Page Title: adding-devices

Adding Devices For Monitoring

What cloud vendors and services are supported by Motadata AIOps?

AWS

: Amazon CloudFront, DocumentDB, DynamoDB, EBS, EC2, RDS, S3, SNS, SQS, ELB, Lambda, Elastic Beanstalk, Auto Scaling

Microsoft Azure

: Web App Service, Storage, VMs, SQL Database, Cosmos DB, Application Gateway, CDN, Load Balancer, Virtual Machine Scale Sets, Service Bus, Functions

Office 365

: Microsoft Teams, Sharepoint, Exchange Online, OneDrive

What are the prerequisites for monitoring AWS resources?

Access Key and Secret Key of the AWS account

IAM role with specific permissions (refer to the provided JSON filein the link below)

Refer

Integrations

for more details about the prerequisites for AWS resources.

What are the prerequisites for monitoring Azure resources?

The Azure account needs to be integrated with Motadata AIOps with the help of Client ID, Tenant ID, and Secret Key of the Azure account.

Refer

Integrations

for more details about the prerequisites for Azure resources.

Which network protocols are supported by Motadata AIOps for network device monitoring?

Motadata AIOps supports SNMP v1/v2c and SNMP v3 protocols.

What are the prerequisites for network device monitoring?

Ensure SNMP is properly configured on the target device.

Verify compatibility with both SNMP v1/v2c and SNMP v3 protocols.

Ensure port 161 is open and accessible on the device.

Configure the community string for authorized access.

Refer

Adding Network Devices for Monitoring

for more details about the prerequisites for Network Monitoring.

What types of servers can be added to Motadata AIOps for monitoring?

Motadata AIOps supports the following types of servers: Windows, Linux, HP-UX, IBM-AIX, and Solaris.

What are the prerequisites for adding a Windows server?

If the server is part of a domain, you'll need to have credentials of a user that is a member of the domain admin group.

For standalone servers, you'll need credentials of a user that is part of the local administrator group.

To ensure proper connectivity, it's important to allow traffic through firewall ports 5985 and 5986.

Enable ICMP protocol on both ports to monitor availability via ping check.

Refer

Adding Servers for Monitoring

for more details about the prerequisites for Network Monitoring.

Page Title: monitor-rediscovery

Monitor Rediscovery

What is monitor rediscovery in Motadata AIOps?

Monitor rediscovery allows you to discover new 'Instances' within existing monitors for monitoring. This is useful for situations where you add new components (applications, VMs, etc.) to a device that's already set up as a monitor in AIOps. For Example, if you have discovered an ESXi as a monitor in AIOps, you can use rediscovery to discover the VMs within that ESXi and set them up as instances for monitoring

What is the difference between a Monitor and an Instance in Motadata AIOps?

A Monitor refers to a device, application, or service that has been set up for monitoring in Motadata AIOps. This is the primary entity being observed for performance, availability, and other metrics.

An Instance is a specific component or sub-element within a Monitor. Instances are often discovered through monitor rediscovery and represent individual units that can be monitored separately within the overarching Monitor. For example, if an ESXi server is set as a Monitor, the individual virtual machines (VMs) hosted on it are Instances.

What types of instances can be rediscovered in AIOps?

Motadata AIOps supports rediscovery for the following types of instances:

Application

Cloud

Virtualization

Interface

Process

Service

File/Directory

HCI Cluster

HCI VM

What are some things to remember when rediscovering instances?

Ensure the server/device you want to monitor is already set up as a monitor in AIOps.

For applications on Windows servers, corresponding processes and services need to be defined in Process Monitor Settings and Service Monitor Settings before rediscovery.

You can add file/directory paths for monitoring in File/Folder Monitor Settings before running a file/directory rediscovery.

How does rediscovery work for file/directory monitoring?

When you run a rediscovery for File/Directory, any paths added to the File/Directory Monitor Settings will be discovered and monitored for the selected monitors.

Can I monitor files and directories from multiple servers?

Yes, you can monitor files and directories on multiple servers by adding their path to the File/Directory Monitor Settings.

Can I set up alerts for file and directory changes?

Yes, you can create alerts based on specific changes, such as file size exceeding a threshold or modification time of a file being outside a accepted range.

How does Motadata AIOps handle process and service monitoring?

Motadata AIOps has a pre-loaded list of well-known processes and services in the Process Monitor Settings and Service Monitor Settings respectively. It automatically monitors these processes if they are active on discovered servers. You can also add custom processes and services for monitoring.

How does process monitoring help rediscover applications?

By monitoring processes, Motadata AIOps can identify and rediscover applications that are running on servers. This ensures that new or updated applications are included in your monitoring.

What prerequisites are needed for rediscovering applications?

For Windows servers:

Corresponding process and service must be added to Process Monitor Settings and Service Monitor Settings.

For Linux servers:

Corresponding process must be added to Process Monitor Settings.

Can I customize process monitoring settings?

Yes, you can configure metric polling settings for individual processes to monitor specific metrics.

What types of processes can be monitored?

Motadata AIOps can monitor a wide range of processes, including system processes, application-specific processes, and custom processes.

Page Title: tags

Tag Management

What are tags in Motadata AIOps?

A tag in Motadata AIOps could be a standalone label or a key-value pair that provides additional context and categorization to your infrastructure elements.

What are the different types of tags?

Simple Value Tag: A standalone label without an associated value. For Example: AWS EC2 and Azure VM

Key-Value Tag: A label with an associated value, providing more detailed categorization. For Example, Environment: Development and Environment: Production

Why use Tagging?

How do tags improve organization?

Tags group related resources, making it easier to locate and manage specific elements.

How do tags enhance visibility?

Tags categorize resources, providing a better understanding of the different aspects of your environment.

How do tags facilitate efficient analysis?

Tags offer a structured way to filter and search for resources, enabling efficient data analysis.