Page Title: Adding%20Cloud%20Devices%20for%20Monitoring

On this page

Adding Cloud Devices for Monitoring

Overview

â€‹

In order to get started with the monitoring for cloud devices, we need to first add the devices to Motadata AIOps and in turn enable it to collect data from these devices for monitoring. This guide helps you with the process of adding cloud devices to Motadata AIOps so that you are able to start monitoring them.

At a high level, this process includes creating a credential profile and a discovery profile, assigning the credential profile to a discovery profile, and executing a successful discovery run.

This is followed by provisioning the discovered devices as monitors in the system. This will enable Motadata AIOps to continuously monitor the resources and generate

alerts

and insights based on their performance metrics. You can also customize the

monitoring settings

for each monitor, such as the polling interval, threshold values, and alert notifications.

Motadata AIOps will collect performance data from the cloud resources and populate them in the system for further analysis.

Cloud Vendors and their Services Supported for Monitoring

â€‹

You can add devices to AIOps to monitor them from all the major cloud vendors which include the following:

Amazon Web Services(AWS)

â€‹

The services supported for monitoring for AWS:

Supported Service

Amazon CloudFront

Amazon DocumentDB

Amazon DynamoDB

Amazon EBS

Amazon EC2

Amazon RDS

Amazon S3

Amazon SNS

Amazon SQS

Amazon ELB

AWS Lambda

AWS Elastic Beanstalk

AWS Auto Scaling

Microsoft Azure

â€‹

The services supported for monitoring for Microsoft Azure:

Supported Service

Web App Service

Azure Storage

Azure VMs

Azure SQL Database

Azure Cosmos DB

Azure Application Gateway

Azure CDN

Azure Load Balancer

Virtual Machine Scale Sets

Azure Service Bus

Azure Functions

Microsoft Office 365 Cloud(O365 Cloud)

â€‹

The services supported for monitoring for O365:

Supported Service

Microsoft Teams

Microsoft Sharepoint

Microsoft Exchange Online

Microsoft OneDrive

Let us look into the process to add AWS, Azure, and O365 cloud to Motadata AIOps in detail.

AWS

Azure

Office 365

Adding AWS resources for Monitoring

â€‹

Prerequisites

â€‹

The

Access Key

and

Secret Key

of the AWS account are required.

Your AWS user needs the following permissions assigned to IAM role to be successfully discovered using the

Access Key

and

Secret Key

. You can

view the .JSON file with required permissions by clicking here

.

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the resource we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

Cloud

as

Protocol

from the drop-down.The option to provide the credential details is then displayed based on the protocol selected.

Cloud Type

Select

AWS

as the

Cloud Type

.

Access Key

and

Secret Key

Enter these details for the AWS account you want to monitor.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile on the credential profile screen by using the Search option

available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the account we are trying to add. Discovery profile allows us to discover devices in a infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select

Cloud

from the menu as shown below.

AWS Cloud

is selected by default.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across the collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

AWS_CLOUD_CRED

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the discovery profile. These tags will in turn be assigned to the device that you discover.

Discover Down Instances

Select

ON

or

OFF

for

Discover Down Instances

- If selected as

â€˜ONâ€™

, the system discovers the instances even if their services are down

- If selected as

â€˜OFFâ€™

, the system doesnâ€™t discover instances if their services are down.

Resources to be Monitored

- Select

Monitor All Resources

if you wish to monitor all the discovered resources using the discovery profile

- Select

Monitor Resources Selected By Tags

if you wish to monitor specific resources based on the tags defined in the AWS environment.

Key/Value

This field is available when you select the

Monitor Resources Selected By Tags

in the previous option. Specify the Key and Value corresponding to the tags of the AWS resources that you wish to monitor.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run via E-mail and SMS:

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you wish to create the discovery profile but do do want to execute a discovery run currently.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

AWS_CLOUD_CRED

in the 1st step. After that, we have created a discovery profile

Aws_Cloud_Dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Cloud

to view all the monitors that are added to the system.

The AWS devices are now successfully added to AIOps.

Adding Azure resources for Monitoring

â€‹

Prerequisites

â€‹

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 this link to understand how to retrieve the above fields from the azure portal.

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

Cloud

as

Protocol

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Cloud Type

Select

Azure

as the

Cloud Type

.

Client ID

,

Tenant ID

, and the

Secret Key

Enter these details for the cloud device you want to monitor.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile screen by using the Search option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select

Cloud

from the menu as shown below.

AWS Cloud

is selected by default. Select

Azure Cloud

to create a discovery profile for Azure.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature

note

Ensure that you select correct Collector(s), based on how you want to distribute the load across all

Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

Azure_Cloud_Cred

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the discovery profile. These tags will in turn be assigned to the device that you discover.

Discover Down Instances

Select

ON

or

OFF

for

Discover Down Instances

- If selected as

â€˜ONâ€™

, the system discovers the instances even if their services are down.

- If selected as

â€˜OFFâ€™

, the system doesnâ€™t discover instances if their services are down.

Resources to be Monitored

- Select

Monitor All Resources

if you wish to monitor all the discovered resources using the discovery profile

- Select

Monitor Resources Selected By Tags

if you wish to monitor specific resources based on the tags defined in the Azure environment.

Key/Value

This field is available when you select the

Monitor Resources Selected By Tags

in the previous option. Specify the Key and Value corresponding to the tags of the Azure resources that you wish to monitor.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

Azure_Cloud_Cred

in the 1st step. After that, we have created a discovery profile

Azure_Cloud_Dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have inititated a discovery run which leads us to our next step, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

 tab from the Main Menu. Select the

Monitor

 tab from the main menu. After that, Select

Cloud

 to view all the monitors that are added to the system.

The Azure devices are now successfully added to AIOps.

Adding a Office 365 Cloud resource (O365)

â€‹

Prerequisites

â€‹

The

Client ID

,

Tenant ID

, and the

Secret Key

 of the O365 are required.

Refer this link to understand how to retrieve the above fields from the O365 portal.

1. Create a Credential Profile

â€‹

  We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

Cloud

as

Protocol

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Cloud Type

Select

O365

as the

Cloud Type

.

Client ID

,

Tenant ID

, and the

Secret Key

Enter these details for the cloud resource you want to monitor.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile interface by using the Search option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select

Cloud

from the menu as shown below.

AWS Cloud

is selected by default. Select

Office 365

to create a discovery profile for a O365 device.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s), based on how you want to distribute the load across all

Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

Office_365_Cred

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the discovery profile. These tags will in turn be assigned to the device that you discover.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through e-mail and SMS

- Specify email addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

Office_365_Cred

in the 1st step. After that, we have created a discovery profile

Office_365_Dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have inititated a discovery run which leads us to our next step, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Cloud

to view all the monitors that are added to the system.

The O365 devices are now successfully added to AIOps.

Page Title: Adding%20Network%20Devices%20for%20Monitoring

On this page

Adding Network Devices for Monitoring

Overview

â€‹

In order to get started with the monitoring for network devices, we need to first add the devices to Motadata AIOps and in turn enabling it to collect data from these devices for monitoring. This guide helps you with the process of adding network devices to Motadata AIOps so that you are able to start monitoring them.

At a high level, this process includes creating a credential profile and a discovery profile, assigning the credential profile to a discovery profile, and executing a successful discovery run. This is followed by provisioning the discovered devices as a monitor in the system.

Network Protocols Supported

â€‹

You can add devices to AIOps for monitoring, where the following network protocols are supported:

SNMP v1/v2c

SNMP v3

Let us look into the process to add them one by one.

Prerequisites for Network Monitoring

â€‹

Ensure that Simple Network Management Protocol (SNMP) is properly configured on the target device.

Verify compatibility with both SNMP v1/v2c and SNMP v3 protocols, ensuring smooth integration with diverse network environments.

Confirm that port 161 is open and accessible on the device, facilitating smooth communication for comprehensive network monitoring by Motadata AIOps.

Ensure the community string is configured and available to enable secure and authorized access for Motadata AIOps.

SNMP v1/v2c

SNMP v3

Adding a device using v1/v2c Protocol

â€‹

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Select

SNMP V1/V2c

as

Protocol

from the drop-down.

The option to provide the credential details is then displayed based on the protocol selected.

Select

V1 or V2c

as the

Version

.

Enter the

Community

in form of password.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile interface by using the Search option available above the list of profiles.

NCM Credential Profile

â€‹

In case you want to enable the device for NCM discovery, follow the steps below:

Select

SSH

as the protocol from the drop-down.

Provide

Username

,

Password

,

SSH Key

, and

Paraphrase

details.

Select the check-box for

CLI

option. A list of options appear on the credential profile for NCM device discvoery.

Select the protocol(TFTP, FTP, SCP/SFTP, No Protocol) from the

Config Transfer Protocol

dropdown.

Enter the username associated with the device's enable mode in the

Enable User Name

field. This is typically the username used to access elevated privileges on the network device.

Specify the corresponding password for the enable mode username in the

Enable Password

field. This password grants access to the device's elevated configuration settings.

Enter the command that switches the device to enable mode in the

Enable Command

field. This command is crucial for Motadata AIOps to access the elevated configurations of the

network device.

Provide the expected prompt that appears when the device transitions to enable mode in the

Enable Prompt

field. Accurate identification of this prompt ensures proper synchronization with the enable mode.

Enter the command that activates the configuration mode on the network device in the

Config Mode Command

field. This command is vital for Motadata AIOps to interact with and retrieve configuration details.

Specify the password required to access the configuration settings on the network device in the

Config Password

field. This password is distinct from the enable password and is used when interacting with the device's configuration.

If the network device operates within a Virtual Routing and Forwarding (VRF) context, provide the name of the VRF in the

VRF Name

field. This information ensures proper segmentation and management of devices within distinct VRFs.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select network from the menu as shown below:

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

IP-Host/IP Range/CIDR/CSV

The address of the device to be discovered in one of the following formats:

-

IP

: The IP address(IPv4 or IPv6) of the device to be discovered.

-

IP Range

: A range of IP addresses(IPv4) in case multiple devices need to be discovered using the same profile.

-

CIDR

: A range of IP addresses(IPv4) using the CIDR notation if multiple devices need to be discovered using the same profile.

-

CSV

: The name of the CSV file used to import a range of addresses. You can enter IPv4, IPv6, or a combination of both addresses in the CSV file that you wish to upload.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

SNMP_v1_2c_Cred

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the discovery profile. These tags will in turn be assigned to the device that you discover.

Port

Port

number field is already populated.

Retry Count

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device withouth doing a ping check.

Interface Discovery

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Schedule

if you have created the discovery profile and wish to schedule its run at a specific time.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

SNMP_v1_2c_Cred

in the 1st step. After that, we have created a discovery profile

SNMP_v1_2c_dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

network

to view all the monitors that are added to the system.

The SNMP v1/v2c network devices are now successfully added to AIOps.

Adding a device from v3 protocol

â€‹

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Select

SNMP v3

as

Protocol

from the drop-down.

Provide the unique security username.

Select the Security Level where other options will get displayed based on the protocol selected.

When you select the option 'Authentication Privacy' the options of Authentication Protocol, Password, Privacy Protocol and Private Password.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile interface by using the Search option available above the list of profiles.

NCM Credential Profile

â€‹

In case you want to enable the device for NCM discovery, follow the steps below:

Select

SSH

as the protocol from the drop-down.

Provide

Username

,

Password

,

SSH Key

, and

Paraphrase

details.

Select the check-box for

CLI

option. A list of options appear on the credential profile for NCM device discvoery.

Select the protocol(TFTP, FTP, SCP/SFTP, No Protocol) from the

Config Transfer Protocol

dropdown.

Enter the username associated with the device's enable mode in the

Enable User Name

field. This is typically the username used to access elevated privileges on the network device.

Specify the corresponding password for the enable mode username in the

Enable Password

field. This password grants access to the device's elevated configuration settings.

Enter the command that switches the device to enable mode in the

Enable Command

field. This command is crucial for Motadata AIOps to access the elevated configurations of the network device.

Provide the expected prompt that appears when the device transitions to enable mode in the

Enable Prompt

field. Accurate identification of this prompt ensures proper synchronization with the enable mode.

Enter the command that activates the configuration mode on the network device in the

Config Mode Command

field. This command is vital for Motadata AIOps to interact with and retrieve configuration details.

Specify the password required to access the configuration settings on the network device in the

Config Password

field. This password is distinct from the enable password and is used when interacting with the device's configuration.

If the network device operates within a Virtual Routing and Forwarding (VRF) context, provide the name of the VRF in the

VRF Name

field. This information ensures proper segmentation and management of devices within distinct VRFs.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select network from the menu as shown below:

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

IP-Host/IP Range/CIDR/CSV

The address of the device to be discovered in one of the following formats:

-

IP

: The IP address(IPv4 or IPv6) of the device to be discovered.

-

IP Range

: A range of IP addresses(IPv4) in case multiple devices need to be discovered using the same profile.

-

CIDR

: A range of IP addresses(IPv4) using the CIDR notation if multiple devices need to be discovered using the same profile.

-

CSV

: The name of the CSV file used to import a range of addresses. You can enter IPv4, IPv6, or a combination of both addresses in the CSV file that you wish to upload.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

SNMP_v3_Cred

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the discovery profile. These tags will in turn be assigned to the device that you discover.

Port

Port

number field is already populated.

Retry Count

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device withouth doing a ping check.

Interface Discovery

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do not want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

SNMP_v3_Cred

in the 1st step. After that, we have created a discovery profile

SNMP_v3_Dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

network

to view all the monitors that are added to the system.

The v3 devices are now successfully added to AIOps.

Page Title: Adding%20Servers%20for%20Monitoring

On this page

Adding Servers for Monitoring

Overview

â€‹

In order to get started with the monitoring for servers, we need to first add them to Motadata AIOps and in turn enable it to collect data from these devices for monitoring. This guide helps you with the process of adding servers to Motadata AIOps so that you are able to start monitoring them.

At a high level, this process includes creating a credential profile and a discovery profile, assigning the credential profile to a discovery profile, and executing a successful discovery run.

This is followed by provisioning the discovered devices as monitors in the system. This will enable Motadata AIOps to continuously monitor the resources and generate

alerts

and insights based on their performance metrics. You can also customize the

monitoring settings

for each monitor, such as the polling interval, threshold values, and alert notifications.

Servers Supported

â€‹

You can add the following servers to AIOps to monitor them:

Types of Servers Supported

Windows

Linux

HP-UX

IBM-AIX

Solaris

Let us look into the process to add the Linux and Windows server one by one to understand the

process of adding a server for monitoring.

Windows

Linux

Adding a Windows Server

â€‹

Prerequisites

â€‹

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.

Before integrating the Windows Server with the AIOPS product, some WinRM configurations need to be done. To do this, log in with the user for whom you'll be performing the discovery, open the command prompt as an administrator, and run the following commands:

winrm set winrm/config/service/Auth @{Basic="true"}

winrm set winrm/config/service @{AllowUnencrypted="true"}

winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}

winrm set winrm/config/client/Auth @{Basic="true"}

winrm set winrm/config/client @{AllowUnencrypted="true"}

winrm set winrm/config/winrs @{MaxProcessesPerShell="2147483647"}

winrm set winrm/config/winrs @{MaxConcurrentUsers="100"}

winrm set winrm/config/service @{MaxConnections="50"}

winrm set winrm/config/winrs @{MaxShellsPerUser="2147483647"}

winrm set winrm/config/service @{MaxConcurrentOperationsPerUser="4294967295"}

net stop winrm

net start winrm

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the Windows Server we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

Powershell

as

Protocol

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Username

and

Password

Enter these details for the windows server you want to monitor.

Select

Test

to check if you are able to access the device you need to monitor using the credential details you provided.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Create Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile on the credential profile screen by using the

Search

option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to

discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed.

Server

is selected by default.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Windows/Windows Cluster

- Select

Windows

if you want to discover a Windows server.

- Select

Windows Cluster

if you want to discover a Windows cluster.

IP-Host/IP Range/CIDR/CSV

The address of the device to be discovered in one of the following formats:

-

IP

: The IP address(IPv4 or IPv6) of the device to be discovered.

-

IP Range

: A range of IP addresses(IPv4) in case multiple devices need to be discovered using the same profile.

-

CIDR

: A range of IP addresses(IPv4) using the CIDR notation if multiple devices need to be discovered using the same profile.

-

CSV

: The name of the CSV file used to import a range of addresses. You can enter IPv4, IPv6, or a combination of both addresses in the CSV file that you wish to upload.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile.

Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

win_server_cred

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the discovery profile. These tags will in turn be assigned to the device that you discover.

Port

Port

number field is already populated.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device withouth doing a ping check.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Schedule

if you have created the discovery profile and wish to schedule its run at a specific time.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

win_server_cred

in the 1st step. After that, we have created a discovery profile

win_server_dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Server & Apps

to view all the monitors that are added to the system.

The Windows Server is now successfully added to AIOps.

Adding a Linux Server

â€‹

Prerequisites

â€‹

For Linux servers, SSH needs to be enabled. Ensure that the SSH service is running and that the server is configured to allow incoming SSH connections.

Additionally, it is mandatory to install the mpstat package on the Linux server to enable the monitoring for CPU, Memory, Running Processes, and more metrics. Use the following commands for installation of the package based on the OS installed on your server.

For RHEL/Fedora/CentOS:

sudo yum install sysstat

For Ubuntu:

sudo apt-get install sysstat

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the Linux Server we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

SSH

as

Protocol

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Username

and

Password

Enter these details for the Linux server you want to monitor.

SSH Key

and

Passphrase

Enter these details for the Linux server you want to monitor if you want to access the server using the

SSH Key

and

Passphrase

Select

Test

to check if you are able to access the device you need to monitor using the credential details you provided.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Create Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile on the credential profile screen by using the

Search

option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed.

Server

is selected by default.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

IP-Host/IP Range/CIDR/CSV

The address of the device to be discovered in one of the following formats:

-

IP

: The IP address(IPv4 or IPv6) of the device to be discovered.

-

IP Range

: A range of IP addresses(IPv4) in case multiple devices need to be discovered using the same profile.

-

CIDR

: A range of IP addresses(IPv4) using the CIDR notation if multiple devices need to be discovered using the same profile.

-

CSV

: The name of the CSV file used to import a range of addresses. You can enter IPv4, IPv6, or a combination of both addresses in the CSV file that you wish to upload.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all

Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

linux_server_cred

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the discovery profile. These tags will in turn be assigned to the device that you discover.

Port

Port

number field is already populated.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device withouth doing a ping check.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Schedule

if you have created the discovery profile and wish to schedule its run at a specific time.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

linunx_server_cred

in the 1st step. After that, we have created a discovery profile

linux_server_dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

 in the system.

Click on

Add Selected Objects

 to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

 tab from the Main Menu. Select the

Monitor

 tab from the main menu. After that, Select

Server & Apps

 to view all the monitors that are added to the system.

The Linux Server is now successfully added to AIOps.

Page Title: Adding%20Virtualization%20Devices%20for%20Monitoring

On this page

Adding Virtualization Devices for Monitoring

Overview

â€‹

In order to get started with the monitoring for virtualization devices, we need to first add the devices to Motadata AIOps and in turn enable it to collect data from these devices for monitoring. This guide helps you with the process of adding virtualization devices to Motadata AIOps so that you are able to start monitoring them.

At a high level, this process includes creating a credential profile and a discovery profile, assigning the credential profile to a discovery profile, and executing a successful discovery run.

This is followed by provisioning the discovered devices as monitors in the system. This will enable Motadata AIOps to continuously monitor the resources and generate

alerts

and insights based on their performance metrics. You can also customize the

monitoring settings

for each monitor, such as the polling interval, threshold values, and alert notifications.

Virtualization Vendors Supported

â€‹

You can add devices to AIOps to monitor them from all the major virtualization vendors which include the following:

Virtualization Solutions Supported

Citrix Xen

Citrix Xen Cluster

ESXi

Vcenter

Hyper-V

Hyper-V Cluster

Let us look into the process to add a device from each vendor.

Citrix Xen

Citrix Xen Cluster

ESXi

vCenter

Hyper-V

Hyper-V Cluster

Adding a Citrix Xen device

â€‹

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

HTTP/HTTPS

as

Protocol

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Username

and

Password

Enter these details for the virtual device you want to monitor.

Authentication Type

Select the correct

Authentication Type

based on the authentication of the device.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Create Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile interface by using the Search option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select

Virtualization

from the menu as shown below:

Select

Citrix Xen

to create a discovery profile.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

IP-Host/IP Range/CIDR/CSV

The address of the device to be discovered in one of the following formats:

-

IP

: The IP address(IPv4 or IPv6) of the device to be discovered.

-

IP Range

: A range of IP addresses(IPv4) in case multiple devices need to be discovered using the same profile.

-

CIDR

: A range of IP addresses(IPv4) using the CIDR notation if multiple devices need to be discovered using the same profile.

-

CSV

: The name of the CSV file used to import a range of addresses. You can enter IPv4, IPv6, or a combination of both addresses in the CSV file that you wish to upload.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all

Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

Citrix_xen_cred

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the discovery profile.

Port

The port number field is already populated.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device withouth doing a ping check.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Schedule

if you have created the discovery profile and wish to schedule its run at a specific time.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

Citrix_xen_Cred

in the 1st step. After that, we have created a discovery profile

Citrix_xen_Dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Virtualization

to view all the monitors that are added to the system.

The Citrix Xen devices are now successfully added to AIOps.

Adding a Citrix Xen Cluster

â€‹

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

HTTP/HTTPS

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Username

and

Password

Enter these details for the wireless device you want to monitor.

Authentication Type

Select the correct

Authentication Type

based on the authentication of the device.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Create Credentials Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile interface by using the Search option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select

Virtualization

from the menu as shown below:

Select

Citrix Xen Cluster

to create a discovery profile.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

IP/Host

The IP address(IPv4 or IPv6) of the device to be discovered.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all

Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

Citrix_xen_cluster_cred

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the discovery profile. These tags will in turn be assigned to the device that you discover.

URL Type

Select

HTTP/HTTPS

as per your protocol.

Port

Port

number field is already populated.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device withouth doing a ping check.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through e-mail and SMS

- Specify email addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

Citrix_xen_cluster_Cred

in the 1st step. After that, we have created a discovery profile

Citrix_xen_cluster_Dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the

Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Virtualization

to view all the monitors that are added to the system.

The Citrix Xen Cluster devices are now successfully added to AIOps.

Adding an ESXi

â€‹

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

HTTP/HTTPS

as

Protocol

from the drop-down.The option to provide the credential details is then displayed based on the

protocol selected.

Username

and the

Password

Enter these details for the wireless device you want to monitor.

Authentication Type

Select the correct

Authentication Type

based on the authentication of the device.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Create Credentials Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile screen by using the Search option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select

Virtualization

from the menu.

Move to the

VMWare

tab and then select

ESX/ESXi

to create a discovery profile for ESXi.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

IP-Host/IP Range/CIDR/CSV

The address of the device to be discovered in one of the following formats:

-

IP

: The IP address(IPv4 or IPv6) of the device to be discovered.

-

IP Range

: A range of IP addresses(IPv4) in case multiple devices need to be discovered using the same profile.

-

CIDR

: A range of IP addresses(IPv4) using the CIDR notation if multiple devices need to be discovered using the same profile.

-

CSV

: The name of the CSV file used to import a range of addresses. You can enter IPv4, IPv6, or a combination of both addresses in the CSV file that you wish to upload.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all

Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

Esxi_cred

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the discovery profile. These tags will in turn be assigned to the device that you discover.

Port

Port

number field is already populated.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device withouth doing a ping check.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through e-mail and SMS

- Specify email addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Schedule

if you have created the discovery profile and wish to schedule its run at a specific time.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

Esxi_Cred

in the 1st step. After that, we have created a discovery profile

Esxi_Dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Virtualization

to view all the monitors that are added to the system.

The ESXi device is now successfully added to AIOps.

Adding a vCenter

â€‹

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

HTTP/HTTPS

as

Protocol

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Username

and

Password

Enter these details for the device you want to monitor.

Authentication Type

Select the correct

Authentication Type

based on the authentication of the device.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Create Credentials Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile by using the Search option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

 and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

 to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select

Virtualization

 from the menu.

Select

VCenter

 to create a discovery profile.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

IP/Host

The IP address(IPv4 or IPv6) of the device to be discovered.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

vCenter_cred

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the discovery profile. These tags will in turn be assigned to the device that you discover.

Port

Port

number field is already populated.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device withouth doing a ping check.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through e-mail and SMS

- Specify email addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

vCenter_Cred

in the 1st step. After that, we have created a discovery profile

vCenter_dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

 tab from the Main Menu. Select the

Monitor

 tab from the main menu. After that, Select

Virtualization

 to view all the monitors that are added to the system.

The vCenter device is now successfully added to AIOps.

Adding a Hyper-V Device

â€‹

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

 and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

 to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

Powershell

as

Protocol

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Username

and

Password

Enter these details for the virtual device you want to monitor.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile interface by using the Search option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Move to the

Virtualization

tab. Click on the

Hyper-V

tab to begin creating a discovery profile.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

IP-Host/IP Range/CIDR/CSV

The address of the device to be discovered in one of the following formats:

-

IP

: The IP address(IPv4 or IPv6) of the device to be discovered.

-

IP Range

: A range of IP addresses(IPv4) in case multiple devices need to be discovered using the same profile.

-

CIDR

: A range of IP addresses(IPv4) using the CIDR notation if multiple devices need to be discovered using the same profile.

-

CSV

: The name of the CSV file used to import a range of addresses. You can enter IPv4, IPv6, or a combination of both addresses in the CSV file that you wish to upload.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing

feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all

Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

Hyperv_cred

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the discovery profile.

Port

The port number field is already populated.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device withouth doing a ping check.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Schedule

if you have created the discovery profile and wish to schedule its run at a specific time.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

HyperV_cred

in the 1st step. After that, we have created a discovery profile

HyperV_dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Virtualization

to view all the monitors that are added to the system.

The Hyper-V devices are now successfully added to AIOps.

Adding a Hyper-V Cluster

â€‹

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

Powershell

as

Protocol

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Username

and

Password

Enter these details for the virtual device you want to monitor.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile interface by using the Search option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Move to the

Virtualization

tab. Click on the

Hyper-V

tab and then select

Hyper-V Cluster

to create a discovery profile.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

IP/Host

The IP address(IPv4 or IPv6) of the device to be discovered.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all

Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

HyperV_cluster_cred

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the discovery profile. These tags will in turn be assigned to the device that you discover.

Port

Port

number field is already populated.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device withouth doing a ping check.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through e-mail and SMS

- Specify email addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

HyperV_cluster_Cred

in the 1st step. After that, we have created a discovery profile

HyperV_cluster_Dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Virtualization

to view all the monitors that are added to the system.

The Hyper-V Cluster devices are now successfully added to AIOps.

Page Title: Adding%20Wireless%20Devices%20for%20Monitoring

On this page

Adding Wireless Devices for Monitoring

Overview

â€‹

In order to get started with the monitoring for wireless devices, we need to first add the devices to Motadata AIOps and in turn enable it to collect data from these devices for monitoring. This guide helps you with the process of adding wireless devices to Motadata AIOps so that you are able to start monitoring them.

At a high level, this process includes creating a credential profile and a discovery profile, assigning the credential profile to a discovery profile, and executing a successful discovery run.

This is followed by provisioning the discovered devices as monitors in the system. This will enable Motadata AIOps to continuously monitor the resources and generate

alerts

and insights based on their performance metrics. You can also customize the

monitoring settings

for each monitor, such as the polling interval, threshold values, and alert notifications.

Motadata AIOps will collect performance data from the cloud resources and populate them in the system for further analysis.

Wireless Vendors Supported

â€‹

You can add devices to AIOps to monitor from all the major wireless vendors including the following:

Vendors

Cisco Wireless

Ruckus Wireless

Aruba Wireless

Let us look into the process to add them one by one.

Cisco

Ruckus

Aruba

Adding a Cisco Wireless Device

â€‹

Prerequisites

â€‹

Ensure that the Cisco device is SNMP enabled before you start the process to discover the device in

Motadata AIOps.

Ensure that the Port 161 is enabled on the device you wish to monitor.

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

SNMP V1/V2c

or

SNMP V3

as

Protocol

from the drop-down based on the configuration of your device.The option to provide the credential details is then displayed based on the protocol selected.

- In case you select

SNMP V1/V2C

, enter the credential details including the SNMP

Version

and the

Community

string.

- In case you select

SNMP V3

, enter the credential details including

Security User Name

and

Security Level

.

Select

Test

to check if the credential details you provided are working against the device you want to discover by providing the details of the device IP.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile screen by using the

Search

option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select

Wireless

from the menu as shown below:

Cisco Wireless

is selected by default.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify the discovery profile.

IP/Host

The IP address(IPv4 or IPv6) of the device to be discovered.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s), based on how you want to distribute the load across all Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select an already created

Credential Profile

to assign it to the discovery profile. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

CISCO_Wireless_CRED

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the devices you want to discover and setup as a monitor

Port

The

Port

number field is already populated.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device without doing a ping check.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through e-mail and SMS

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger E-mail notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

Cisco_Wireless_Cred

in the 1st step. After that, we have created a discovery profile

Cisco_Wireless_Dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices and the following screen appears.

Once the discovery run is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Network

to view all the monitors that are added to the system.

The Cisco device is now successfully added to AIOps.

Adding a Ruckus device

â€‹

Prerequisites

â€‹

Before configuring the AIOps integration with Ruckus Wireless, ensure that you have the credentials for HTTP/HTTPS access to the Ruckus device.

Ensure that the Port 8443 is enabled on the device you wish to monitor.

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

HTTP/HTTPS

as

Protocol

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Username

and the

Password

Enter these details for the wireless device you want to provision as a monitor.

Authentication Type

Select the

Authentication Type

from the dropdown.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile screen by using the

Search

option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select

Wireless

from the menu as shown below.

Cisco Wireless

is selected by default. Select

Ruckus Wireless

to create a discovery profile for Ruckus.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify the discovery profile.

IP/Host

The IP address(IPv4 or IPv6) of the device to be discovered.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s), based on how you want to distribute the load across all

Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select an already created

Credential Profile

to assign it to the discovery profile. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

Ruckus_Wireless_CRED

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the devices you want to discover and setup as a monitor.

URL Type

Select

HTTP/HTTPS

as per your device protocol.

Port

The

Port

number field is already populated.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device withouth doing a ping check.

Notify via E-mail

and

Notify via SMS

- The system allows notifying users about a discovery run through e-mail and SMS

Specify email addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

Ruckus_Wireless_Cred

in the 1st step. After that, we have created a discovery profile

Ruckus_Wireless_Dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Network

to view all the monitors that are added to the system.

The wireless devices are now successfully added to AIOps.

Adding a Aruba device

â€‹

Prerequisites

â€‹

Ensure that the Aruba device is SNMP enabled before configuring the AIOps integration.

Ensure that the Port 161 is enabled on the device you wish to monitor.

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

SNMP V1/V2c

or

SNMP V3

as

Protocol

from the drop-down based on the configuration of your device.The option to provide the credential details is then displayed based on the protocol selected.

- In case you select

SNMP V1/V2C

, enter the credential details including the SNMP

Version

and the

Community

string.

- In case you select

SNMP V3

, enter the credential details including

Security User Name

and

Security Level

.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile interface by using the Search option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select Wireless from the menu as

shown below.

Cisco Wireless

is selected by default. Select

ARUBA Wireless

to create a discovery profile for ARUBA.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

IP/Host

The IP address(IPv4 or IPv6) of the device to be discovered.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s), based on how you want to distribute the load across all

Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select a created

Credential Profile

to assign it to the discovery profile you are trying to create. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile

Aruba_Wireless_Cred

we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the devices you want to discover and setup as a monitor.

Port

The

Port

number field is already populated.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device withouth doing a ping check.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through e-mail and SMS

- Specify email addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a credential profile

Aruba_Wireless_Cred

in the 1st step. After that, we have created a discovery profile

Aruba_Wireless_Dis

in the 2nd step and assigned the credential profile to the discovery profile. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Cloud

to view all the monitors that are added to the system.

The Wireless devices are now successfully added to AIOps.

Page Title: Adding-hcl-devices-for-monitoring

On this page

Adding Hyperconverged Infrastructure devices for Monitoring

Overview

â€‹

In order to start monitoring Hyperconverged Infrastructure devices, we need to first add the devices to Motdata AIOps and in turn enable it to collec data from these devices for monitoring. This guide helps you with the process of adding HCI devices to Motadata AIOps so that you are able to start monitoring them.

At a high level, this process includes creating a credential profile and a discovery profile, assigning the credential profile to a discovery profile, and executing a successful discovery run.

This is followed by provisioning the discovered devices as monitors in the system. THis will enable Motadata AIOps to continously monitor the resources and generate alerts and insights based on their performance metrics. You can also customize the monitoring settings for each monitor, such as polling interval, threshold values, and alert notifications.

HCI Vendors Supported

â€‹

Vendors

Nutanix

Adding a Nutanix HCI Device

â€‹

Motadata AIOps supports discovery of Nutanix Cluster as well Nutanix AHV (Host). The discovery of Nutanix Cluster is performed through Prism which will also fetch details of all the hosts associated with the cluster. When discoverying the latter, Nutanix Host will be provisioned as the Monitor and all the VMs will be considered as the instances of Nutanix Host.

Prerequisites

â€‹

1. Create a Credential Profile

â€‹

We will start by creating a credential profile.

Navigation

â€‹

Go to menu. Select

Settings

. After that, go to

Network Discovery

 and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

 to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

Powershell

as

Protocol

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Username

and

Password

Enter these details for the virtual device you want to monitor.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile interface by using the Search option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select

Hyperconverged Infrastructure

from the menu as shown below:

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify the discovery profile.

IP/Host

The IP address(IPv4 or IPv6) of the device to be discovered.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a

Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s), based on how you want to distribute the load across all Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select an already created

Credential Profile

to assign it to the discovery profile. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile which we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the devices you want to discover and setup as a monitor

Port

The

Port

number field is already populated.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device without doing a ping check.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through e-mail and SMS

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger E-mail notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the clusters and their hosts discovered is displayed. Select the devices that you want to be listed as Monitors in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

HCI

to view all the monitors that are added to the system.

The HCI devices are now successfully added to AIOps.

Page Title: Adding-IPSLA-devices-for-monitoring

On this page

Adding WAN Link For Monitoring

Overview

â€‹

In order to monitor WAN Link statistics, you will need to add IP SLA supported network devices to Motadata AIOps. This guide will walk you through the entire process of adding and enabling an IP SLA supported device(s) to Motadata AIOps.

At a high level, this process includes creating a credential profile and adding the WAN Link from its corresponding provisioned monitor. Once the WAN Link has been added, you can then start monitoring it and receive all the network insights.

This will enable Motadata AIOps to continuously monitor the resources and generate alerts and insights based on their performance metrics. You can also customize the monitoring settings for each monitor, such as the polling interval, threshold values, and alert notifications.

Prerequisites

â€‹

Ensure the device you are adding has the IP SLA capabilities.

Ensure the Port 161 is enabled for the device you wish to monitor.

Ensure you have the

Write Community

and

Read Community

string before creating a credential profile for WAN Link.

Let us now look into the process to add Cisco IP SLA for monitoring.

Cisco IP SLA

Adding a Cisco IP SLA Device

â€‹

1. Create a Credential Profile

â€‹

We will start by creating a credential profile for the device we are trying to add.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

SNMP V1/V2c

or

SNMP V3

as

Protocol

from the drop-down based on the configuration of your device.The option to provide the credential details is then displayed based on the protocol selected.

- In case you select

SNMP V1/V2C

, enter the credential details including the SNMP

Version

,

Read Community

string, and

Write Community

string.

- In case you select

SNMP V3

, enter the credential details including

Security User Name

and

Security Level

.

note

If the

Write Community

field is blank, the IP SLA operation will fail.

Select

Test

to check if the credential details you provided are working against the device you want to discover by providing the details of the device IP.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Create Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile screen by using the

Search

option available above the list of profiles.

2. Add WAN Link

â€‹

After creating the credential profile, you will need to add the WAN Link to start monitoring it. Do note, the WAN Link you wish to monitor must be linked to an existing monitor. You will not be able to add a WAN Link that is not associated with an existing monitor.

Navigation

â€‹

Go to Menu. Select

Monitors

. After that, select the

Network

option. Then, select the monitor from which you wish to monitor the WAN Link. Finally, click on the

WAN Link

button.

A new screen to Add WAN Link will be displayed.

Single WAN Link Configuration

is selected by default.

Now, let us looking into the setup of both

Single WAN Link Configuration

and

Bulk WAN Link Configuration

.

Single WAN Link Configuration

Bulk WAN Link Configuration

Adding WAN Link Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Credential Profile

Select an already created

Credential Profile

to assign it to the discovery profile. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile we created in the 1st step while creating a credential profile.

WAN Probe

Select the Probe type using the drop-down. Every Probe type provides different insights and

statistics of WAN link. Choose one according to your requirements:

ICMP Echo:

The ICMP Echo operation measures end-to-end response time between a Cisco router and any devices using IP. Response time is computed by measuring the time taken between sending an ICMP Echo request message to the destination and receiving an ICMP Echo reply.

ICMP Jitter:

ICMP Jitter uses two ICMP time stamp messages, an ICMP Timestamp Request and an ICMP Timestamp Reply, to provide jitter, packet loss, Round Trip Time (RTT), and latency. IP SLAs utilizes the time stamps to calculate jitter for each direction, based on the difference between arrival and departure delay for two successive packets.

ICMP Path Echo:

ICMP Path Echo monitors end-to-end as well as hop-by-hop response time between source and destination routers. ICMP Path Echo operation determines the hop-by-hop response time using the Traceroute facility. The results of the ICMP Path Echo operation can be analysed to determine how ICMP is performing.

Internet Service Provider

Enter the name of destination Internet Service Provider. This will help in bifurcation of WAN Links coming from same source.

Source Interface

Choose the specific interface of the device for the originating link. If none is chosen, by defualt, Motadata AIOps will select the default IP which can generate unwanted results if your device has 2 or more interfaces.

Source Router Location

You can enter the city, office location, or any other geo-location related information that will help you identify the router location. The location will be displayed on the monitor screen which will help you quickly identify where the device is situated.

Destination IP

Enter the IP address for the destination device.

Destination Router Location

Specify the location of the destination device.

Payload

Define the size of ping packet that will be exchanged between the source and destination devices.

Type of Service

Type of Service value defines the type of IP SLA operation you wish to perform. The default value for ICMP operations is 30.

Frequency

Define the time interval (in miliseconds) between two consecutive pings between source and destination device.

Timeout

Specify the time interval Motadata AIOps will wait after a failed ping to assume the destination is in the down state.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Credential Profile

Select an already created

Credential Profile

to assign it to the discovery profile. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile we created in the 1st step while creating a credential profile.

CSV

Upload the CSV file comprising multiple WAN Links using the

Upload File

option. Create the CSV file as per the format of the sample csv file available in this field.

Payload

Define the size of ping packet that will be exchanged between the source and destination devices.

Type of Service

Type of Service value defines the type of IP SLA operation you wish to perform. The default value for ICMP operations is 30.

Frequency

Define the time interval (in miliseconds) between two consecutive pings between source and destination device.

Timeout

Specify the time interval Motadata AIOps will wait after a failed ping to assume the destination is in the down state.

We have created a credential profile in the 1st step. After that, we have added the WAN Link parameters in the 2nd step using a credential profile. After selecting,

Add WAN Link

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision Discovered WAN Links

â€‹

After initiating the adding of WAN Links, AIOps starts the process to look for all availaible WAN Links.

Once the discovery execution is complete, the list of all the links discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected links as Monitors. These WAN links listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

WAN Link

to view all the monitors that are added to the system.

Page Title: Adding-SDN-devices-for-monitoring

On this page

Adding Software Defined Network Devices for Monitoring

Overview

â€‹

In order to start monitoring Software Defined Network devices, we need to first add the devices to Motdata AIOps in turn enable it to collect data from these devices for monitoring. This guide helps you with the process of adding SDN devices to Motadata AIOps so that you are able to start monitoring them.

At a high level, this process includes creating a credential profile and a discovery profile, assigning the credential profile to a discovery profile, and executing a successful discovery run.

This is followed by provisioning the discovered devices as monitors in the system. This will enable Motadata AIOps to continously monitor the resources and generate alerts and insights based on their performance metrics. You can also customize the monitoring settings for each monitor, such as polling interval, threshold values, and alert notifications.

SDN Solutions Supported

â€‹

Vendors

Cisco Catalyst SD-WAN

Cisco Meraki

Cisco Catalyst SD-WAN

Cisco Meraki

Adding a Cisco Catalyst SD-WAN Device

â€‹

Motadata AIOps supports discovery of Manager, Controller, Validator, and WAN-Edge. The discovery of Controller, Validator, and WAN-Edge devices will be performed through Manager which

will also fetch the Tunnel information. Here, each Controller, Validator, Controller, and WAN-Edge device will be discovered as an individual monitor.

Prerequisites

â€‹

1. Create a Credential Profile

â€‹

We will start by creating a credential profile.

Navigation

â€‹

Go to menu. Select

Settings

. After that, go to

Discovery Settings

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

HTTP/HTTPS

as

Protocol

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Username

and

Password

Enter these details for the virtual device you want to monitor.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile interface by using the Search option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Create Discovery Profile

â€‹

Let us create a discovery profile for the device we are trying to add. Discovery profile allows us to discover devices in an infrastructure using the device address and associated credential profile.

Go to Menu. Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed. Select

SDN

from the menu as shown below:

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify the discovery profile.

IP/Host

The IP address(IPv4 or IPv6) of the device to be discovered.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile.

Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s), based on how you want to distribute the load across all Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select an already created

Credential Profile

to assign it to the discovery profile. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile which we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the devices you want to discover and setup as a monitor

Port

The

Port

number field is already populated.

URL Type

Select on of the URL types. By default,

HTTPS

will be selected.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device without doing a ping check.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through e-mail and SMS

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger E-mail notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the Controllers, Validators, Managers, and WAN-Edge devices discovered is displayed. Select the devices that you want to be listed as Monitors in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

Adding a Cisco Meraki Device

â€‹

Motadata AIOps supports discovery of Meraki Security, Meraki Switch, Meraki Radios, Meraki Vision, and Meraki Cellular Gateway. The holistic view of all the device types will be facilitated through Meraki Controller. Here each device type will be discovered as an individual monitor.

Prerequisites

â€‹

1. Create a Credential Profile

â€‹

We will start by creating a credential profile.

Navigation

â€‹

Go to menu. Select

Settings

. After that, go to

Discovery Settings

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

HTTP/HTTPS

as

Protocol

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Authentication Type

Select the

API Key

from the drop downn menu.

API Key

Paste your API key from Cisco Meraki here.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

You can view the newly created profile in the credential profile interface by using the Search option available above the list of profiles.

Now, let's move to the next step and create a discovery profile.

2. Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify the discovery profile.

URI Endpoint

Enter the base URI provided by Cisco Meraki.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s), based on how you want to distribute the load across all

Collectors

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Credential Profile

Select an already created

Credential Profile

to assign it to the discovery profile. You can also create a new credential profile from this screen using the

Create Credential Profile

button. In this case, we will select the credential profile which we created in the 1st step while creating a credential profile.

Tags

Select one or more

Tags

that you wish to assign to the devices you want to discover and setup as a monitor.

Retry Count

Enter a numerical value for AIOps to try connecting to Cisco Meraki should the first attempt fails to connect.

Ping Check

The

Ping Check

button is switched

ON

by default. This means that AIOps will only discover the device if the ping is available for that device. Toggle this button

OFF

if you want AIOps to discover the device without doing a ping check.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through e-mail and SMS

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger E-mail notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the Controllers, Validators, Managers, and WAN-Edge devices discovered is displayed. Select the devices that you want to be listed as Monitors in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

SDN

to view all the monitors that are added to the system.

The SDN devices are now successfully added to AIOps.

Page Title: Adding-service-checks-for-monitoring

On this page

Adding Service Checks for Monitoring

Overview

â€‹

In order to get started with monitoring service checks, we need to first add them to Motadata AIOps and in turn enable it to collect data from these devices for monitoring. This guide helps you with the process of adding service checks to Motadata AIOps so that you are able to start monitoring them.

At a high level, this process includes creating a discovery profile and executing a successful discovery run.

This is followed by provisioning the discovered devices as monitors in the system. This will enable Motadata AIOps to continuously monitor the resources and generate

alerts

and insights based on their performance metrics. You can also customize the

monitoring settings

for each monitor, such as the polling interval, threshold values, and alert notifications.

Service Checks Supported

â€‹

You can add the following service checks to AIOps to monitor them:

Types of Service Checks Supported

Ping

Port

URL

RADIUS

NTP

Domain

DNS

FTP

Email

SSL Certificate

Let us look into the process to add these service checks one by one to understand the process of adding a service check for monitoring.

Ping

Port

URL

RADIUS

NTP

Domain

DNS

FTP

Email

SSL

Adding Ping for Monitoring

â€‹

1. Create a Discovery Profile

â€‹

Let us create a discovery profile for ping monitoring.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed.

Server

is selected by default. Select

Service Check

to create the discovery profile for service check.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Type

Select the type of service check from the dropdown. In this case, select

Ping

.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all Collectors

Agent

Use this toggle button to turn ON/OFF the monitoring through agent.

Agents

Select the agent that you want to use to discover the selected service check on a target device. This field is only available if you turn the toggle button ON in the previous field.

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Target Type

The address of the device on which the ping needs to be checked in one of the following formats:

-

Monitor

: The monitor on which the ping needs to be checked.

-

IP

: The IP address of the device on which the ping needs to be checked.

-

IP Range

: A range of IP addresses on which the ping needs to be checked

-

CIDR

: A range of IP addresses using the CIDR notation if ping needs to be checked on multiple devices.

-

CSV

: The name of the CSV file used to import a range of addresses.

Target

The target monitor(s)/device(s) on which the ping service needs to be checked.

Tags

Select the tags that you need to assign to the discovered monitors using the discovery profile.

Retry Count

Specify the number of times the system will do a ping check to get a successfull response before the service is considered unavailable.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Schedule

if you have created the discovery profile and wish to schedule its run at a specific time.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a discovery profile

ping_check_pmg_server

by configuring all the details. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

2. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

 tab from the Main Menu. Select the

Monitor

 tab from the main menu. After that, Select

Service Check

 to view all the monitors that are added to the system.

The Ping Service Check for the selected device is now successfully added to AIOps.

Adding Port for Monitoring

â€‹

1. Create a Discovery Profile

â€‹

Let us create a discovery profile for port monitoring.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

 and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

 to create a new discovery profile.

A new screen to create the discovery profile is now displayed.

Server

is selected by default. Select

Service Check

to create the discovery profile for service check.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Type

Select the type of service check from the dropdown. In this case, select

Port

.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all

Collectors

Agent

Use this toggle button to turn ON/OFF the monitoring through agent.

Agents

Select the agent that you want to use to discover the selected service check on a target device. This field is only available if you turn the toggle button ON in the previous field.

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Target Type

The address of the device on which the port availability needs to be checked in one of the following formats:

-

Monitor

: The monitor on which the port availability needs to be checked.

-

IP

: The IP address of the device on which the port availability needs to be checked.

-

IP Range

: A range of IP addresses on which the port availability needs to be checked

-

CIDR

: A range of IP addresses using the CIDR notation if port availability needs to be checked on multiple devices.

-

CSV

: The name of the CSV file used to import a range of addresses.

Target

The target monitor(s)/device(s) on which the port availability needs to be checked.

Tags

Select the tags that you need to assign to the discovered monitors using the discovery profile.

Port

Specify the port for which you need to check the availability.

Send Command

Use this toggle button to turn the advance option ON/OFF to execute commands on the target port.

Command

This field allows you to specify a command that will be executed on the target port.It is the action or query you want to check for on the specified port.

Max Command Output Lines

This field determines the maximum number of lines of output that the system will consider when analyzing the command execution results. If you set it to 1, the system will only inspect the first line of the command output for relevant information. This parameter helps control the scope of output analysis.

Search Keyword

The search keyword is the specific string or pattern that the system will look for in the output of the executed command.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

 to send SMS notifications.

Select

Reset

 to erase all the current field values, if required.

Select

Save and Exit

 if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Schedule

 if you have created the discovery profile and wish to schedule its run at a specific time.

Select

Save and Run

 if you want execute the discovery run immediately after creation.

We have created a discovery profile

ping_check_pmg_server

 by configuring all the details. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

2. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

 in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Service Check

to view all the monitors that are added to the system.

The Port Service Check for the selected device is now successfully added to AIOps.

Adding URL for Monitoring

â€‹

1. Create a Credential Profile

â€‹

We will start by creating a credential profile.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Credential Profile

. The credential profile screen is displayed. Select

Create Credential Profile

to create a new credential profile.

A pop-up for entering the credential profile details is displayed.

Credential Profile Parameters

â€‹

Enter the required details in the pop-up as follows:

Field

Description

Credential Profile Name

Provide a unique

Credential Profile Name

. This name is used to identify a credential profile.

Protocol

Select

HTTP/HTTPS

as

Protocol

from the drop-down. The option to provide the credential details is then displayed based on the protocol selected.

Username

and the

Password

Enter these details for the url you want to provision as a monitor.

Authentication Type

Select the

Authentication Type

from the dropdown.

Select

Reset

to erase all the current field values entered in the pop-up, if required.

Select

Add Credential Profile

to create the credential profile in the system. The credential profile is now created.

Now, let's move to the next step and create a discovery profile.

2. Create a Discovery Profile

â€‹

Let us create a discovery profile for URL monitoring.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed.

Server

is selected by default. Select

Service Check

to create the discovery profile for service check.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Type

Select the type of service check from the dropdown. In this case, select

URL

.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all

Collectors

Agent

Use this toggle button to turn ON/OFF the monitoring through agent.

Agents

Select the agent that you want to use to discover the selected service check on a target device. This field is only available if you turn the toggle button ON in the previous field.

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Target Type

The target on which the URL availability needs to be checked:

-

Monitor

: The monitor on which the URL availability needs to be checked.

-

URL

: The URL for which the availability needs to be checked.

Target

Specify the target monitor(s)/URL on which the URL availability needs to be checked.

URL Endpoint

Specify the URL endpoint that you need to monitor.

Tags

Select the tags that you need to assign to the discovered monitors using the discovery profile.

URL Type

Select the URL type(HTTP/HTTPS) that you wish to monitor.

URL Method

Select the URL Method(GET/POST) to specify the method to access the URL.

JSON URL

Specify whether the URL is a JSON URL.

URL Content

Specify the URL content that you wish to search in a URL.

Credential Profile

Select the credential profile that you want to associate with the discovery profile.

Create Credential Profile

Use this button if you need to create a new credential profile.

Parameters

Enter the parameters to monitor a specific API endpoint in your URL

Headers

Enter the headers to monitor a specific API endpoint in your URL

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a discovery profile

url_check_google

by configuring all the details. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

3. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Service Check

to view all the monitors that are added to the system.

The URL Service Check for the specified URL is now successfully added to AIOps.

Adding RADIUS for Monitoring

â€‹

1. Create a Discovery Profile

â€‹

Let us create a discovery profile for RADIUS monitoring.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed.

Server

is selected by default. Select

Service Check

to create the discovery profile for service check.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Type

Select the type of service check from the dropdown. In this case, select

RADIUS

.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all

Collectors

Agent

Use this toggle button to turn ON/OFF the monitoring through agent.

Agents

Select the agent that you want to use to discover the selected service check on a target device. This field is only available if you turn the toggle button ON in the previous field.

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Target Type

The target on which the RADIUS availability needs to be checked:

-

Monitor

: The monitor on which the RADIUS availability needs to be checked.

-

IP/Host

: The IP/Host for which the RADIUS availability needs to be checked.

Target

Specify the target monitor(s)/IP on which the RADIUS availability needs to be checked.

Tags

Select the tags that you need to assign to the discovered monitors using the discovery profile.

Port

The default port is already specified. You can change the default port if required.

Username

Specify the Username of the RADIUS server.

Password

Specify the Password of the RADIUS server.

RADIUS Secret

Specify the RADIUS secret of the RADIUS network.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a discovery profile

radius_service_check

by configuring all the details. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

2. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Service Check

to view all the monitors that are added to the system.

The RADIUS Service Check is now successfully added to AIOps.

Adding NTP for Monitoring

â€‹

1. Create a Discovery Profile

â€‹

Let us create a discovery profile for NTP monitoring.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed.

Server

is selected by default. Select

Service Check

to create the discovery profile for service check.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Type

Select the type of service check from the dropdown. In this case, select

NTP

.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all Collectors

Agent

Use this toggle button to turn ON/OFF the monitoring through agent.

Agents

Select the agent that you want to use to discover the selected service check on a target device. This field is only available if you turn the toggle button ON in the previous field.

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Target Type

The target on which the NTP availability needs to be checked:

-

Monitor

: The monitor on which the NTP availability needs to be checked.

-

IP/Host

: The IP/Host for which the NTP availability needs to be checked.

Target

Specify the target monitor(s)/IP on which the NTP availability needs to be checked.

Tags

Select the tags that you need to assign to the discovered monitors using the discovery profile.

Port

The default port is already specified. You can change the default port if required.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a discovery profile

ntp_discovery

by configuring all the details. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

2. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Service Check

to view all the monitors that are added to the system.

The NTP Service Check is now successfully added to AIOps.

Adding Domain for Monitoring

â€‹

1. Create a Discovery Profile

â€‹

Let us create a discovery profile for Domain monitoring.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed.

Server

is selected by default. Select

Service Check

to create the discovery profile for service check.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Type

Select the type of service check from the dropdown. In this case, select

Domain

.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all Collectors

Agent

Use this toggle button to turn ON/OFF the monitoring through agent.

Agents

Select the agent that you want to use to discover the selected service check on a target device. This field is only available if you turn the toggle button ON in the previous field.

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Target Type

The target on which the NTP availability needs to be checked:

-

Monitor

: The monitor on which the Domain availability needs to be checked.

-

IP/Host

: The IP/Host for which the Domain availability needs to be checked.

Target

Specify the target monitor(s)/IP on which the Domain availability needs to be checked.

Tags

Select the tags that you need to assign to the discovered monitors using the discovery profile.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a discovery profile

domain_check_motadata

by configuring all the details. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

2. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

 in the system.

Click on

Add Selected Objects

 to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

 tab from the Main Menu. Select the

Monitor

 tab from the main menu. After that, Select

Service Check

 to view all the monitors that are added to the system.

The Domain Service Check is now successfully added to AIOps.

Adding DNS for Monitoring

â€‹

1. Create a Discovery Profile

â€‹

Let us create a discovery profile for DNS monitoring.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed.

Server

is selected by default. Select

Service Check

to create the discovery profile for service check.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Type

Select the type of service check from the dropdown. In this case, select

DNS

.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all Collectors

Agent

Use this toggle button to turn ON/OFF the monitoring through agent.

Agents

Select the agent that you want to use to discover the selected service check on a target device. This field is only available if you turn the toggle button ON in the previous field.

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Target Type

The target on which the DNS availability needs to be checked:

-

Monitor

: The monitor on which the DNS availability needs to be checked.

-

IP/Host

: The IP/Host for which the DNS availability needs to be checked.

Target

Specify the target monitor(s)/IP on which the DNS availability needs to be checked.

Tags

Select the tags that you need to assign to the discovered monitors using the discovery profile.

Port

The default port is already specified. You can change the default port if required.

Lookup Address

Specify the Lookup Address of the DNS server.

DNS Type

Select the DNS record type that you want to monitor.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

2. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Service Check

to view all the monitors that are added to the system.

The DNS Service Check is now successfully added to AIOps.

Adding FTP for Monitoring

â€‹

1. Create a Discovery Profile

â€‹

Let us create a discovery profile for FTP monitoring.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed.

Server

is selected by default. Select

Service Check

to create the discovery profile for service check.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Type

Select the type of service check from the dropdown. In this case, select

FTP

.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all Collectors

Agent

Use this toggle button to turn ON/OFF the monitoring through agent.

Agents

Select the agent that you want to use to discover the selected service check on a target device. This field is only available if you turn the toggle button ON in the previous field.

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Target Type

The target on which the FTP availability needs to be checked:

-

Monitor

: The monitor on which the FTP availability needs to be checked.

-

URL

: The IP/Host for which the FTP availability needs to be checked.

Target

Specify the target monitor(s)/IP on which the FTP availability needs to be checked.

Tags

Select the tags that you need to assign to the discovered monitors using the discovery profile.

Port

The default port is already specified. You can change the default port if required.

Username

Specify the Username of the FTP server.

Password

Specify the Password of the FTP server.

Notify via E-mail

 and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

 field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

 to send SMS notifications.

Select

Reset

 to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a discovery profile

ftp_check_pmg_server

by configuring all the details. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

2. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Service Check

to view all the monitors that are added to the system.

The FTP Service Check is now successfully added to AIOps.

Adding Email for Monitoring

â€‹

1. Create a Discovery Profile

â€‹

Let us create a discovery profile for Email monitoring.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed.

Server

is selected by default. Select

Service Check

to create the discovery profile for service check.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Type

Select the type of service check from the dropdown. In this case, select

Email

.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all

Collectors

Agent

Use this toggle button to turn ON/OFF the monitoring through agent.

Agents

Select the agent that you want to use to discover the selected service check on a target device. This

field is only available if you turn the toggle button ON in the previous field.

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Target Type

The target on which the Email availability needs to be checked:

-

Monitor

: The monitor on which the Email availability needs to be checked.

-

IP/Host

: The IP/Host for which the Email availability needs to be checked.

Target

Specify the target monitor(s)/IP on which the Email availability needs to be checked.

Tags

Select the tags that you need to assign to the discovered monitors using the discovery profile.

Port

The default port is already specified. You can change the default port if required.

Security Type

Select the security type of the Email server.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a discovery profile

email_discovery

by configuring all the details. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

2. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Service Check

to view all the monitors that are added to the system.

The Email Service Check is now successfully added to AIOps.

Adding SSL for Monitoring

â€‹

1. Create a Discovery Profile

â€‹

Let us create a discovery profile for SSL monitoring.

Navigation

â€‹

Go to Menu. Select

Settings

. After that, Go to

Discovery Settings

and select

Discovery Profile

. The discovery profile screen is displayed. Select

Create Discovery Profile

to create a new discovery profile.

A new screen to create the discovery profile is now displayed.

Server

is selected by default. Select

Service Check

to create the discovery profile for service check.

Discovery Profile Parameters

â€‹

Enter the required details in the screen as follows:

Field

Description

Discovery Profile Name

Provide a unique

Discovery Profile Name

. This name is used to identify a discovery profile.

Type

Select the type of service check from the dropdown. In this case, select

SSL

.

Collectors

Select one or more

Collectors

that should be used for collecting data from the devices discovered using this Discovery Profile. Select multiple Collectors for load balancing and failover mechanism. In case you donâ€™t select a Collector, the AIOps shall automatically select a relevant collector to leverage the load balancing feature.

note

Ensure that you select correct Collector(s) based on how you want to distribute the load across all Collectors

Agent

Use this toggle button to turn ON/OFF the monitoring through agent.

Agents

Select the agent that you want to use to discover the selected service check on a target device. This field is only available if you turn the toggle button ON in the previous field.

Groups

Select one or more

Groups

that will be assigned to the monitors you provision using this discovery profile.

Target Type

The target on which the SSL availability needs to be checked:

-

Monitor

: The monitor on which the SSL availability needs to be checked.

-

IP/Host

: The IP/Host for which the SSL availability needs to be checked.

Target

Specify the target monitor(s)/IP on which the SSL availability needs to be checked.

Tags

Select the tags that you need to assign to the discovered monitors using the discovery profile.

Port

The default port is already specified. You can change the default port if required.

Notify via E-mail

and

Notify via SMS

The system allows notifying users about a discovery run through E-mail and SMS.

- Specify E-mail addresses (comma separated) in the

Notify via E-mail

field to trigger email notifications.

- Specify mobile numbers (comma separated) in the

Notify via SMS

to send SMS notifications.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile but do do want to execute a discovery run.

Select

Save and Run

if you want execute the discovery run immediately after creation.

We have created a discovery profile

SSL_Youtube

by configuring all the details. After selecting,

Save and Run

, we have initiated a discovery run which leads us to our next step, which is, Provision the Discovered Devices as Monitors.

2. Provision the Discovered Devices as Monitors

â€‹

After initiating the discovery profile execution, AIOps starts the process to discover the devices.

Once the discovery execution is complete, the list of all the devices discovered is displayed. Select the devices that you want to be listed as

Monitors

in the system.

Click on

Add Selected Objects

to add the selected devices as Monitors. These devices listed as Monitors will now be monitored further by AIOps.

These devices can be viewed under the

Monitor

tab from the Main Menu. Select the

Monitor

tab from the main menu. After that, Select

Service Check

to view all the monitors that are added to the system.

The SSL Service Check is now successfully added to AIOps.

Page Title: Azure-Integration-steps

On this page

Integration through the Azure Portal

Overview

â€‹

Integrate your Microsoft Azure account with Motadata AIOps from the Azure portal in the following two steps:

Create an app registration in your Active Directory and pass the credentials to Motadata AIOps.

Provide the application read-access to the subscriptions you would like to monitor.

Let us look into each of these steps in detail.

Create the App Registration

â€‹

Select

Azure Active Directory

. After that, select

App Registrations

and then click on

New Registration

.

Enter

MotadataAuth

as the

Name

and select

Accounts in this organizational directory only

in the

Supported account types

field.

After that click on the

Register

button.

Now, let us move to the next step.

Providing Read Permissions to the Application

â€‹

Navigate to

Subscriptions

to assign access at the individual subscription level.

note

You can also assign the access at

Management Group

level. Navigate to

Management Groups

and select the

Management Group

that contains the subscriptions you would like to monitor. Similarly, to configure the monitoring for the entire tenant, you can assign access to the

Tenant Root Group

Select the

subscription

you would like to monitor.

Select

Access control (IAM)

from the subscription menu and navigate to

Add

. After that, click on

Add role assignment

.

Under

Role Assignment

, select

Monitoring Reader

from the

Role

tab. Under

Members

tab, select the name of the application you created above i.e.

MotadataAuth

in our case.

Repeat these steps for any other subscriptions that you wish to monitor in the future.

Retreiving the Client ID, Tenant ID, and Secret Key to complete the integration.

â€‹

Navigate to

App Registrations

. Select the App you created. Note down the Application ID,Tenant ID to use later when discovering the Azure resources as

Client ID

and

Tenant ID

respectively while creating a

credential profile for Microsoft Azure account

.

From the same App, navigate to

Manage

and then select

Certificates and Secrets

Add a new

Client Secret

called

MotadataClientSecret

. Select a timeframe for

Expires

as per your preference and click

Add

.

When the key value is shown, note down the key value to use later when discovering the Azure resources.

Now, Client ID, Tenant ID, and Key value are available to discover Azure resources for monitoring.

Page Title: Credential%20Profile

On this page

Credential Profile

Overview

â€‹

The Credential Profile is an essential part of Motadata AIOps, allowing you to configure and manage device credentials. These credentials enable Motadata AIOps to communicate with your devices, which is a fundamental step in monitoring their data.

By setting up a Credential Profile, you ensure that Motadata AIOps can access the device, gather data, and provide you with valuable insights. This profile becomes especially useful when multiple devices share the same credentials, as it simplifies the management of access details.

Credential Profile Screen

â€‹

On the Credential Profile screen, you can:

View existing credential profiles.

Create new credential profiles.

Edit and delete existing profiles.

You'll need to associate a Credential Profile with a Discovery Profile when creating the latter. Refer to the

Discovery Profile

section for more details.

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Network Discovery

and select

Credential Profile

. The credential profile screen is displayed.

The credential profile screen displays the following details:

Field

Description

Credential Profile Name

The name of the created credential profile.

Used Count

Indicates the total number of entities using the credential profile. Click on the number in the Used Count column to view the different type of entities associated with the credential profile:

Discoveries

: The number indicates count of discovery profiles configured using the credential profile.

Monitors

: The number indicates the count of monitors configured using the credential profile.

Apps

: The number indicates the count of applications being monitored using the credential profile.

Metrics

: The number indicates the count of metric policies configured using the credential profile.

Protocol

Displays the protocol associated with the credential profile.

Actions

Select

to display the permissible actions for the credential profile:

Edit Credential Profile

: This action allows you to change the details of an already existing credential profile.

Assign Credential Profile

: This action allows you to assign a credential profile to a discovery profile.

Delete Credential Profile

: This action allows you to delete a credential profile.

How to Create a Credential Profile?

â€‹

The parameters to create a credential profile differ based on the type of the device for which you are trying to create the profile. We will look in detail about creating a credential profile while covering Addition of devices in Motadata AIOps for each of the following category:

Server & Apps

Network

Cloud

Service Check

Virtualization

Wireless

How to Edit a Credential Profile?

â€‹

Select

from the

Actions

column against the credential profile in the credential profile screen. Select

Edit Credential Profile

.

A pop-up to edit the credential profile details is displayed.

Edit the credential details as required.

Select the

Test

button to check whether the device you want to monitor is accessible according to the credential details entered in the profile.

Select the

Reset

button to erase all the current field values entered in the pop-up, if required.

Select

Update Credential Profile

to update the credential profile in the system.

How to Delete a Credential Profile?

â€‹

Select

from the

Actions

column against the credential profile in the credential profile screen. Select

Delete Credential Profile

.

A pop-up asking to delete the credential profile details is displayed.

Select

Yes

to confirm the deletion of the credential profile.

Select

No

if you do not wish to delete the credential profile.

How to Assign a Credential Profile?

â€‹

Select

 from the

Actions

 column against the credential profile in the credential profile screen. Select

Assign Credential Profile

.

A pop-up that lists all the monitors using the same protocol as the credential profile is displayed.

Select the check box against the monitor which needs to be assigned the credential profile. Now, click on

Assign Credential Profile

. The credential profile is now assigned to the monitor.

Page Title: Discovery%20Profile

On this page

Discovery Profile

Overview

â€‹

Network discovery is a process to identify the devices present in an infrastructure. Discovery helps to build an inventory of devices present in an infrastructure that can further be provisioned to be configured as a

monitor

.

The monitors are categorized in AIOps based on the type of the infrastructure. Refer

supported infrastructure types in Motadata AIOps

to understand the type of infrastructure that can be monitored in Motadata AIOps. The discovery profile corresponding to each infrastructure type can be created to discover the respective device in Motadata AIOps to configure them as a Monitor.

Discovery Profile Screen

â€‹

This screen is used to check details of the already existing discovery profiles, create a discovery profile, edit, and delete the existing ones. This interface can also be used to schedule discovery to run at a particular time or specified intervals in the future.

Navigation

â€‹

Go to Menu, Select

Settings

. After that, Go to

Network Discovery

and select

Discovery Profile

. The discovery profile screen is displayed.

The discovery profile interface displays the following details:

Field

Description

Discovery Profile Name

The name of the discovery profile. This name is used to identify a discovery profile.

IP/Host/IP Range/CIDR/CSV

The address of the device to be discovered in one of the following formats:

IP

:The IP address of the device to be discovered.

Host

: The hostname of the device to be discovered.

IP Range

: A range of IP addresses in case multiple devices are discovered using the same profile.

CIDR

: A range of IP addresses using the CIDR notation if multiple devices need to be discovered using the same profile.

CSV

: The name of the CSV file used to import a range of addresses.

Type

Displays the type of device that needs to be discovered. The Type is based on the device type for which the corresponding credential profile is created.

Discovered Objects

The total number of entities discovered after the last successful execution of the discovery profile.

Status

The time and date of the last run of discovery using the corresponding discovery profile.

Scheduler

The scheduling details of a discovery that is scheduled to run in the future. Select

to display the scheduler details. The icon is displayed to view the scheduler details when a discovery profile is scheduled to run in the future.

Actions

Select

to display the permissible actions for the discovery profile:

Edit Discovery Profile

: This action allows you to change the details of an already existing discovery profile.

Schedule Discovery Profile

: This action allows you to schedule a discovery run at a future time period.

Delete Discovery Profile

: This action allows you to delete a discovery profile.

Select

to execute a re-run of a discovery profile.

How to Create a Discovery Profile?

â€‹

The parameters to create a discovery profile differ based on the type of the device for which you are trying to create the profile. We will look in detail about creating a discovery profile while covering Addition of devices in Motadata AIOps for each of the following category:

Server & Apps

Network

Cloud

Service Check

Virtualization

Wireless

How to Schedule a Discovery Profile?

â€‹

The discovery profile screen allows you to schedule the run of a discovery profile at a specified time in the future. The discovery can also be scheduled at pre-defined intervals in the future.

Select

under the

Actions

column from the discovery profile screen. Then, select the

Schedule Discovery Profile

from the drop-down menu.

A pop-up is displayed which allows to schedule the discovery run at a pre-defined time.

The pop-up displays the following columns to be filled:

Field

Description

Scheduler Type

Select the interval in which the discovery is run, whether Daily, Weekly, or Monthly. Select Once if the discovery has to run only once.

Start Date

Select the date of the first run of discovery.

Hours

Select the time at which the discovery will run.

Notify via Email/Notify via SMS

The system allows notifying users about new service discovery through e-mail and SMS channels:

Specify email addresses (comma separated) to trigger email notifications

Specify mobile numbers (comma separated) to send SMS notifications

Auto Provision

Select the check-box to enable provisioning all the discovered devices for monitoring after the discovery run.

Select

Reset

to erase all the current field values, if required.

Select

Schedule

to schedule the discovery according to the specified parameters.

How to Edit a Discovery Profile?

â€‹

Select

from the Actions column against the discovery profile on the discovery profile screen.

Select

Edit Discovery Profile

from the drop-down menu.

The interface to edit the parameters of a discovery profile is now displayed.

Make changes to the discovery profile as required.

Select

Reset

to erase all the current field values, if required.

Select

Save and Exit

if you have created the discovery profile for future use.

Select

Save and Run

if you want run the discovery immediately after creation.

You should see a success message once the information is saved.

How to Delete a Discovery Profile?

â€‹

Select

 under the

Actions

 column from the discovery profile screen. Then, select

Delete Discovery Profile

 from the drop-down menu.

A pop-up to confirm the deletion of the discovery profile is displayed.

Select

Yes

 to delete the discovery profile.

The discovery profile is now deleted.

Select

No

 if you donâ€™t want to delete the discovery profile.

Page Title: office-integration-steps

On this page

Office 365 Integration Steps

Integration through the O365 Portal

â€‹

Integrate your O365 account with Motadata AIOps from the O365 portal with the following steps:

Retrieve the Tenant ID of the Active Directory

â€‹

Login to the O365 account you want to setup for mmonitoring.

Click on the

App Launcher

 icon from the panel on the left of the your screen and then select

Admin

.

Click on the

Show All

 button.

Under

Admin Center

, Click on

Identity

.

The

Tenant ID

 is now available on the screen under the

Overview

section. Note down the Tenant ID to use later when discovering the O365 resources.

Retrieve the Client ID by registring an Application

â€‹

Click on

Applications

from the the panel on the left of your screen and then select

App Registrations

Select

New registration

.

Enter the details required to register the application and then click on

Register

.

The

Application(Client) ID

is now available on the screen under the

Essentials

details. Note down the Application(Client) ID to use later when discovering the O365 resources.

Retrieve the Secret Key

â€‹

Click on

Certificates & secrets

and then click on

New Client Secret

.

The

Secret ID

is available under the

Client secrets

tab. Note down the Secret ID to use later when discovering the O365 resources.

Now, Client ID, Tenant ID, and Secret Key are available to discover O365 resources for monitoring.

Page Title: overview

On this page

Adding and Managing Devices

Overview

â€‹

In Motadata AIOps, understanding and monitoring your infrastructure begins with adding and managing devices. This process involves setting up two key profiles: the

Credential Profile

and the

Discovery Profile

.

Why Configure These Profiles?

â€‹

Before gaining insights into your infrastructure, Motadata AIOps needs to recognize and setup individual devices as

monitors

in Motadata AIOps. Here's why you configure these profiles:

Credential Profile

: This profile allows you to pre-configure credentials for accessing devices. By creating a credential profile, you can easily apply the same credentials to multiple devices, saving valuable time and manual effort.

Discovery Profile

: Use the discovery profile to identify devices within your infrastructure. A discovery run, initiated by the discovery profile, scans your infrastructure, ensuring that Motadata AIOps can monitor them effectively.

The Three-Step Process

â€‹

Adding and managing devices for monitoring in Motadata AIOps is a streamlined three-step process:

Set Up Profiles

: Begin by configuring the credential profile and discovery profile. These profiles serve as the foundation for recognizing and monitoring your devices.

Discover Devices

: Execute a discovery run, and Motadata AIOps will identify the devices present in your infrastructure. This step ensures that no device goes unnoticed.

Provision Devices

: After discovering your devices, you can choose which ones to monitor and provision them accordingly.

Ready to get started? Let's dive into configuring the Credential Profile and Discovery Profile in the following sections.