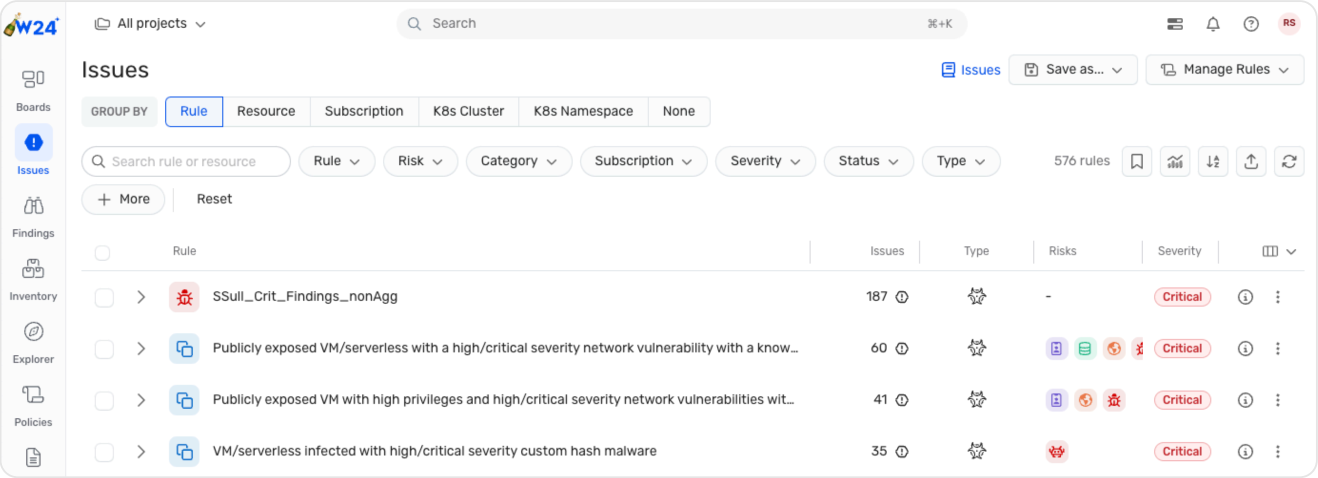
Issues

The Issues page presents the risks and threats that Wiz has identified in your cloud environment, as defined by Policies. By default, Issues are generated by Controls or critical/high severity Threat Detection Rules. Cloud Configuration Rules can be set to generate Issues. Learn about Controls & Issues.



Rule	Issues	Type	Risks	Severity
SSull_Crit_Findings_nonAgg	187		-	Critical
Publicly exposed VM/serverless with a high/critical severity network vulnerability with a know...	60			Critical
Publicly exposed VM with high privileges and high/critical severity network vulnerabilities wit...	41			Critical
VM/serverless infected with high/critical severity custom hash malware	35			Critical

From the Issues page, you can investigate and manage Issues, as well as configure automations and actions:

Investigate

- Group and filter Issues
- Investigate a resource
- Ignore an Issue
- Reopen an ignored Issue
- Export single Issue to PDF
- Export multiple Issues
- View compliance by Project
- View system activity for an Issue

Manage

- Reassess an Issue
- Re-run a Policy
- Edit a Policy
- Disable a Policy

- Delete a Policy

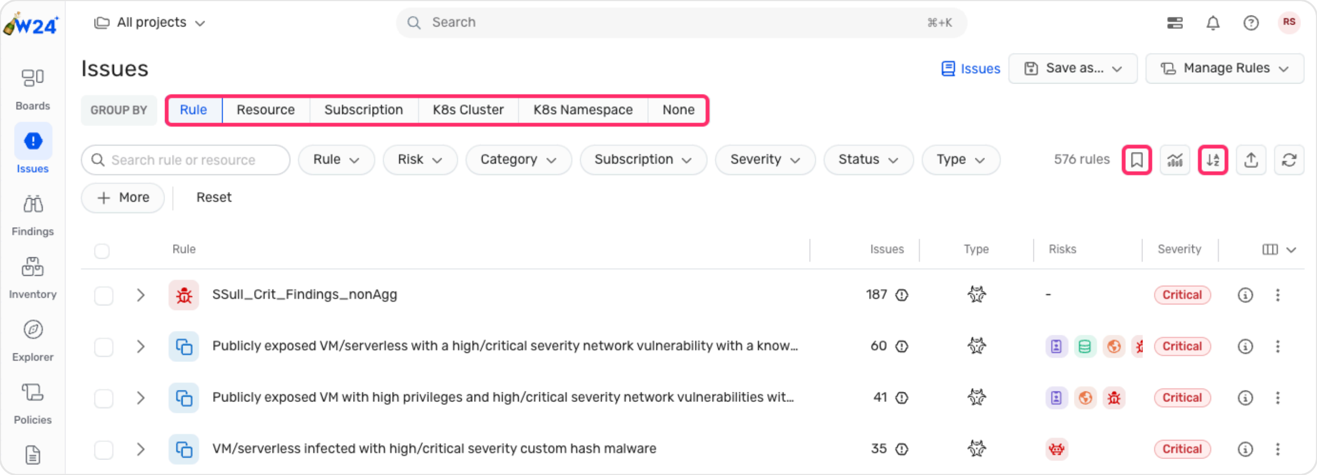
Actions & Automation

- View or generate remediation steps for an Issue
- Create an Automation Rule for a single Policy
- Create an Automation Rule for multiple Policies
- Create a ticket for a single Issue
- Create a ticket for all Issues generated by a single Policy
- Associate or disassociate an Issue with a ticket
- Associate or disassociate a Policy with a ticket
- Remediate an Issue
- Run an Action on an Issue
- Run an Action on (or update) multiple Issues
- Run an Action on multiple Policies

Investigate

Group and filter Issues

By default, the Issues page lists all open Issues grouped by Policy and sorted by severity.



Rule	Issues	Type	Risks	Severity
SSull_Crit_Findings_nonAgg	187		-	Critical
Publicly exposed VM/serverless with a high/critical severity network vulnerability with a know...	60			Critical
Publicly exposed VM with high privileges and high/critical severity network vulnerabilities wit...	41			Critical
VM/serverless infected with high/critical severity custom hash malware	35			Critical

To group, filter, or reorder Issues:

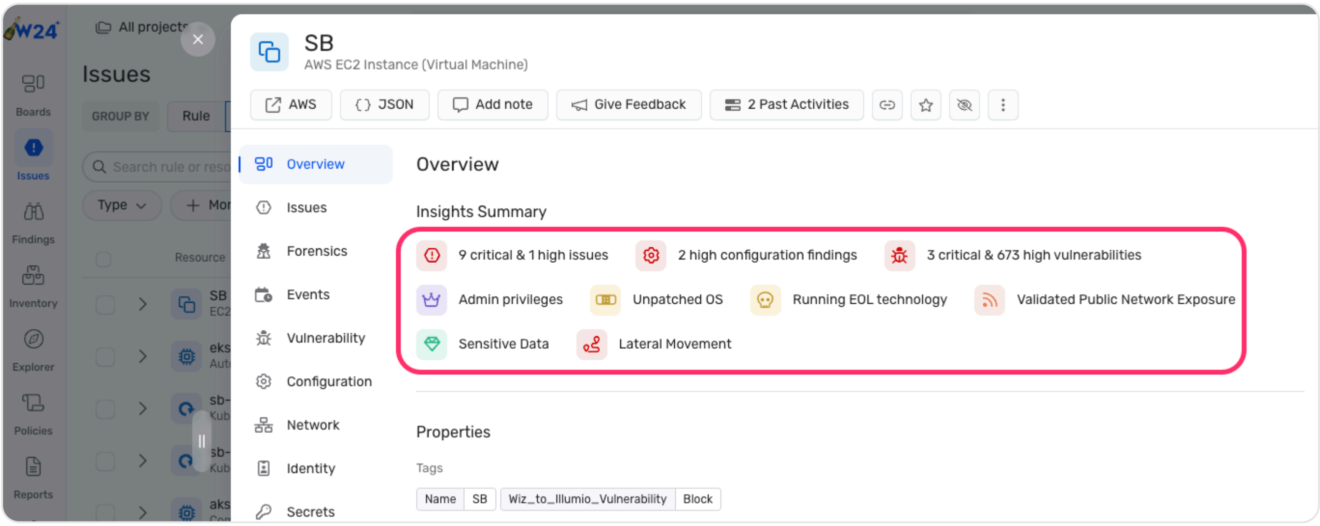
- Click Rule, Resource, Subscription, K8s Cluster, K8s Namespace, or None to change how Issues are grouped.
- Search for a Rule, resource, Subscription, cluster, or namespace.
- Select one or more filter criteria.
- At the top right, click Quick Filters to apply a built-in filter.
- At the top right, click Order Options to change how the currently displayed Issues are ordered.

> ℹ A logical AND operator is applied between different types of filter criteria, but a logical OR operator is applied between the same types of filter criteria. For example, applying a filter for Critical and Open Issues returns only Issues that are both critical AND open, but applying a filter for Critical, High, Open, and In Progress Issues returns Issues that are either critical OR high AND whose status is either open OR in progress.

Investigate a resource

To identify the most problematic resources in your cloud environments:

1. At the top, click Resource. The list of Issues is updated and sorted by resources with the greatest number of critical severity (then high severity) Issues.
2. Click a resource with multiple critical and/or high severity Issues. The details drawer opens on the right.
3. In the details drawer, click one of the insights to switch directly to the relevant tab, or inspect the properties for information to decide how to respond. For instance:
   - Is it active?
   - Is it accessible from the public internet?
   - Does it possess high or admin privileges?
   - Have any users logged in recently?



4. (Recommended) Switch to the Issues tab to review the Issues associated with the resource, each of which can be opened in a new details drawer that shows a preview of the Issue on the Security Graph.
5. (Optional) View or generate remediation steps for the Issue.

Resolve an Issue

> ⚠ Only Issues generated by Threat Detection Rules can be manually resolved. All other types of Issues are automatically resolved by Wiz when a later scan

> indicates that at least one of their risks were remediated.

Issues generated by Threat Detection Rules are automatically resolved by Wiz 30 days after the last detection. As long as the Issue keeps gathering evidence, you must resolve it manually.

To manually resolve an Issue generated by a Threat Detection Rule:

1. At the top of the Issues page, filter for Type > Threat Detection.
2. Open the details drawer for an Issue associated with a specific resource. If Issues are grouped by...
   - ...Rule, click a Rule, then click a Resource, or
   - ...Resource, click a Resource, then click an Issue, or
   - ...Subscription, click a Subscription, then click an Issue, or
   - ...K8s Cluster, click a Cluster, then click an Issue, or
   - ...K8s Namespace, click a Namespace, then click an Issue, or
   - ...None, click an Issue.
3. In the details drawer, click Status > Resolved.
4. In the Resolve Issue dialog:
   i. Select a Reason.
   ii. Provide a Comment.
   iii. Click Resolve Issue.

Ignore an Issue

You can ignore an Issue to silence any new future detections for the selected pairing of Control/Rule and resource. While an Issue is ignored, the underlying Policy can still generate Issues on other resources, and other Controls or Rules can still generate different Issues on the original resource. Ignored Issues can always be reopened later on.

> ✓ To better monitor why Issues were ignored, you can require a note when they are ignored.

To ignore an Issue:

1. From the Issues page, open the details drawer for an Issue associated with a specific resource. If Issues are grouped by...

   - ...Rule, click a Rule and then click a resource, or
   - ...Resource, click a resource, then click an Issue, or
   - ...Subscription, click a Subscription, then click an Issue, or
   - ...K8s Cluster, click a cluster, then click an Issue, or

- ...K8s Namespace, click a namespace, then click an Issue, or
- ...None, click an Issue.

2. In the details drawer, click Status > Ignored.

3. In the Ignore Issue dialog:

   i. Select a Reason.
   ii. Provide a Comment.
   iii. (Strongly recommended) Select a date on which the Issue will automatically transition from Ignored to Open. If no date is selected, the Issue will remain ignored forever.
   iv. Click Ignore Issue.

> ℹ You can view all ignored Issues by filtering on Status > Ignored, or view only Issues that were ignored as exceptions, by design, or false positives.

Reopen an ignored Issue

Because ignoring an Issue prevents the related Policy from generating new Issues on that resource either forever or until the selected date, you may need to reopen an ignored Issue:

1. From the Issues page, filter for Status > Ignored (direct link).
2. Open the details drawer for an Issue associated with a specific resource. If Issues are grouped by...
   - ...Rule, click a Rule, then click a resource, or
   - ...Resource, click a resource, then click an Issue, or
   - ...Subscription, click a Subscription, then click an Issue, or
   - ...K8s Cluster, click a cluster, then click an Issue, or
   - ...K8s Namespace, click a namespace, then click an Issue, or
   - ...None, click an Issue.
3. In the details drawer, you can:
   - Change the Status to Open, In Progress, or (for Threat Detection Issues only) Resolved.
   - Set a Due date, or
   - If a ticket has been created from Wiz, click Related Tickets, then select a ticket to open it in your ticketing platform.

> ℹ
>
> - Issues generated by built-in Controls or Cloud Configuration Rules are automatically resolved by Wiz when a later scan shows that their risks have been remediated. You cannot manually resolve such Issues.

> - Issues generated by Threat Detection Rules are automatically resolved by Wiz 30 days after the last detection. As long as the Issue keeps gathering evidence, you must resolve it manually.

4. In a few days or weeks, you can return to the Issues page and filter by status or due date to verify that the responsible party has addressed the Issue.

Export single Issue to PDF

You can export the Issue drawer to PDF to share with colleagues who don't have access to Wiz.

From the Issues page, open the details drawer for the Issue you want to export, then click 🖶.

Export multiple Issues

You can export the current list of Issues to share with colleagues who don't have access to Wiz.

1. (Optional) Group and/or filter such that only the relevant Issues are displayed.
2. At the top right, click 💾 Save as, then select whether to generate a full Report or a simple CSV File.
3. If you select Report, configure the report:
   1. (Optional) Give the report a more meaningful Name.
   2. Select the Project Scope.
   3. Select a Report Type. If you select Custom, enter the columns to include.
   4. (Optional) Modify the default Filters to include or exclude Issues by their severity, status, cloud platform, etc.
   5. (Optional) Enable report Scheduling.
   6. (Optional) Enable Notifications.
   7. (Optional) Enable Export to data storage like S3 or Snowflake. The relevant integration with the third-party data storage tool must already exist.
   8. (Optional) Configure Compression.
   9. (Optional) Click Advanced Options then select a different CSV Delimiter.
4. Click Create Report.

> ⚠ Reports and their results are subject to limits. Learn more.

View compliance by Project

> ℹ This procedure applies only to Issues generated by Controls or Cloud Configuration Rules. It does not apply to Threat Detection Issues.

You can view how a Control affects each Project and how many Issues each Project has.

To view compliance by Project:

1. Click More Options > View compliance by Project. The Projects page opens.
2. (Optional) Click Issues Breakdown is to filter on other Controls.

View system activity for an Issue

The ⚙ Settings > System Activity Log page lists detailed information about system activities such as Actions.

To view system activity related to an Issue:

1. From the Issues page, open the details drawer for an Issue associated with a specific resource.
2. At the top right, click ⋮ More options > View related system activity. The system activity log opens, filtered for the selected Issue.

Manage

You can only manage Issues generated by Controls or Cloud Configuration Rules. The procedures in this section do not apply to Issues generated by Threat Detection Rules.

Reassess an Issue

Reassessing an Issue causes the underlying Policy's saved query to be re-evaluated for only the selected Issue's primary resource using the current state of the Security Graph. To reassess all Issues generated by a specific Policy, re-run that Policy.

> ℹ Reassessing an Issue does *not* fetch new metadata from your cloud environment or trigger new disk scans. For that, you must rescan an individual resource, an Application Endpoint, or a Connector.

To reassess an Issue:

1. From the Issues page, open the details drawer for an Issue associated with a specific resource. If Issues are grouped by...
    - ...Rule, click a Rule, then click a resource, or
    - ...Resource, click a Resource, then click an Issue, or
    - ...Subscription, click a Subscription, then click an Issue, or

   - ...K8s Cluster, click a cluster, then click an Issue, or
   - ...K8s Namespace, click a namespace, then click an Issue, or
   - ...None, click an Issue.
2. In the details drawer, click ⋮ More Options > Reassess Issues.

Re-run a Policy

Re-running a Policy causes the Policy's saved query to be re-evaluated using the current state of the Security Graph. Results typically take 10-20 minutes to be updated, but Rules with a larger number of resources may take longer.

> ℹ Re-running a Rule does *not* fetch new metadata from your cloud environment or trigger new disk scans. For that, you must rescan an individual resource, an Application Endpoint, or a Connector.

To re-run a Policy, click ⋮ More Options > Re-run.

Edit a Policy

You may only edit custom Controls or Rules created in your environment. Built-in Controls and Rules can only be disabled.

To edit a custom Policy, click ⋮ More Options > Edit.

Disable a Policy

Disabling a Policy automatically closes all open Issues associated with it, which may trigger Automation Rules.

> ℹ Cloud Configuration Controls that have been set to generate Issues must be disabled from the Policies > Cloud Configuration Rules page.

To disable a Policy, click ⋮ More Options > Disable.

Delete a Policy

Only custom Policies can be deleted. Built-in Policies can only be disabled. Deleting a custom Policy resolves all open Issues associated with it, which may trigger Automation Rules.

To delete a custom Policy, click ⋮ More Options > Delete.

Actions & automation

Automation Rules can be defined to automatically send Issues from Wiz to third-party tools. Learn about actions & automation.

View or generate remediation steps for an Issue

Wiz analysts write generic remediation steps for most Issues. If AI-generated remediation steps have been enabled for your tenant, you can also generate custom, Issue-specific remediation steps for a selected platform.

1. From the Issues page, open the details drawer for an Issue associated with a specific resource. If Issues are grouped by...
   - ...Rule, click a Rule, then click a resource, or
   - ...Resource, click a resource, then click an Issue, or
   - ...Subscription, click a Subscription, then click an Issue, or
   - ...K8s Cluster, click a cluster, then click an Issue, or
   - ...K8s Namespace, click a namespace, then click an Issue, or
   - ...None, click an Issue.
2. In the details drawer, switch to the Remediation tab.
3. Inspect the generic remediation steps.

> ❗ You must validate AI-generated remediation steps before executing them in your environment.

4. (Optional) If AI-generated remediation steps have been enabled for your tenant:
   1. Select a platform like CLI or Terraform, then click Generate Remediation Steps.
   2. Validate the AI-generated remediation steps before executing them in your environment.

> ⚠
>
> - AI-generated remediation steps are subject to limits. Learn more.
> - AI-generated remediation steps are only available for built-In Controls.

Create an Automation Rule for a single Policy

1. On the Issues page, click ⋮ More Options > Create automation. The New Automation Rule page open, with the current Policy pre-populated as an IF rule condition.
2. Provide other required information. See the guide on adding an Automation Rule.

Create an Automation Rule for multiple Policies

1. Build a filter using only the supported filter criteria.

> The supporter filter criteria are: Category, Cloud Platform, Control, Has Comments, Has Ticket, Native Type, Project, Region, Resolution, Resource, Resource Group, Resource Status, Resource Tags, Resource Type, Risk, Severity, Status, Subscription, and Type.

2. At the top right, click Save as > Automation Rule. The New Automation Rule page opens, with the current filter pre-populated as IF rule conditions.
3. Provide other required information. See the guide on adding an Automation Rule.

Create a ticket for a single Issue

If you have integrated a third-party ticketing service such as Jira or ServiceNow, you can create a ticket for a single Issue directly from that Issue's details drawer.

1. From the Issues page, open the details drawer for an Issue associated with a specific resource. If Issues are grouped by...
   - ...Rule, click a Rule, then click a resource, or
   - ...Resource, click a resource, then click an Issue, or
   - ...Subscription, click a Subscription, then click an Issue, or
   - ...K8s Cluster, click a cluster, then click an Issue, or
   - ...K8s Namespace, click a namespace, then click an Issue, or
   - ...None, click an Issue.
2. In the details drawer, click Create a Ticket.
3. In the Create a Ticket dialog:
   i. Select an Integration associated with your third-party ticketing service.
   ii. For the selected Integration, you can:
      - Use an existing Action template by clicking Load from template, selecting an Action template, and then clicking Use template.
      - Modify the Action parameters. See the relevant Integration guide for detailed instructions.
      - Save your modifications by clicking Save as template, entering a Template name, selecting a Project Scope, and clicking Save.
   iii. Click Create ticket.

Create a ticket for all Issues generated by a single Policy

If you have integrated a third-party ticketing service like Jira or ServiceNow, you can create a single ticket for all Issues generated by a Control directly from the Issues page in Wiz.

1. At the top of the Issues page, group Issues by Rule.
2. On the Control, click ⋮ More Options > Tickets > Create a new ticket.
3. In the Create a ticket dialog:

    i. (Optional) Select a specific Project Scope to only associate the new ticket with Issues linked to resources in the selected Project.
    ii. Select an Integration. The "Create ticket" Action type is selected automatically.
    iii. For the selected Integration, you can:
        - Use an existing Action template by clicking Load from template, selecting an Action template, and then clicking Use template.
        - Modify the Action parameters. See the relevant Integration guide for detailed instructions.
        - Save your modifications by clicking Save as template, entering a Template name, selecting a Project Scope, and clicking Save.
    iv. Click Create ticket.

Associate or disassociate an Issue with a ticket

Associating a ticket with an Issue adds the URL of the ticket to the details drawer for that Issue. The content of the ticket itself does not change.

To associate or disassociate an Issue with a ticket:

1. On the Issue page, click an Issue to open it.
2. Click Related tickets, then:
    - Click Associate an existing ticket, or
    - Click ▯ to remove an existing ticket.

Associate or disassociate a Policy with a ticket

You can associate (or disassociate) an existing Jira or ServiceNow ticket with a Control.

To associate a ticket:

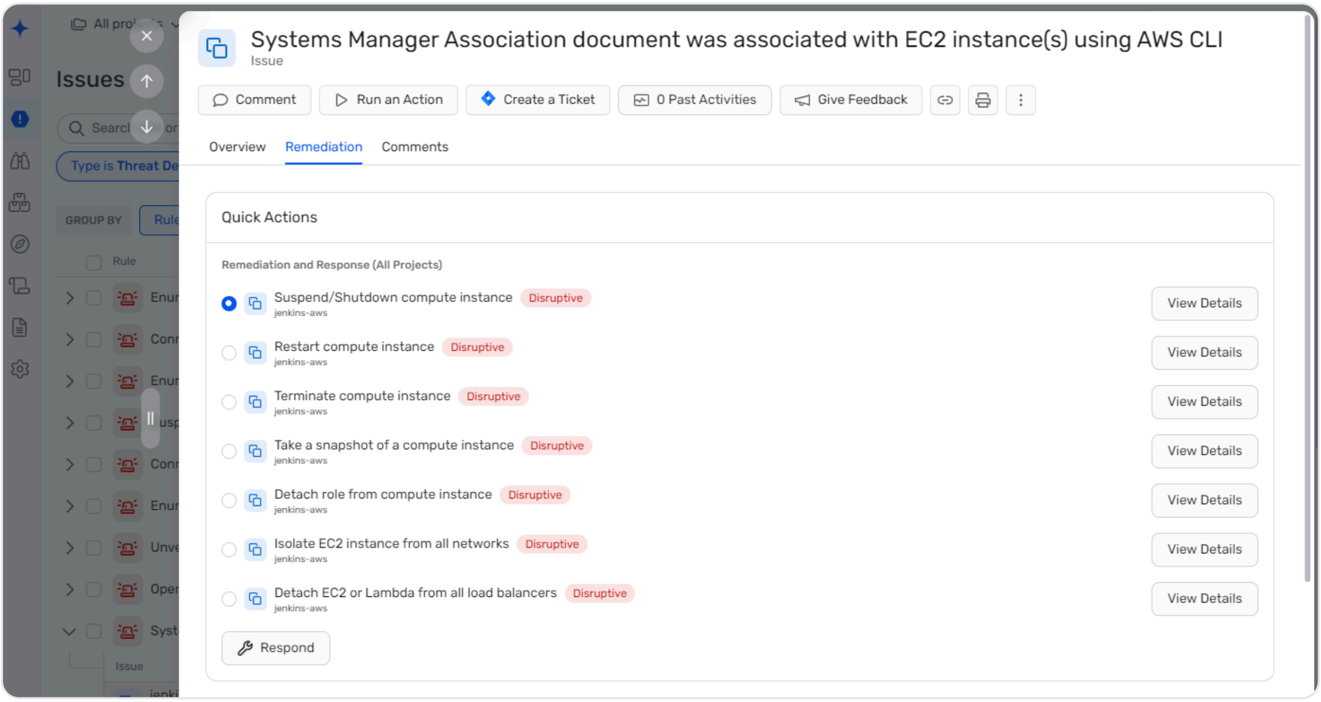
1. At the top of the Issues page, group Issues by Rule.
2. On a Rule, click ⋮ More Options > Tickets > Associate an existing ticket.
3. (Optional) Select a specific Project Scope to only update Issues linked to resources in the selected Project.
4. Enter an existing Ticket ID, e.g. ACM-1234.
5. Enter the existing ticket's URL, e.g. `https://acme.atlassian.net/browse/ACM-1234`.
6. Click Associate Ticket.

To disassociate a ticket:

1. At the top of the Issues page, group Issues by Rule.
2. At the top right of the table of Issues, click Show/Hide Table Columns > Ticket. The column of associated tickets is displayed.
3. Hover over a ticket, then click ▯.
4. Click Confirm.

Remediate an Issue

> Remediating Issues directly in your cloud infrastructure is possible only if you deployed Remediation & Response.



Systems Manager Association document was associated with EC2 instance(s) using AWS CLI
Issue

Comment | Run an Action | Create a Ticket | 0 Past Activities | Give Feedback

Overview | Remediation | Comments

Quick Actions

Remediation and Response (All Projects)

- ● Suspend/Shutdown compute instance Disruptive — jenkins-aws — View Details
- ○ Restart compute instance Disruptive — jenkins-aws — View Details
- ○ Terminate compute instance Disruptive — jenkins-aws — View Details
- ○ Take a snapshot of a compute instance Disruptive — jenkins-aws — View Details
- ○ Detach role from compute instance Disruptive — jenkins-aws — View Details
- ○ Isolate EC2 instance from all networks Disruptive — jenkins-aws — View Details
- ○ Detach EC2 or Lambda from all load balancers Disruptive — jenkins-aws — View Details

Respond

1. Click an Issue to open its details drawer on the right. Available response actions are listed in the Remediation tab.
2. Select a response action.
3. Click Respond. A dialog box opens.
4. Review the target resource and action you are about to run.
5. Click Run.

Run an Action on an Issue

Wiz integrates with third-party platforms using Integrations and Actions in order to send an email or Slack message, call a webhook, perform auto-remediation, etc.

1. From the Issues page, open the details drawer for an Issue associated with a specific resource. If Issues are grouped by...
   - ...Rule, click a Rule, then click a resource, or
   - ...Resource, click a resource, then click an Issue, or
   - ...Subscription, click a Subscription, then click an Issue, or
   - ...K8s Cluster, click a cluster, then click an Issue, or
   - ...K8s Namespace, click a namespace, then click an Issue, or
   - ...None, click an Issue.
2. At the top of the details drawer, click Run an Action.
3. Select an Action Type, then click Continue.

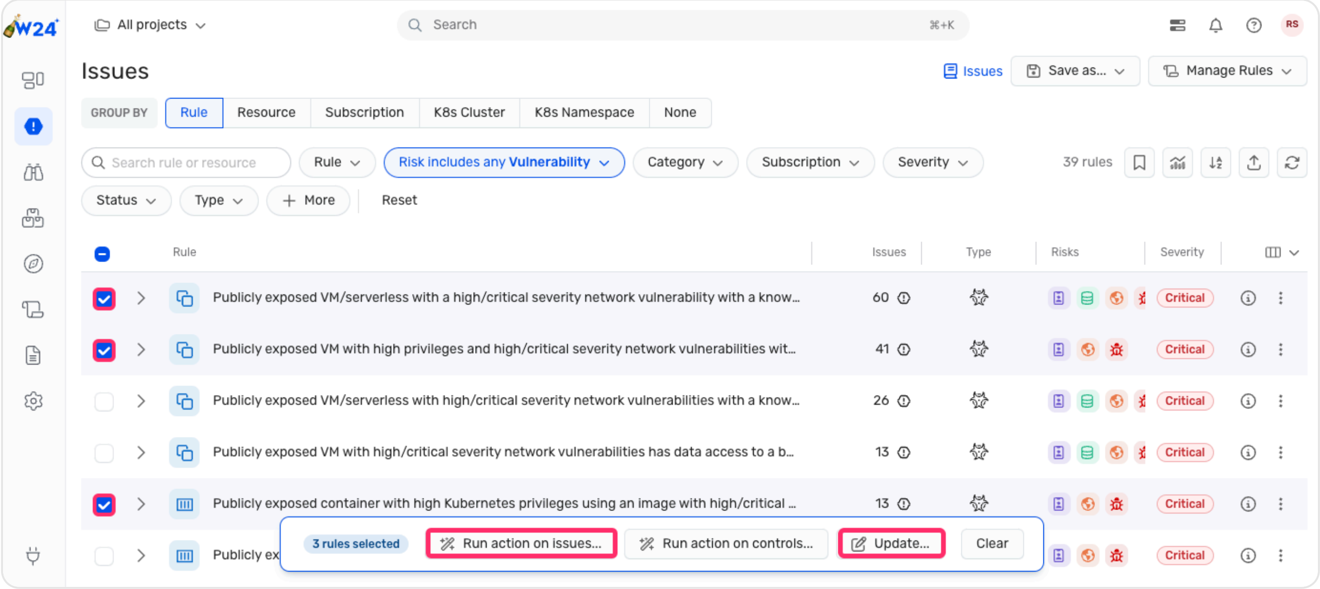
4. For the selected Action, you can:
    - Use an existing Action template by clicking Load from template, selecting an Action template, and then clicking Use template.
    - Modify the Action parameters. See the relevant Integration guide for detailed instructions.
    - Save your modifications by clicking Save as template, entering a Template name, selecting a Project Scope, and clicking Save.
5. (Optional) Click Test to run the selected Action using mock data.
6. Click Run Action.

Run an Action on (or update) multiple Issues

Wiz integrates with third-party platforms using Integrations and Actions in order to send an email or Slack message, call a webhook, perform auto-remediation, etc. You can run an Action on, change the status of, add a note to, or set the due date of multiple Issues in bulk.

> ⚠ Running an Action on (or updating) multiple Issues is subject to limits. Learn more.

1. (Optional) Group and/or filter such that only the relevant Issues are displayed.
2. On the left, select multiple Controls or Rules (or, if grouped by resource, multiple resources). The multi-select dialog appears at the bottom of the screen.



	Rule	Issues	Type	Risks	Severity
☑	Publicly exposed VM/serverless with a high/critical severity network vulnerability with a know...	60			Critical
☑	Publicly exposed VM with high privileges and high/critical severity network vulnerabilities wit...	41			Critical
☐	Publicly exposed VM/serverless with high/critical severity network vulnerabilities with a know...	26			Critical
☐	Publicly exposed VM with high/critical severity network vulnerabilities has data access to a b...	13			Critical
☑	Publicly exposed container with high Kubernetes privileges using an image with high/critical ...	13			Critical
☐	Publicly ex				Critical

3. In the multi-select dialog, click Run action on Issues or Update.

Run Actions on Issues

Running an Action on Issues means the same Action is run over and over, once for every Issue.

1. Select an Action Type.
2. For the selected Action type, you can:
   - Use an existing Action template by clicking Load from template, selecting an Action template, and then clicking Use template.
   - Modify the Action parameters. See the relevant Integration guide for detailed instructions.
   - Save your modifications by clicking Save as new template, entering a Template name, selecting a Project Scope, and clicking Save.
3. (Optional) Click Test to run the selected Action using mock data.
4. Click Run Action on X Issues (where X is the sum of the numbers of Issues generated by the selected Controls or Rules; in the screenshot above X would be 43 + 22 + 19 = 84).

Update

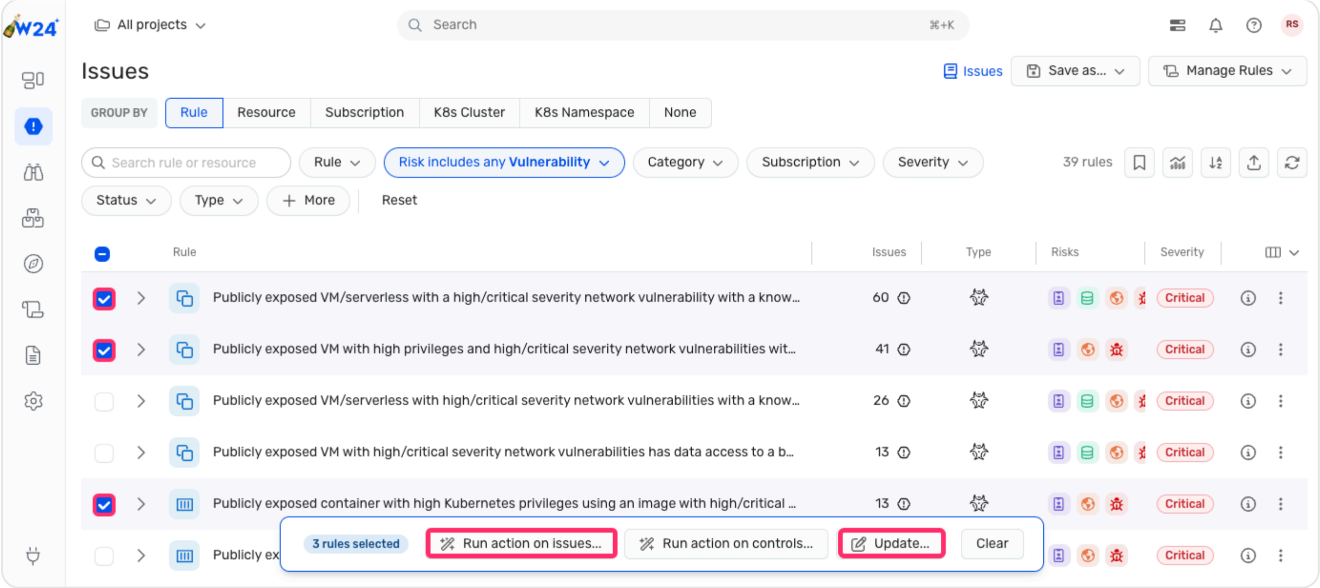
1. Enable Status, Due Date, and/or Comment.
2. Select a status, enter a date, and/or enter a comment.
3. Click Update X Issues (where X is the sum of the numbers of Issues generated by the selected Controls or Rules; in the screenshot above X would be 43 + 22 + 19 = 84).

Run an Action on multiple Policies

Wiz integrates with third-party platforms using Integrations and Actions in order to send an email or Slack message, call a webhook, perform auto-remediation, create a ticket, etc. You can run an Action on one or more Policies in order to send a single email, create a single ticket, etc. for the entire group of Issues generated by that Policy instead of an email, ticket, etc. for each Issue.

> ℹ If you would like to run the same Action on every Issue individually—i.e. a one-to-one mapping that would send an email, call a webhook, etc. for every Issue separately—then you should run an Action on (or update) multiple Issues.

1. At the top of the Issues page, group Issues by Rule.
2. On the left, select one or more Controls or Rules. The multi-select dialog appears at the bottom of the screen.



	Rule	Issues	Severity
☑	Publicly exposed VM/serverless with a high/critical severity network vulnerability with a know...	60	Critical
☑	Publicly exposed VM with high privileges and high/critical severity network vulnerabilities wit...	41	Critical
□	Publicly exposed VM/serverless with high/critical severity network vulnerabilities with a know...	26	Critical
□	Publicly exposed VM with high/critical severity network vulnerabilities has data access to a b...	13	Critical
☑	Publicly exposed container with high Kubernetes privileges using an image with high/critical ...	13	Critical
□	Publicly ex		Critical

3. In the multi-select dialog, click Run Action on Controls.
4. In the Run an Action dialog:
   i. Select a Project Scope.
   ii. Select an Action Type.
   iii. For the selected Action type, you can:
      - Use an existing Action template by clicking Load from template, selecting an Action template, and then clicking Use template.
      - Modify the Action parameters. See the relevant Integration guide for detailed instructions.
      - Save your modifications by clicking Save as new template, entering a Template name, selecting a Project Scope, and clicking Save.
   iv. (Optional) Click Test to run the selected Action using mock data.
   v. Click Run Action on X Controls (where X is the number of selected Controls or Rules; in the screenshot above X would be 3).

Updated about 2 months ago

← Threat Center

Findings →