



AWS

Inventorying of Amazon Web Services (AWS)

TITLE	AWS
AUTHOR	Docusnap Consulting
DATE	18/11/2024
VERSION	4.0 valid from November 18, 2024

This document contains proprietary information and may not be reproduced in any form or parts whatsoever, nor may be used by or its contents divulged to third parties without written permission of itelio GmbH. All rights reserved.

TABLE OF CONTENTS

1. Introduction	4
2. Prerequisites	5
3. Create policies	5
4. Configure user	7
5. Inventory AWS in Docusnap.	7

1. Introduction

The Amazon Web Services scan provides the ability to inventory core areas of your AWS infrastructure

- Elastic Compute Cloud (EC2)
- Identity and Access Management (IAM)
- Simple Storage Service (S3)
- Relational Database Services (RDS)
- Batch orders (batch)
- Lambda
- SQS
- AWSOrganizationsReadOnlyAccess

2. Prerequisites

AWS Inventory requires policies for each of the core areas to be inventoried. The policies are then assigned to a user for programmatic access. This assignment enables an Access Key ID and a Secret Access Key.

An appropriately authorized user is required to create the policies:

- Creating policies
- Creating a user, as well as assigning the created policies.

For the actual inventory, the following data is required:

- Access key ID
- Secret access key
- Region

3. Create policies

The following policy is always needed, regardless of which core areas / services are to be inventoried as a result:

- AWSOrganizationsReadOnlyAccess

A separate policy is also required for each core area / service that you use and want to inventory with Docusnap.

- EC2
- IAM
- S3
- RDS
- batch
- Lambda
- SQS

Log in to your AWS console and open

- **Services - IAM**
- **Policies - Create Policies**

Then use the visual editor to define the Service, Actions and Resources sections one by one.

- **Service**
Using **Select Service**, you then search for the appropriate service for which to create the policy, e.g. EC2
- **Actions**
The actions allowed in EC2 are set to access level **List** as well as **Read**.
- **Resources**
It is recommended to authorize the actions through **All Resources** of the services.

Assign a unique name for the created policy (e.g. Docusnap_EC2_Inventory) as well as an optional description. Click **Create Policy** to complete the configuration.

The steps described above for creating the policy using the EC2 service as an example must now be repeated for the other services that are to be inventoried with Docusnap.

4. Configure user

The previously created policies are now assigned to a user. Within AWS, switch again to the

- **Services - IAM** - and now select **Users - Add User**.

Important: The arrangement of the mapped data in the Docusnap tree structure is based on the inventorying user, this has the region binding described at the beginning as background. Please select relevant user names for different regions here in order to be able to assign them uniquely.

- Assign a unique **User name**
- Select the access type: **Programmatic access**

In the next step, assign the created policies to the user - select

- **Attach existing policies directly**
- Navigate to the **Filter policies** option and set the filter to **Managed by customer**
 - Now select the created policies and add them to this user.

Important: The final created data (user, access key ID as well as the secret access key) is needed for inventory and can be downloaded as CSV. These can only be viewed once after configuration!

5. Inventory AWS in Docusnap.

Launch the AWS Inventory Wizard:

- **Discovery - All Wizards - AWS**
- **Inventory - All Wizards - AWS**
- **All Jobs - All Wizards - AWS**

Select the desired company and tenant domain.

In the display name, you should specify the name of the user for which you will then enter the

- Access Key ID
- Secret access key
- and region

should be entered.

LIST OF FIGURES

ES KONNTEN KEINE EINTRÄGE FÜR EIN ABBILDUNGSVERZEICHNIS GEFUNDEN WERDEN.

VERSION HISTORY

Date	Description
October 4, 2019	Version 1.0 - Description of the "Amazon Web Services" inventory module
April 23, 2020	Version 2.0 - Revision of the HowTo for Docusnap 11
December 21, 2022	Version 3.0 – Revision of the HowTo for Docusnap 12
November 18, 2024	Version 4.0 - New policy required, described

