, Github etc)

c) Provide the repository details and authentication information

d) Click **Save and continue**
Add Task

5. Under ‘Create tasks’, click **Add tasks**.

6. Search for the Qualys IaC Scan plugin and Install it.
7. You can select from your available linked repositories or add more repositories from ‘Source Code Checkout’. Once selected, you can proceed to run a scan.

8. To run a scan, select the ‘Qualys IaC Security’ tab.

7. Enter your Qualys credentials.

8. Click **Test Connection** to ensure you are authenticated. The plugin will not be able to perform scans unless the test connection is successful.

9. Enter the path to the IaC template (file extension must be .yml, .yaml, JSON or .tf).

10. You can choose to display failed results only, set the build failure conditions and timeout period.

11. Click **Save** and then click **Create**.
Run IaC Scan

Once we’ve deployed the IaC plugin and authenticated ourselves, we can run scans on selected templates.

1. On the Build dashboard of your new plan, click **Run > Run Plan**.
2. Wait till the build is generated.
View Scan Output

At the end of the job, the Bamboo plan creates the artifact file.

Go to **Qualys IaC Scan Results** to view the scan report for a selected plan.

The Build Summary displays the failed controls of all the scanned templates. The failed scans are categorized based on their criticality.
View the failed controls on the IaC Posture tab.

Lastly, check the Remediation tab to learn how you can resolve the misconfiguration.