



Inventorying – AWS

Inventorying of Amazon Web Services (AWS)

TITLE	Inventorying – AWS
AUTHOR	Docusnap Consulting
DATE	09/15/2020
VERSION	2.0 valid from October 01, 2020

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 Docusnap GmbH. All rights reserved.

TABLE OF CONTENTS

1.	About this document	4
	Important Information	4
2.	Prepare your AWS environment for Docusnap	5
2.1	Create policy	6
2.1.1	Check policy	9
2.2	Configure user	10
2.2.1	Create user	11
2.2.2	Define authorizations	12
2.2.3	Receive user keys for inventory	13
3.	Inventory of the AWS in Docusnap	14

1. About this document

The Amazon Web Services scan provides the ability to inventory core areas of your AWS infrastructure. This HowTo describes the necessary steps and requirements to perform a successful AWS inventory.

The core areas that can be read out in this extension are:

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

Chapter 2 describes the preparations within AWS to perform the inventory with Docusnap.

- Creating a policy
- Assign this policy

Chapter 3 then describes the inventory with Docusnap.

The last revision of this HowTos and the screenshots took place on April 24, 2020. Please note that some information on the screenshots may not exist anymore. However, the basic steps remain valid.

Important Information

The Amazon Web Services are regionally bound. If you use these services in different regions, you must ensure that a separate user and policies are created for each region.

2. Prepare your AWS environment for Docusnap

In this chapter we will describe what needs to be prepared in your AWS Identity and Access Management to be able to perform an inventory with Docusnap.

Within the Inventory Wizard, the following information is required:

- Display name
- Access key ID
- Secret access key
- Region

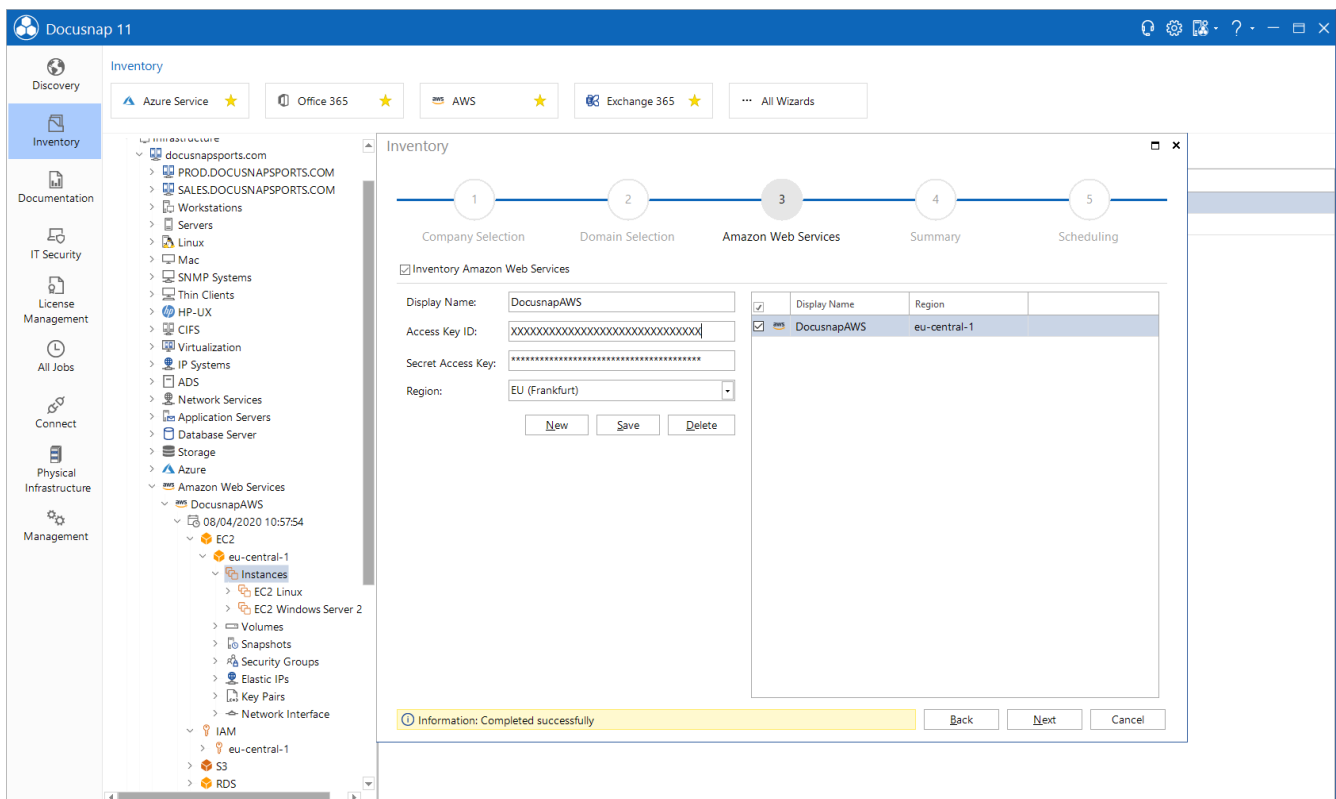


Fig. 1 - AWS Inventory Wizard

Please make sure to use a sufficiently authorized user. The latter must be allowed to make the following changes:

- Create policies
- Creating a user and assigning the created guidelines

2.1 Create policy

This paragraph uses EC2 as an example to describe how to create a dedicated policy for inventorying your AWS in Docusnap. This procedure must then be carried out for the other AWS core areas:

- EC2
- IAM
- S3
- RDS
- Batch
- Lambda
- SQS

Open the services and select IAM.

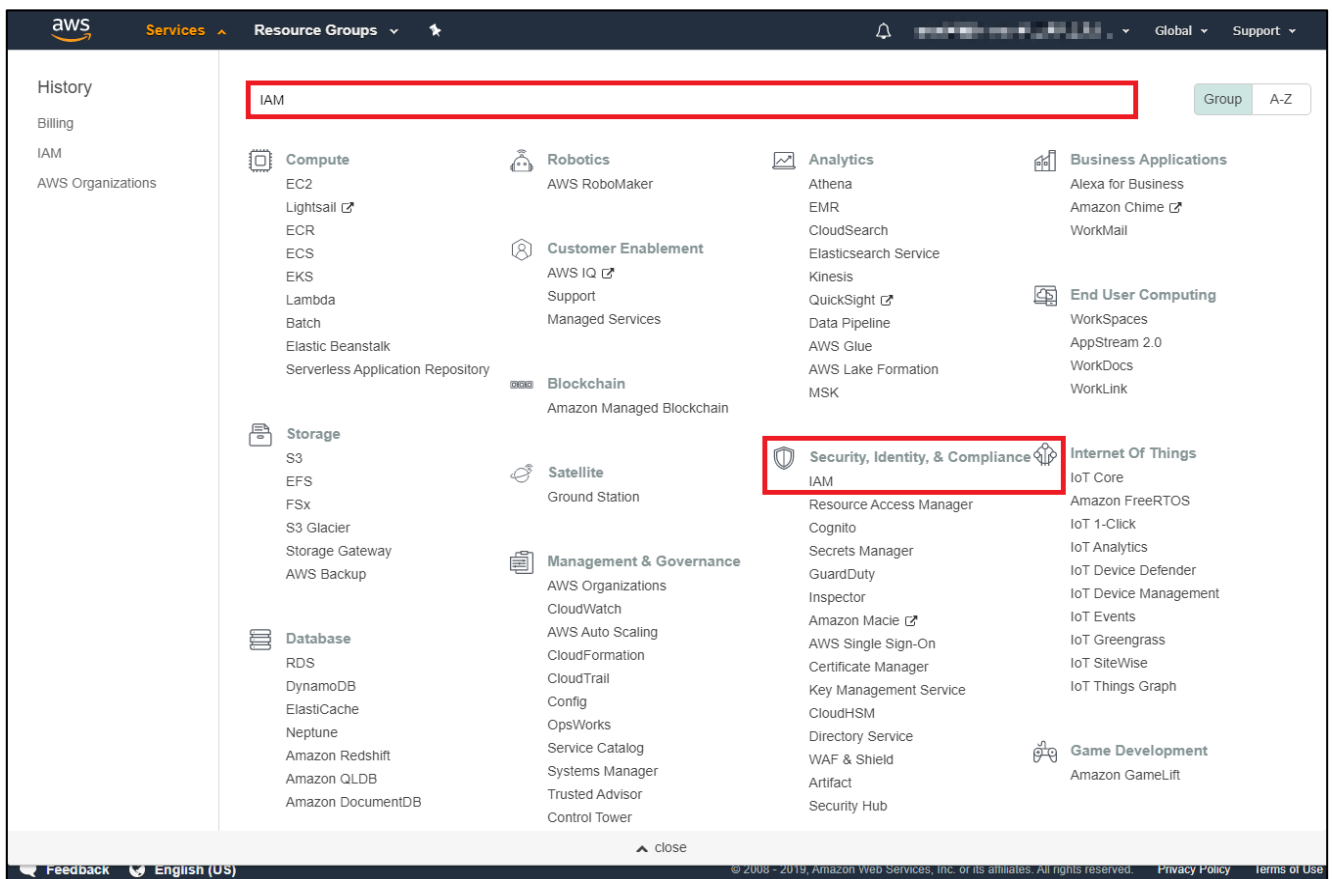
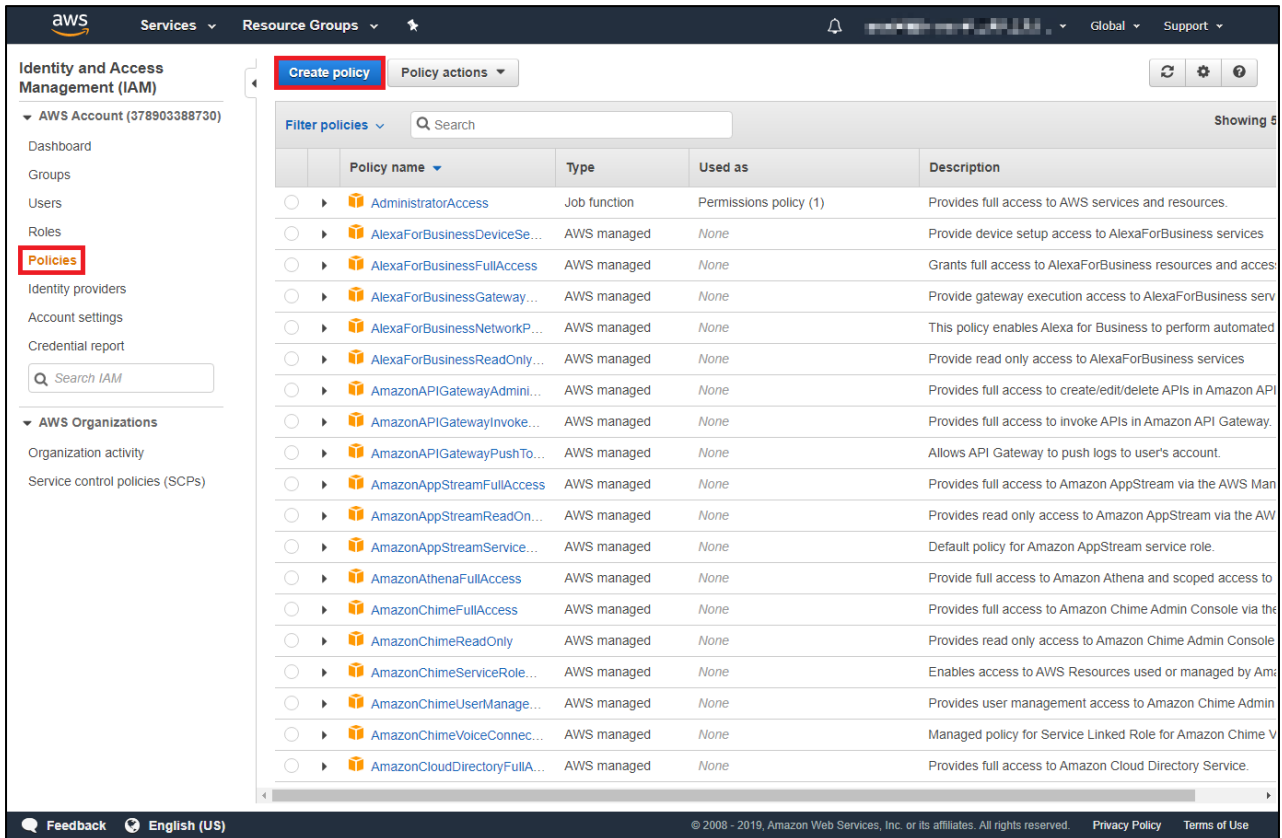


Fig. 2 The configuration of the policies and users takes place in the IAM area

Now select Policies and create a new policy.



The screenshot shows the AWS IAM console interface. On the left sidebar, under 'Identity and Access Management (IAM)', the 'Policies' link is highlighted with a red box. At the top of the main content area, the 'Create policy' button is highlighted with a red box. The main area displays a table of AWS managed policies.




















	Policy name	Type	Used as	Description
<input type="radio"/>	 AdministratorAccess	Job function	Permissions policy (1)	Provides full access to AWS services and resources.
<input type="radio"/>	 AlexaForBusinessDeviceSe...	AWS managed	None	Provide device setup access to AlexaForBusiness services
<input type="radio"/>	 AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness resources and acces
<input type="radio"/>	 AlexaForBusinessGateway...	AWS managed	None	Provide gateway execution access to AlexaForBusiness serv
<input type="radio"/>	 AlexaForBusinessNetworkP...	AWS managed	None	This policy enables Alexa for Business to perform automated
<input type="radio"/>	 AlexaForBusinessReadOnly...	AWS managed	None	Provide read only access to AlexaForBusiness services
<input type="radio"/>	 AmazonAPIGatewayAdmini...	AWS managed	None	Provides full access to create/edit/delete APIs in Amazon API
<input type="radio"/>	 AmazonAPIGatewayInvoke...	AWS managed	None	Provides full access to invoke APIs in Amazon API Gateway.
<input type="radio"/>	 AmazonAPIGatewayPushTo...	AWS managed	None	Allows API Gateway to push logs to user's account.
<input type="radio"/>	 AmazonAppStreamFullAccess	AWS managed	None	Provides full access to Amazon AppStream via the AWS Man
<input type="radio"/>	 AmazonAppStreamReadOn...	AWS managed	None	Provides read only access to Amazon AppStream via the AW
<input type="radio"/>	 AmazonAppStreamService...	AWS managed	None	Default policy for Amazon AppStream service role.
<input type="radio"/>	 AmazonAthenaFullAccess	AWS managed	None	Provide full access to Amazon Athena and scoped access to
<input type="radio"/>	 AmazonChimeFullAccess	AWS managed	None	Provides full access to Amazon Chime Admin Console via the
<input type="radio"/>	 AmazonChimeReadOnly	AWS managed	None	Provides read only access to Amazon Chime Admin Console
<input type="radio"/>	 AmazonChimeServiceRole...	AWS managed	None	Enables access to AWS Resources used or managed by Ami
<input type="radio"/>	 AmazonChimeUserManage...	AWS managed	None	Provides user management access to Amazon Chime Admin
<input type="radio"/>	 AmazonChimeVoiceConnec...	AWS managed	None	Managed policy for Service Linked Role for Amazon Chime V
<input type="radio"/>	 AmazonCloudDirectoryFullA...	AWS managed	None	Provides full access to Amazon Cloud Directory Service.

Fig. 3 - Amazon Web Services Policy Management

The Service, Actions and Resources areas are then defined one after the other using the visual editor.

- **Service**
Select **Service**, you then search for the service for which you want to create the policy, in this case EC2.
- **Actions**
The actions permitted in **EC2** are set at access level **List** and **Read**.
- **Resources**
Here it is recommended to authorize the actions via **All resources** of the services.
- **Request conditions**
This item is optional and is not required for a successful inventory.

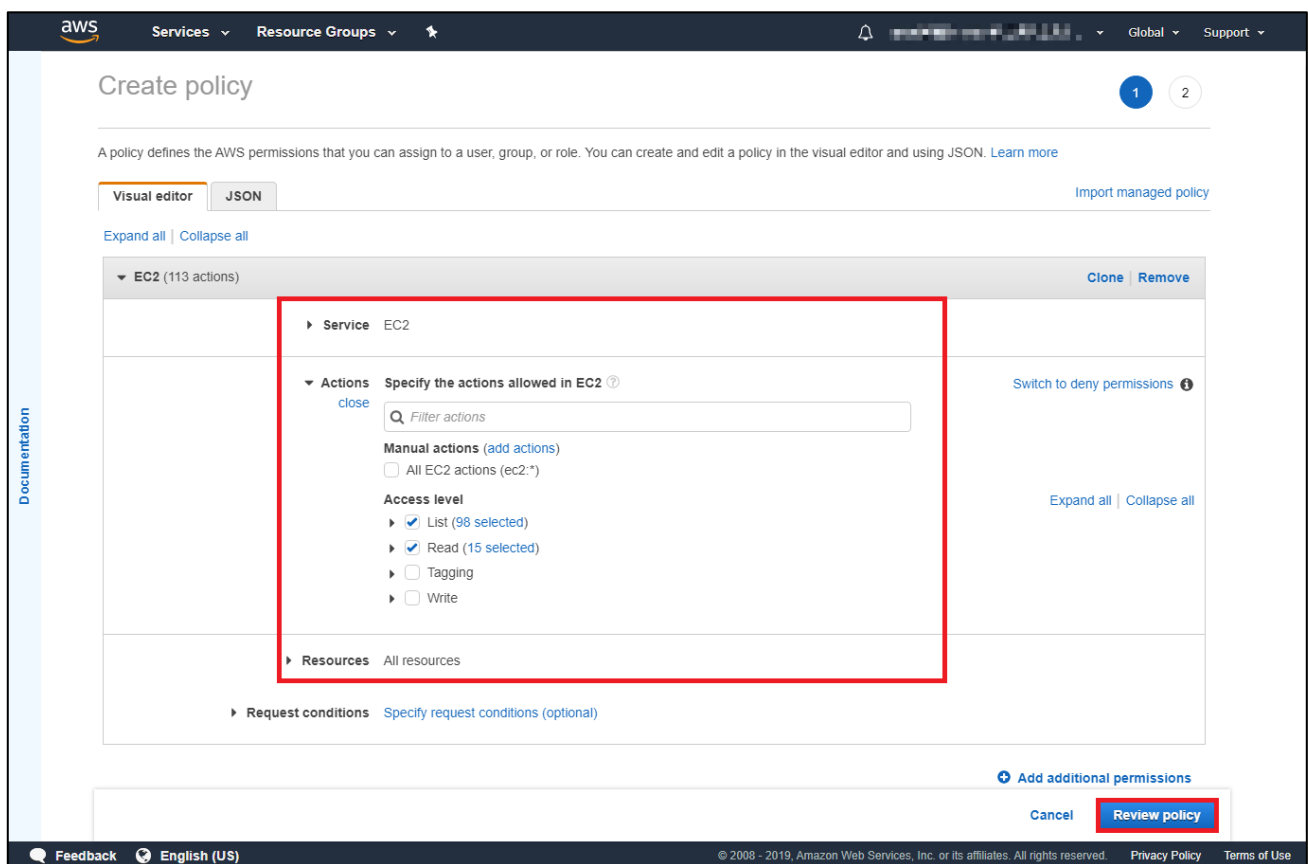
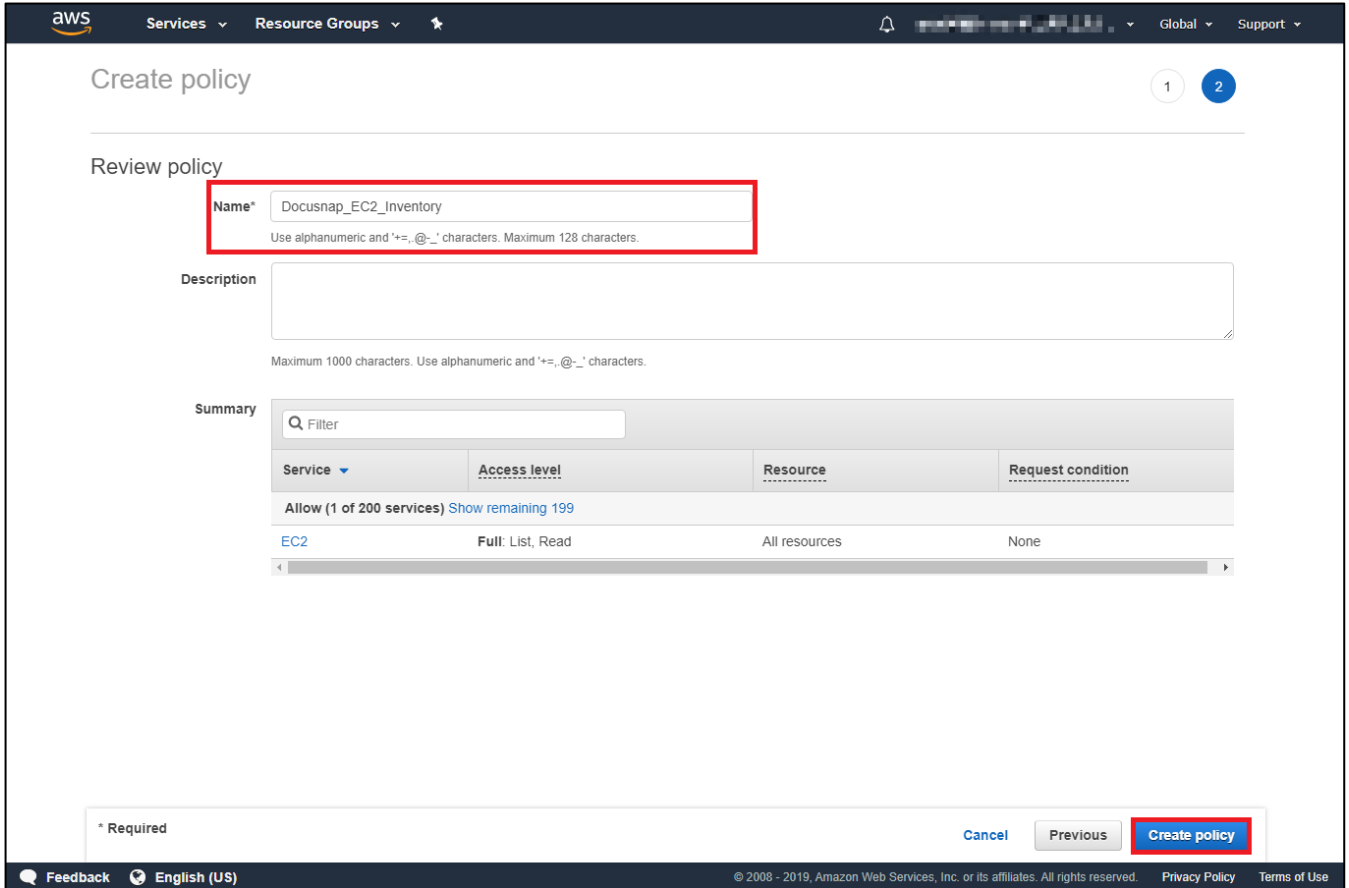


Fig. 4 - "Review policy" takes you to the next step of configuration

2.1.1 Check policy

Assign a unique name for the created policy (e.g. Docusnap_EC2_Inventory) and an optional description. The configuration is completed via **Create policy**.



Create policy

Review policy

Name* Docusnap_EC2_Inventory
Use alphanumeric and '+-=,@_.' characters. Maximum 128 characters.

Description
Maximum 1000 characters. Use alphanumeric and '+-=,@_.' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 200 services) Show remaining 199			
EC2	Full: List, Read	All resources	None

* Required

[Cancel](#) [Previous](#) **Create policy**

Fig. 5 - Complete policy configuration

The previously described steps 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.

Create the appropriate policies for the areas:

- EC2
- IAM
- S3
- RDS
- Batch
- Lambda
- SQS

2.2 Configure user

The previously created policies are now assigned to a user. Within AWS, switch to the Services - IAM again and select Users in the next step.

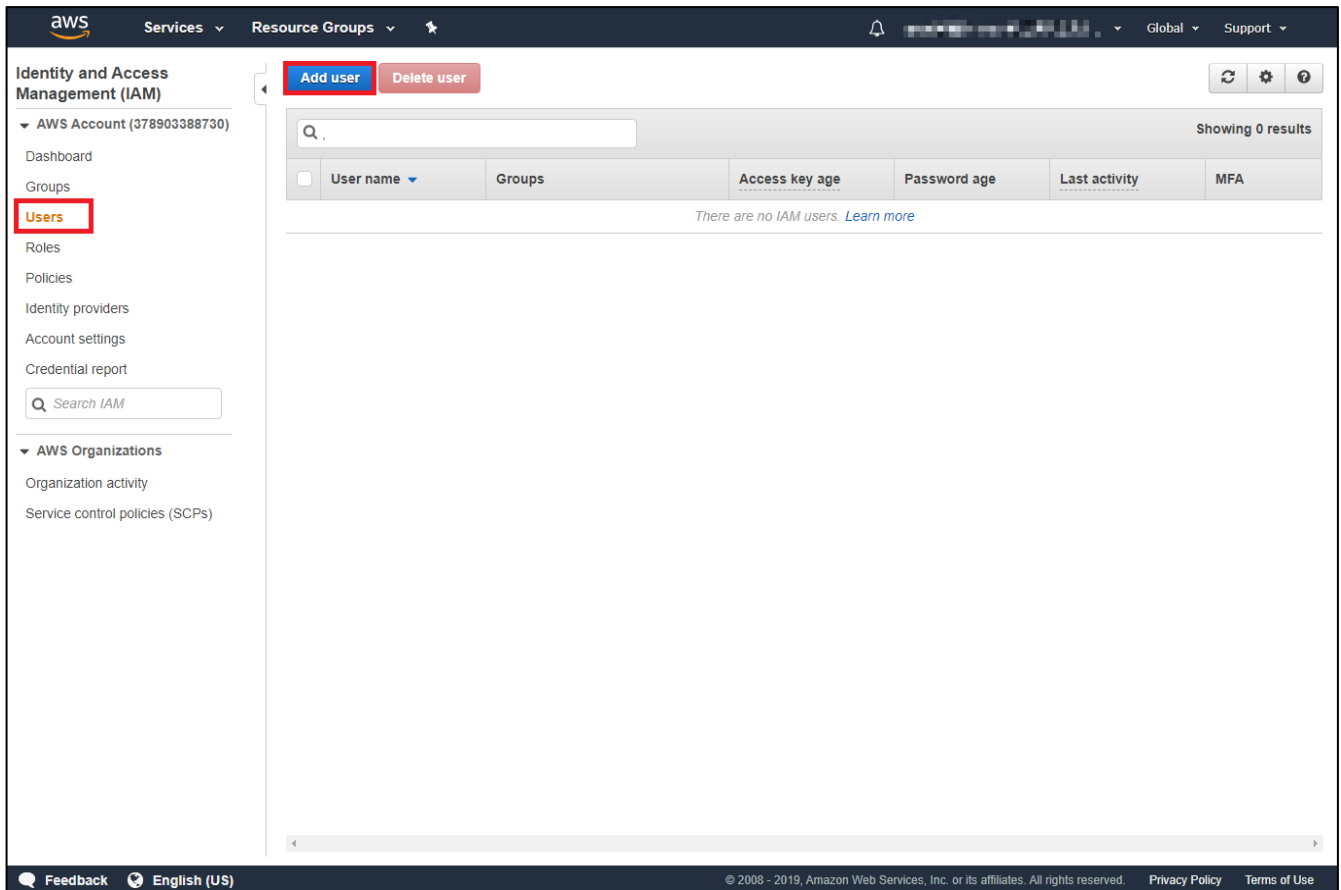


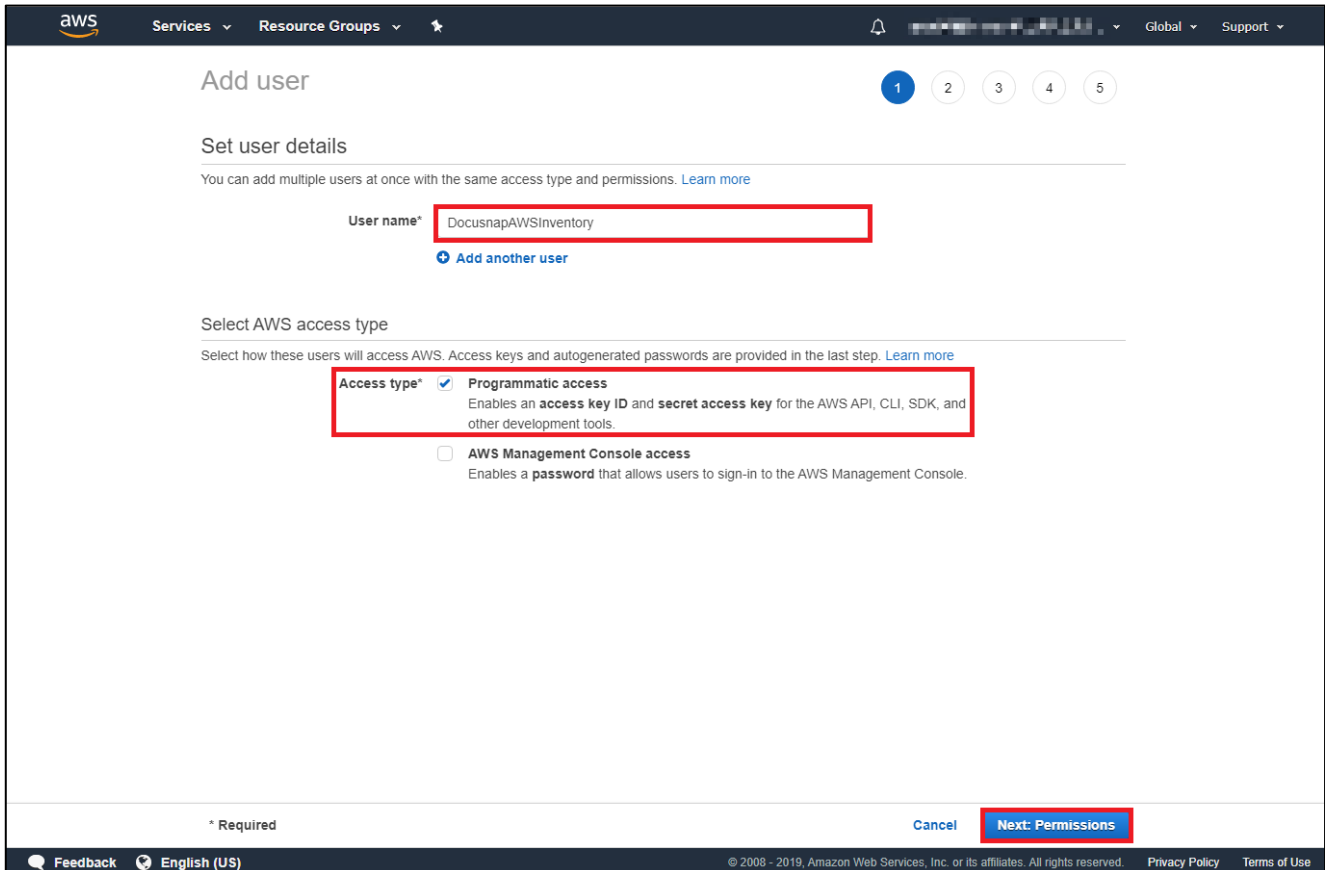
Fig. 6 - User Administration of Amazon Web Services

Important: The arrangement of the displayed 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 the relevant usernames for different regions here in order to assign them unambiguously.

2.2.1 Create user

Use Add user to create a new user. A username and AWS access type are required.

As AWS access type select **Programmatic access**, via the button **Next: Permissions** you come to the next step.



The screenshot shows the AWS 'Add user' console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and a search icon. The main heading is 'Add user' with a progress indicator showing five steps, with the first step being active. The 'Set user details' section includes a note about adding multiple users and a 'User name*' field containing 'DocusnapAWSInventory'. Below this is a link to 'Add another user'. The 'Select AWS access type' section includes a note about access keys and passwords. Two options are listed: 'Programmatic access' (selected with a checkbox) and 'AWS Management Console access' (unchecked). The 'Programmatic access' option is described as enabling an 'access key ID' and 'secret access key'. At the bottom, there is a '* Required' label, a 'Cancel' button, and a 'Next: Permissions' button which is highlighted with a red box. The footer contains 'Feedback', 'English (US)', copyright information, and links to 'Privacy Policy' and 'Terms of Use'.

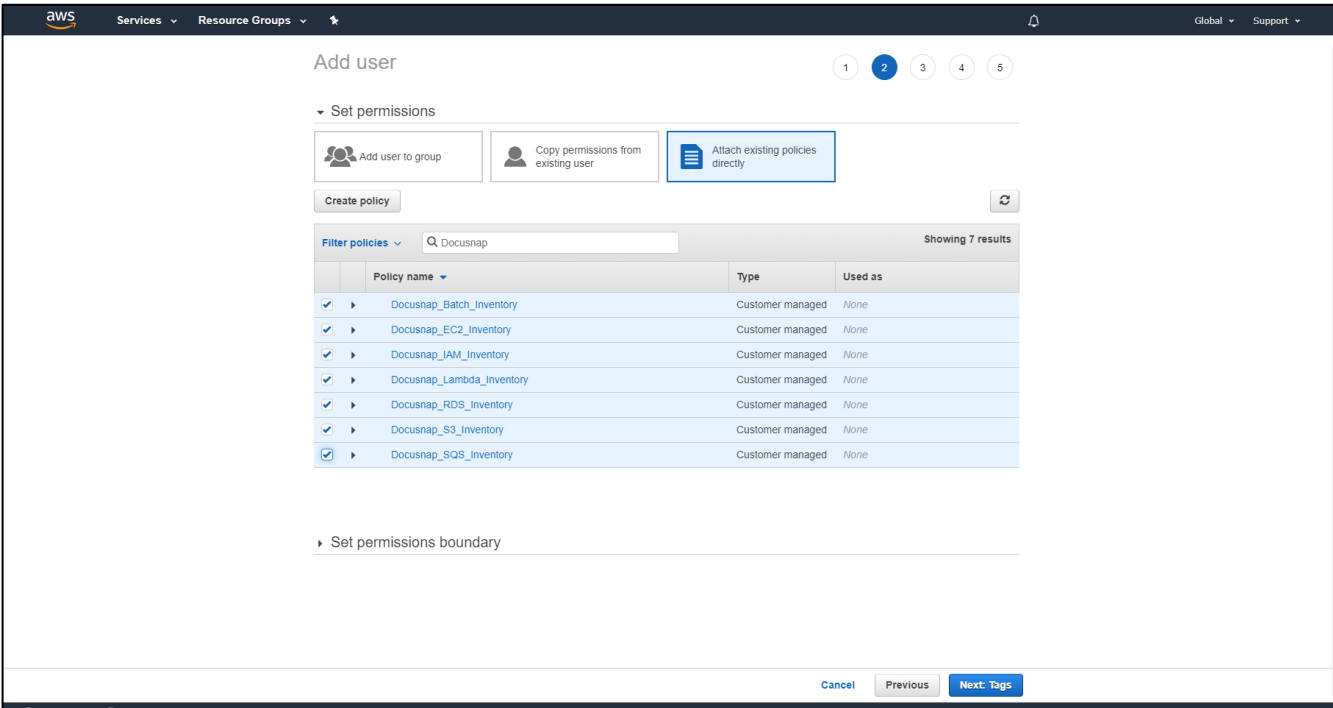
Fig. 7 - Defining the User Details for the Inventory Account

2.2.2 Define authorizations

Here you have two different possibilities to authorize your user for inventory.

- Add user to group
This option can be selected if you want to assign the created policies to a group. However, it is advisable to always carry out the inventory with the same user.
- Attach existing policies directly
This option is described in this HowTo to bind the pre-created policies directly to a user.

Select **Add existing policies directly** and 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.



The screenshot shows the AWS IAM console 'Add user' page, specifically the 'Set permissions' step (step 2 of 5). The 'Attach existing policies directly' option is selected under 'Set permissions'. Below this, there is a 'Filter policies' section with a search bar containing 'Docusnap' and a 'Showing 7 results' indicator. A table lists the following policies, all of which are checked for selection:

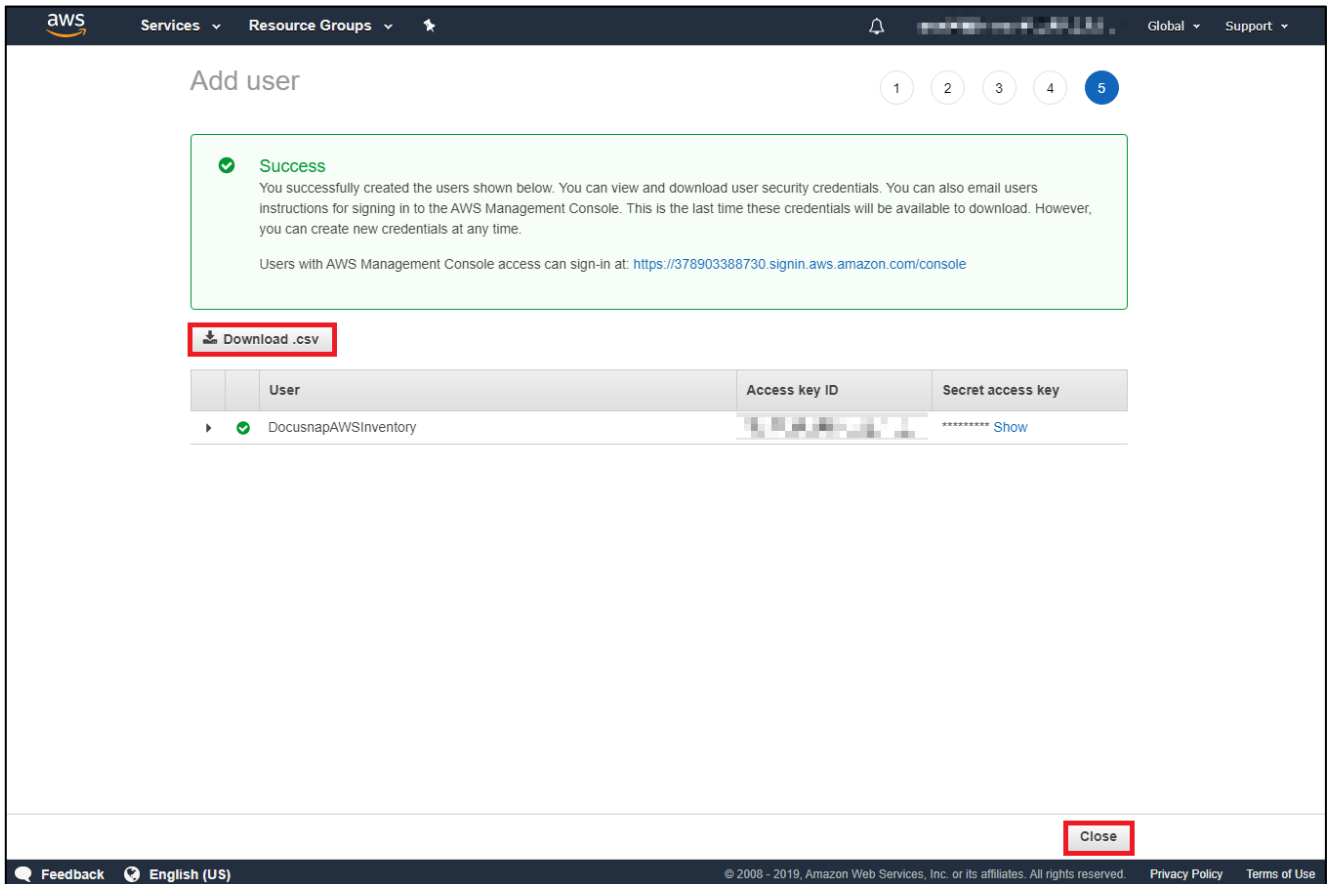
	Policy name	Type	Used as
<input checked="" type="checkbox"/>	Docusnap_Batch_Inventory	Customer managed	None
<input checked="" type="checkbox"/>	Docusnap_EC2_Inventory	Customer managed	None
<input checked="" type="checkbox"/>	Docusnap_IAM_Inventory	Customer managed	None
<input checked="" type="checkbox"/>	Docusnap_Lambda_Inventory	Customer managed	None
<input checked="" type="checkbox"/>	Docusnap_RDS_Inventory	Customer managed	None
<input checked="" type="checkbox"/>	Docusnap_S3_Inventory	Customer managed	None
<input checked="" type="checkbox"/>	Docusnap_SQS_Inventory	Customer managed	None

At the bottom of the page, there are buttons for 'Cancel', 'Previous', and 'Next: Tags'.

Fig. 8 - Assignment of created Docusnap Inventory Policies

2.2.3 Receive user keys for inventory

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



The screenshot shows the AWS IAM 'Add user' console. At the top, there's a navigation bar with 'aws', 'Services', 'Resource Groups', and a user profile. Below the navigation bar, the title 'Add user' is displayed with a progress indicator showing 5 steps, with step 5 being the current step. A green success message box states: 'Success. You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time. Users with AWS Management Console access can sign-in at: <https://378903388730.signin.aws.amazon.com/console>'. Below the message, there is a 'Download .csv' button. A table lists the created users:

	User	Access key ID	Secret access key
▶	✓ DocusnapAWSInventory	AKIAI44QH8DHBVS7GALM	***** Show

At the bottom right of the console, there is a 'Close' button. The footer contains 'Feedback', 'English (US)', copyright information '© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.', and links to 'Privacy Policy' and 'Terms of Use'.

Fig. 9 - After completion of user creation, you will receive your keys

3. Inventory of the AWS in Docusnap

The created user is now used in combination with the created keys to perform the inventory in Docusnap.

To do this, please open the **AWS Wizard** within the Inventory section. If you do not see the control panel for the AWS inventory, you can open it via **All Wizards**.

Then select your client, the domain to which the inventory results are to be assigned, and the Discovery Service in the subsequent dialog, and then enter the user created in the **Display name** field and the keys generated accordingly.

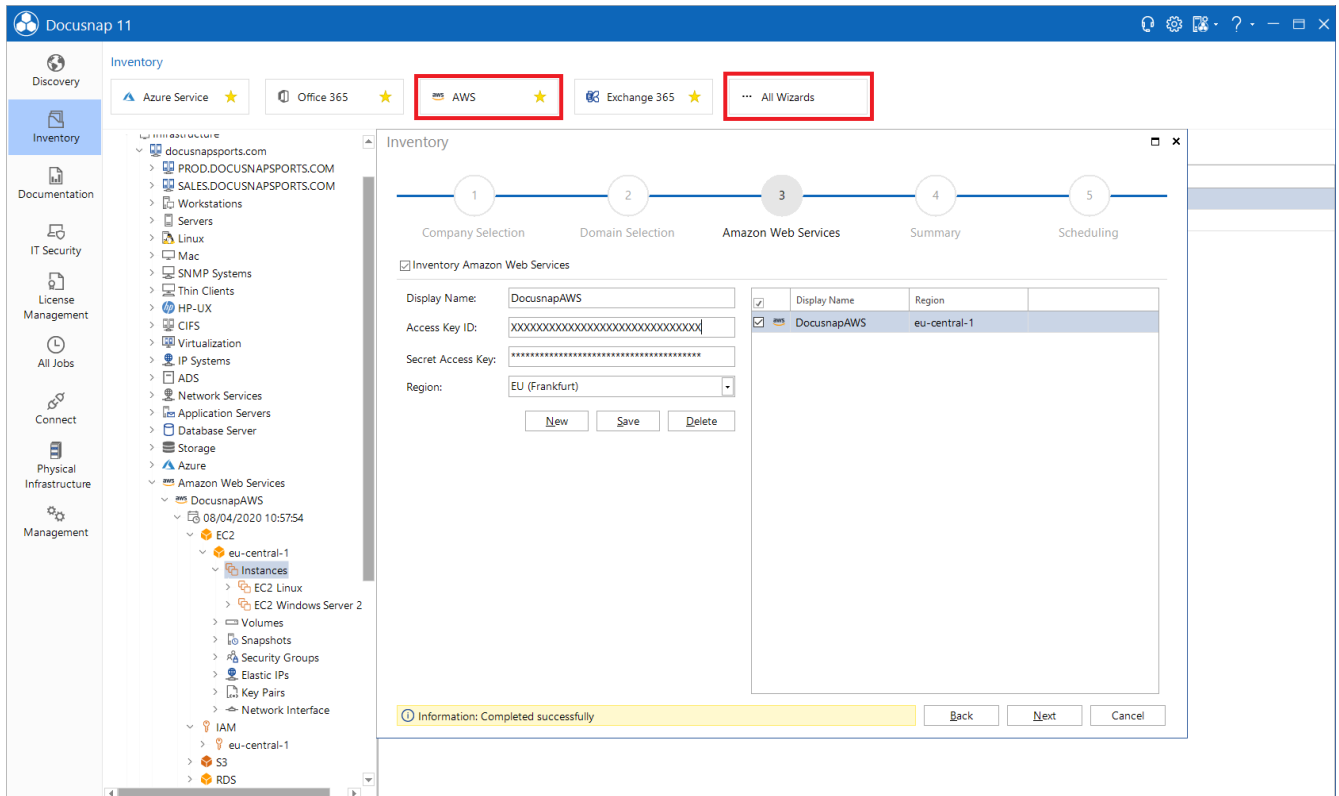


Fig. 10 - The Create Keys are Entered in the Wizard

After successful saving, you will see a short summary via **Next** and can define in the last step whether you want to schedule the inventory time controlled.

LIST OF FIGURES

FIG. 1 - AWS INVENTORY WIZARD.....	5
FIG. 2- THE CONFIGURATION OF THE POLICIES AND USERS TAKES PLACE IN THE IAM AREA.....	6
FIG. 3 - AMAZON WEB SERVICES POLICY MANAGEMENT	7
FIG. 4 - "REVIEW POLICY" TAKES YOU TO THE NEXT STEP OF CONFIGURATION.....	8
FIG. 5 - COMPLETE POLICY CONFIGURATION	9
FIG. 6 - USER ADMINISTRATION OF AMAZON WEB SERVICES	10
FIG. 7 - DEFINING THE USER DETAILS FOR THE INVENTORY ACCOUNT	11
FIG. 8 - ASSIGNMENT OF CREATED DOCUSNAP INVENTORY POLICIES.....	12
FIG. 9 - AFTER COMPLETION OF USER CREATION, YOU WILL RECEIVE YOUR KEYS	13
FIG. 10 - THE CREATE KEYS ARE ENTERED IN THE WIZARD	14

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 HowTos for Docusnap 11



Docusnap[®]

support@docusnap.com | www.docusnap.com/support
© Docusnap GmbH - www.docusnap.com