AWS Connector

- AWS Connector

AWS Connector

Introduction

Description

AWS Connector allows to manage the Amazon AWS IAM (Identity and Access Management)

Managed Systems

This connector is specific for integration with the Amazon AWS IAM (Identity and Access Management) through the CLI AWS IAM

> For more information to check if your system may be synchronized with this connector, do not hesitate to contact us through our Contact form

Prerequisites

It is needed a AWS IAM user with access and privileges to the required operations.

It cannot detect password changes to be propagated to other systems.

Download and install

This addon is located in the Connectors section and its name is **AWS plugin**.

> For more information about the installation process you can visit the Addons Getting started page.

Agent Configuration

Basic

Generic parameters

After the installation of the addon, you may create and configure agent instances.

To configure this AWS connector you must select "Amazon WS" in the attribute "Type" of the generic parameters section in the agents page configuration.

> For more information about how you may configure the generic parameters of the agent, see the following link: Agents configuration

Custom parameters

Below there are the specific parameters for this agent implementation:

Parameter	Description
Access Key	Access key provided by the AWS IAM account
Secret Key	Secret key provided by the AWS IAM account
AWS Endpoint	AWS endpoint provided by the AWS IAM account
Enable debug	Two options: [Yes / No]. When it is enabled more log traces are printed in the Synchronization Server log

Attribute mappings

This connector could manage **Users** and **Roles**

Properties

The following properties are defined for each object type:

Property	Meaning
preventDeletion (optional)	Two options: [True / False]. If true, it will prevent the deletion of any object that is no longer needed.

Attributes

You can customize attribute mappings, you only need to select system objects and the Soffid objects related, manage their attributes, and make either inbound and outbound attribute mappings.

Users

The following attributes can be mapped on User objects

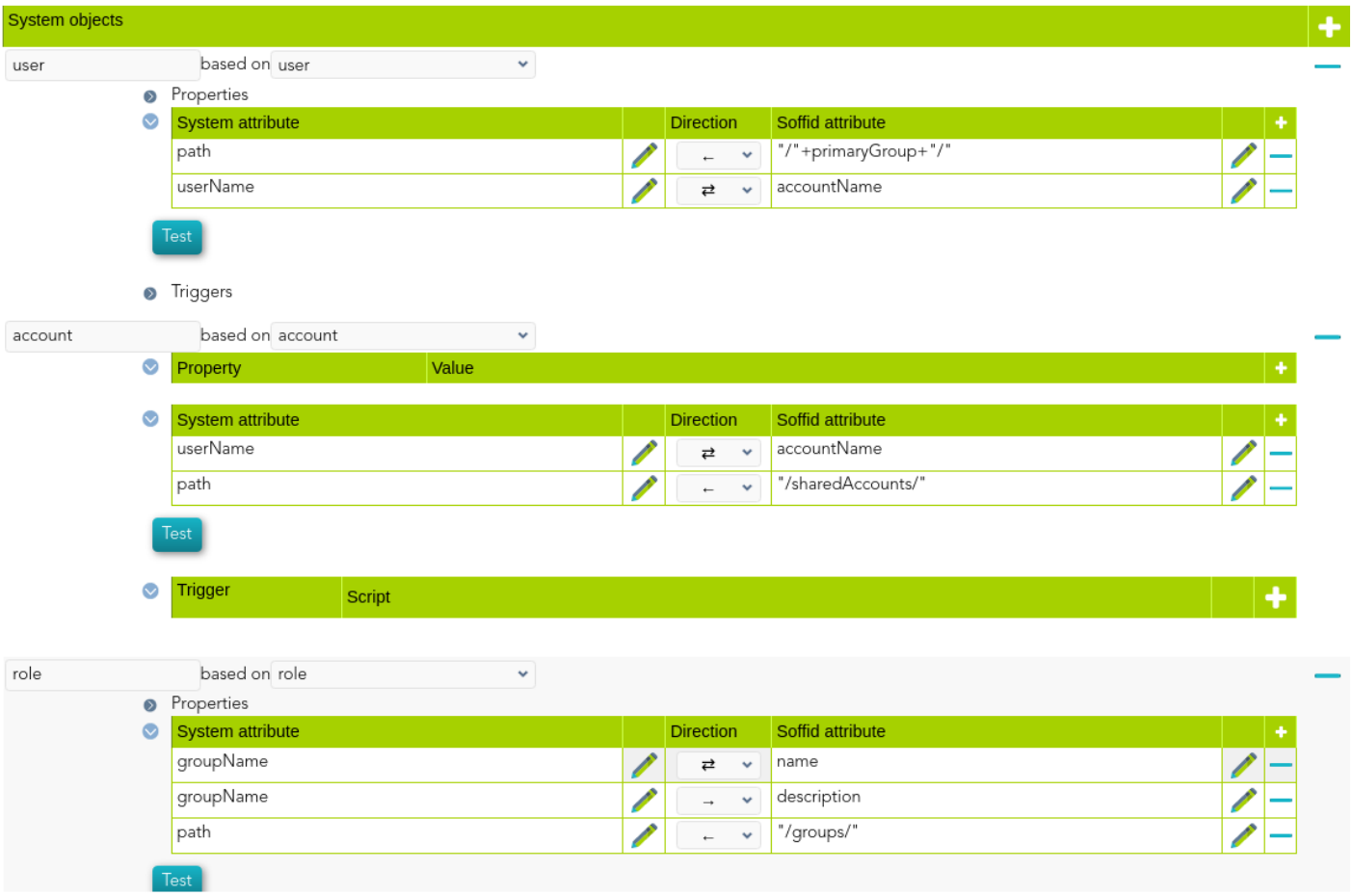
Attribute	Value
userName	User name
path	User path
arn	AWS arn (read only)
createDate	Creation date (read only)
passwordLastUsed	Passsword last use (read only)
userId	Internal user id

Groups

The following attributes can be mapped on Role (AWS Group) objects:

Attribute	Value
groupName	Group name
path	Group path
arn	AWS arn (read only)
createDate	Creation date (read only)
groupId	Internal group id

> For more information about how you may configure attribute mapping, see the following link: Soffid Attribute Mapping Reference



Triggers

You can define BeanShell scripts that will be triggered when data is loaded into the target system (outgoing triggers). The trigger result will be a boolean value, true to continue or false to stop.

Triggers can be used to validate or perform a specific action just before performing an operation or just after performing an operation into target objects.

> To view some examples, visit the Outgoing triggers examples page.

Load triggers

You can define BeanShell scripts that will be triggered when data is loaded into Soffid (incoming triggers). The trigger result will be a boolean value, true to continue or false to stop.

Triggers can be used to validate or perform a specific action just before performing an operation or just after performing an operation into Soffid objects.

> To view some examples, visit the Incoming triggers examples page.

Account metadata

Agents allow you to create additional data, on the "Account metadata" tab, to customize the accounts created for that agent. This additional information will be loaded with the agent's information, or calculated as defined in the mappings.
The additional data can be used in both mappings and triggers.

The attributes which you define here will be shown when you click on the proper account, on the Accounts Tabs at user page.

Operational

Monitoring

After the agent configuration you could check on the monitoring page if the service is running in the Synchronization Server, please go to:

> Start Menu > Administration > Monitoring and reporting > Syscserver monitoring

Tasks

Authoritative

If you are checked "Authorized identity source", an automatic task to load identities from the managed system to Soffid is available, please go to:

> Start Menu > Administration > Monitoring and reporting > Scheduled tasks

And you will something like "Import authoritative data from <AGENT_NAME>".

Reconcile

If you are configured the "Attribute Mapping" tab with some of our objects: "user or role", an automatic task to synchronize these objects from the managed system to Soffid is available, please go to:

> Start Menu > Administration > Monitoring and reporting > Scheduled tasks

And you will do something like "Reconcile all accounts from <AGENT_NAME>".

Synchronization

Regarding the synchronization of the objects, there are two possible options:

- If you are checked the generic attribute "Read Only" in the "Basics" tab, only the changes in the managed systems will be updated in Soffid. We recommend these options until the global configuration of Soffid will be tested.
- If you are not checked the generic attribute "Read Only" in the "Basics" tab, all the changes in Soffid or the managed system will be updated in the other. Note that this synchronization must be configured in the "Attribute mapping" tab correctly.

> For more information about how you may configure the generic parameters of the agent, see the following link: Agents configuration