Page Title: anomaly-policy

On this page

Anomaly Policy

The Anomaly policy in Motadata AIOps is a powerful tool designed to detect and alert on anomalous behavior in system metrics, log data, and flow data. It utilizes sophisticated algorithms to identify deviations from expected patterns and triggers alerts when unusual or abnormal behavior is detected. This policy evaluation occurs every 15 minutes, providing real-time insights into potential issues or anomalies within the IT environment.

Anomaly detection is particularly useful for monitoring metrics that exhibit strong trends and recurring patterns, making it challenging to effectively monitor using traditional threshold-based alerting. By considering trends, the Anomaly policy can accurately identify deviations from expected behavior, even in complex and dynamic environments.

Use Case

â€‹

Imagine a scenario where a company's e-commerce website experiences a sudden surge in page load times. Typically, the website's performance remains consistent during peak hours, with an average page load time of 2 seconds. However, due to a technical glitch or increased user traffic, the page load times start fluctuating significantly, sometimes exceeding 10 seconds.

With the Anomaly Policy enabled, the system monitors the page load time metric continuously. During the regular evaluation intervals, it compares the current page load times with historical data and expected patterns. In this case, the policy detects the sudden spikes and prolonged delays in page load times, which deviate significantly from the normal range.

Upon detecting the anomaly, the Anomaly Policy triggers an alert, notifying the IT operations team about the performance degradation. The team can promptly investigate the issue, identify the root cause, and take appropriate actions to optimize the website's performance, ensuring a seamless user experience.

By leveraging the Anomaly Policy, organizations can identify unexpected variations in performance metrics, such as response times, latency, or throughput. This empowers them to proactively address issues, maintain high service levels, and enhance customer satisfaction.

Anomaly Policy Mechanism

â€‹

Minimum Polling data required for the policy to work

â€‹

To ensure the effectiveness of the Anomaly policy, a minimum of 8 hours of polling data is required for each monitored metric. This duration allows the alert engine to establish a baseline of expected values and intelligently determine the acceptable range for that metric. Any values that fall outside this range are considered anomalous and may trigger an alert if other conditions are met.

Polling values aggregation

â€‹

To aggregate the polling values effectively, the alert engine consolidates all the polling values into a single sample point every half hour. This aggregation provides a more comprehensive view of the metric's behavior and facilitates accurate anomaly detection.

Sample Lookup

â€‹

The Anomaly policy offers flexibility through the

Sample Lookup

field, which determines the number of samples used for evaluating the policy. By specifying the sample lookup as, for example, '30,' the policy will consider the last 30 samples for evaluation. This will be explained further in detail below under the 'Assumption Based Scenarios' section.

The Anomaly policy in Motadata AIOps empowers IT teams to proactively detect and respond to abnormal behavior in their IT infrastructure. By leveraging advanced anomaly detection algorithms and real-time monitoring, organizations can swiftly identify and address potential issues, ensuring optimal performance, and minimizing disruptions.

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Policy Settings

. Select

Metric/Log/Flow policy

based on the type of policy you want to create. The list of the created policies is now displayed.

Select

to start creating a policy. Select

Anomaly Policy

.

Configuring Anomaly policy

â€‹

Enter the following parameters to create Anomaly policy:

Field	Description
Policy Name	Enter a unique name of the policy you want to create.
Tag	Enter a name to logically categorize the policy. You can quickly and easily identify a policy based on the tag assigned to it. This tag can be used later on to filter the policies as per your requirement.

Set Conditions

â€‹

Field

Description

Counter

Select the metric for which you want to create the policy. Click on the dropdown to view the available options.

Source Filter

- Select

Monitor

if you want to create the policy for a single monitor.

- Select

Group

if you want to create the policy for a group of monitors. In case you create the policy for a group, it is configured for all the monitors present in the group individually.

- Select

Everywhere

if you want to create the policy for all the monitors created in the system. This option is selected by default.

Source

Select the specific Monitor or Group for which you want to create the policy. This dropdown will show results based on the option you have selected in the previous option. Leave this field blank if you have selected

'Everywhere'

in the previous option.

note

Make sure that in case you select a specific monitor(s) in the previous selection, the monitor(s) has the metric for which you are creating the policy. In case you select

Everywhere

, the policy will be created for all the monitors in the system having the metric you have selcted.

Critical/Major/Warning

Kindly use these fields to set the criteria under which the alert will be triggered. Here, you can also decide the alert severity based on the conditions you set.

Sample Lookup

This field determines the number of samples used for evaluating the policy.

Auto Clear

Kindly enter the time in which you want the alert to be cleared irrespective of any other conditions.

Assumption Based Scenarios

â€‹

To further understand the last two parameters, let us consider a few scenarios with following assumptions in mind:

Let us assume that the

Sample Lookup

is configured as '10', this means that the policy will consider the last 10 samples for policy evaluation.

The policy is configured to trigger a critical alert when more than 40% samples are anomalous, a major alert when more than 30% samples are anomalous, and a warning alert when more than 20% of the samples exhibit anomalies as shown in the screenshot below.

Let us consider a policy evaluation which starts at 8:00 PM(as explained earlier, policy evaluation for AI/ML policies occurs every 15 Mins).

Here, the policy is configured to trigger a critical alert when more than 40% (5 out of 10) samples are anomalous, a major alert when more than 30% (4 out of 10) samples are anomalous, and a warning alert when more than 20%(3 out of 10) samples exhibit anomalies. No Alert will be triggered if less than 3 samples are anomalous.

Scenario 1

â€‹

In this case, the alert will be triggered with

Critical

severity based on the policy configuration mentioned above.

Scenario 2

â€‹

In this case, the alert will be triggered with

Major

severity based on the policy configuration mentioned above.

Scenario 3

â€‹

In this case, the alert will be triggered with

Warning

severity based on the policy configuration mentioned above.

Scenario 4

â€‹

In this case, No alert will be triggered based on the policy configuration mentioned above.

Now, let us get back to other parameters to start creating the policy.

Notify Team

â€‹

Field

Description

Notify

There are two ways you can populate this field:

Username of

registered user

in MotadataAIOps (The alert notification will be sent over email and SMS to the mapped email address and phone number respectively).

Any email address (In case the recipient whom you wish to notify is not a registered user, you can enter an email address).

If severity is

Select the severity level using individual checkboxes in the dropdown.You can select multiple, all, or a single option as per your requirement. You can also have different recipients notified at different severity levels. For instance, you can notify

johndoe@motadata.com

when severity level hits

Critical

and send an alert notification to

janedoe@motadata.com

when severity level is

Major

.

Play Sound

Activate this toggle to enable sound notifications when an alert is triggered.

If Severity is

Choose the severity level at which the sound notification should be triggered. This option becomes visible only when the

Play Sound

toggle is switched ON.

Renotification

Turning on the toggle will resend the alert at a specific interval defined by the user if the alert severity is not changed for the time specified. If turned off, Motadata AIOps will not renotify about the alert.

Renotify

Similar to

Notify Team

field, enter the username or email address of the recipient. Also choose a preset duration for renotification along with the severity level at which they system will renotify you if the alert severity is not changed.

Do not renotify if acknowledged

If the toggle is turned on, Motadata AIOps will not send a renotification to the recipient if they mark the alert as acknowledged.

Take Action

â€‹

Field

Description

Action to be taken

Select a runbook from the dropdown to be executed when the alert is triggered.

When Severity is

You can use this option to map the action you selected in the previous step to status of the alert. This means that you can execute different runbooks based on the whether the alert is in the 'Down' state or 'Clear' state respectively.

Create New

Select this button to start creating a new runbook which you might want to assign to the policy you are creating.

Select the

Create Policy

button to create the policy based on the details entered.

Select the

Reset button

to erase all the current field values, if required.

Page Title: forecast-policy

On this page

Forecast Policy

Overview

â€‹

The Forecast Policy is designed to leverage historical data to forecast future values of a metric. By analyzing patterns and trends from the past 24 hours, this policy predicts the expected values and compares them with the actual values in real-time. If there is a significant deviation between the forecasted and actual values, an alert is triggered, enabling proactive investigation and response by IT teams.

Use-Case

â€‹

The Forecast Policy finds practical application in various scenarios. Consider a scenario where a cloud-based application experiences fluctuating CPU utilization throughout the day. By applying the Forecast Policy, the system analyzes the historical CPU utilization data over the past 24 hours, taking into account factors such as time of day, day of the week, and any recurring patterns. It then generates a forecasted range of CPU utilization values for the upcoming hours.

In this use-case, if the actual CPU utilization deviates significantly from the forecasted range, it indicates a potential performance issue. The Forecast Policy promptly detects this anomaly and triggers an alert, allowing IT teams to proactively investigate and address the underlying problem, such as a resource bottleneck or an inefficient algorithm.

Forecast Policy Mechanism

â€‹

The Forecast Policy works by leveraging statistical algorithms and machine learning techniques to analyze historical data and predict future values. The policy considers various factors, including trends, seasonality, and recurring patterns, to generate accurate forecasts.

To implement the Forecast Policy effectively, a minimum of 24 hours of historical data is required for a given metric. This data is used to train the forecasting model, which then generates the expected range of values for the upcoming hours. The policy continuously evaluates the actual metric values against the forecasted range at regular intervals, typically every 15 minutes.

During each evaluation, the Forecast Policy calculates the degree of deviation between the actual and forecasted values. If the deviation exceeds a predefined threshold, an alert is triggered, indicating a potential deviation from expected behavior. This enables IT teams to take proactive measures, such as optimizing resource allocation or investigating underlying issues, to ensure optimal system performance.

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Policy Settings

. Select

Metric/Log/Flow policy

. The list of the created policies is now displayed.

Click on

to start creating a policy. From the panel on the left side of the screen, click on the

Forecast

tab to start creating a forecast policy. The screen to create a

Forecast

Policy is now displayed.

Configuring Forecast policy

â€‹

Enter the following parameters to create forecast policy:

Field

Description

Policy Name

Enter a unique name of the policy you want to create.

Tag

Enter a name to logically categorize the policy. You can quickly and easily identify a policy based on the tag assigned to it. This tag can be used later on to filter the policies as per your requirement.

Set Conditions

â€‹

Field

Description

Select Counter

Select the metric for which you want to create the policy. Click on the dropdown to view the available options.

Monitor/Group/Everywhere

- Select

Monitor

if you want to create the policy for a single monitor.

- Select

Group

if you want to create the policy for a group of monitors. In case you create the policy for a group, it is configured for all the monitors present in the group individually.

- Select

Everywhere

if you want to create the policy for all the monitors created in the system. This option is selected by default.

Select Monitor/Select Group

Select the specific Monitor or Group for which you want to create the policy. This dropdown will show results based on the option you have selected in the previous option. Leave this field blank if you have selected

'Everywhere'

in the previous option.

note

Make sure that in case you select a specific monitor(s) in the previous selection, the monitor(s) has the metric for which you are creating the policy. In case you select

Everywhere

, the policy will be created for all the monitors in the system having the metric you have selcted.

Auto Clear

Kindly enter the time in which you want the alert to be cleared irrespective of any other conditions.

Critical/Major/Warning

Kindly use these fields to set the criteria under which the alert will be triggered. Here, you can also decide the alert severity based on the conditions you set.

Assumption Based Scenarios

â€‹

Consider the conditions in the diagram below showing the forecast policy configuration.

During each evaluation, the Forecast Policy calculates the degree of deviation between the actual and forecasted values. If the deviation exceeds a predefined threshold, an alert is triggered, indicating a potential deviation from expected behavior.

As we can see here, if the actual value of the used memory bytes goes above 60% compared to the forecasted value , the alert will be triggered in the Critical status.

If the actual value of the used memory bytes goes above 40% compared to the baseline value, the alert will be triggered in the Major status.

If the actual value of the used memory bytes goes above 30% compared to the baseline value, the alert will be triggered in the Warning status.

Notify Team

â€‹

Field

Description

Notify

There are two ways you can populate this field:

Username of

registered user

in MotadataAIOps (The alert notification will be sent over email and SMS to the mapped email address and phone number respectively).

Any email address (In case the recipient whom you wish to notify is not a registered user, you can enter an email address).

If severity is

Select the severity level using individual checkboxes in the dropdown.You can select multiple, all, or a single option as per your requirement. You can also have different recipients notified at different severity levels. For instance, you can notify

johndoe@motadata.com

when severity level hits

Critical

and send an alert notification to

janedoe@motadata.com

when severity level is

Major

.

Play Sound

Activate this toggle to enable sound notifications when an alert is triggered.

If Severity is

Choose the severity level at which the sound notification should be triggered. This option becomes visible only when the

Play Sound

toggle is switched ON.

Renotification

Turning on the toggle will resend the alert at a specific interval defined by the user if the alert severity is not changed for the time specified. If turned off, Motadata AIOps will not renotify about the alert.

Renotify

Similar to

Notify Team

field, enter the username or email address of the recipient. Also choose a preset duration for renotification along with the severity level at which they system will renotify you if the alert severity is not changed.

Do not renotify if acknowledged

If the toggle is turned on, Motadata AIOps will not send a renotification to the recipient if they mark the alert as acknowledged.

Take Action

â€‹

Field

Description

Action to be taken

Select a runbook from the dropdown to be executed when the alert is triggered.

When Severity is

You can use this option to map the action you selected in the previous step to status of the alert. This means that you can execute different runbooks based on the whether the alert is in the 'Down' state or 'Clear' state respectively.

Create New

Select this button to start creating a new runbook which you might want to assign to the policy you are creating.

Select the

Create Policy

button to create the policy based on the details entered.

Select the

Reset button

to erase all the current field values, if required.

Page Title: overview

AI/ML Policies

AI/ML policies in Motadata AIOps introduce an advanced level of intelligence and automation to streamline IT operations, enhance efficiency, and enable proactive problem resolution. These policies leverage machine learning algorithms, data analytics, and contextual insights to deliver actionable recommendations, automated actions, and predictive capabilities for managing IT infrastructure and services.

AI/ML policies in Motadata AIOps go beyond traditional monitoring and alerting by enabling intelligent automation and decision-making based on real-time and historical data. They provide a comprehensive framework for organizations to proactively monitor, analyze, and optimize their IT environment, leading to improved service availability, reduced downtime, and enhanced performance.

These policies encompass a wide range of functionalities, including anomaly detection, root cause analysis, performance optimization, capacity planning, and predictive maintenance. By leveraging AI and machine learning algorithms, these policies can automatically identify abnormal patterns, detect emerging issues, and provide actionable insights to IT teams, enabling them to take preemptive measures.

The AI/ML policies in Motadata AIOps are customizable, allowing organizations to tailor them to their specific requirements and IT infrastructure. They provide flexibility in defining rules, thresholds, and actions, enabling organizations to align these policies with their unique business needs and operational goals.

Configuring AI/ML policies is a user-friendly process within the Motadata AIOps platform. Users can easily define the scope of policies, specify the desired metrics, set up thresholds, and configure automated actions. The platform continuously ingests data from various sources, applies machine learning models and algorithms, and generates insights and recommendations in real-time.

With AI/ML policies in place, organizations can gain deep visibility into their IT infrastructure, services, and applications. They can proactively identify and address issues before they impact end-users, anticipate potential bottlenecks, optimize resource utilization, and ensure optimal performance across the IT landscape.

Furthermore, these policies in Motadata AIOps empower IT teams to shift from reactive incident response to a proactive and predictive operational model. By leveraging historical data, trend analysis, and predictive algorithms, organizations can forecast future trends, plan capacity requirements, and implement preventive measures to mitigate risks and maintain service levels.

In summary, AI/ML policies in Motadata AIOps provide a comprehensive solution for intelligent IT operations management. By harnessing the power of AI, machine learning, and automation, these policies enable organizations to optimize their IT infrastructure, improve service quality, and drive business success. Embracing AI/ML policies empowers organizations to stay ahead of potential issues, enhance operational efficiency, and deliver superior experiences to their end-users.

The AI/ML Policies can be further divided as follows:

Forecast Policy

Outlier Policy

Anomaly Policy

Let us look into all these policies one by one in the next sections.

Page Title: alert-correlation

On this page

Alert Correlation

Motadata AIOps incorporates an intelligent alert correlation module that prevents the system from bombarding administrators with numerous alerts when multiple devices are affected by a common issue. This feature is particularly useful when dealing with interconnected devices such as switches, firewalls, and their associated devices.

Understanding Alert Correlation

â€‹

Consider a scenario where a policy is created for multiple devices linked to a specific switch or firewall. If the switch or firewall goes down, it will cause all the connected devices to become unreachable, triggering alerts for each individual device. However, flooding the administrator with multiple alerts for the same underlying issue can be overwhelming and counterproductive.

Motadata AIOps addresses this challenge by implementing alert correlation. When correlated alerts are detected, the system intelligently combines them into a single alert, providing a consolidated view of the problem. Instead of receiving multiple alerts for each affected device, administrators receive a single comprehensive alert that captures the overall impact of the issue.

Benefits of Alert Correlation

â€‹

The alert correlation feature offers several benefits, including:

Simplified Alert Management

: By consolidating related alerts, administrators can quickly grasp the overall situation without being overwhelmed by a flood of individual alerts. This enables efficient troubleshooting and reduces the time required to identify and address the root cause.

Streamlined Communication

: Instead of dealing with separate alerts for each affected device, administrators can focus on one consolidated alert. This facilitates better communication and collaboration among team members, as they can collectively analyze and respond to the issue.

Improved Incident Resolution

: Alert correlation enhances incident resolution by providing a holistic view of the problem. Administrators can gain better insights into the affected devices, their dependencies, and the underlying issue. This enables them to take appropriate actions and resolve the incident efficiently.

Reduced Alert Fatigue

: By avoiding the barrage of redundant alerts, alert correlation prevents alert fatigue among administrators. It helps maintain a cleaner and more manageable alert stream, ensuring that critical alerts are not overlooked or disregarded due to excessive noise.

Implementing Alert Correlation

â€‹

Motadata AIOps applies the alert correlation module to alerts generated for servers, virtual stack devices, and network devices. When these alerts are correlated, the system intelligently identifies the affected devices and consolidates the information into a single alert. This ensures that administrators receive only relevant and actionable alerts, minimizing unnecessary disruptions.

To illustrate the concept of alert correlation, let's consider a practical scenario. Suppose a policy is created to monitor a group of devices connected to a specific switch. If the switch goes down, all the devices that are connected become unreachable. Instead of overloading the administrator with individual alerts for each affected device, Motadata AIOps correlates the alerts and generates a single consolidated alert for the parent device (the switch) with relevant details and impact analysis.

Go to Menu, Select

Alerts

. The alert screen is now displayed.

Click on the

Correlated policies

section on the alert screen. Once you click on the

Correlated policies

section, a screen showing all the coorelated alerts will be shown.

The above screen shows the consolidated alert for the parent monitor affecting all the other monitors for which the alert is raised.

As shown above, you can drill-down on the correlated alert to view the details of all the alerts that have been consolidated into that particular correlated alert

Motadata AIOps' alert correlation feature helps reduce alert overload by intelligently consolidating related alerts into a single comprehensive notification. By implementing this module, administrators can efficiently manage alerts, improve incident resolution, and alleviate alert fatigue. The system intelligently analyzes interconnected devices and ensures that relevant information is presented in a concise and actionable manner, enhancing the overall monitoring and troubleshooting experience.

Page Title: availability-policy

On this page

Availability Policy

Overview

â€‹

The Availability Policy can be created to alert you whenever a particular monitor or any monitor out of a group of monitors goes down. Let us consider how to create a policy so that an alert is sent out whenever the availability state of a monitor changes.

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Policy Settings

. Select

Metric/Log/Flow policy

based on the type of policy you want to create. The list of the created policies is now displayed.

Select

to start creating a policy. The screen to create

Availability

Policy is now displayed.

Configuring Availability policy

â€‹

Enter the following parameters to create availability policy:

Field

Description

Policy Name

Enter a unique name of the policy you want to create.

Tag

Enter a name to logically categorize the policy. You can quickly and easily identify a policy based on the tag assigned to it. This tag can be used later on to filter the policies as per your requirement.

Set Conditions

â€‹

Field

Description

Select Counter

Select the metric for which you want to create the policy. Click on the dropdown to view the available options.

Monitor/Group/Tag/Everywhere

- Select

Monitor

if you want to create the policy for a single monitor.

- Select

Group

if you want to create the policy for a group of monitors. In case you create the policy for a group, it is configured for all the monitors present in the group individually.

- Select

Tag

if you want to create the policy for all monitors that belong a specific

Tag

.

- Select

Everywhere

if you want to create the policy for all the monitors created in the system. This option is selected by default.

Select Monitor/Select Group/Add Tag

Select the specific Monitor, Group, or the Tag for which you want to create the policy. This dropdown will show results based on the option you have selected in the previous option. Leave this field blank if you have selected

'Everywhere'

in the previous option.

note

Make sure that in case you select a specific monitor(s) in the previous selection, the monitor(s) has the metric for which you are creating the policy. In case you select

Everywhere

, the policy will be created for all the monitors in the system having the metric you have selcted.

Notify if Monitor/Instance is down for

Specify the time window during which the policy will check the monitor/instance to have the 'Down' value for the metric you selected above. This is the evaluation window in which the AIOps will check if the polling value comes up as 'Down'.

Abnormality occurrence

Specify the number of times the monitor/monitor instance should be 'Down' consecutively within the evaluation window specified above to trigger an alert.

Assumption Based Scenarios

â€‹

To further understand the last two parameters, let us consider a few scenarios with following assumptions in mind:

The polling period is 1 min.

The

Notify if Monitor/Instance is down for

is â€˜5 minâ€™

The

Abnormality Occurrence

is â€˜3â€™ i.e., the system will check for 3 consecutive occurrences of â€˜downâ€™ polling value for the selected metric in the 5-minute window to trigger an alert. Kindly note that the 5 min(in this case) window to check the metric will be reset everytime a value other than 'down' comes up for the metric in question.

Now, let us consider a few scenarios to understand the concept better.

Scenario 1

â€‹

In this case, no Alert gets triggered because 3 consecutive instances of down occurences do not occurr in the 5 min time window.

Scenario 2

â€‹

In this case, alert gets triggered because we get 3 consecutive instances of down occurences at 10:00, 10:01, and 10:02 which falls within the 5 minutes of time window that starts at 10:00 with the 1st 'Down' occurence.

Scenario 3

â€‹

In this case, a 5 minute window to check the metric value starts at 10:00 but it gets reset at 10:01 due to the occurence of 'Up' value. The alert then gets triggered because we get 3 consecutive instances of 'Down' occurence at 10:02, 10:03, and 10:04.

Now, let us get back to other parameters to start creating the policy.

Notify Team

â€‹

Field

Description

Notify

There are two ways you can populate this field:

Username of

registered user

in MotadataAIOps (The alert notification will be sent over email and SMS to the mapped email address and phone number respectively).

Any email address (In case the recipient whom you wish to notify is not a registered user, you can enter an email address).

If severity is

Select the severity level using individual checkboxes in the dropdown.You can select multiple, all, or a single option as per your requirement. You can also have different recipients notified at different severity levels. For instance, you can notify

johndoe@motadata.com

when severity level hits

Critical

and send an alert notification to

janedoe@motadata.com

when severity level is

Major

.

Play Sound

Activate this toggle to enable sound notifications when an alert is triggered.

If Severity is

Choose the severity level at which the sound notification should be triggered. This option becomes visible only when the

Play Sound

toggle is switched ON.

Renotification

Turning on the toggle will resend the alert at a specific interval defined by you. If turned off, Motadata AIOps will not renotify about the alert.

Renotify

Similar to

Notify Team

field, enter the username or email address of the recipient. Also choose a preset duration for renotification along with the severity level at which they system will renotify you if the alert severity is not changed.

Do not renotify if acknowledged

If the toggle is turned on, Motadata AIOps will not send a renotification to the recipient if they mark the alert as acknowledged.

Take Action

â€‹

Field

Description

De-provision the Monitor/Instance when Down Occurrences

Select the time period for which you want the monitor to be de-provisioned after it goes down.

Action to be taken

Select a runbook from the dropdown to be executed when the alert is triggered.

When Status is

You can use this option to map the action you selected in the previous step to status of the alert. This means that you can execute different runbooks based on the whether the alert is in the 'Down' state or 'Clear' state respectively.

Create New

Select this button to start creating a new runbook which you might want to assign to the policy you are creating.

Select the

Create Policy

button to create the policy based on the details entered.

Select the

Reset

button to erase all the current field values, if required.

Page Title: flow-policy

On this page

Flow Policy

Overview

â€‹

The flow policy functionality in Motadata AIOps empowers you to monitor and analyze network traffic flow data, such as NetFlow or sFlow, and generate alerts based on defined conditions. By leveraging flow policies, you can gain valuable insights into network performance, detect anomalies, and take appropriate actions to optimize your network.

Use-Case

â€‹

Network Performance Monitoring: Set up flow policies to trigger alerts on network traffic metrics such as bandwidth utilization, packet loss, or latency. This helps you identify and resolve performance issues, ensuring optimal network operation.

Security Incident Detection: Configure flow policies to detect and alert on suspicious network traffic patterns, potentially indicating network-based attacks, malware infections, or unauthorized access attempts.

Capacity Planning: Utilize flow policies to monitor network traffic trends and patterns, allowing you to make informed decisions regarding network capacity upgrades, bandwidth allocation, or traffic shaping.

Application Dependency Mapping: Use flow policies to analyze communication flows between applications and services, facilitating the understanding of dependencies and improving troubleshooting and optimization processes.

By effectively utilizing flow policies in Motadata AIOps, you can proactively monitor and manage both log data and network traffic, ensuring the stability, security, and optimal performance of your IT infrastructure. Remember to tailor the instructions and details to match the specific features and options available in your Motadata AIOps product.

Default Flow Alert Policies

â€‹

Motadata AIOps simplifies flow network monitoring with Default Flow Alert Policies, offering users a predefined set of alerts designed to proactively notify specific issues related to their flow network. These default flow alerts, including High BPS for TCP and UDP, ICMP Flood Attack, Malicious Activity with Black IP (Threat Feed Integration), and Very Low or No Flow, aim to promptly alert users to potential network issues.

Create Flow Policy

â€‹

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Policy Settings

. Select

Metric/Log/Flow policy

. The list of the created policies is now displayed.

Click on

to start creating a policy. From the panel on the left side of the screen, click on the

Flow

tab to start creating a metric policy. The screen to create a

Flow

Policy is now displayed.

Enter the details of the following parameters to create a Flow Policy:

Field

Description

Policy Name

Enter a unique name of the policy you want to create.

Tag

Enter a name to logically categorize the policy. You can quickly and easily identify a policy based on the tag assigned to it.

Set Conditions

â€‹

Field

Description

Counter

Choose the specific counter you wish to create a policy for by selecting from the available options in the dropdown menu. This counter will be the basis for monitoring and generating alerts.

Aggregation

Determine the aggregation function that best suits your monitoring needs for the selected counter. This function allows you to consolidate and analyze the metric data over a defined period.

Operator

Select the operator that will be applied to the aggregated counter values to define the triggering condition for the alert. Different operators such as greater than, less than, equal to, and more are available to provide flexibility in defining your alert conditions.

Value

Specify the threshold value against which the aggregated counter values will be compared. Once the counter value meets the specified condition, an alert will be triggered, notifying you of the issue.

Source Filter

- Select

Source Host

if you want to create the policy for specific flow source(s).

- Select

Group

if you want to create the policy for flow sources that belong to specific groups.

- Select

Everywhere

if you want to create the policy for all the flow sources in the system. This option is selected by default.

Source

Select the specific Source Host or Group for which you want to create the policy. This dropdown will show results based on the option you have selected in the previous option. You can leave this field blank if you have selected

'Everywhere'

in the previous option.

Result By

Specify the grouping criteria for the aggregated values. This field allows you to define how the flow data will be grouped and aggregated for analysis.

Scenario

â€‹

Suppose we want to create a flow policy to trigger an alert whenever there is no flow data or very low flow data detected from any particular source.

In this way, we can configure a flow policy to raise an alert.

We will discuss the other conditions for the alert to be triggered now.

Field

Description

Alert Type

- Select

Scheduled

if you wish to schedule the alert evaluation at specified time(s) in the future.

- Select

Real Time

if you wish to schedule the alert evaluation in real-time as soon as you create the policy

Scheduler Type

This option is available only when you select

Scheduled

as the

Alert Type

- Select

Once

if you want the policy evaluation to occur only once. In this case, the policy will evaluate the data from the past hour at the time of evaluation.

- Select

Daily

if you want the policy evaluation to occur daily. The policy will evaluate the data from the past 24 hours at the time of evaluation.

- Select

Weekly

if you want the policy evaluation to occur weekly. The policy will evaluate the data from the past 7 days at the time of evaluation.

- Select

Monthly

if you want the policy evaluation to occur monthly. The policy will evaluate the data from the past 30 days at the time of evaluation..

Start Date

This option is available only when you select

Scheduled

as the

Alert Type

. Select the date at which you want to start the policy evaluation.

Hours

This option is available only when you select

Scheduled

as the

Alert Type

. Select the time(s) at which you want to start the policy evaluation.

Days

This option is available only when you select

Scheduled

as the

Alert Type

and

Weekly

as the

Scheduler Type

. Select the day(s) at which you want to start the policy evaluation.

Months

This option is available only when you select

Scheduled

as the

Alert Type

and

Monthly

as the

Scheduler Type

. Select the month(s) in which you want to start the policy evaluation.

Dates

This option is available only when you select

Scheduled

as the

Alert Type

and

Monthly

as the

Scheduler Type

. Select the date(s) at which you want to start the policy evaluation.

Critical/Major/Warning

Kindly use these fields to set the severity under which the alert will be triggered.

Supress Action

Switch this Toggle button ON to supress the actions and notifications mapped to the policy. Once you switch this button ON and the alert is triggered, the action will be executed once and you will receive a single notification before the actions and notifications configured in the policy are supressed for the time-period specified in the field

Supress Window

.

Supress Window

Specify the time-period for which you do not wish to execute the actions and receive the notifications mapped to policy.

Notify Team

â€‹

Field

Description

Notify

There are two ways you can populate this field:

Username of

registered user

in MotadataAIOps (The alert notification will be sent over email and SMS to the mapped email address and phone number respectively).

Any email address (In case the recipient whom you wish to notify is not a registered user, you can enter an email address).

Play Sound

Activate this toggle to enable sound notifications when an alert is triggered.

If Severity is

Choose the severity level at which the sound notification should be triggered. This option becomes visible only when the

Play Sound

toggle is switched ON.

Take Action

â€‹

Field

Description

Action to be taken

Select a runbook from the dropdown to be executed when the alert is triggered.

Create New

Select this button to start creating a new runbook which you might want to assign to the policy you are creating.

Select the

Create Policy

button to create the policy based on the details entered.

Select the

Reset

button to erase all the current field values, if required.

Page Title: log-policy

On this page

Log Policy

Overview

â€‹

The log policy feature in Motadata AIOps empowers you to effectively monitor and analyze log events in real-time, enabling proactive identification and resolution of potential issues in your IT infrastructure. With log policies, you can define rules and conditions to generate alerts based on log data, ensuring the smooth operation of your systems and applications.

Use-Case

â€‹

Security Monitoring: Configure log policies to detect and alert on security-related events, such as failed login attempts, suspicious access patterns, or potential breaches.

Error and Exception Tracking: Create log policies to identify critical errors or exceptions occurring within your applications, enabling you to quickly respond and resolve issues before they impact users.

Compliance and Audit: Set up log policies to monitor specific compliance requirements, such as tracking access to sensitive data or ensuring adherence to regulatory guidelines.

Performance Optimization: Utilize log policies to identify performance bottlenecks, anomalies, or resource-intensive activities in your infrastructure, allowing you to optimize system performance and enhance user experience.

Default Log Alert Policies

â€‹

Motadata AIOps supports Default Log Alert Policies, enhancing the platform's alerting capabilities. This feature is designed to include predefined alert policies for logs such as Malicious Activity with Black IP (Threat Feed Integration), ensuring that users receive timely notifications for critical events within their log data.

Create Log Policy

â€‹

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Policy Settings

. Select

Metric/Log/Flow policy

. The list of the created policies is now displayed.

Click on

to start creating a policy. From the panel on the left side of the screen, click on the

Log

tab to start creating a metric policy. The screen to create a

Log

Policy is now displayed.

Enter the details of the following parameters to create a Log Policy:

Field

Description

Policy Name

Enter a unique name of the policy you want to create.

Tag

Enter a name to logically categorize the policy. You can quickly and easily identify a policy based on the tag assigned to it.

Set Conditions

â€‹

Field

Description

Counter

Choose the specific counter you wish to create a policy for by selecting from the available options in the dropdown menu. This counter will be the basis for monitoring and generating alerts.

Aggregation

Determine the aggregation function that best suits your monitoring needs for the selected counter. This function allows you to consolidate and analyze the metric data over a defined period.

Operator

Select the operator that will be applied to the aggregated counter values to define the triggering condition for the alert. Different operators such as greater than, less than, equal to, and more are available to provide flexibility in defining your alert conditions.

Value

Specify the threshold value against which the aggregated counter values will be compared. Once the counter value meets the specified condition, an alert will be triggered, notifying you of the issue.

Source Filter

- Select

Source Host

if you want to create the policy for specific log source(s).

- Select

Source Type

if you want to create the policy for log sources that belong to specific log types.

- Select

Group

if you want to create the policy for log sources that belong to specific groups.

- Select

Everywhere

if you want to create the policy for all the log sources in the system. This option is selected by default.

Source

Select the specific Source Host, Source Type, or Group for which you want to create the policy. This dropdown will show results based on the option you have selected in the previous option. You can leave this field blank if you have selected

'Everywhere'

in the previous option.

Result By

Specify the grouping criteria for the aggregated values. This field allows you to define how the log data will be grouped for evaluation of the policy.

Scenario

â€‹

Suppose we want to create a log policy to trigger an alert whenever an activity by a root user is detected.

In the filter condition shown in the diagram below, we have specified the condition to identify any log messages that contain the word 'sudo', 'su', and 'root'. This helps to identify the messages indicating activity related to root user.

Once we have identified the messages(if any) indicating activity by a root user, we now configure the policy to trigger an alert whenever the count of such messages goes above 1 i.e., we raise an alert even if a single message comes up with the words 'sudo', 'su', and 'root'.

In this way, we can configure a log policy to raise an alert whenever an activity from a root user is detected.

We will discuss the other conditions for the alert to be triggered now.

Field

Description

Alert Type

- Select

Scheduled

if you wish to schedule the alert evaluation at specified time(s) in the future.

- Select

Real Time

if you wish to schedule the alert evaluation in real-time as soon as you create the policy

Scheduler Type

This option is available only when you select

Scheduled

as the

Alert Type

- Select

Once

if you want the policy evaluation to occur only once. In this case, the policy will evaluate the data from the past hour at the time of evaluation.

- Select

Daily

if you want the policy evaluation to occur daily. The policy will evaluate the data from the past 24 hours at the time of evaluation.

- Select

Weekly

if you want the policy evaluation to occur weekly. The policy will evaluate the data from the past 7 days at the time of evaluation.

- Select

Monthly

if you want the policy evaluation to occur monthly. The policy will evaluate the data from the past 30 days at the time of evaluation..

Start Date

This option is available only when you select

Scheduled

as the

Alert Type

. Select the date at which you want to start the policy evaluation.

Hours

This option is available only when you select

Scheduled

as the

Alert Type

. Select the time(s) at which you want to start the policy evaluation.

Days

This option is available only when you select

Scheduled

as the

Alert Type

and

Weekly

as the

Scheduler Type

. Select the day(s) at which you want to start the policy evaluation.

Months

This option is available only when you select

Scheduled

as the

Alert Type

and

Monthly

as the

Scheduler Type

. Select the month(s) in which you want to start the policy evaluation.

Dates

This option is available only when you select

Scheduled

as the

Alert Type

and

Monthly

as the

Scheduler Type

. Select the date(s) at which you want to start the policy evaluation.

Critical/Major/Warning

Kindly use these fields to set the severity under which the alert will be triggered.

Supress Action

Switch this Toggle button ON to supress the actions and notifications mapped to the policy. Once you switch this button ON and the alert is triggered, the action will be executed once and you will receive a single notification before the actions and notifications configured in the policy are supressed for the time-period specified in the field

Supress Window

.

Supress Window

Specify the time-period for which you do not wish to execute the actions and receive the notifications mapped to policy.

Notify Team

â€‹

Field

Description

Notify

There are two ways you can populate this field:

Username of

registered user

in MotadataAIOps (The alert notification will be sent over email and SMS to the mapped email address and phone number respectively).

Any email address (In case the recipient whom you wish to notify is not a registered user, you can enter an email address).

Play Sound

Activate this toggle to enable sound notifications when an alert is triggered.

If Severity is

Choose the severity level at which the sound notification should be triggered. This option becomes visible only when the

Play Sound

toggle is switched ON.

Take Action

â€‹

Field

Description

Action to be taken

Select a runbook from the dropdown to be executed when the alert is triggered.

Create New

Select this button to start creating a new runbook which you might want to assign to the policy you are creating.

Select the

Create Policy

button to create the policy based on the details entered.

Select the

Reset

button to erase all the current field values, if required.

Page Title: metric-policy

On this page

Metric Policy

Overview

â€‹

The Metric policy can be configured to send out an alert whenever a metric of a monitor goes above or below a certain threshold value. Let us consider a scenario where this can policy can be used. The metric policies can further be divided into:

Threshold Alert

Baseline Alert

Threshold Alert

Baseline Alert

Threshold Alert

â€‹

Use-Case

â€‹

Suppose, you want to monitor the performance of an EC2 instance in your AWS cloud infrastructure. You need Motadata AIOps to raise an alert whenever the metric measuring the CPU percentage goes above a certain threshold value. You can create a metric policy to do the same.

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Policy Settings

. Select

Metric/Log/Flow policy

. The list of the created policies is now displayed.

Click on

to start creating a policy. From the panel on the left side of the screen, click on the

Metric

tab to start creating a metric policy. The interface to create a

Metric

Policy is now displayed.

Configuring Threshold Metric policy

â€‹

Enter the details of the following parameters to create a threshold metric policy:

Field

Description

Policy Name

Enter a unique name of the policy you want to create.

Tag

Enter a name to logically categorize the policy. You can quickly and easily identify a policy based on the tag assigned to it.

Threshold Alert/Baseline Alert

Select the parameter as per the type of policy you want to create. In this case, we will select

Threshold Alert

to move forward.

Set Conditions

â€‹

Field

Description

Counter

Select the metric for which you want to create the policy. Click on the dropdown to view the available options. You can also search the specific metric you are looking for from the search bar.

Source Filter

- Select

Monitor

if you want to create the policy for specific monitor(s).

- Select

Group

if you want to create the policy for a group of monitors. In case you create the policy for a group, it is configured for all the monitors present in the group individually.

- Select

Everywhere

if you want to create the policy for all the monitors created in the system. This option is selected by default.

- Select

Tag

if you want to create the policy for all the monitors assigned with the same Tags.

Source

Select the specific Monitor, Group, or the Tag for which you want to create the policy. This dropdown will show results based on the option you have selected in the previous option. You can leave this field blank if you have selected

'Everywhere'

in the previous option.

Critical/Major/Warning

Kindly use these fields to set the criteria under which the alert will be triggered. Here, you can also decide the alert severity based on the conditions you set.

Assumption Based Scenario

â€‹

In the context of a Threshold alert, consider the following scenario:

Abnormality Occurrence

: Set to 3, indicating that the threshold breach should happen for three consecutive occurrences.

Notify if Threshold Value Breach Within

: Configured as 5 Minutes, defining the time window within which the consecutive threshold breaches must occur.

When threshold is breached, the alert will trigger with varying severity levels:

Warning

: Triggered when the CPU utilization percent goes above 60% thrice consecutively within 5 minutes.

Critical

: Triggered when the CPU utilization percent goes above 80% thrice consecutively within 5 minutes.

note

In case the metric in the policy crosses the value for multiple severity thresholds, the alert will be raised with the highest severity applicable. As shown in the diagram above, values above 80% CPU utilisation qualify for both

Warning

and

Critical

severity. In this case, the alert will be raised with

Critical

severity because it is the highest qualified severity.

We will discuss the other conditions for the alert to be triggered now.

Field

Description

Notify if Threshold value breach within

Specify the time-period during which the policy will check the for the metric you selected above. This is the evaluation window in which the AIOps will check if the polling value crosses the threshold values configured in the policy.

Abnormality occurrence

Specify the number of times the conditions set within the policy should be met consecutively within the evaluation window specified in the previous field.

Auto Clear

Kindly enter the time in which you want the alert to be cleared irrespective of any other conditions.

Notify Team

â€‹

Field

Description

Notify

There are two ways you can populate this field:

Username of

registered user

in MotadataAIOps (The alert notification will be sent over email and SMS to the mapped email address and phone number respectively).

Any email address (In case the recipient whom you wish to notify is not a registered user, you can enter an email address).

If severity is

Select the severity level using individual checkboxes in the dropdown.You can select multiple, all, or a single option as per your requirement. You can also have different recipients notified at different severity levels. For instance, you can notify

johndoe@motadata.com

when severity level hits

Critical

and send an alert notification to

janedoe@motadata.com

when severity level is

Major

.

Play Sound

Activate this toggle to enable sound notifications when an alert is triggered.

If Severity is

Choose the severity level at which the sound notification should be triggered. This option becomes visible only when the

Play Sound

toggle is switched ON.

Renotification

Turning on the toggle will resend the alert at a specific interval defined by the user if the alert severity is not changed for the time specified. If turned off, Motadata AIOps will not renotify about the alert.

Renotify

Similar to

Notify Team

field, enter the username or email address of the recipient. Also choose a preset duration for renotification along with the severity level at which they system will renotify you if the alert severity is not changed.

Do not renotify if acknowledged

If the toggle is turned on, Motadata AIOps will not send a renotification to the recipient if they mark the alert as acknowledged.

Take Action

â€‹

Field

Description

Action to be taken

Select a runbook from the dropdown to be executed when the alert is triggered.

Create New

Select this button to start creating a new runbook which you might want to assign to the policy you are creating.

Declare Incident

â€‹

Field

Description

When Alert Severity is

Select an Alert severity from the dropdown.

Select Integration Profile to Trigger

Choose an Integration profile to be executed from the dropdown when the chosen alert severity is reached.

Create Integration Profile

Select this button to start creating a new Integration profile that you might want to assign to the policy you are creating.

You can click on

to define a new Alert severity and Integration Profile combination. You can have separate Integration profile triggered at different levels of Alert severity.

Select the

Create Policy

button to create the policy based on the details entered.

Select the

Reset

 button to erase all the current field values, if required.

Now let us look into the

Baseline Alert

.

Baseline Alert

â€‹

The Baseline Alert is a powerful feature within Motadata AIOps that enables proactive monitoring of metrics by comparing their real-time values to a dynamically generated baseline. By analyzing historical data and establishing a baseline range, this alerting mechanism helps identify deviations in metric behavior, allowing organizations to detect potential issues and take preventive action.

With the Baseline Alert, organizations gain deeper insights into the normal behavior of their metrics by leveraging historical data from the past 15 days. By dynamically adjusting the baseline range using advanced statistical techniques, the alerting mechanism adapts to changes in metric behavior, ensuring accurate detection of deviations in real-time.

When a metric value breaches the dynamic baseline threshold during a policy evaluation, the Baseline Alert triggers a policy violation. Organizations can customize the actions taken when a violation occurs, such as sending notifications to stakeholders, or executing Runbooks to ensure corrective action.

Use-Case

â€‹

The Baseline Alert is particularly useful in scenarios where it's crucial to maintain optimal performance and prevent critical problems. By continuously evaluating metric values against the established baseline, it provides early warning signs of performance bottlenecks, abnormal patterns, or unexpected variations in key metrics. This proactive approach empowers IT teams to address potential issues before they escalate, minimizing downtime, optimizing resource utilization, and enhancing overall operational efficiency.

Baseline Metric Policy Mechanism

â€‹

Policy Evaluation

The Baseline policy evaluations start as soon as the policy is created. During each evaluation, the system considers the metric data from the last 15 days to create a baseline range.

Baseline Calculation

To generate the baseline range, the system utilizes advanced statistical methods. These techniques analyze the historical data points within the last 15 days and produces a dynamically adjusted baseline.

Baseline Threshold Violation

Baseline threshold violation occurs when a metric's data point deviates from the expected behavior, surpassing the predefined acceptable range known as the baseline threshold. This violation triggers an alert based on the configured parameters within the baseline policy.

In the baseline policy configuration, users set the criteria for triggering an alert by specifying the number of times a data point can deviate from the baseline threshold within a defined time window, as configured in the

Abnormality Occurrence

and

Notify if the Threshold value breach within

fields, respectively.

Actions on Baseline Policy Triggering

Once the baseline alert is triggered, you can define specific actions to be taken. These actions may include sending notifications to relevant stakeholders, executing scripts to automate remedial tasks.

By leveraging thme Baseline Alert, organizations can proactively monitor critical metrics, detect unusual patterns, and take prompt action to ensure smooth operations and optimal performance.

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Policy Settings

. Select

Metric/Log/Flow policy

. The list of the created policies is now displayed.

Click on

to start creating a policy. From the panel on the left side of the screen, click on the

Metric

tab to start creating a metric policy. The interface to create a

Metric

Policy is now displayed.

Configuring Baseline Metric policy

â€‹

Enter the details of the following parameters to create a Baseline Metric Policy:

Field

Description

Policy Name

Enter a unique name of the policy you want to create.

Tag

Enter a name to logically categorize the policy. You can quickly and easily identify a policy based on the tag assigned to it.

Threshold Alert/Baseline Alert

Select the parameter as per the type of policy you want to create. In this case, we will select

Baseline Alert

to move forward.

Set Conditions

â€‹

Field

Description

Select Metric

Select the metric for which you want to create the policy. Click on the dropdown to view the available options.

Source Filter

- Select

Monitor

if you want to create the policy for specific monitor(s).

- Select

Group

if you want to create the policy for a group of monitors. In case you create the policy for a group, it is configured for all the monitors present in the group individually.

- Select

Everywhere

if you want to create the policy for all the monitors created in the system. This option is selected by default.

- Select

Tag

if you want to create the policy for all the monitors assigned with the same Tags.

Select Monitor/Select Group

Select the specific Monitor or the Group for which you want to create the policy. This dropdown will show results based on the option you have selected in the previous option. You can leave this field blank if you have selected

'Everywhere'

in the previous option.

Absolute/Relative

- Select

Absolute

to define specific numerical values. When selecting this option, users specify the exact values that metrics should deviate from the baseline to trigger an alert.

- Select

Relative

to set thresholds based on percentages. This option allows users to define deviations from the baseline as a percentage, triggering alerts when metrics deviate by the specified percentage.

Critical/Major/Warning

Kindly use these fields to set the criteria under which the alert will be triggered. Here, you can also decide the alert severity based on the conditions you set.

Notify if the Threshold value breach within

Specify the time window during which the policy will check the monitor/instance to breach the threshold value for the metric you selected above.

Abnormality occurrence

Specify the number of times the threshold value should be breached consecutively within the evaluation window specified above to trigger an alert.

Auto Clear

Kindly enter the time in which you want the alert to be cleared irrespective of any other conditions.

Assumption Based Scenario

â€‹

In the context of a

Relative

Baseline alert, consider the following scenario:

Abnormality Occurrence

: Set to 2, indicating that the metric must deviate from the baseline threshold for two consecutive occurrences.

Notify if Threshold Value Breach Within

: Configured as 5 Minutes, defining the time window within which the consecutive deviations must occur.

If the actual value of the used memory bytes exceeds specific percentage thresholds compared to the baseline value, the alert will trigger with varying severity levels:

Critical

: Triggered when the actual value surpasses 50% compared to the baseline value twice consecutively within 5 minutes.

Major

: Triggered when the actual value exceeds 30% compared to the baseline value twice consecutively within 5 minutes.

Warning

: Triggered when the actual value goes below 10% compared to the baseline value twice consecutively within 5 minutes.

note

In case the metric in the policy crosses the value for multiple severity thresholds, the alert will be raised with the highest severity applicable. As shown in the diagram above, values above 30% qualify for both

Major

and

Critical

severity. In this case, the alert will be raised with

Critical

severity because it is the highest qualified severity.

Notify Team

â€‹

Field

Description

Notify

There are two ways you can populate this field:

Username of

registered user

in MotadataAIOps (The alert notification will be sent over email and SMS to the mapped email address and phone number respectively).

Any email address (In case the recipient whom you wish to notify is not a registered user, you can enter an email address).

If severity is

Select the severity level using individual checkboxes in the dropdown.You can select multiple, all, or a single option as per your requirement. You can also have different recipients notified at different severity levels. For instance, you can notify

johndoe@motadata.com

when severity level hits

Critical

and send an alert notification to

janedoe@motadata.com

when severity level is

Major

.

Play Sound

Activate this toggle to enable sound notifications when an alert is triggered.

If Severity is

Choose the severity level at which the sound notification should be triggered. This option becomes visible only when the

Play Sound

toggle is switched ON.

Renotification

Turning on the toggle will resend the alert at a specific interval defined by the user if the alert severity is not changed for the time specified. If turned off, Motadata AIOps will not renotify about the alert.

Renotify

Similar to

Notify Team

field, enter the username or email address of the recipient. Also choose a preset duration for renotification along with the severity level at which they system will renotify you if the alert severity is not changed.

Do not renotify if acknowledged

If the toggle is turned on, Motadata AIOps will not send a renotification to the recipient if they mark the alert as acknowledged.

Take Action

â€‹

Field

Description

Action to be taken

Select a runbook from the dropdown to be executed when the alert is triggered.

Create New

Select this button to start creating a new runbook which you might want to assign to the policy you are creating.

Select the

Create Policy

button to create the policy based on the details entered.

Select the

Reset

button to erase all the current field values, if required.

Page Title: overview

On this page

Overview

Overview

â€‹

The basic policies have a fixed threshold value and they trigger an alert when the value of the metric or the event attributes for which these policies are configured goes above the configured threshold.

The Basic Policies can be further divided as follows:

Availability Policy

Metric Policy

Log Policy

Flow Policy

Default Out-of-Box Alerts

â€‹

Default Out-of-Box Alerts in Motadata AIOps offer predefined metric, log, and flow-based alerts. These built-in alerts cover a spectrum of potential issues, from detecting malicious IPs in logs or flows to signaling the unavailability of an ESXi VM, critical CPU utilization levels, multiple failed login attempts, and various other system-related events.

Create Custom Policy

â€‹

Apart from default Out-of-Box Alerts, Motadata AIOps also offers the facility to create policies with customised threshold.

Let us look into all these policies one by one in the next sections

Page Title: trap-policy

On this page

Trap Policy

Overview

â€‹

The trap policy feature in Motadata AIOps enables effective monitoring and analysis of SNMP trap data, allowing proactive identification and resolution of network device issues. With trap policies, you can define rules and conditions to generate alerts based on trap data, ensuring smooth network operation and timely response to potential issues.

Use-Case

â€‹

Network Device Monitoring: Configure trap policies to detect and alert on various SNMP trap events generated by network devices, such as link status changes, hardware failures, or configuration errors.

Performance Monitoring: Create trap policies to monitor network device performance metrics, including CPU utilization, memory usage, or interface bandwidth, enabling you to optimize device performance and prevent bottlenecks.

Fault Detection: Utilize trap policies to identify and alert on critical faults or abnormalities in network device behavior, helping you mitigate risks and maintain network reliability.

Create Trap Policy

â€‹

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Policy Settings

. Select

Metric/Log/Flow/Trap policy

. The list of the created policies is now displayed.

Click on

to start creating a policy. From the panel on the left side of the screen, click on the

Flow

tab to start creating a metric policy. The screen to create a

Flow

Policy is now displayed.

Enter the details of the following parameters to create a Trap Policy:

Field

Description

Policy Name

Enter a unique name of the policy you want to create.

Tag

Enter a name to logically categorize the policy. You can quickly and easily identify a policy based on the tag assigned to it.

Set Conditions

â€‹

Field

Description

Trigger Condition

Choose the specific trap event you wish to create a policy for by selecting from the available options. This event will be the basis for monitoring and generating alerts.

Operator

Select the operator that will be applied to the trap event values to define the triggering condition for the alert. Different operators such as equal to, not equal to, greater than, less than, etc., are available to provide flexibility in defining your alert conditions.

Value

Specify the threshold value against which the trap event values will be compared. Once the trap event value meets the specified condition, an alert will be triggered.

Source Filter

Source Host will be selected by default.

Source

Select the specific Source Host for which you want to create the policy.

Filter Criteria

â€‹

Field

Description

Criterias

You can choose the type of operation to be performed on inter-filters. Below is a gist of available options:

-

ALL

:When selected, this will ensure that filtering criteria defined in all of the defined filters is being met.

-

ANY

: When selected, this will ensure that filtering criteria of any ONE among the defined filters is met.

Varbind

Select a Varbind value using the dropdown menu.

Operator

Choose an operator as per requirement using the dropdown.

Value

Enter a numerical value which will be used for the filteration.

Critical/Major/Warning

Kindly use these fields to set the severity under which the alert will be triggered.

Supress Action

Switch this Toggle button ON to supress the actions and notifications mapped to the policy. Once you switch this button ON and the alert is triggered, the action will be executed once and you will receive a single notification before the actions and notifications configured in the policy are supressed for the time-period specified in the field

Supress Window

.

Supress Window

Specify the time-period for which you do not wish to execute the actions and receive the notifications mapped to policy. (Enter a numerical value and use the drop-down to choose a duration unit.)

Enable this option specify criteria for resolving the alert to a clear state

Turn on this toggle to define a criteria to resolve an alert to a clear state.

note

The following fields are only visible when the toggle is turned on.

Field

Description

Criterias

You can choose the type of operation to be performed on inter-filters. Below is a gist of available options:

-

ALL

:When selected, this will ensure that filtering criteria defined in all of the defined filters is being met.

-

ANY

: When selected, this will ensure that filtering criteria of any ONE among the defined filters is met.

Varbind

Select a Varbind value using the dropdown menu.

Operator

Choose an operator as per requirement using the dropdown.

Value

Enter a numerical value which will be used for the filteration.

Notify Team

â€‹

Field

Description

Notify

There are two ways you can populate this field:

Username of

registered user

in MotadataAIOps (The alert notification will be sent over email and SMS to the mapped email address and phone number respectively).

Any email address (In case the recipient whom you wish to notify is not a registered user, you can enter an email address).

Play Sound

Activate this toggle to enable sound notifications when an alert is triggered.

If Severity is

Choose the severity level at which the sound notification should be triggered. This option becomes visible only when the

Play Sound

toggle is switched ON.

Take Action

â€‹

Field

Description

Action to be taken

Select a runbook from the dropdown to be executed when the alert is triggered.

Create New

Select this button to start creating a new runbook which you might want to assign to the policy you are creating.

Select the

Create Policy

button to create the policy based on the details entered.

Select the

Reset

button to erase all the current field values, if required.

Page Title: configuring-policies-to-setup-alerts

On this page

Configuring Policies to Setup Alerts

Overview

â€‹

Alerts are triggered via policies when a specific event occurs in your infrastructure. The type of policies created and the threshold values mentioned while configuring the policies determine the conditions under which alerts are triggered.

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Policy Settings

. Select

Metric/Log/Flow policy

based on the type of policy you want to create. The list of the created policies is now displayed. Here, you can view all the different types of policies available in the system.

Configuration

â€‹

In order to configure policies, you need to perform the following steps:

Select the policy type, provide policy name & policy tags.

Define the conditions for the alert to be triggered.

Select the teams to notify when an alert is triggered.

Define the actions to take when an alert is triggered.

The steps to configure policy will be discussed in detail for each

Alert type

in detail on the next page.

From the alerts screen, click on

to start creating a policy. The screen to create policy is now displayed.

Select Policy Type

â€‹

The

Metric

Policy is selected by default. Select the type of policy you want to create from the panel on the left of the screen. Once you select the policy type, the parameters to create the selected policy type appears on the screen.

Enter the

Policy Name

and

Tag

details to identify and categorise the policy for future reference.

Set Conditions

â€‹

The alert conditions vary based on the monitor type. Configure monitors to trigger if the query value crosses a threshold, or if a certain number of consecutive checks failed.

Next, you need to set the conditions under which the alert will be triggered. The conditions and parameters for the policies vary based on the type of the policy selected. Configure the policies to trigger alerts whenever a specific entity crosses a threshold or in case some services are not available.

You can configure policies to trigger an alert when:

A specific metric is

Greater Than

,

Greater Than or Equal to

,

Less Than

,

Less Than or Equal To

,

Not Equals

,

Equals

the threshold during the selected time period specified in the policy configuration.

A specific service or a monitor is not available.

Notify Team

â€‹

While configuring a policy, you can decide the teams to notify when an alert is raised. You can set the email addresses and the phone number of the relevant personnel to be notified via E-mail and SMS respectively.

You can configure a policy to notify the relevant team members whenever the polling gets failed for a monitor after an alert is raised.

You can configure a policy to notify the relevant team members whenever the flap(alert severity) changes.

You can configure a policy to send a customised notification if you do not wish to use the default message that is sent by Motadata AIOps.

Take Action

â€‹

There might be a situation where you want to take an immediate action when an alert of a certain significance is raised i.e., when a critical alert is raised in the system.

Configure a policy to automate the appropriate action based on the severity of the alert raised. This means you can customise your policy to take different actions based on the severity of the alert.

Suppose you have configured a policy to trigger an alert when the CPU utilisation of a Virtual Machine goes above a certain threshold. You have configured the policy to trigger alerts in
Major
and
Critical
severity based on the threshold values specified in the policy.

Now, you want to automate different actions based on the alert severity. When the alert is in
Major
severity, you might want to restart the top processes consuming the CPU but when the alert is in
Critical
severity, you might want to restart the VM to make sure that the issue is resolved. Motadata AIOps allows you to automate this process by allowing a different Runbook to be executed based on the alert severity.

Page Title: how-do-alerts-and-policies-work

On this page

How Alerts and Policies work?

Overview

â€‹

An alert is an automated notification to indicate a specific event has occurred in your infrastructure. Policies are used to trigger alerts when specific events occur, and can even notify relevant teams and execute runbooks when an alert is triggered.

Use-Case

â€‹

Suppose you want to receive an alert whenever the disk space of a monitor goes above a specified threshold. Here's how you would set this up:

Create a policy to trigger an alert when a monitor's disk space utilization goes above 70%.

At some point, the disk space utilization goes above the threshold of 70%. This means that the networking event connected to the policy you configured has occurred.

Motadata AIOps triggers an alert based on the policy you configured.

The notifications are sent out to the relevant teams and the appropriate action is taken as configured while setting up the policy.

The alerts generated by Motadata AIOps are intelligently classified based on severity, host, and the group of the monitor, making it easy to filter them based on their category.

You can

gain detailed insights into every alert by drilling down into it on the alerts screen

Here, you can collaborate with your teammates by providing comments on an alert, which can speed up the root cause analysis and resolution by saving crucial time on communication.

Page Title: macros-alerts-and-policies

On this page

Macros in Alerts & Policies

You can customize your alert messages by including pre-defined Macros. These Macros serve as placeholders that are automatically replaced with actual values when the alert is triggered. By leveraging Macros, you can tailor your alert messages to provide precise information about the event that triggered the alert, facilitating quicker and more informed decision-making.

Navigation

â€‹

While configuring a policy, click on the

 to modify the default alert messages. Here, you can use the pre-defined macros to customize the alert message and the subject.

How to Use Macros

â€‹

To use Macros in your alert messages, simply include the Macros within your customised alert message. When the alert is triggered, these Macros will be replaced with the actual values associated with the event.

Below is an example of how you can incorporate Macros in your alert message:

An alert $$$policy.name$$$ was triggered with $$$severity$$$ severity for the monitor $$$object.name$$$ (IP: $$$object.ip$$$) because the $$$counter$$$ breached the threshold with the value $$$value$$$.

Supported Macros

â€‹

Here's a list of supported Macros along with the descriptions of what these macros display in the actual alert message:

Macro

Description

$$$policy.trigger.time$$$

The exact time when the alert was triggered.

$$$object.name$$$

The name of the monitor that triggered the policy.

$$$object.ip$$$

The IP address of the monitor that triggered the policy.

$$$object.host$$$

The host name of the monitor that triggered the policy.

$$$object.type$$$

The type of monitor.

$$$counter$$$

The counter for which the alert is triggered.

$$$value$$$

The value of the counter at which the alert is triggered.

$$$severity$$$

The severity level of the triggered alert.

$$$policy.name$$$

The name of the policy that triggered the alert.

$$$policy.type$$$

The type of policy that triggered the alert.

$$$object.groups$$$

The monitor group for which the alert is triggered .

$$$instance$$$

The specific instance for which the alert is triggered.

$$$active.since$$$

The duration of the alert in its current severity state.

$$$trigger.condition$$$

The policy evaluation criteria for the received alert.

With these Macros, you can create customized alert messages tailored to your specific requirements, ensuring that you receive the most relevant information when alerts are triggered.

Page Title: view-and-manage-alerts

On this page

View and Manage Alerts

Overview

â€‹

You can view all the alerts triggered currently in the system, all the alerts raised in the past, the different states the alert has been in, and many other details related to the alerts at one place. You can also search, clear, and acknowledge the alerts in the system. The alert screen gives you deeper visibility into each alert to help minimize downtime and maximize infrastructure performance.

Navigation

â€‹

Go to Menu, Select

Alerts

. The alert screen is now displayed.

Classification of Alerts

â€‹

The alerts are classified intelligently based on the alert severity and the alert type. Alert section in Motadata AIOps has superior intelligence as it identifies alerts and groups them based on alert type, severity, host and the device type of the monitor. This helps you to pinpoint the alert you are looking for in a easy manner.

On the alert screen, you can see that the alerts are mainly categorized based on their device type (

Cloud, Network, Service Check, Server, and Virtualization

). They are also further categorized based on their severities (

Down, Unreachable, Critical, Major, Warning

).

Suppose you want to view all the

Down

alerts received for the

Cloud

device type, click on the circle titled

Down

under the

Cloud

tab. The list of all the

Down

alerts for the

Cloud

device type will be displayed.

View Alert Details

â€‹

After selecting the alert category by clicking on the apprpriate circle from the alert screen as described above, a list of all the alerts under that category is displayed.

The following fields appear in the alert list:

Field

Description

Alert

The name of the alert.

Type

The type of the alert.

Monitor

The name of the monitor for which the alert is created.

Last Seen

The last triggered timestamp of the alert.

Instance

The instance name (if applicable) for which the alert is created.

Value

The threshold value at which the alert is triggered.

Duration

The time passed since the alert was triggered.

24 Hours Count

This field displays the count of the all the severities in which the alert has been in the last 24 hours.

Acknowledged

This field displays whether the alert has been acknowledged or not.

Actions

There are multiple actions available for an alert which we will discuss later in the next section.

We can explore an alert in even further detail. Click on the alert name from the alert list to view the details related to that alert. The details shown would be relevant to the type of the alert triggered i.e. metric, log, or flow alert. Let us first look at the detail screen for a metric alert.

Metric Alert Details

â€‹

Here, you can see details such as the

Monitor

,

IP

,

Group

,

Alert ID

,

Metric

for which the alert is triggered, and much more.

You can also visualise important details via widgets available on this screen to take a deep dive into that alert.

Widget

Description

Alert History

This Widget shows the metric values for which the policy is configured, the threshold values configured in the policy, and the severity of the alerts over time based on the selected timeline.

History

This widget shows the changes in the severity of the alert based on the selected timeline.

Metric Trend

This widget shows the changes in the values of the metric for which the alert is triggered based on the selected timeline.

Now, let us look into the details available for log alert.

Log Alert Details

â€‹

Here, you can see details such as the

Alert ID

,

Counter

,

Trigger Condition

,

Severity

, for which the alert is triggered, and much more.

You can also visualise important details via widgets available on this screen to take a deep dive into that alert.

Widget

Description

Alert Trend

This widget shows count of log messages that qualify for alert evaluation based on the selected timeline and also highlights the point at which the alert is triggered.

Alert Count

This widget shows the number of times the alert is triggered at various points of time based on the selected timeline.

History

This widget records the alert message and the time at which the alert is triggered

Log Explorer Widget

This widget helps you to analyse the log messages that trigger the alert by directing you to that exact log message in

Log Explorer

.

Now, let us look into the details available available for flow alert.

Flow Alert Details

â€‹

Here, you can see details such as the

Alert ID

,

Counter

,

Trigger Condition

,

Severity

, for which the alert is triggered, and much more.

You can also visualise important details via widgets available on this screen to take a deep dive into that alert.

Widget

Description

Alert Trend

This widget shows count of flows that qualify for alert evaluation based on the selected timeline and also highlights the point at which the alert is triggered.

Alert Count

This widget shows the number of times the alert is triggered at various points of time based on the selected timeline.

History

This widget records the alert message and the time at which the alert is triggered

Flow Explorer Widget

This widget helps you to analyse the flow that triggers the alert by directing you to that exact flow in Flow Explorer

Action on Alerts

â€‹

Clear Alert

â€‹

You can manually move an alert into the clear state if needed. Search the alert that you want to clear on the alert screen.

Click on

to display the actions available for the alert. Select

Clear Alert

to move the alert into the clear state.

Supress Alert

â€‹

You can supress an alert for a maximum of 48 hours in case you do not wish to receive any further notifications related to that alert. Search for the alert that you want to acknowledge on the alert screen.

Click on

to display the actions available for the alert. Select

Suppress Alert

and then select the number of hours for which you want to suppress alert from the pop-up.

Acknowledge Alert

â€‹

You can acknowledge an alert to indicate that appropriate action is being taken on the alert. Search the alert that you want to acknowledge on the alert screen.

Click

to acknowledge the alert.

Page Title: what-are-the-different-alert-severities

On this page

What are the different Alert Severities?

Overview

â€‹

While setting up policies to trigger alerts, you can specify the severity levels based on the seriousness of the event which in turn indicates how quickly it needs to be dealt with.

The alerts can be categorized into 4 different severity levels. These severities may have different meanings as per the requirements of your organization but as per the general understanding they may mean as written below.

Detailed Explanation of Alert Severities

â€‹

Critical

â€‹

This severity level is reserved for the most severe and critical issues that require immediate attention. Critical alerts indicate that there is a major problem in your network that is causing significant disruption and needs to be resolved as soon as possible. For example, a critical alert might indicate that a critical application or service is down, causing a significant impact on your business operations.

Major

â€‹

This severity level indicates an issue in your network that requires attention but may not be as severe as a critical alert. Major alerts may indicate potential problems that could impact your network's performance, security, or reliability. For example, a major alert might indicate that a network device is experiencing a high CPU or memory usage, which could lead to performance issues if not addressed.

Warning

â€‹

This severity level indicates that there might be a potential issue in your network that you need to be informed about, but it may not be causing a problem as of now. Warning alerts may indicate potential problems that could affect your network's performance, security, or reliability in the future. For example, a warning alert might indicate that a network device is running low on disk space, which could cause issues in the future if not addressed.

Clear

â€‹

This severity level indicates that there is no issue in your network, and everything is running fine. Clear alerts are useful to confirm that a previously generated alert has been resolved and no further action is required.

Down

â€‹

This severity level indicates that the service or monitor in question is down and not available for monitoring. Down alerts are generated when a device or service is unreachable or not responding to monitoring requests. This alert is useful for troubleshooting connectivity issues or identifying devices that are not functioning as expected.

In conclusion, configuring different alert severities helps to prioritize the issues and take the necessary actions accordingly. It also ensures that critical issues are not missed, and the relevant teams are notified immediately for the prompt resolution of the issues.

Page Title: what-are-the-different-alert-types

On this page

What are the different Alert Types?

Overview

â€‹

Alerts are an essential part of any monitoring system. They notify users when an event or issue occurs in their infrastructure that requires attention. Motadata AIOps offers a variety of alert types to help users stay on top of their infrastructure's health and performance. These alerts can be configured through policies, which define the conditions for triggering alerts, the actions to take when an alert is raised, and the teams to notify.

The policies can be categorized into two major categories:

Basic Policies

Availability Policy

Metric Policy

Log Policy

Flow Policy

AIOps Policies

Forecast Policy

Anomaly Policy

There are two types of policies available in Motadata AIOps - Basic Policies and AIOps Policies. Basic Policies include Availability, Metric, Log, and Flow Policies, while AIOps Policies include Forecast and Anomaly Policies.

Availability Policies are used to monitor the availability of various entities in your infrastructure, such as servers, applications, and services. Metric Policies are used to monitor performance metrics, such as CPU usage, memory usage, and disk space. Log Policies are used to monitor logs generated by various applications and systems, while Flow Policies are used to monitor network flows.

AIOps Policies, on the other hand, are advanced policies that leverage machine learning algorithms to detect anomalies and patterns in your infrastructure's data. Forecast Policies predict future trends and patterns in your data while Anomaly Policies detect anomalies in your data using various statistical methods.

Overall, the variety of alert types available in Motadata AIOps ensures that users can configure policies that suit their unique monitoring needs, and stay on top of their infrastructure's health and performance.

Let us understand how to create all the policies for each category in the next sections.