Alert and Respond

On this page:

Related pages:

- Roles and Permissions
- Enable an Email Server

This topic introduces you to the automated alert and response capabilities in AppDynamics.

About Alerts and Responses in AppDynamics

AppDynamics can generate notifications or take other types of actions based on conditions or events you configure. Using the alert and respond feature, you can find out about problems as they happen, or even before they happen when you define alerts on warning conditions.

In AppDynamics, policies serve as the central configuration artifact for the alert and respond feature. A policy ties one or more conditions or events to the measures to take when the condition is met or event happens.

The condition or event is defined by a health rule, while the steps to take are encapsulated by an action. AppDynamics comes with several preconfigured health rules, giving you a head start and examples for you to following when creating your own. For example, built-in health rules test for whether the "Business Transaction error rate is much higher than normal" or "CLR Garbage Collection Time is too high". See Default Health Rules for more.

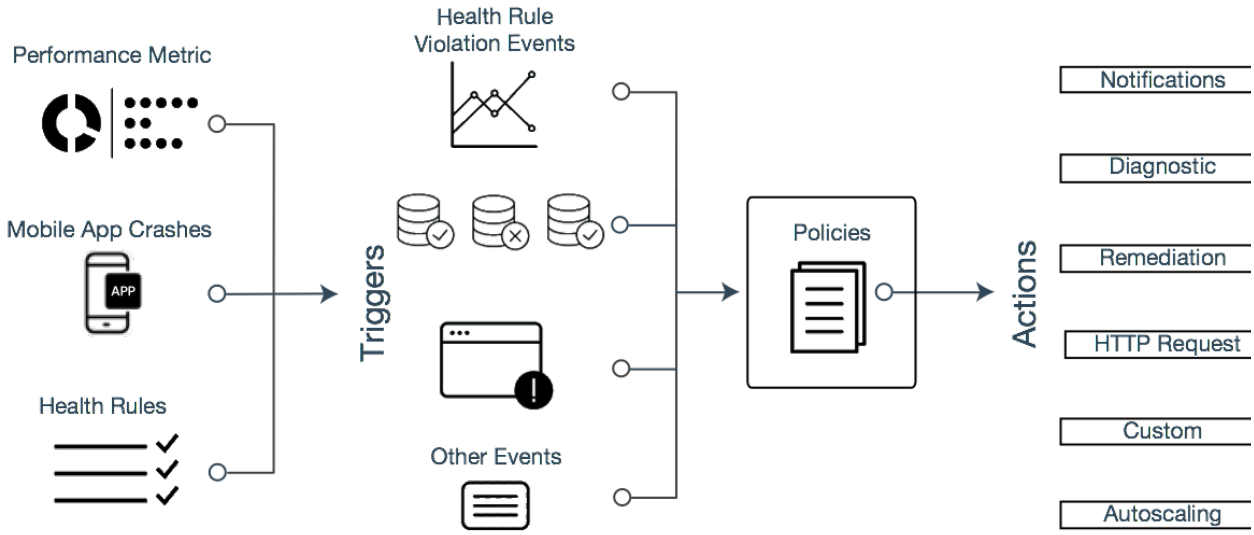
Actions automate the response to an event, such as the sending of an alert or performing diagnostic or remediation actions. See Alert and Respond API to learn how to create custom URLs for notifications.

While policies generate real-time responses to detected conditions, email digests generate email messages about the conditions and events in a system on a scheduled basis.

Notification actions that use email or SMS and email digests require that the SMTP server be configured for the controller. See Enable an Email Server.

Alert and Respond Policy Structure

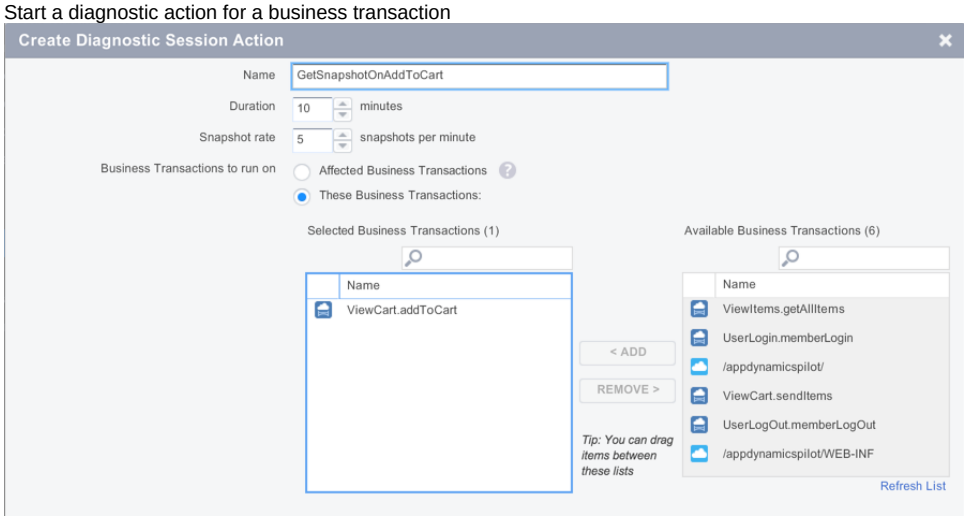
A policy matches evaluated event triggers with actions to be taken in response to those triggers.



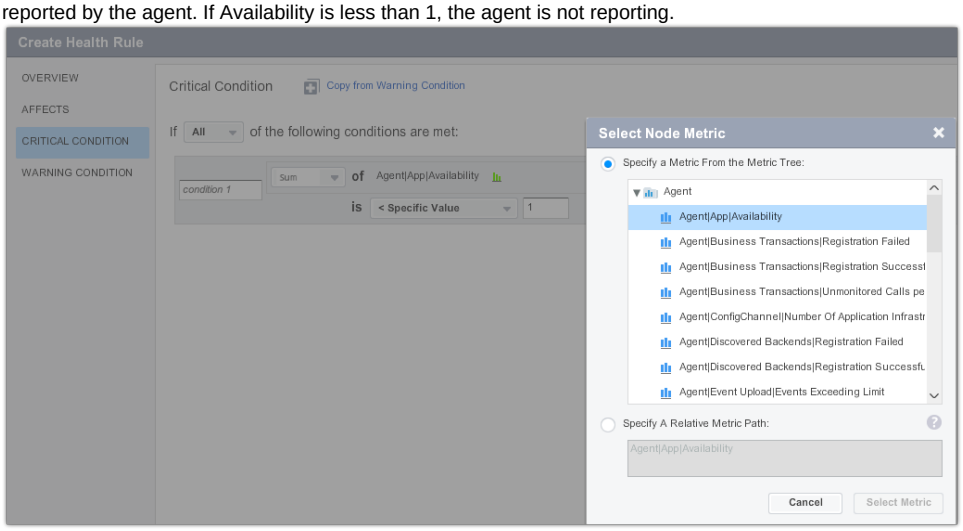
What You Can Do with Alert and Respond

The following use cases illustrate the types of things you can do with the alert and respond feature in AppDynamics. While not an exhaustive list, it should give you an idea about the length and breadth of the feature.

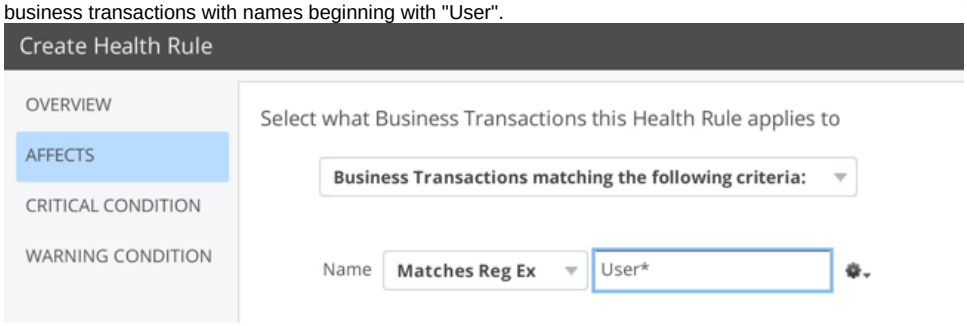
- Define health rules that apply to specific tiers or nodes. Instead of choosing specific nodes, you can trigger a rule when more than a certain percentage of nodes are unhealthy, say 20%.
- Start a diagnostic action for a business transaction



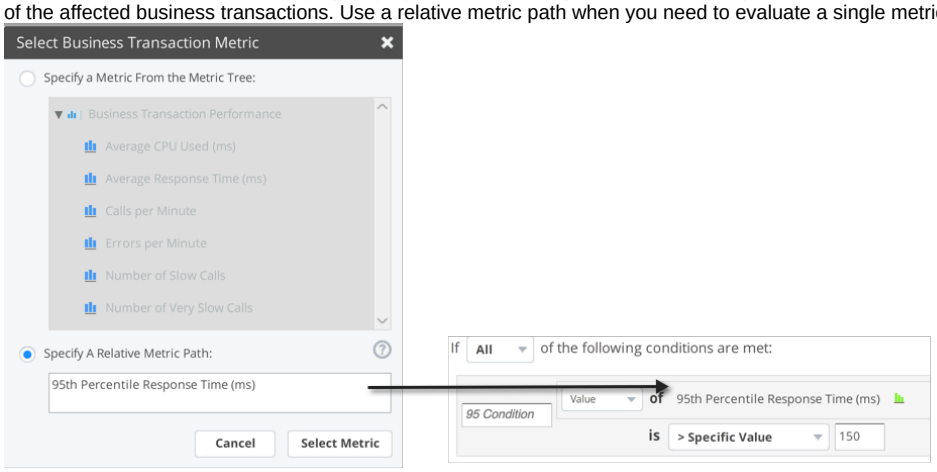
- Alert when an app agent stops reporting to the Controller. Create a node health rule based on the value of the Availability metric reported by the agent. If Availability is less than 1, the agent is not reporting.



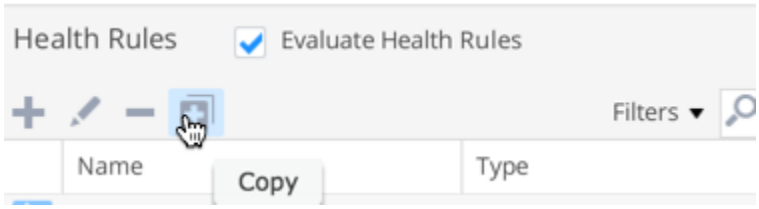
- Alert when the 95th percentile metrics for specific business transactions reach a certain value. You want to apply this rule only to business transactions with names beginning with "User".



- You can generalize a health rule by specifying a relative metric path, rather than a specific metric. The health rule is evaluated for each of the affected business transactions. Use a relative metric path when you need to evaluate a single metric for multiple entities.

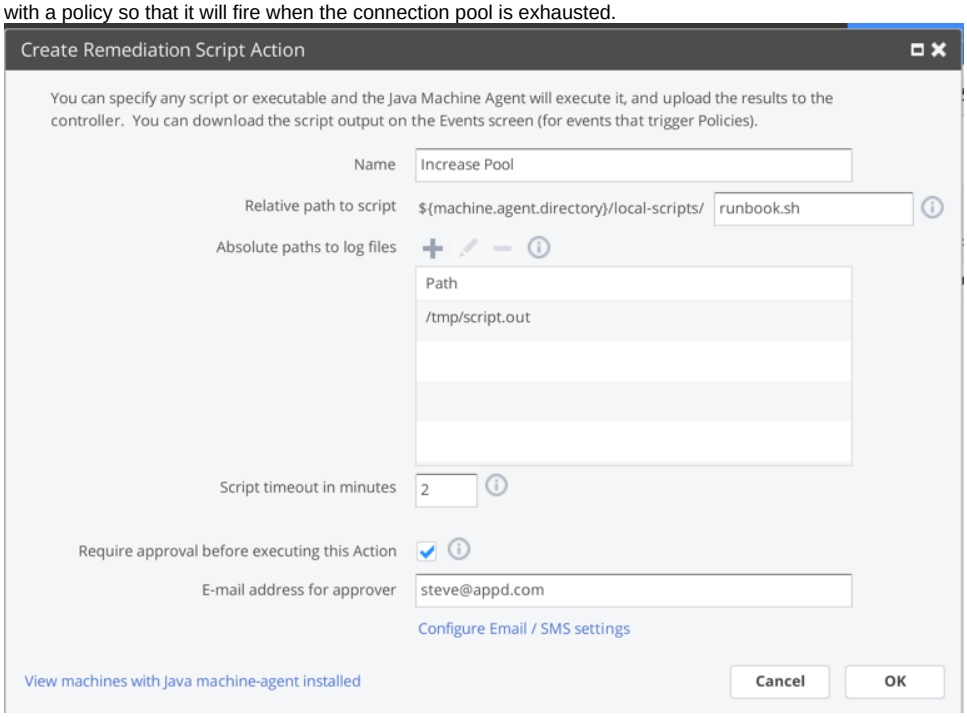


- You have a large operation with several development teams, each responsible for a different service. You create a health rule for one service and then copy it. Then create different policies in which you can pair each copy of the health rule to an alert addressed to the appropriate team.

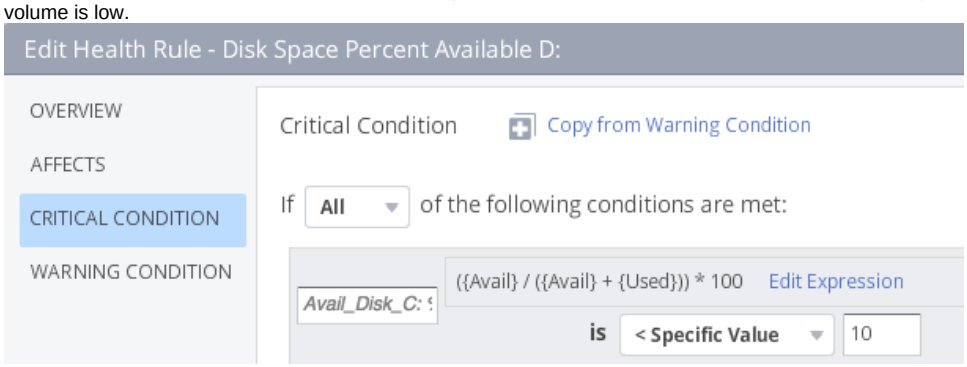


- Start a script to change the size of the connection pool. You have an application that performs well for normal load. However, peak loads can cause the application to slow. During peak load, the AppDynamics not only detects the connection pool contention, but also

allows you to create a remediation script that can automate increasing or decreasing the size of connection pool. You can require human approval to run this script or simply configure it to execute automatically when it is triggered. Create a runbook and associate it with a policy so that it will fire when the connection pool is exhausted.



- Alert when available disk volume is low. Use an expression over two metrics - available and used disk space - to be alerted when disk volume is low.



Watch the Video

Click this link to see a full screen version of the video, Configuring Actions and Policies.

Alert and Respond across the Platform

The alert and respond features work across AppDynamics products, including Infrastructure Visibility, Analytics, EUM, and Application Monitoring. Unless otherwise noted, this documentation describes the features in the context of Application Monitoring, which, by its nature, offers the broadest range of configuration and use case options. Certain features as described may not apply to other AppDynamics products.

Additional usage notes include:

- Policy triggers for applications can be health rule violation events or other types of events. Policy triggers for databases and analytics must be health rule violation events.
- The types of actions that you can create for an application include notifications, diagnostics, remediation, HTTP requests, custom actions and cloud auto-scaling. The types of actions that you can create for a database or analytics are limited to notifications, HTTP requests and custom actions.
- The types of entities affected by a health rule are more limited for databases and analytics than for applications.
- For information on using polices triggered by browser synthetic events see Alerting and Synthetics in Browser Synthetic Monitoring.

Scope and Access

Typically different types of users with different types of roles set up and use different alert and respond features.

Email templates, HTTP request templates, and Email/SMS configuration are account-level features. The scope of these features, once set up, is the entire AppDynamics account. The items created at the account level are available to all the applications in that account. Account-level items are created and managed by users who have account-level roles that include permissions to create them.

By default these roles belong to the account owner and could be granted to an account administrator. Custom roles could also be created that include some of these permissions. For example, an account owner could create an email template manager role that could be assigned to other users to give them the ability to create and modify email templates.

Policies, health rules, actions and email digests are application-level or tier-level features. The scope of these features is the application or tier in which they were created. Only roles with application-level or tier-level permissions are required to create and manage these items.

See the Application- and Tier-Level Permissions section in Roles and Permissions for details about these permissions.