



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.

For supported templates, other integrations, and features of Cloud IaC Security, refer to [CloudView User Guide](#) and [CloudView API User Guide](#).

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](#)

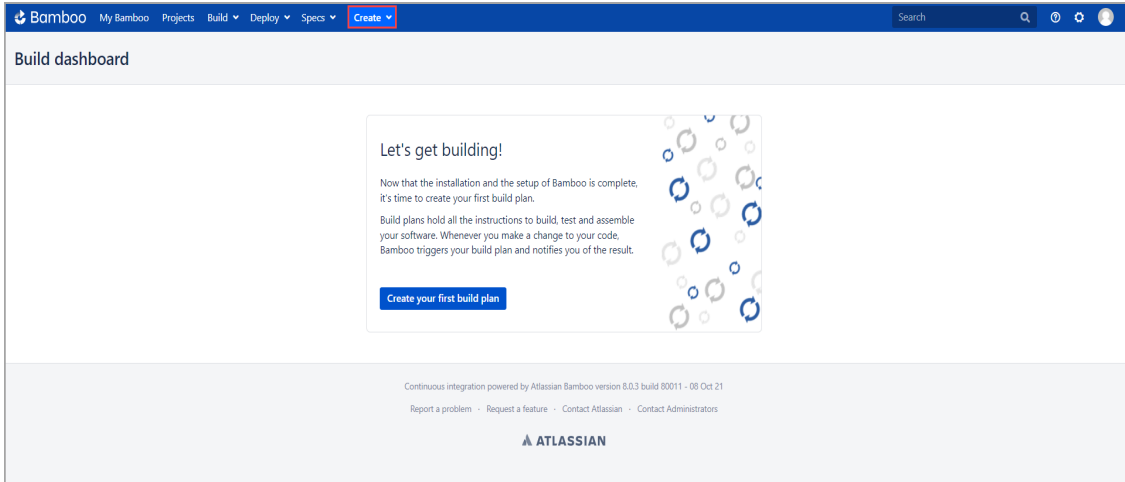
[Run IaC Scan](#)

[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**.

The screenshot shows the 'Create plan' configuration screen. At the top, there's a breadcrumb trail: 'Configure plan' > 'Link repositories' > 'Configure job'. The main heading is 'Create plan'. Below it, the sub-heading is 'Select a project and configure a plan'. A blue box contains a tip: 'Your build plan defines everything about your build process. Each plan has a Default job when it is created. More advanced configuration options, including those for apps, and the ability to add more jobs will be available to you after creating this plan. Learn more on creating a plan'. The form fields are: 'Project' (dropdown menu with 'TestProject' selected), 'Plan name' (text input with 'test'), 'Plan key' (text input with 'TEST'), and 'Plan description' (text input with 'test description'). There's also a 'Plan access' checkbox labeled 'Allow all users to view this plan; this applies to all new projects.' which is checked. At the bottom, there are 'Create' and 'Cancel' buttons.

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**

The screenshot shows the 'Repository host' configuration section in Bamboo. At the top, it displays 'Project: TestProject', 'Plan: test1', and 'Plan key: TEST1'. The 'Repository host' section has two radio buttons: 'None' and 'Link new repository' (which is selected). Below this is a 'Git' dropdown menu. The 'Display name' field contains 'e.g. My repository (branch alpha)'. The 'Git details' section includes a 'Repository URL' field with 'https://github.com/test/Terraform-IaC-Scan' and a help icon. Below the URL is the text 'The URL of your Git repository.' The 'Authentication type' dropdown is set to 'Username and password'. Below this are three radio buttons: 'Use shared credentials', 'Provide username and password' (selected), and a note 'Reuse predefined shared credentials or provide custom username/password pair for authentication.' The 'Username' field contains 'test' with the text 'Username you want to use to authenticate with http(s) or SSH repository.' below it. The 'Password' field is masked with dots with the text 'Password you want to use to authenticate with http(s) or SSH repository.' below it. The 'Branch' field contains 'main' with the text 'The name of a branch or a tag that contains the source code.' below it. There is a 'Test connection' button. At the bottom, the 'Who has access' section has two radio buttons: 'All users have access to this repository.' (selected) and 'Only you have access to this repository.' At the very bottom are 'Save and continue' and 'Cancel' buttons.

Project: TestProject
Plan: test1
Plan key: TEST1

Repository host* ☐ None ☒ Link new repository

Git

Display name* e.g. My repository (branch alpha)

Git details

Repository URL* https://github.com/test/Terraform-IaC-Scan ⓘ
The URL of your Git repository.

Authentication type Username and password
☐ Use shared credentials
☒ Provide username and password
Reuse predefined shared credentials or provide custom username/password pair for authentication.

Username test
Username you want to use to authenticate with http(s) or SSH repository.

Password
Password you want to use to authenticate with http(s) or SSH repository.

Branch main
The name of a branch or a tag that contains the source code.

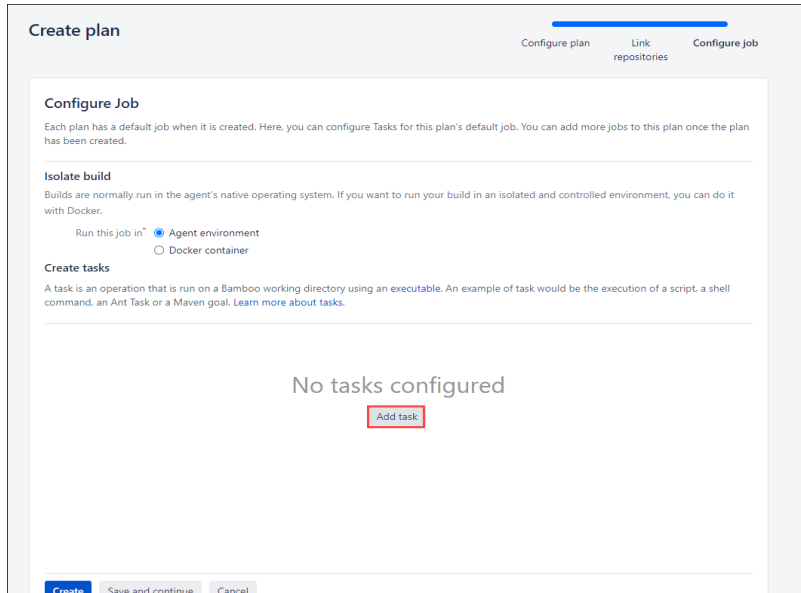
Test connection

Who has access ☒ All users have access to this repository.
☐ Only you have access to this repository.

Save and continue Cancel

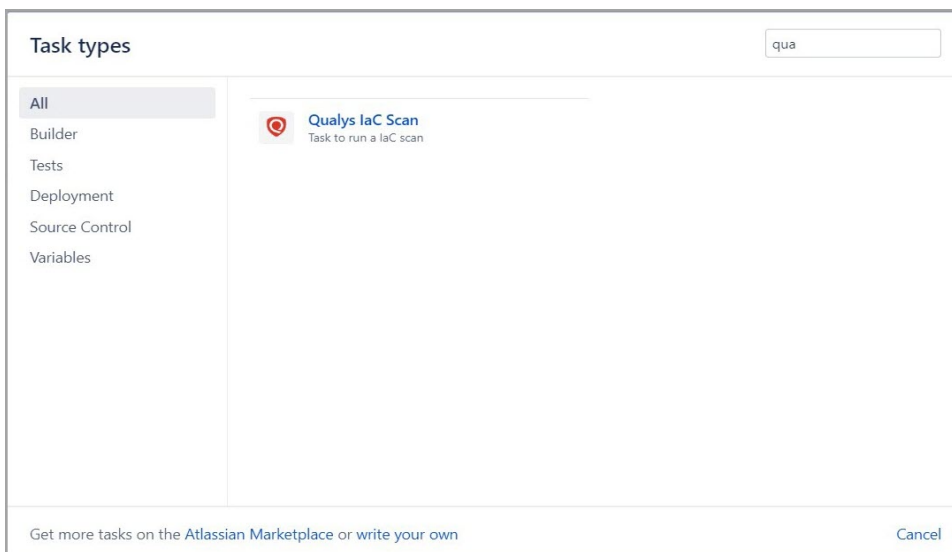
Add Task

5. Under 'Create tasks', click **Add tasks**.



The screenshot shows the 'Create plan' dialog with the 'Configure job' tab selected. The 'Create tasks' section is highlighted, and the 'Add task' button is visible. The dialog includes sections for 'Configure Job', 'Isolate build', and 'Create tasks'. The 'Create tasks' section states: 'A task is an operation that is run on a Bamboo working directory using an executable. An example of task would be the execution of a script, a shell command, an Ant Task or a Maven goal. [Learn more about tasks.](#)'

6. Search for the Qualys IaC Scan plugin and Install it.



The screenshot shows the 'Task types' dialog with a search bar containing 'qua'. The 'All' category is selected in the left sidebar. The 'Qualys IaC Scan' task type is displayed, described as 'Task to run a IaC scan'. The dialog includes a sidebar with categories: All, Builder, Tests, Deployment, Source Control, and Variables. At the bottom, it says 'Get more tasks on the Atlassian Marketplace or write your own' and has a 'Cancel' button.

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.

The screenshot shows the Bamboo web interface for configuring a task. The top navigation bar includes 'Job details', 'Docker', 'Tasks' (selected), 'Requirements', 'Artifacts', and 'Other'. The main heading is 'Tasks'. Below it, a brief description states: 'A task is a piece of work that is being executed as part of the build. The execution of a script, a shell command, an Ant Task or a Maven goal are only few examples of Tasks. [Learn more about tasks.](#)' A note below says: 'You can use [runtime](#), [plan](#), [project](#) and [global](#) variables to parameterize your tasks.' On the right, it says '1 agent has the [capabilities](#) to run this job' and 'How to use the Source Code Checkout task'.

The left sidebar shows a list of tasks under the 'Source Code Checkout' category. The first task is 'Test Repository', which is selected. Below it, a list of repositories is shown, with 'Qualys IaC Security' selected. An 'Add task' button is at the bottom of the sidebar.

The main content area is titled 'Source Code Checkout configuration'. It contains the following fields and options:

- Task description:** A text input field with the value 'Test Repository'.
- ☐ **Disable this task**
- ☐ **Add condition to task** (with a help icon)
- You can check out one or more repositories with this Task. You can choose to check out the Plan's [Default Repository](#) or specify a [Specific Repository](#). You can add additional repositories to this Plan via the [Plan configuration](#).
- Repository***: A dropdown menu with 'test' selected.
- Default always points to Plans default repository.*
- Checkout Directory**: A text input field.
- (Optional) Specify an alternative sub-directory to which the code will be checked out.
- ☐ **Force Clean Build**
Removes the source directory and checks it out again prior to each build. This may significantly increase build times.
- [+ Add repository](#)
- Save** and **Cancel** buttons at the bottom.

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

9. Enter your Qualys credentials.

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

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

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

13. Click **Save** and then click **Create**.

The screenshot shows the Bamboo web interface for configuring a task named 'Qualys IaC Security'. On the left, a sidebar lists 'Source Code Checkout' and 'Test Repository' under 'Final tasks'. The main panel is titled 'Qualys IaC Security configuration'. It includes a 'Task description' field with the value 'test'. Below this are checkboxes for 'Disable this task' and 'Add condition to task'. The 'API Login' section contains fields for 'Qualys Platform URL*' (https://qualysguard.qg3.apps.qualys.com/), 'Qualys Username*' (masked with dots), and 'Qualys Password*' (masked with asterisks). A 'Test Connection' button is located below the password field. The 'Launch Scan API Parameters' section has a 'Scan Name' field (test) and a 'Compressed File path/Directory to be scanned*' field (Terraform-IaC-Scan/terraform sample). A note at the bottom states: 'Note: Qualys IaC Scan will only recognize files with the extensions .yaml, .json, .tf, .template for scans. Other files in the directory will be ignored. Relative path should start from checkout directory, if folder is checked from git repository.' At the bottom, there are checkboxes for 'Failed results only' and 'Build Failure Conditions' (which is checked).

Source Code Checkout
Test Repository

Final tasks: Are always executed even if a previous task fails

Qualys IaC Security
test

Add task

Qualys IaC Security configuration

Task description

test

☐ Disable this task

☐ Add condition to task ⓘ

API Login

Qualys Platform URL*

https://qualysguard.qg3.apps.qualys.com/

Qualys Username*

.....

Qualys Password*

Test Connection

Launch Scan API Parameters

Scan Name

test

Compressed File path/Directory to be scanned*

Terraform-IaC-Scan/terraform sample

Note: Qualys IaC Scan will only recognize files with the extensions .yaml, .json, .tf, .template for scans. Other files in the directory will be ignored. Relative path should start from checkout directory, if folder is checked from git repository.

☐ Failed results only

☒ Build Failure Conditions

Run IaC Scan

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

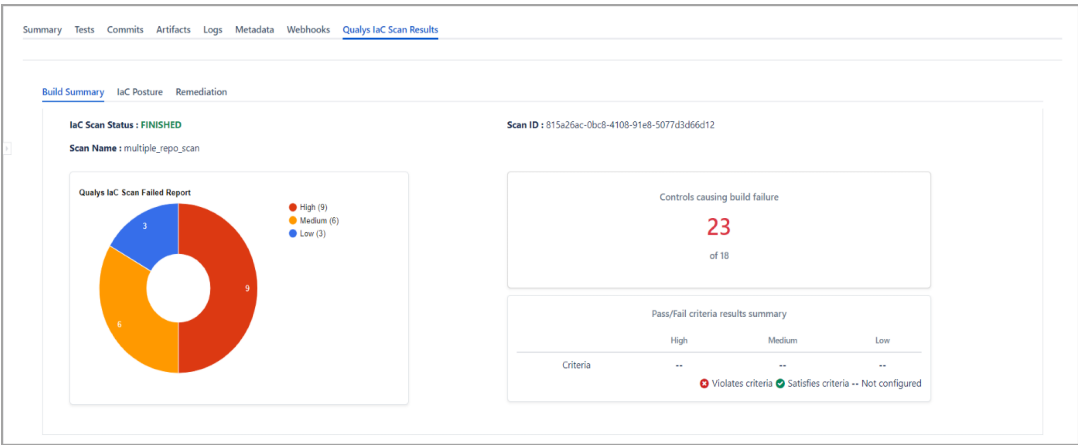
1. On the Build dashboard of your new plan, click **Run > Run Plan**.
2. Wait till the build is generated.

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.

Summary Tests Commits Artifacts Logs Metadata Webhooks <u>Qualys IaC Scan Results</u>						
Build Summary <u>IaC Posture</u> Remediation						
Control ID	Control Name	Criticality	Result	File Path	Resource	
299	Ensure no hard coded AWS access key and secret key exists in provider	HIGH	PASSED	/aws_iam_account_password_policy/provider.tf	aws.default	
299	Ensure no hard coded AWS access key and secret key exists in provider	HIGH	PASSED	/aws_lambda_function/provider.tf	aws.default	
299	Ensure no hard coded AWS access key and secret key exists in provider	HIGH	PASSED	/aws_s3_bucket/provider.tf	aws.default	
299	Ensure no hard coded AWS access key and secret key exists in provider	HIGH	PASSED	/iam-policies/provider.tf	aws.default	
10	Ensure IAM password policy require at least one number	HIGH	PASSED	/aws_iam_account_password_policy/iam-password-expiry.tf	aws_iam_account_password_policy.pass_expiry_90	
11	Ensure IAM password policy requires minimum length of 14 or greater	HIGH	PASSED	/aws_iam_account_password_policy/iam-password-expiry.tf	aws_iam_account_password_policy.pass_expiry_90	
12	Ensure IAM password policy prevents password reuse	HIGH	PASSED	/aws_iam_account_password_policy/iam-password-expiry.tf	aws_iam_account_password_policy.pass_expiry_90	
13	Ensure IAM password policy expires passwords within 90 days or less	HIGH	FAILED	/aws_iam_account_password_policy/iam-password-expiry.tf	aws_iam_account_password_policy.pass_expiry_90	
7	Ensure IAM password policy requires at least one uppercase letter	HIGH	PASSED	/aws_iam_account_password_policy/iam-password-expiry.tf	aws_iam_account_password_policy.pass_expiry_90	
8	Ensure IAM password policy require at least one lowercase letter	HIGH	PASSED	/aws_iam_account_password_policy/iam-password-expiry.tf	aws_iam_account_password_policy.pass_expiry_90	
9	Ensure IAM password policy require at least one symbol	HIGH	PASSED	/aws_iam_account_password_policy/iam-password-expiry.tf	aws_iam_account_password_policy.pass_expiry_90	
10	Ensure IAM password policy require at least one number	HIGH	PASSED	/aws_iam_account_password_policy/iam-password-expiry.tf	aws_iam_account_password_policy.pass_lowercase	

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

Build dashboard / TestProject / test

Build #4

Plan branch:

main

Actions

4 failed – Manual run by

Summary

Tests

Commits

Artifacts

Logs

Metadata

Webhooks

Qualys IaC Scan Results

Build Summary

IaC Posture

Remediation

Show 10 entries

Search:

Control ID	Remediation
7	Ensure aws_iam_account_password_policy resource has require_uppercase_characters argument set to True.
8	Ensure aws_iam_account_password_policy resource has require_lowercase_characters argument set to True.
9	Ensure aws_iam_account_password_policy resource has require_symbols argument set to True.
10	Ensure aws_iam_account_password_policy resource has require_numbers argument set to True.
11	Ensure aws_iam_account_password_policy resource has minimum_password_length argument set to 14 or more.
12	Ensure aws_iam_account_password_policy resource has password_reuse_prevention argument set to 24 or more.
13	Ensure aws_iam_account_password_policy resource has max_password_age argument set to 90 Days or less.
17	Ensure that aws_iam_user_policy aws_iam_user_policy_attachment or aws_iam_policy_attachment resource is not used for adding IAM policy to the users.
17	Ensure that aws_iam_user_policy aws_iam_user_policy_attachment or aws_iam_policy_attachment resource is not used for adding IAM policy to the users.
17	Ensure that aws_iam_user_policy aws_iam_user_policy_attachment or aws_iam_policy_attachment resource is not used for adding IAM policy to the users.

Showing 1 to 10 of 60 entries

Previous

1

2

3

4

5

6

Next