Page Title: SNMP-Trap-Explorer

On this page

SNMP Trap Explorer

Overview

â€‹

Trap Explorer is a comprehensive tool in Motadata AIOps that enables users to view all the ingested SNMP traps in Motadata AIOps. The tool provides various features to analyze and manage the ingested SNMP traps.

It provides an intuitive graphical interface for viewing the count of traps received at specific time period and also allows selecting timeline for the same.

The tool also allows drilling down on a trap to view details such as trap message, trap count, and trap history. Additionally, users can acknowledge specific traps indicating that work is done on them, although the acknowledgment is overridden if the trap comes again.

One of the key features of the Trap Explorer is its search functionality, which allows users to view specific traps based on filters such as Trap severity, Trap OID, source, and vendor. Users can filter the displayed traps to view only those that meet specific criteria. With these capabilities, the Trap Explorer provides a powerful tool for managing SNMP traps in Motadata AIOps.

Navigation

â€‹

Go to Menu. Select

Trap Explorer

. The Trap Explorer is now displayed.

Trap Explorer Screen

â€‹

Viewing Trap Count

â€‹

On the Trap Explorer Screen you can view a graphical representation of the trap count received in Motadata AIOps as per the selected timeline. This feature may be useful in identifying the peak periods of traps received and helps to allocate resources accordingly. The timeline can be adjusted to view the trap count for specific intervals, such as the last hour, day, week, or month.

Viewing Trap List

â€‹

The Trap Explorer allows you to search for specific traps and provides the option to filter traps by severity, trap OID, source, and vendor. This enables you to easily navigate through the traps and view only specific traps that meet the filtering criteria.

The following trap details are available just below the trap count graph on the Trap Explorer screen:

Field

Description

Trap Name

The name of the trap.

Trap OID

The OID of the trap.

Source

The source device from which the trap is generated.

Count

The number of times that particular trap is recevied in the timeline selected above.

Message

The trap message associated with the trap indicating the issue that caused the trap.

Date & Time

The Date & Time at which the trap is received in the AIOps server.

Actions

Select this option to acknowledge a trap indicating that the issue that caused the trap hase been

worked upon.

Trap Details

â€‹

The Trap Explorer tool allows you to drill down on individual traps and view their details, including the raw message, trap message, trap count, and trap history. This feature is especially useful in identifying patterns and trends in the traps received as it shows the trap history, enabling you to take proactive measures to prevent recurring issues.

Filtering traps

â€‹

The Trap Explorer also provides the option to filter and view specific traps. This is especially helpful when dealing with a large number of traps ingested by the system. Users can filter the traps based on different fields such as severity, trap OID, source, and vendor.

Select

present at the top-right of the screen to display the option to filter the traps as follows:

Now, if a user wants to view only the traps with a severity level of 'Critical', they can select the

Critical

option in the severity filter, and the system will display only the traps with a critical severity level.

Similarly, a user can filter the traps based on the trap OID, source, and vendor. This helps the user to quickly identify specific traps and their sources without going through a large number of traps. Additionally, the filtering option also allows users to search for specific traps based on specific keywords or phrases.

The filtering option in the Trap Explorer provides users with greater control and flexibility in viewing and managing the traps ingested by Motadata AIOps.

Live Trap Viewer

â€‹

The Trap Explorer allows you to view all incoming Traps in real-time. The Live Trap Viewer will display the received time, OID, source, translated Trap message, along with the raw Trap message.

Select

Live Trap Viewer

button on the top right corner. On the next screen, you shall be able to view the list of all incoming Traps.

Page Title: SNMP-Trap-Forwarder

On this page

SNMP Trap Forwarder

Overview

â€‹

SNMP Trap Forwarder is a crucial component in Motadata AIOps trap monitoring that acts as an intermediary to map SNMP Trap Profiles to a destination IP address and route the SNMP trap to a specific destination IP address.

When a trap is received by Motadata AIOps, the forwarder matches the trap's OID with the trap OID configured in the SNMP profile mapped to the forwarder. If a match is found, the trap is forwarded to the destination IP address configured in the forwarder.

In addition to mapping the SNMP profile, you can also specify the destination IP address and port to which the traps are to be forwarded.

However, whether a trap is forwarded to a destination or not, it will be visible in Motadata AIOps if it is received by the configured

SNMP Trap Listener

. The forwarder does not act as a gatekeeper or prevent the traps from being ingested by the server. Instead, it is a means of routing traps to specific destinations based on their SNMP profile. This helps in efficient handling of traps as well as streamlining the monitoring process.

note

You can assign multiple SNMP Trap Profiles to a single SNMP Trap Forwarder.

Navigation

â€‹

Go to Menu. Select Settings. Then, select

SNMP Trap

. After that, Select

SNMP Trap Forwarder

. The screen to view and create a SNMP Trap Forwarder is now displayed.

SNMP Trap Forwarder Screen

â€‹

The following fields are available on the SNMP Trap Forwarder screen:

Field

Description

SNMP Trap Forwarder Name

This name is used to identify an SNMP Trap Forwarder.

SNMP Trap Profiles

This field is used to indicate the SNMP Trap Profile mapped to the forwarder.

Destination IP/Host

This field is used to indicate the destination IP/Host to which the trap should be forwarded.

Actions

-

Edit SNMP Trap Forwarder

: Select this option if you want to edit the details of the Trap Forwarder.

-

Delete SNMP Trap Forwarder

: Select this option if you want to delete the SNMP Trap Forwarder.

How to create a SNMP Trap Forwarder?

â€‹

You can create a new SNMP Trap Forwarder based on the destination to which you want to send your traps.

Go to Menu. Select

Settings

. Then, Select

SNMP Trap

. After that,

Select SNMP Trap Forwarder

. Select

to create a new SNMP Trap Forwarder.

The screen to create a new SNMP Trap Forwarder is now displayed.

The following fields are available on the

Create SNMP Trap Forwarder

screen:

Field

Description

SNMP Trap Forwarder Name

Enter the name of the SNMP Trap Forwarder.

SNMP Trap Profiles

Select the Profile(s) that you wish to map with the forwarder.

Destination IP/Host

Enter the destination IP/Hostname of the device to which you wish to forward the trap.

Port

Enter the port number of the device to which you wish to forward the trap.

Select the

Create

button to create the SNMP Trap Forwarder.

Select the

Reset

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

Page Title: SNMP-Trap-Listener

On this page

SNMP Trap Listener

Overview

â€‹

SNMP Trap Listener is a component that allows the server to configure Motadata AIOps to listen to SNMP traps and ingest them in Motadata AIOps.

Navigation

â€‹

Go to Menu. Select

Settings

. Then, select

SNMP Trap

. After that, Select

SNMP Trap Listener

. The screen to configure SNMP Trap Listener is now displayed.

SNMP v1/v2c Listener Configuration

â€‹

Field

Description

Port

Enter the Port number of Motadata AIOps server to which you will send the traps. This will be chosen as 1620 by default.

Community

Enter the community string of the SNMP devices that will send the traps to the AIOps server.

SNMP v3 Listener Configuration

â€‹

Field

Description

Port

Enter the Port number of Motadata AIOps server at which you will send the traps. This will be chosen as 1630 by default.

Security User Name

Enter the security user name of the SNMP devices that will send the traps to the AIOps server.

Security Level

Select the Security Level from the dropdown. Provide subsequent details such as

Authentication Protocol

,

Authentication Password

,

Privacy Protocol

,

Privacy Password

based on the

Security Level

you select.

Once the listener is configured, it will start listening for SNMP traps and ingest them in Motadata AIOps. The traps will be parsed based on the configured SNMP Trap Profile and the notifications for the traps will be generated accordingly. The SNMP Trap Listener provides an efficient way to monitor SNMP-enabled devices and receive real-time alerts about any issues in infrastructure.

Page Title: SNMP-trap-overview

On this page

SNMP Trap Monitoring

Overview

â€‹

One of the key features of Motadata AIOps is its ability to monitor and analyze SNMP traps. SNMP (Simple Network Management Protocol) is a standard protocol used for managing and monitoring network devices.

By leveraging SNMP traps, AIOps is able to provide instant notifications for critical events occurring within your network environment. This allows you to identify and resolve issues before they make a massive impact on your business operations. With the AIOps trap explorer, you can easily view the traps being sent by your infrastructure devices and gain valuable insights into your network performance.

When there is a very large count of devices in an infrastructure, requesting data from several devices to monitor them seems like a very inefficient option. This brings SNMP traps into the picture. Instead of AIOps going to every device and seeking information for monitoring, we can configure network devices to send traps to AIOps as and when needed to inform AIOps about any device health related issue.

SNMP Trap is a passive mode of monitoring that helps us to detect any concerns related to device health that occurs between the two polls. This ensures that any major event that occurs between two polls is not missed because sending SNMP traps does not require polling of data from monitors.

In this section, we will provide step-by-step instructions on how to send SNMP traps to Motadata AIOps for monitoring, as well as understand the SNMP traps processing mechanism in AIOps, followed by guidance on how to view the traps in AIOps. This will ensure the optimal performance and reliability of your network infrastructure.

Pre-requisites for SNMP Trap Monitoring in AIOps

â€‹

Configure devices to send SNMP traps to the Motadata AIOps server.

Make sure the UDP port 1620 and 1630 are open on the server for SNMP v1/v2c and SNMP v3 respectively.

The

SNMP trap listener

has to be configured on the Motadata AIOps server.

Page Title: SNMP-Trap-Profile

On this page

SNMP Trap Profile

Overview

â€‹

The SNMP Trap Profile in Motadata AIOps is a crucial feature that allows the application to identify and process SNMP traps. Each SNMP Trap Profile is mapped to a unique Trap OID which helps Motadata AIOps to first identify and then assign a severity to a trap when it is received by Motadata AIOps. The SNMP trap profile also has a message mapped to it. This message helps you to identify what the issue is about.

Navigation

â€‹

Go to Menu. Select

Settings

. Then, Select

SNMP Trap

. After that, Select

SNMP Trap Profile

. The screen to view and create SNMP Trap Profiles is now displayed.

SNMP Trap Profile Screen

â€‹

The following fields are available on the SNMP Trap Profile screen:

Field

Description

SNMP Trap Profile Name

This name is used to identify an SNMP Profile.

Trap OID

This field is used to indicate the OID corresponding to the Trap.

Used Count

This count is used to indicate the number of SNMP forwarders using the profile.

Actions

Select the option

Edit SNMP Trap Profile

to modify any details of the trap profile that you might have created.

How to create an SNMP Profile?

â€‹

In addition to the inbuilt set of trap profiles, you can also create custom trap profiles for specific devices or applications for which a trap profile is not already available in the inbuilt set of profiles. In case you are able to view a trap in trap explorer but the name, message, and the severity corresponding to that trap is not visible, it means that the SNMP trap profile corresponding to that trap OID is not available. You can create a SNMP trap profile for that trap OID so that Motadata AIOps is able to identify the trap.

In summary, the SNMP Trap Profile in Motadata AIOps enables the application to identify and process SNMP traps efficiently. By creating and configuring the SNMP Trap Profiles, you can ensure that the application assigns the appropriate severity to each trap, enabling you to prioritize and resolve issues quickly.

Select

to create a new SNMP Trap profile.

The screen to create a new SNMP Trap profile is now displayed.

The following fields are available on the

Create SNMP Trap Profile

screen:

Field

Description

SNMP Trap Profile Name

Enter the name of the SNMP Trap Profile you wish to create.

Trap OID

Enter the Trap OID of the trap for which you are creating the SNMP Trap Profile.

Filter

-

Yes

: Select this option if you want Motadata AIOps to drop this trap and in turn not show it in the Trap Explorer.

-

No

: Select this option if you want Motadata AIOps to ingest this trap and show it in the Trap Explorer.

SNMP Trap Translator

Enter the message that you wish to display in the trap explorer after the trap is received by Motadata AIOps.

Select the

Create

button to create the SNMP trap profile.

Select the

Reset

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

Page Title: Trap-Processing

On this page

SNMP Trap Mechanism in AIOps

Overview

â€‹

In this module, we will explore how Motadata AIOps processes and monitors SNMP traps to provide real-time trap notifications via the Trap Explorer.

Trap Monitoring in Motadata AIOps includes several major components, including the

SNMP Trap Profile

,

SNMP Trap Forwarder

,

SNMP Trap Listener

, and

Trap Explorer

. Let's take a closer look at how these components work together.

To begin SNMP trap monitoring in Motadata AIOps, you need to enable SNMP Trap Listener to receive the traps. Once the application is enabled to receive the traps, ensure that your SNMP device is configured to send traps on the listener port of the AIOps server.

The SNMP traps are then sent to Motadata AIOps, where the application is able to collect and process them thanks to the SNMP Trap Listener you configured previously. Next, The Trap Explorer can be used to view and analyze the trap messages.

Motadata AIOps is able to identify the traps and assign a severity level to them because of the inbuilt database of Trap profiles. This database assigns severity levels to many well-known trap OIDs, enabling Motadata AIOps to identify and assign a severity level to various traps.

In cases where Motadata AIOps is unable to identify a trap because the SNMP trap profile

corresponding to it hasn't been pre-built in the system, you can easily create an SNMP profile of your own. Once created, Motadata AIOps will be able to identify the trap the next time it is received.

note

In case an SNMP trap profile corresponding to an OID is not available in the system, you would still be able to view the trap in the trap explorer but the name, message, and the severity corresponding to the trap would not be visible in the trap explorer.

Now that we have seen how these different components work together to enable you to view trap messages, let's explore each component in detail and understand how they work.