Page Title: aiops-to-serviceops-integration

On this page

Configuring AIOps to ServiceOps Integration

Overview

â€‹

The ServiceOps Integration module in Motadata AIOps facilitates seamless integration with Motadata ServiceOps, an IT Service Management (ITSM) tool. This integration empowers users to create incidents in ServiceOps automatically when specific alerts with predefined severities are triggered in Motadata AIOps. By streamlining incident management processes, organizations can enhance their response efficiency and ensure timely resolution of critical issues.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Integration

and select

Motadata ServiceOps

. The Motadata ServiceOps integration screen is displayed.

Integration Steps

â€‹

Ensure that the necessary prerequisites are met, including the creation of the integration in ServiceOps and obtaining the related Client ID and Client Secret, before proceeding with the integration configuration.

To configure the integration with Motadata ServiceOps, enter the following details on the ServiceOps integration screen:

Field

Description

Server URL

Provide the URL of the ServiceOps server.

URL Timeout

Specify the timeout duration for establishing the connection with the ServiceOps server.

User Name

Enter the username of the ServiceOps account to be used for integration.

Password

Provide the password for the ServiceOps account.

Client ID

Enter the

client ID

of the integration obtained from ServiceOps.

Client Secret

Provide the client secret of the integration obtained from ServiceOps.

Source

Specify the ServiceOps source that you have registered in ServiceOps. The value in this field will be shown as the

Source

in the ServiceOps incident. For example, if you have registered 'AIOps' as a

Source

in ServiceOps, you can enter 'AIOps' in this field. When the

incident is created in ServiceOps via AIOps

, the incident will have

Source

as 'AIOps'.

Failover Email

Specify the email address where notifications will be sent in case the integration gets disconnected.

Urgency:Low

Map the selected alert severity to create incidents with low urgency in ServiceOps.

Urgency:Medium

Map the selected alert severity to create incidents with medium urgency in ServiceOps.

Urgency:High

Map the selected alert severity to create incidents with high urgency in ServiceOps.

Urgency:Urgent

Map the selected alert severity to create incidents with urgent urgency in ServiceOps.

Auto Close Ticket

Toggle this button to automatically close the ticket in ServiceOps when the corresponding alert moves to a clear severity in AIOps.

Ticket Status

Select the status (Resolved or Closed) of the incident to which the ticket should move once it is auto-closed.

Select the

Reset

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

Select the

Test

button to test the integration configuration.

Select the

Save

button to save the integrations configuration.

Page Title: serviceops-incidents-using-aiops-alerts

On this page

Create Incidents in ServiceOps via AIOps Alerts

To enable incident creation in ServiceOps via the integration established between AIOps and ServiceOps, you can configure the action within the policy settings in AIOps. This action allows you to trigger an alert in AIOps, which subsequently generates an incident in ServiceOps when specific events occur in your infrastructure.

Configuration Steps

â€‹

Navigate to the specific policy or create a new policy from

Policy Settings

 to map incident creation in ServiceOps with alerts in AIOps.

In the policy configuration settings, locate the

Take Action

 section. This section allows you to define the actions to be taken when the policy conditions are met and an alert is triggered.

Within the

Take Action

 section, locate the field labeled

Action to be taken

. Here, you need to assign a runbook to the alert. Choose

ServiceOps Ticket

 from the available options.

Next, specify the alert severity for which you want to trigger incident creation in ServiceOps. This is done by selecting the appropriate severity level from the dropdown

When Severity is

.

Example Scenario

â€‹

For example, if you have configured the following settings:

Action to be taken

: ServiceOps Ticket

When Severity is

: Critical

In this scenario, when an alert with a critical severity is triggered in AIOps as per the configured policy conditions, AIOps will automatically create an incident in ServiceOps. The urgency of the ticket created in ServiceOps will be determined based on the mapping between alert severities and incident urgency that you have previously configured while establishing the

ServiceOps integration

.

Page Title: serviceops-to-aiops-integration

On this page

Configuring ServiceOps to AIOps Integration

The ServiceOps to AIOps Integration facilitates the synchronization between Motadata ServiceOps and Motadata AIOps platforms, ensuring streamlined incident management and alert resolution processes. This integration enables automatic clearing of alerts in AIOps when corresponding tickets are closed in ServiceOps. By establishing this bidirectional communication, organizations can maintain consistency across their IT operations.

Configuration Steps

â€‹

To configure the integration from ServiceOps to AIOps, follow these steps:

Open the ServiceOps portal and click on the Settings button located on the top right corner of the screen.

Navigate to the

Automation

tab and select

Workflow

.

Click on

Create Workflow

and provide a name, such as

AIOps

to identify the workflow.

In the

Module

field, select

Request

, and choose

Event

as the

Workflow Type

.

Under the

Trigger

tab, select

Status is Changed

to trigger the workflow when a ticket status changes.

Specify the trigger conditions by selecting

From: Any

and

To: Closed

to indicate the transition from any status to

Closed

.

Click

Done

to confirm the trigger condition.

Add a condition by clicking the plus icon and selecting

Add Condition

.

Under the

Condition

tab, select

Source

as the

Condition

,

In

as the

Operator

, and enter

AIOps

and

HA

as

Value

.

Click

Done

to confirm the condition.

Specify the action to be taken when the condition is met by clicking the plus icon and selecting

Action for Yes

.

Under the

Action

tab, select

Run Webhook

and choose

POST

as the

Request Type

.

Enter the following URL:

https://MotadataServerIP/api/v1/settings/integrations/clear-alert

where MotadataServerIP is the IP address of the Motadata Server.

In the

Request JSON

 field, enter the following JSON payload:

```
{
    "name": "{#name#}",
    "id": "{#id#}",
    "status": "{#status#}"
}
```

Add headers by selecting

Add Header

 and entering

Cookie

 as the

Key

 and the following as the

Value

:

client.id=Q5VZ97naQhyLIH0Vz4MSXvzbMyCYTjPwz+1hVJ643pA=

Add another header with

Authorization

 as the

Key

and the following as the

Value

:

Bearer UserAccessKey

where UserAccessKey is the

Access Key

of the User used for integration. You can find the access key of the user from the

User

tab under

User Settings

.

Select

Credential Type

as

No Auth

and click

Done

to confirm the action.

Finally, click

Save Workflow

to establish the integration.

Once this connection is established, whenever a ticket is closed in ServiceOps, the corresponding alert in AIOps will automatically move into the

Clear

state. This ensures that incidents resolved in ServiceOps are accurately reflected in AIOps, maintaining data consistency and facilitating efficient incident management.