Process Group Settings

Dynatrace Training Module

dynatrace

Agenda

- Process Group Monitoring
- Process Group Detection

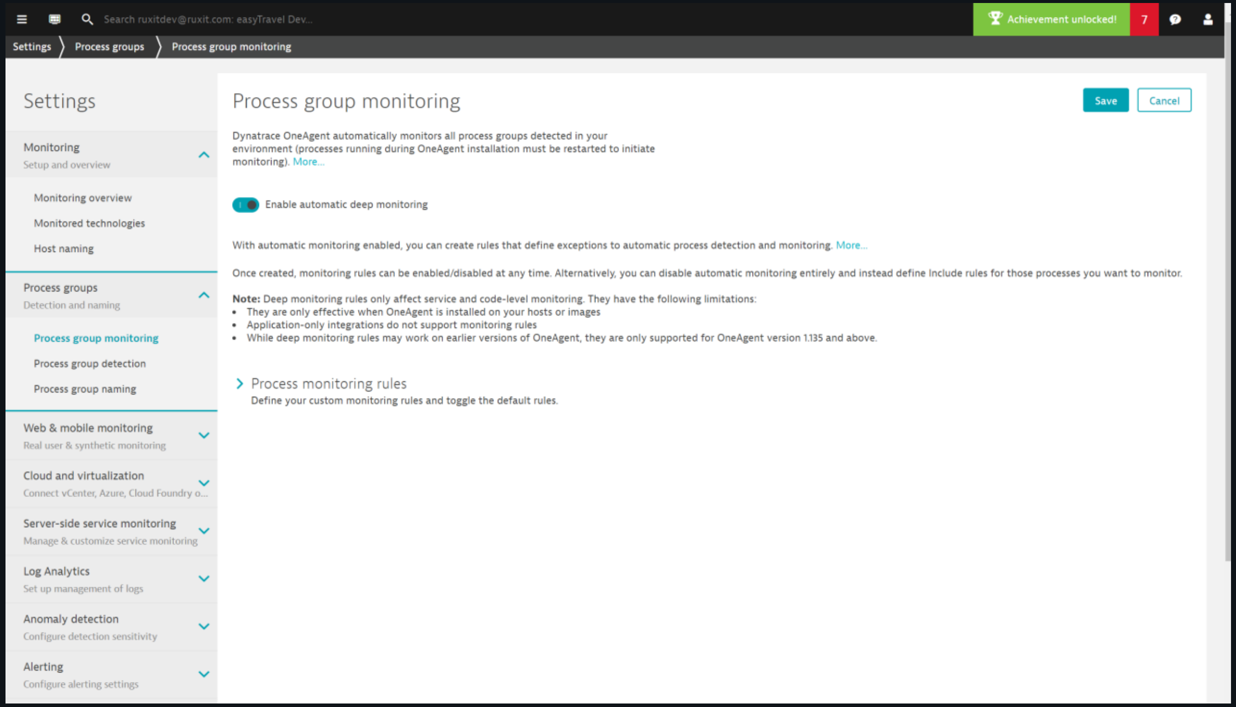
Process Group Monitoring

Process Group Monitoring

- Create rules to instruct the OneAgent which processes to target for Deep Monitoring
- Although the OneAgent automatically detects and monitors supported processes for service insights (purepath level), we recognize not all processes are of equal importance to your monitoring needs.
  - You may have a number of unimportant, or short-lived processes that you do not want to monitor at a code level.
  - You may not be able to run deep monitoring on applications that belong to your customers and are outside of your control.
  - Allow strict control over which processes are monitored
  - Dynatrace doesn't automatically perform deep monitoring of .NET and Go processes, as there are many arbitrary processes that rely on these processes.
- Process group monitoring rules can help

Set up process group monitoring

- The enable deep monitoring switch determines whether Dynatrace One Agent automatically runs deep monitoring of detected processes
  - When ON (the default setting), OneAgent runs deep monitoring for all processes it can monitor unless you specify exceptions for a specific process or by creating rules that define exceptions
  - When OFF Dynatrace OneAgent only runs deep monitoring on processes that match defined rules



Process group monitoring

Dynatrace OneAgent automatically monitors all process groups detected in your environment (processes running during OneAgent installation must be restarted to initiate monitoring). More...

● Enable automatic deep monitoring

With automatic monitoring enabled, you can create rules that define exceptions to automatic process detection and monitoring. More...

Once created, monitoring rules can be enabled/disabled at any time. Alternatively, you can disable automatic monitoring entirely and instead define Include rules for those processes you want to monitor.

Note: Deep monitoring rules only affect service and code-level monitoring. They have the following limitations:

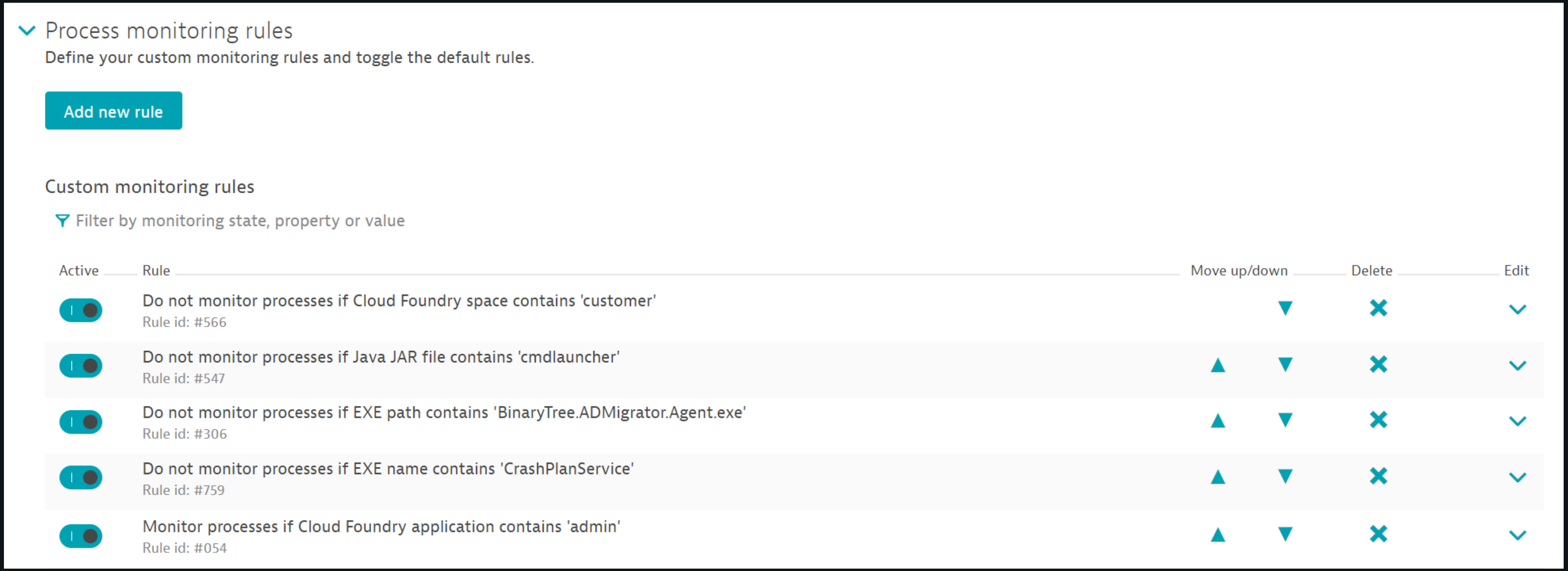
- They are only effective when OneAgent is installed on your hosts or images
- Application-only integrations do not support monitoring rules
- While deep monitoring rules may work on earlier versions of OneAgent, they are only supported for OneAgent version 1.135 and above.

Process monitoring rules

Define your custom monitoring rules and toggle the default rules.

How Process Monitoring rules are applied

- Monitoring rules are split into two categories, custom rules and built-in rules.
- Custom monitoring rules are used to suit your needs for specific process monitoring



Process monitoring rules

Define your custom monitoring rules and toggle the default rules.

Custom monitoring rules

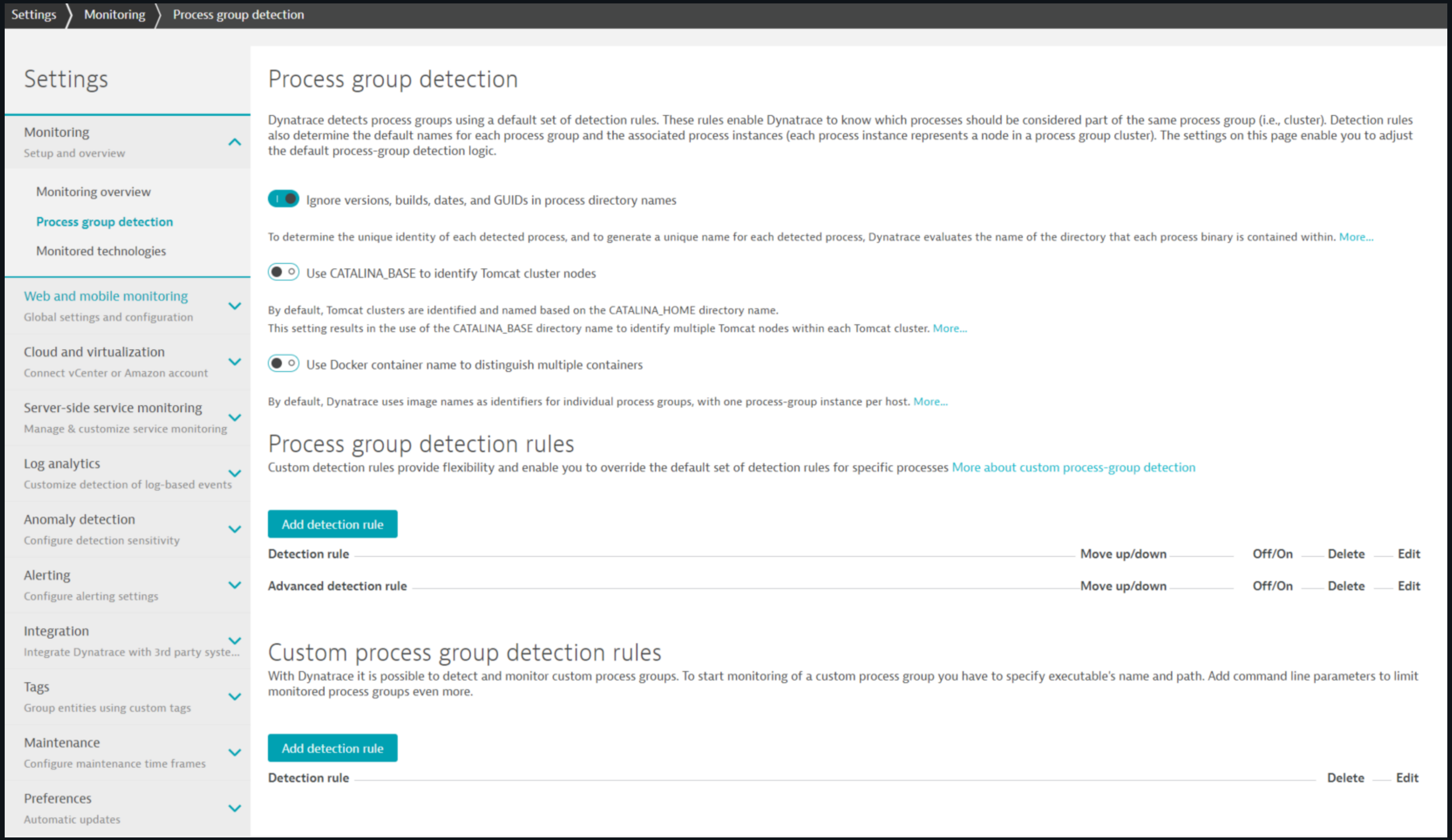
Active	Rule	Move up/down	Delete	Edit
●	Do not monitor processes if Cloud Foundry space contains 'customer' Rule id: #566	▼	✖	⌄
●	Do not monitor processes if Java JAR file contains 'cmdlauncher' Rule id: #547	▲ ▼	✖	⌄
●	Do not monitor processes if EXE path contains 'BinaryTree.ADMigrator.Agent.exe' Rule id: #306	▲ ▼	✖	⌄
●	Do not monitor processes if EXE name contains 'CrashPlanService' Rule id: #759	▲ ▼	✖	⌄
●	Monitor processes if Cloud Foundry application contains 'admin' Rule id: #054	▲ ▼	✖	⌄

Process Group Detection

Process group detection

- Dynatrace automatically detects process
- Dynatrace also recognizes when multiple processes should be included in the same process group
- This approach to process detection works fine in most cases, but isn’t perfect
- This is why we’ve enabled you to customize how Dynatrace detects and identifies host processes in your environment

Process group detection


Settings 〉 Monitoring 〉 Process group detection
Settings
Monitoring
Setup and overview
Monitoring overview
Process group detection
Monitored technologies
Web and mobile monitoring
Global settings and configuration
Cloud and virtualization
Connect vCenter or Amazon account
Server-side service monitoring
Manage & customize service monitoring
Log analytics
Customize detection of log-based events
Anomaly detection
Configure detection sensitivity
Alerting
Configure alerting settings
Integration
Integrate Dynatrace with 3rd party syste...
Tags
Group entities using custom tags
Maintenance
Configure maintenance time frames
Preferences
Automatic updates

Process group detection

Dynatrace detects process groups using a default set of detection rules. These rules enable Dynatrace to know which processes should be considered part of the same process group (i.e., cluster). Detection rules also determine the default names for each process group and the associated process instances (each process instance represents a node in a process group cluster). The settings on this page enable you to adjust the default process-group detection logic.

Ignore versions, builds, dates, and GUIDs in process directory names

To determine the unique identity of each detected process, and to generate a unique name for each detected process, Dynatrace evaluates the name of the directory that each process binary is contained within. More...

Use CATALINA_BASE to identify Tomcat cluster nodes

By default, Tomcat clusters are identified and named based on the CATALINA_HOME directory name.
This setting results in the use of the CATALINA_BASE directory name to identify multiple Tomcat nodes within each Tomcat cluster. More...

Use Docker container name to distinguish multiple containers

By default, Dynatrace uses image names as identifiers for individual process groups, with one process-group instance per host. More...

Process group detection rules

Custom detection rules provide flexibility and enable you to override the default set of detection rules for specific processes More about custom process-group detection

Add detection rule

Detection rule	Move up/down	Off/On	Delete	Edit
Advanced detection rule	Move up/down	Off/On	Delete	Edit

Custom process group detection rules

With Dynatrace it is possible to detect and monitor custom process groups. To start monitoring of a custom process group you have to specify executable's name and path. Add command line parameters to limit monitored process groups even more.

Add detection rule

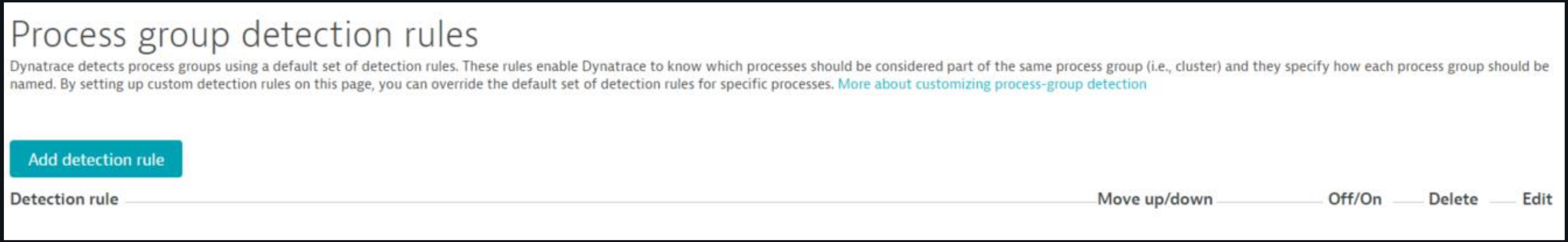
Detection rule	Delete	Edit

Process group detection

- Ignore versions, builds, dates, and GUIDs in process directory names
  - To determine the unique identity of each detected process, and to generate a unique name for each detected process, Dynatrace evaluates the name of the directory that each process binary is contained within
- Use CATALINA_BASE to identify Tomcat cluster nodes
  - By default, Tomcat clusters are identified and named based on the CATALINA_HOME directory name
- Use Docker container name to distinguish multiple containers
  - By default, Dynatrace uses image names as identifiers for individual process groups

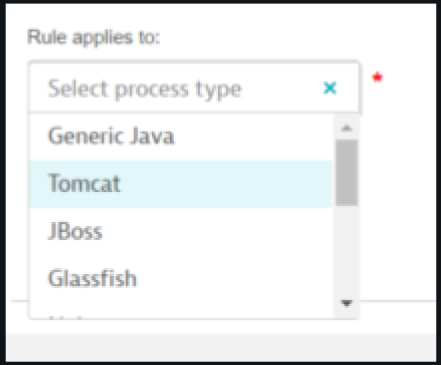
Process group detection

- Create manual rules on how you want to detect and group together certain processes



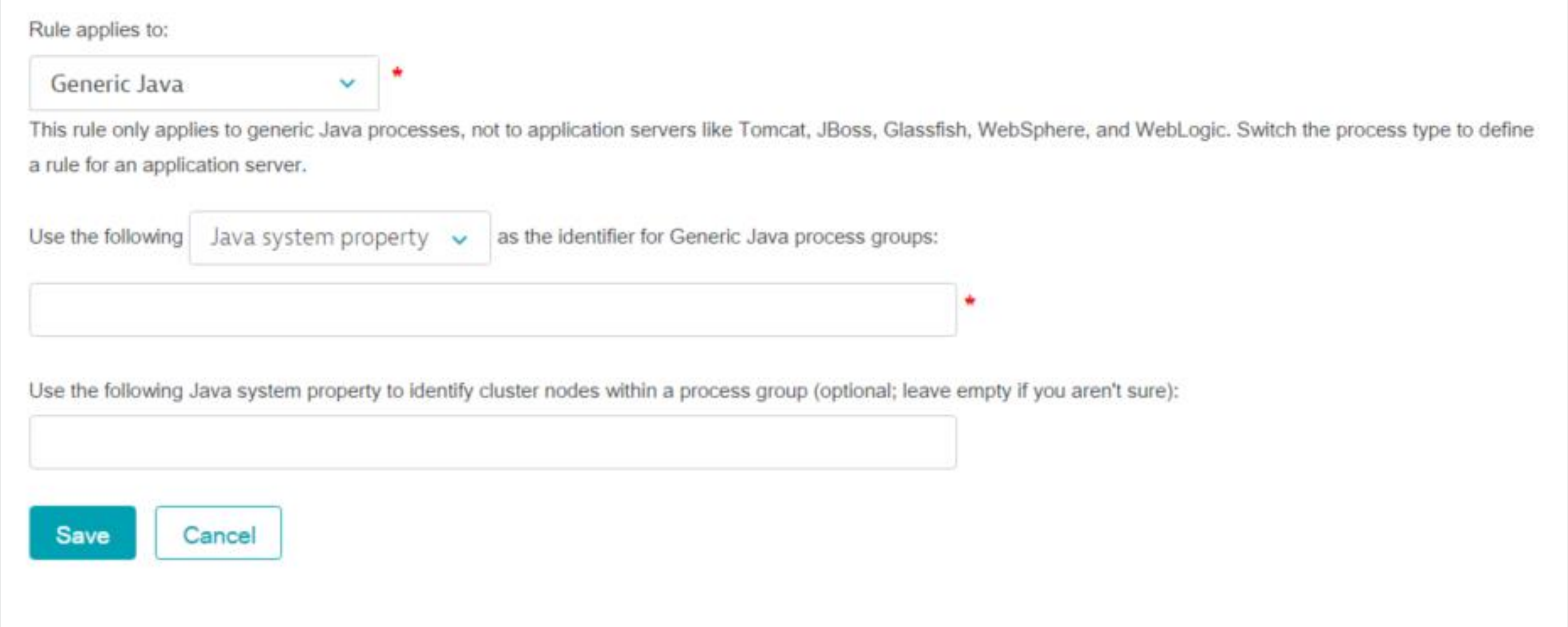
Process group detection rules

Dynatrace detects process groups using a default set of detection rules. These rules enable Dynatrace to know which processes should be considered part of the same process group (i.e., cluster) and they specify how each process group should be named. By setting up custom detection rules on this page, you can override the default set of detection rules for specific processes. More about customizing process-group detection



Process group detection

- While system properties remain the preferred method for setting up process-group detection for Java processes, we've extended the new functionality to Java process-group detection as well
- So, now when you set up process-group detection for Java processes, you have the option of using either Java system properties or environment variables to identify your process groups.



Rule applies to:

Generic Java *

This rule only applies to generic Java processes, not to application servers like Tomcat, JBoss, Glassfish, WebSphere, and WebLogic. Switch the process type to define a rule for an application server.

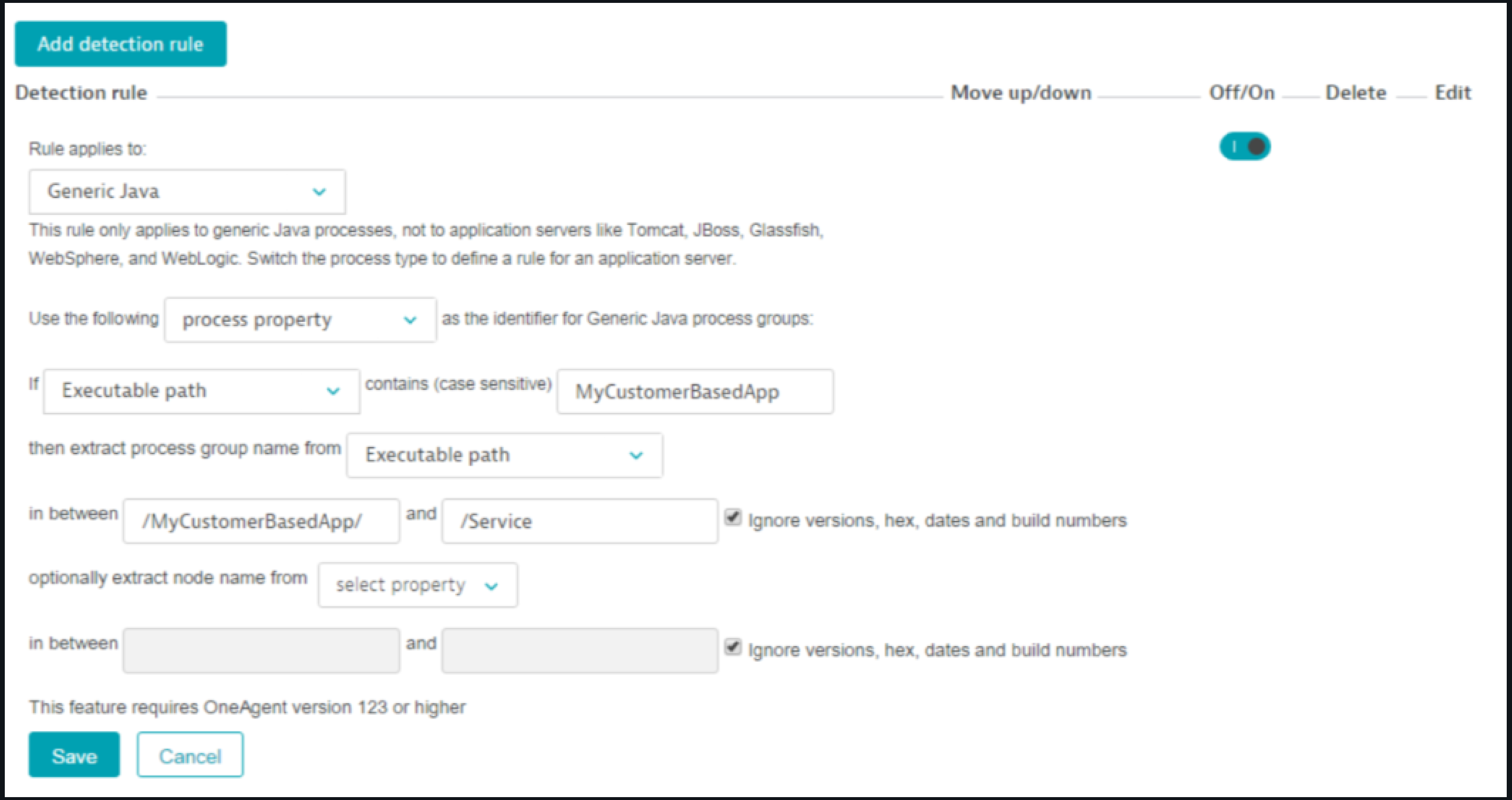
Use the following Java system property as the identifier for Generic Java process groups:

*

Use the following Java system property to identify cluster nodes within a process group (optional; leave empty if you aren't sure):

Process group detection

- Dynatrace gathers a lot of domain knowledge about the processes it monitors
- This domain knowledge can now be leveraged for enhanced process-group detection in your environment



Rule applies to: Generic Java

This rule only applies to generic Java processes, not to application servers like Tomcat, JBoss, Glassfish, WebSphere, and WebLogic. Switch the process type to define a rule for an application server.

Use the following process property as the identifier for Generic Java process groups:

If Executable path contains (case sensitive) MyCustomerBasedApp

then extract process group name from Executable path

in between /MyCustomerBasedApp/ and /Service ☑ Ignore versions, hex, dates and build numbers

optionally extract node name from select property

in between and ☑ Ignore versions, hex, dates and build numbers

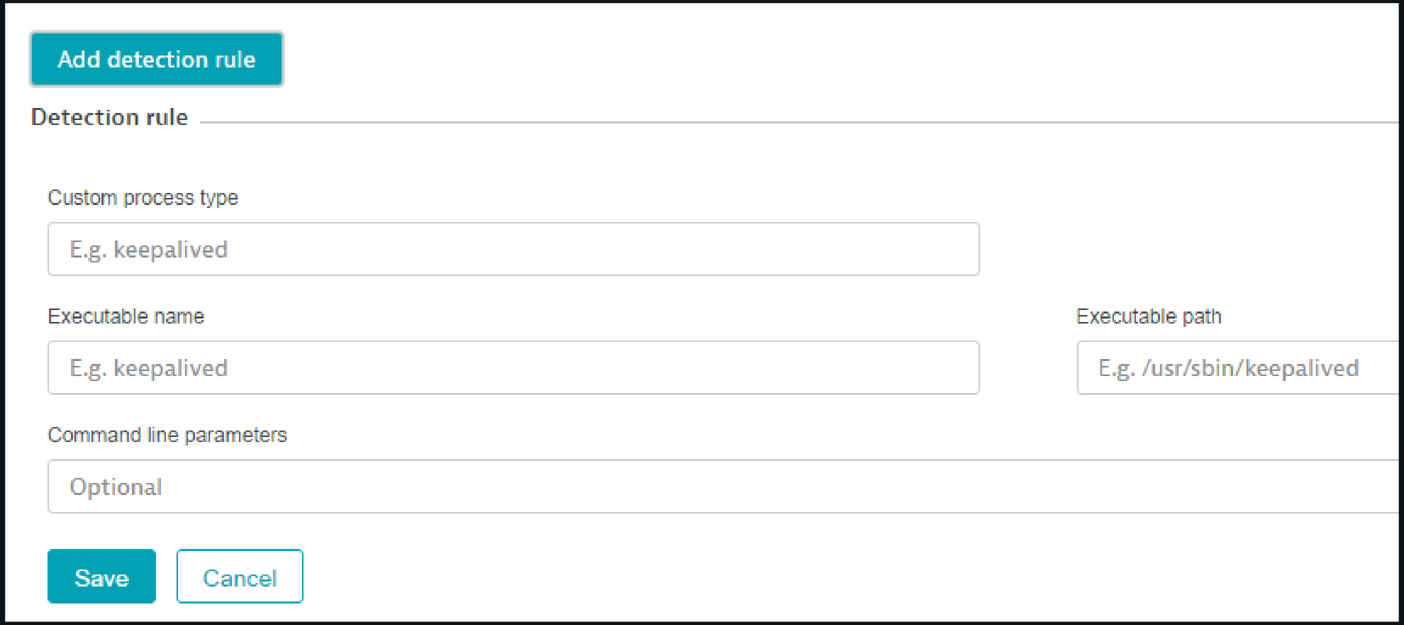
This feature requires OneAgent version 123 or higher

Custom process group detection

- Dynatrace only monitors process group types that are considered to be important
- Valuable process group types that Dynatrace reports on by default include:
  - Java application server (for example, Tomcat, WebSphere, WebLogic, Glassfish, and JBoss)
  - All other Java applications
  - All .NET applications
  - Databases (for example, MS SQL, Oracle, MySQL, and Cassandra)
  - Additional technologies (for example, Node.js and PHP)
  - Web servers (for example, Apache and IIS)
  - Processes that have an open TCP listening port or for which CPU/memory usage or network traffic exceeds 5% within 3 samples taken within 5 minutes

Custom process group detection

- Click the Add detection rule button
- Type in the information that OneAgent needs to identify the custom process group (Custom process type, Executable name, and Executable path)
- (Optional) Type in any Command line parameters to filter the monitored process groups further



Questions?

dynatrace

Simply smarter clouds