



Inventarisierung – AWS

Inventarisierung der Amazon Web Services (AWS)

TITEL Inventarisierung – AWS
AUTOR Docusnap Consulting
DATUM 03.11.2020
VERSION 2.0 | gültig ab 01.10.2020

Die Weitergabe, sowie Vervielfältigung dieser Unterlage, auch von Teilen, Verwertung und Mitteilung ihres Inhaltes ist nicht gestattet, soweit nicht ausdrücklich durch die Docusnap GmbH zugestanden. Zuwiderhandlung verpflichtet zu Schadenersatz. Alle Rechte vorbehalten.

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.

INHALTSVERZEICHNIS

1. Einleitung	4
Wichtige Informationen	4
2. Ihre AWS Umgebung für Docusnap vorbereiten	5
2.1 Richtlinie erstellen	6
2.1.1 Richtlinie überprüfen	9
2.2 Benutzer konfigurieren	10
2.2.1 Benutzer anlegen	11
2.2.2 Berechtigungen festlegen	12
2.2.3 Benutzerschlüssel für die Inventarisierung erhalten	13
3. Inventarisierung der AWS in Docusnap	14

1. Einleitung

Der Scan der Amazon Web Services liefert die Möglichkeit, Kernbereiche Ihrer AWS Infrastruktur zu inventarisieren. Dieses HowTo beschreibt die notwendigen Schritte sowie Voraussetzungen, eine erfolgreiche AWS Inventarisierung durchzuführen.

Die in dieser Erweiterung auslesbaren Kernbereiche sind:

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

Kapitel 2 beschreibt die Vorbereitungen innerhalb von AWS, damit die Inventarisierung mit Docusnap durchgeführt werden kann.

- Erstellen einer Richtlinie
- Zuweisen dieser Richtlinie

Kapitel 3 beschreibt anschließend die Inventarisierung mit Docusnap.

Die letzte Überarbeitung dieses HowTos und der Screenshots haben am 24.04.2020 stattgefunden. Bitte beachten Sie daher, dass einige Informationen auf den Screenshots so nicht mehr existieren könnten. Die grundlegenden Schritte sind jedoch weiterhin gültig.

Wichtige Informationen

Die Amazon Web Services sind regional gebunden. Sollten Sie entsprechende Services in unterschiedlichen Regionen nutzen, müssen Sie darauf achten, dass für jede Region ein eigener Benutzer sowie die entsprechenden Richtlinien erstellt werden müssen.

2. Ihre AWS Umgebung für Docusnap vorbereiten

In diesem Kapitel wird beschrieben, was in Ihrem AWS Identity and Access Management vorzubereiten ist, um eine Inventarisierung mit Docusnap durchführen zu können.

Innerhalb des Inventarisierungsassistenten werden die folgenden Informationen von Ihnen benötigt:

- Anzeigename
- Zugriffsschlüssel-ID
- Geheimer Zugriffsschlüssel
- Region

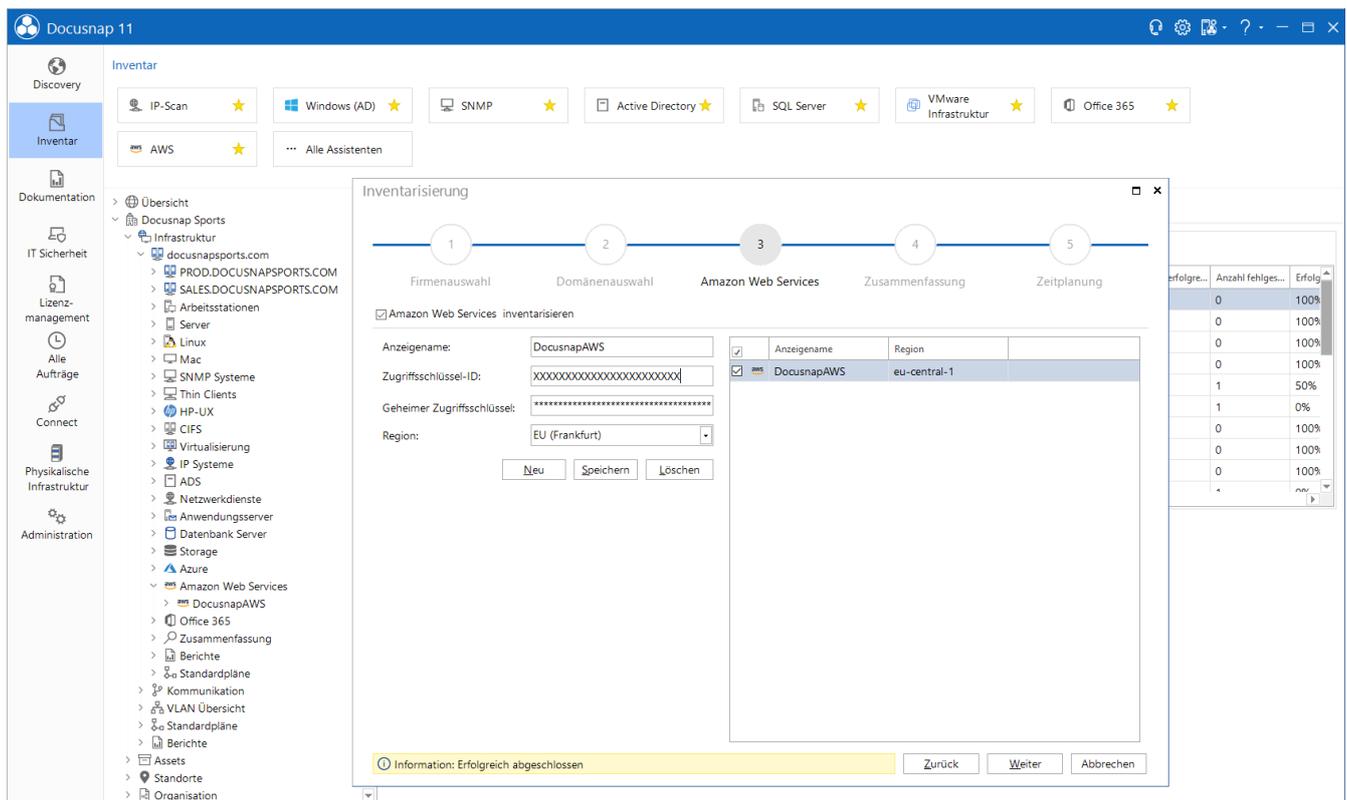


Abbildung 1 - AWS Inventarisierungsassistent

Stellen Sie bitte sicher, einen ausreichend berechtigten Benutzer zu verwenden. Dieser muss folgende Änderungen durchführen dürfen:

- Erstellen von Richtlinien
- Erstellen eines Benutzers sowie Vergabe der erstellten Richtlinien

2.1 Richtlinie erstellen

In diesem Absatz wird am Beispiel EC2 beschrieben, wie eine dedizierte Richtlinie für die Inventarisierung Ihrer AWS in Docusnap erstellt wird. Diese Vorgehensweise muss anschließend für die weiteren AWS Kernbereiche durchgeführt werden. Es können die folgenden Services inventarisiert werden:

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

Öffnen Sie die Services und wählen Sie IAM aus.

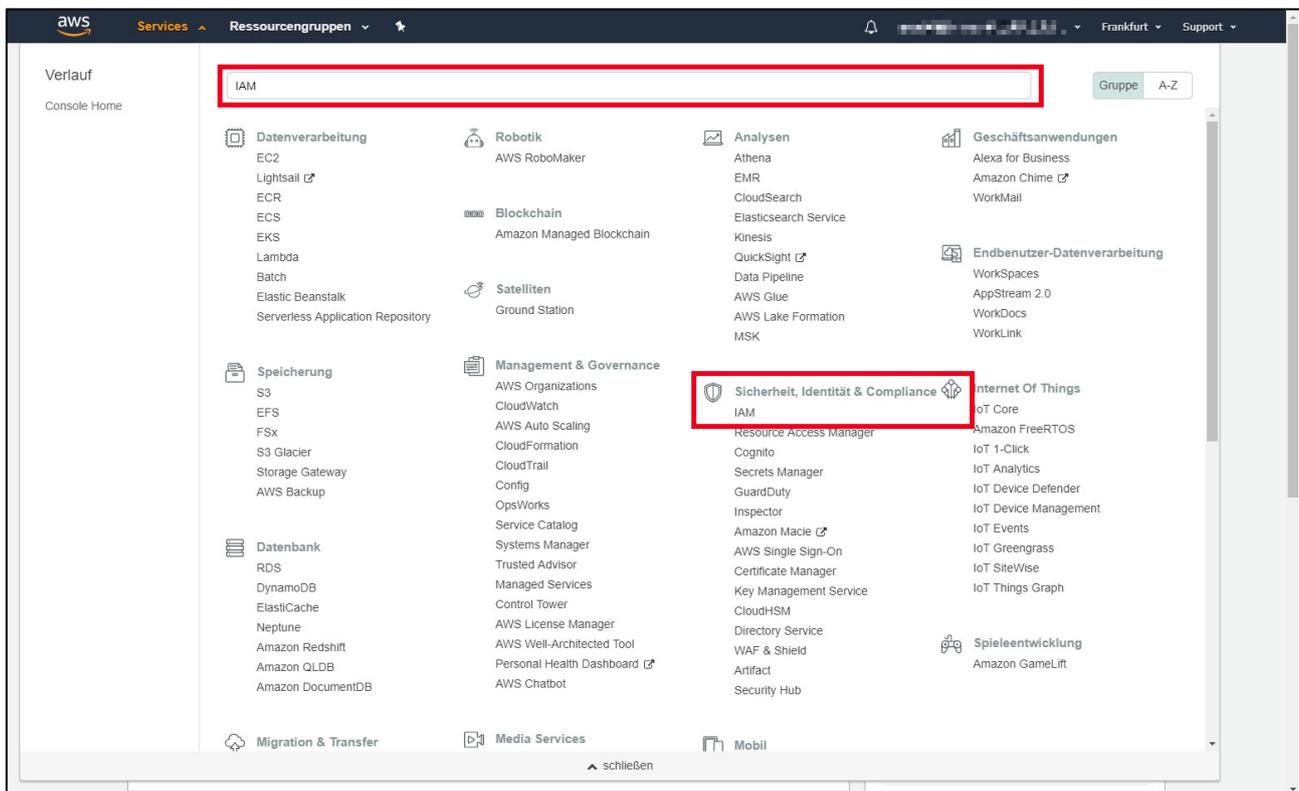
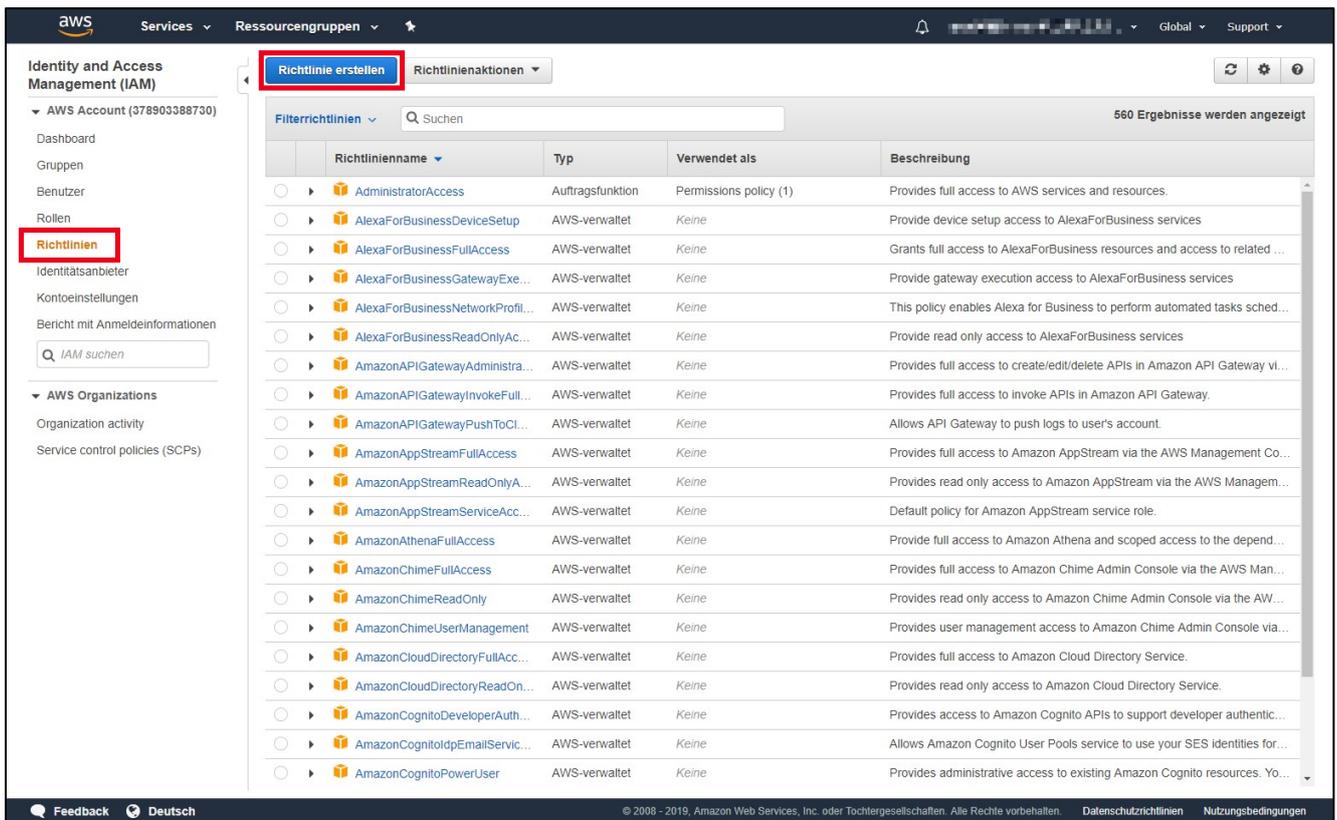


Abbildung 2- Die Konfiguration der Richtlinien und Benutzer findet im Bereich IAM statt

Wählen Sie nun Richtlinien und erstellen Sie eine neue Richtlinie.



The screenshot shows the AWS IAM console interface. On the left sidebar, the 'Richtlinien' (Policies) menu item is highlighted with a red box. At the top of the main content area, the 'Richtlinie erstellen' (Create Policy) button is also highlighted with a red box. Below this, there is a search bar and a table listing various AWS policies. The table has the following columns: 'Richtlinienname', 'Typ', 'Verwendet als', and 'Beschreibung'. The table contains 20 rows of policy entries, each with a radio button for selection and a right-pointing arrow for details.

Richtlinienname	Typ	Verwendet als	Beschreibung
AdministratorAccess	Auftragsfunktion	Permissions policy (1)	Provides full access to AWS services and resources.
AlexaForBusinessDeviceSetup	AWS-verwaltet	Keine	Provide device setup access to AlexaForBusiness services
AlexaForBusinessFullAccess	AWS-verwaltet	Keine	Grants full access to AlexaForBusiness resources and access to related ...
AlexaForBusinessGatewayExe...	AWS-verwaltet	Keine	Provide gateway execution access to AlexaForBusiness services
AlexaForBusinessNetworkProfil...	AWS-verwaltet	Keine	This policy enables Alexa for Business to perform automated tasks sched...
AlexaForBusinessReadOnlyAc...	AWS-verwaltet	Keine	Provide read only access to AlexaForBusiness services
AmazonAPIGatewayAdministra...	AWS-verwaltet	Keine	Provides full access to create/edit/delete APIs in Amazon API Gateway vl...
AmazonAPIGatewayInvokeFull...	AWS-verwaltet	Keine	Provides full access to invoke APIs in Amazon API Gateway.
AmazonAPIGatewayPushToCl...	AWS-verwaltet	Keine	Allows API Gateway to push logs to user's account.
AmazonAppStreamFullAccess	AWS-verwaltet	Keine	Provides full access to Amazon AppStream via the AWS Management Co...
AmazonAppStreamReadOnlyA...	AWS-verwaltet	Keine	Provides read only access to Amazon AppStream via the AWS Managem...
AmazonAppStreamServiceAcc...	AWS-verwaltet	Keine	Default policy for Amazon AppStream service role.
AmazonAthenaFullAccess	AWS-verwaltet	Keine	Provide full access to Amazon Athena and scoped access to the depend...
AmazonChimeFullAccess	AWS-verwaltet	Keine	Provides full access to Amazon Chime Admin Console via the AWS Man...
AmazonChimeReadOnly	AWS-verwaltet	Keine	Provides read only access to Amazon Chime Admin Console via the AW...
AmazonChimeUserManagement	AWS-verwaltet	Keine	Provides user management access to Amazon Chime Admin Console via...
AmazonCloudDirectoryFullAcc...	AWS-verwaltet	Keine	Provides full access to Amazon Cloud Directory Service.
AmazonCloudDirectoryReadOn...	AWS-verwaltet	Keine	Provides read only access to Amazon Cloud Directory Service.
AmazonCognitoDeveloperAuth...	AWS-verwaltet	Keine	Provides access to Amazon Cognito APIs to support developer authentic...
AmazonCognitoEmailServic...	AWS-verwaltet	Keine	Allows Amazon Cognito User Pools service to use your SES identities for...
AmazonCognitoPowerUser	AWS-verwaltet	Keine	Provides administrative access to existing Amazon Cognito resources. Yo...

Abbildung 3 - Die Richtlinienverwaltung der Amazon Web Services

Anschließend werden über den visuellen Editor die Bereiche Service, Aktionen und Ressourcen nacheinander definiert.

- Service
Über **Service auswählen** suchen Sie anschließend nach dem entsprechenden Service, für welchen die Richtlinie erstellt werden soll, in diesem Fall **EC2**.
- Aktionen
Die in **EC2** zulässigen Aktionen werden auf Zugriffsebene **Auflisten** sowie **Lesen** gesetzt.
- Ressourcen
Hier wird empfohlen, die Aktionen über **Alle Ressourcen** der Services zu berechtigen.
- Bedingungen anfordern
Dieser Punkt ist optional und wird für eine erfolgreiche Inventarisierung nicht benötigt

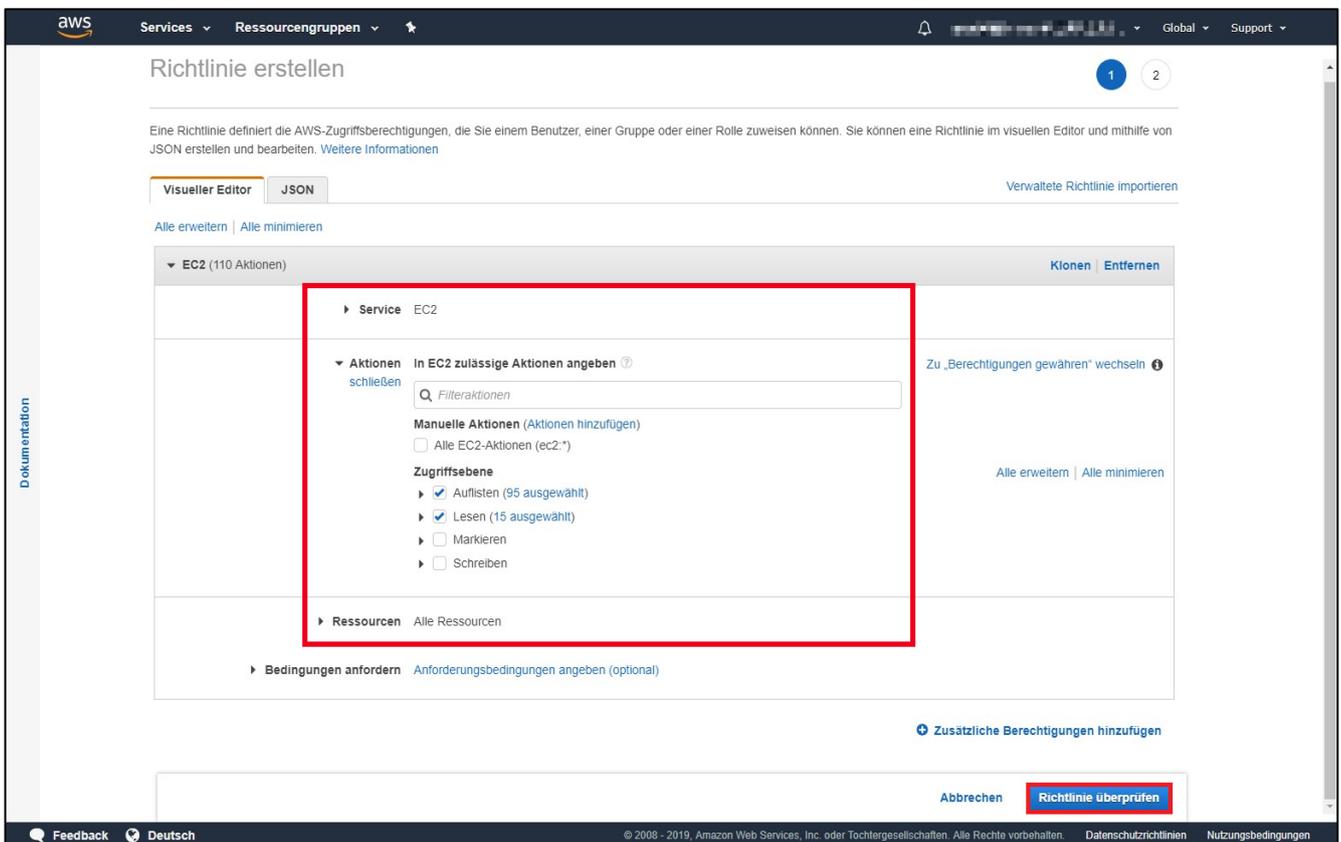
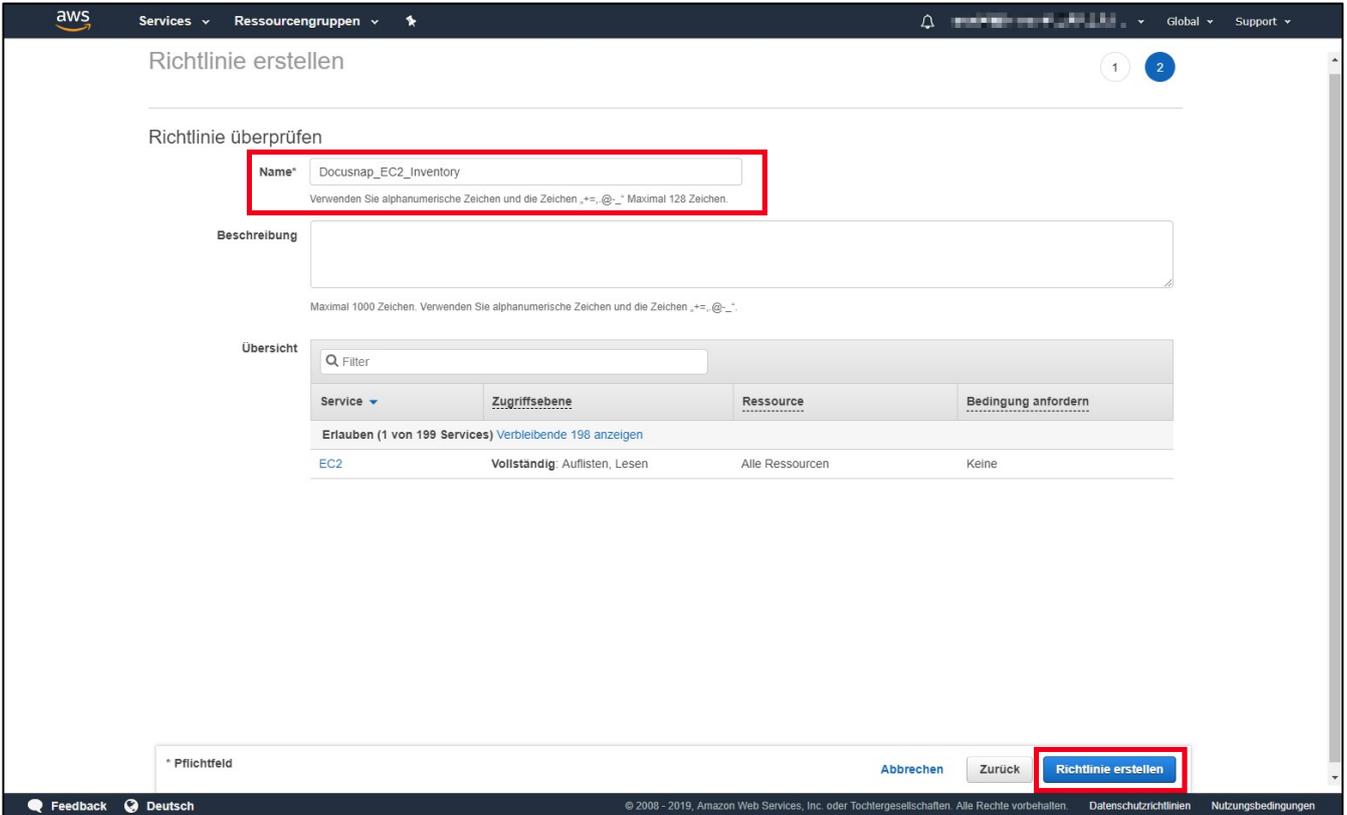


Abbildung 4 - „Richtlinie prüfen“ führt Sie zum nächsten Schritt der Konfiguration

2.1.1 Richtlinie überprüfen

Vergeben Sie einen eindeutigen Namen für die erstellte Richtlinie (z.B. Docusnap_EC2_Inventory) sowie eine optionale Beschreibung. Über Richtlinie erstellen wird die Konfiguration abgeschlossen.



Richtlinie erstellen

Richtlinie überprüfen

Name*

Verwenden Sie alphanumerische Zeichen und die Zeichen "+", "@", "-" Maximal 128 Zeichen.

Beschreibung

Maximal 1000 Zeichen. Verwenden Sie alphanumerische Zeichen und die Zeichen "+", "@", "-".

Übersicht

Filter

Service	Zugriffsebene	Ressource	Bedingung anfordern
Erlauben (1 von 199 Services) Verbleibende 198 anzeigen			
EC2	Vollständig: Auflisten, Lesen	Alle Ressourcen	Keine

* Pflichtfeld

Abbrechen Zurück **Richtlinie erstellen**

Feedback Deutsch © 2008 - 2019, Amazon Web Services, Inc. oder Tochtergesellschaften. Alle Rechte vorbehalten. Datenschutzrichtlinien Nutzungsbedingungen

Abbildung 5 - Abschluss der Richtlinienkonfiguration

Die zuvor beschriebenen Schritte zu Erstellung der Richtlinie am Beispiel des Service EC2 müssen nun für die weiteren Services, welche mit Docusnap inventarisiert werden sollen, wiederholt werden.

Erstellen Sie die entsprechenden Richtlinien für die Bereiche:

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

2.2 Benutzer konfigurieren

Die zuvor erstellten Richtlinien werden nun einem Benutzer zugewiesen. Wechseln Sie innerhalb von AWS erneut in die Services – IAM und wählen im nächsten Schritt Benutzer aus.

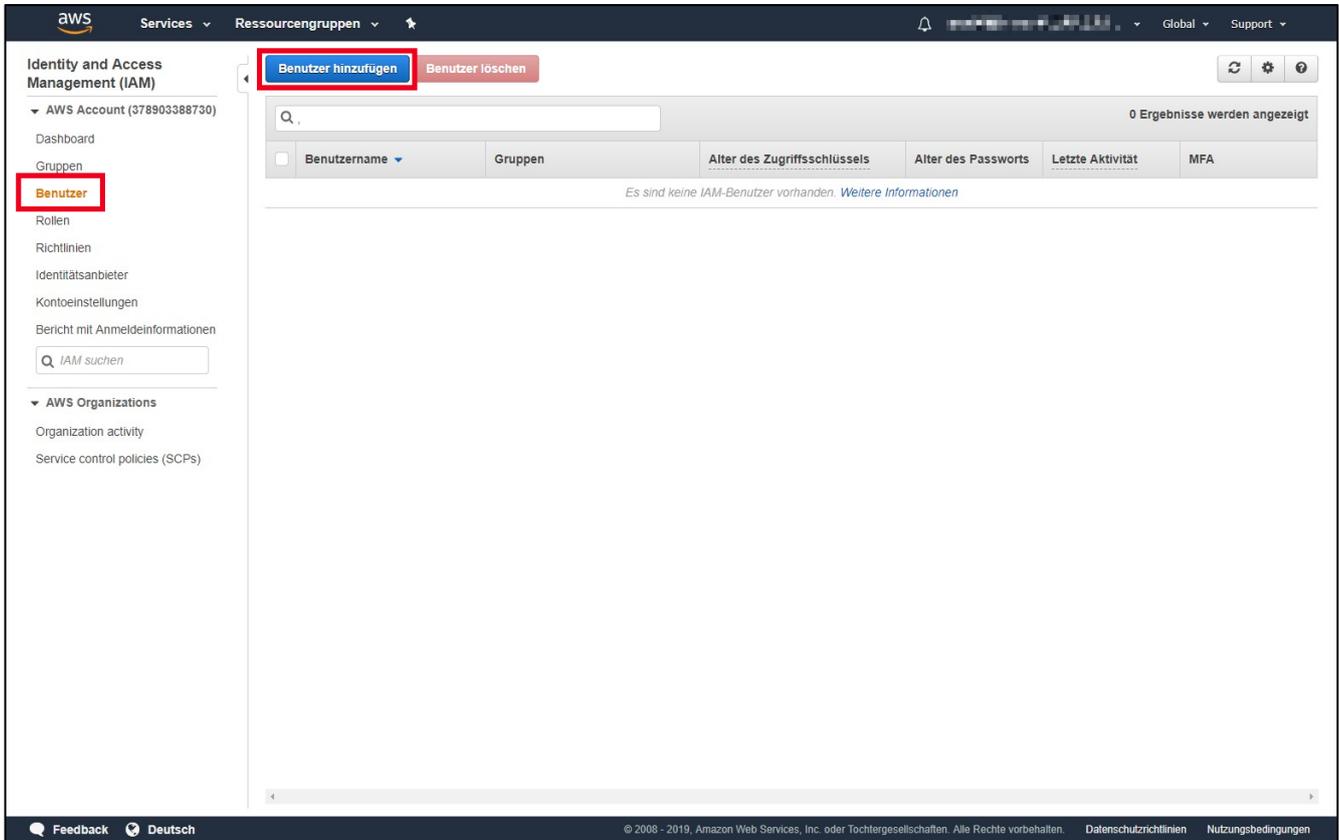


Abbildung 6 - Benutzerverwaltung der Amazon Web Services

Wichtig: Die Anordnung der abgebildeten Daten in der Docusnap Baumstruktur orientiert sich anhand des inventarisierenden Benutzers, dies hat die eingangs beschriebene Regionsbindung als Hintergrund. Wählen Sie hier bitte für verschiedene Regionen einschlägige Benutzernamen aus, um diese eindeutig zuweisen zu können.

2.2.1 Benutzer anlegen

Über Benutzer hinzufügen können Sie einen neuen Benutzer erstellen. Ein Benutzername und AWS-Zugriffstyp werden benötigt.

Als AWS-Zugriffstyp wählen Sie **Programmgesteuerter Zugriff** aus, über den Button **Weiter: Berechtigungen** kommen Sie zum nächsten Schritt.

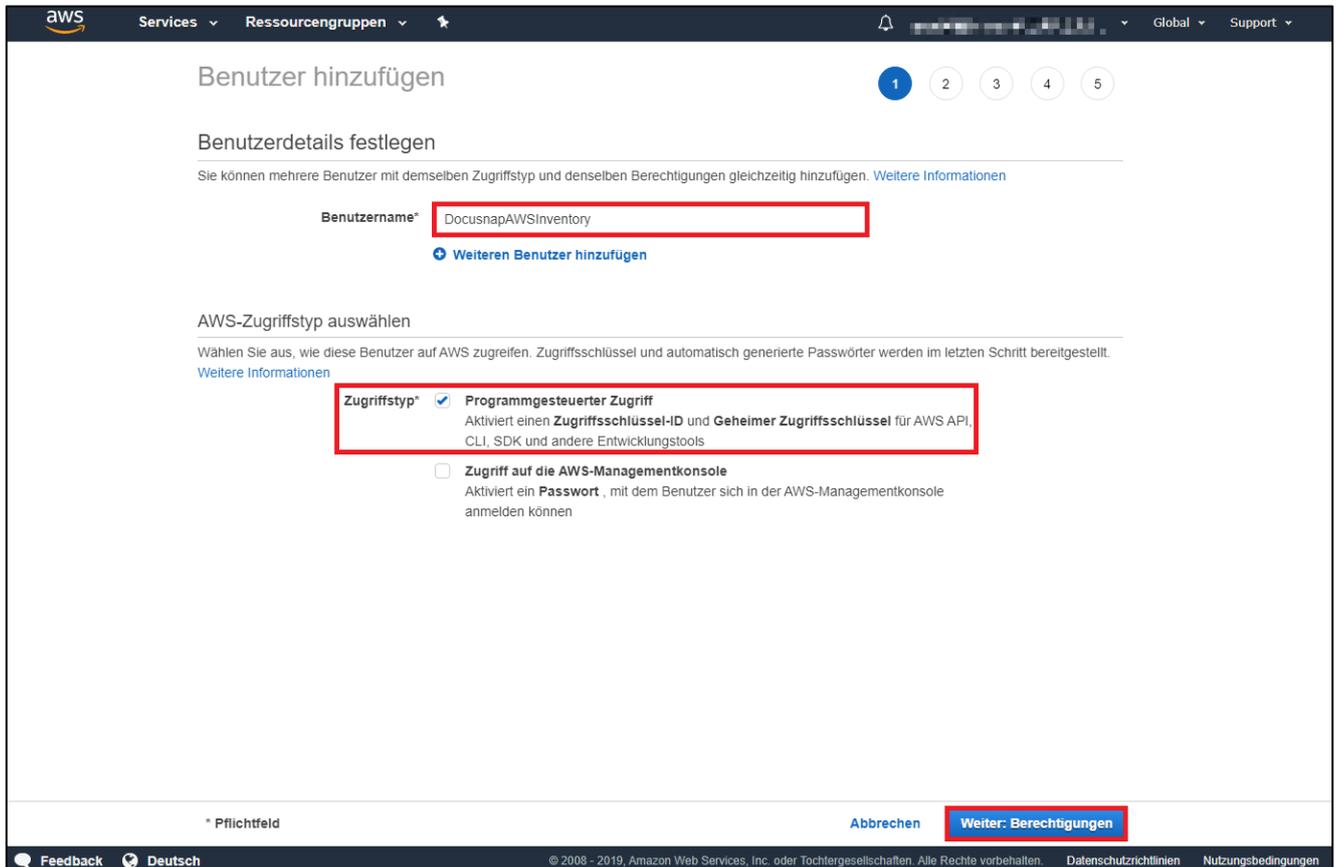


Abbildung 7 - Festlegung der Benutzerdetails für den Inventarisierungsaccount

2.2.2 Berechtigungen festlegen

Hier bieten sich Ihnen zwei verschiedene Möglichkeiten, Ihren Benutzer zur Inventarisierung zu berechtigen.

- Benutzer zur Gruppe hinzufügen
Diese Option kann gewählt werden, sollten Sie die erstellten Richtlinien an eine Gruppe vergeben wollen. Es empfiehlt sich jedoch, die Inventarisierung stets mit dem gleichen Benutzer durchzuführen.
- Vorhandene Richtlinien direkt anfügen
Diese Option wird in diesem HowTo beschrieben, um die vorab erstellten Richtlinien direkt an einen Benutzer zu binden.

Wählen Sie **Vorhandene Richtlinien direkt anfügen** und navigieren Sie zur Option **Filterrichtlinien** und setzen den Filter auf **Vom Kunden verwaltet**. Wählen Sie nun die erstellten Richtlinien und fügen sie diesem Benutzer hinzu.

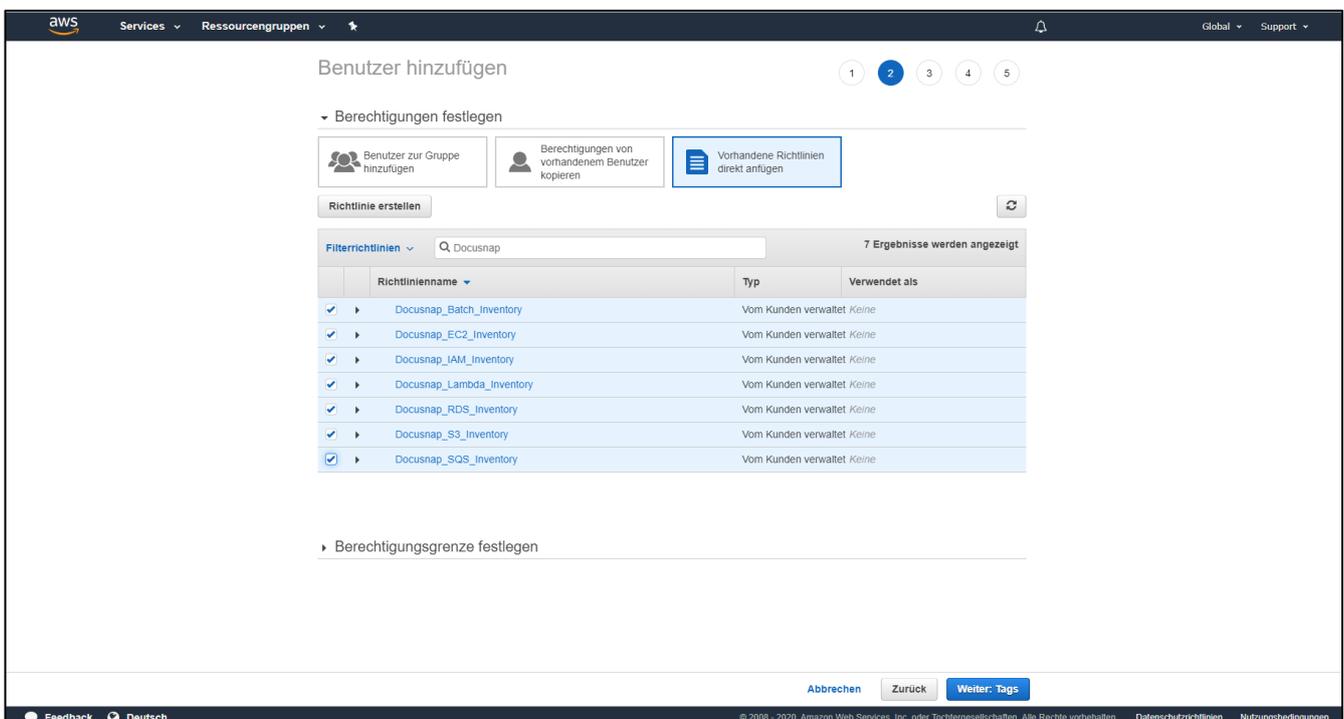


Abbildung 8 - Zuweisung der erstellten Richtlinien für die Docusnap Inventarisierung

2.2.3 Benutzerschlüssel für die Inventarisierung erhalten

Wichtig: Die abschließend erstellten Daten (Benutzer, Zugriffsschlüssel-ID sowie der geheime Zugriffsschlüssel) werden zur Inventarisierung benötigt und können als CSV heruntergeladen werden. Diese sind nur einmalig nach der Konfiguration einsehbar!

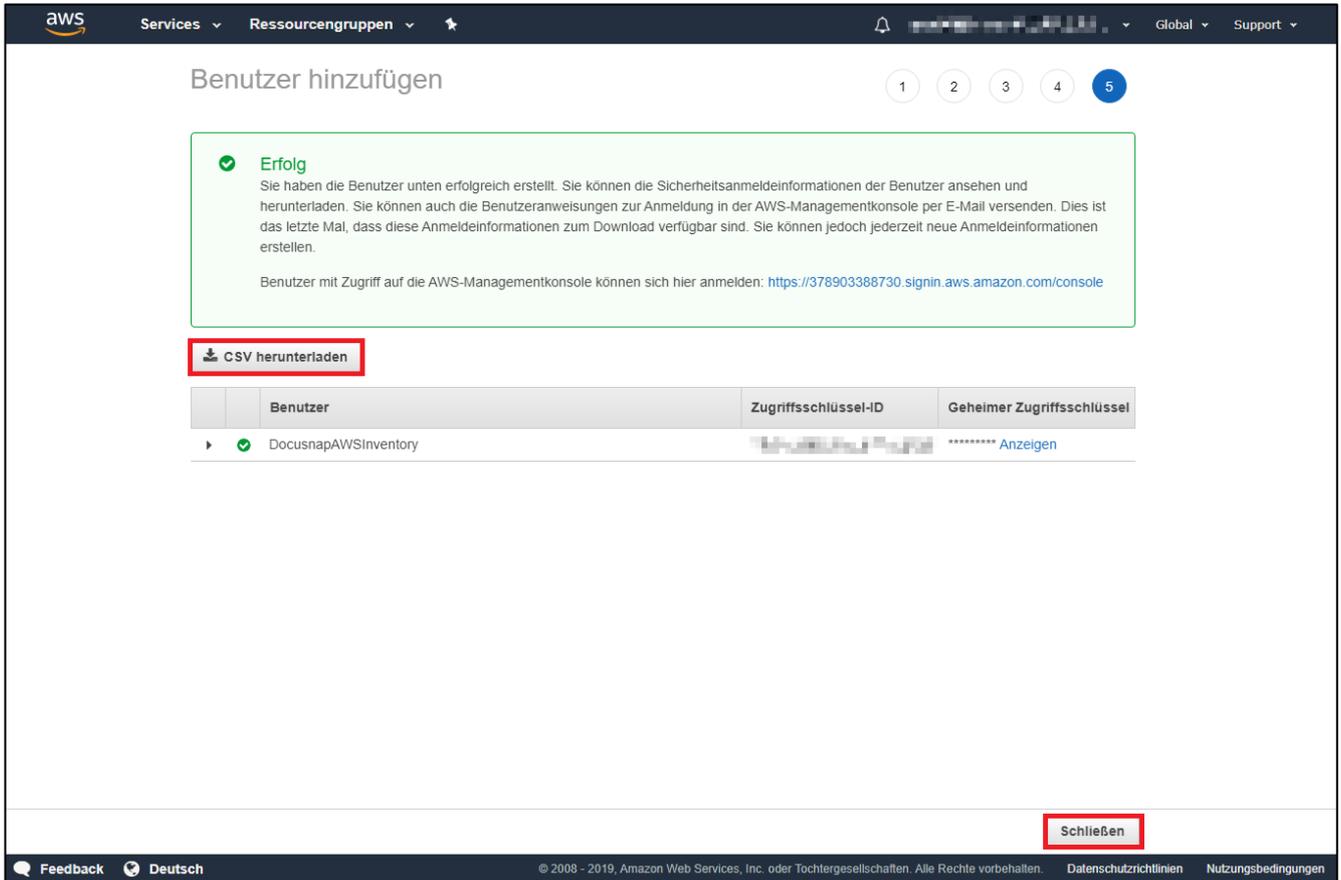


Abbildung 9 - Nach Abschluss der Benutzererstellung erhalten Sie Ihre Schlüssel

3. Inventarisierung der AWS in Docusnap

Der angelegte Benutzer wird nun in Kombination mit den erstellten Schlüsseln verwendet, um die Inventarisierung in Docusnap durchzuführen.

Dazu öffnen Sie bitte den Assistenten **AWS** innerhalb des Bereichs **Inventar**. Sollten Sie die Steuerfläche für die AWS Inventarisierung nicht sehen, können Sie diese über **Alle Assistenten** aufrufen.

Anschließend wählen Sie Ihren Mandanten, im Folgedialog die Domäne, welcher die Ergebnisse der Inventarisierung zugeordnet werden sollen, sowie den Discovery Service aus und tragen dann den erstellten Benutzer im Feld **Anzeigename** sowie die entsprechend generierten Schlüssel ein.

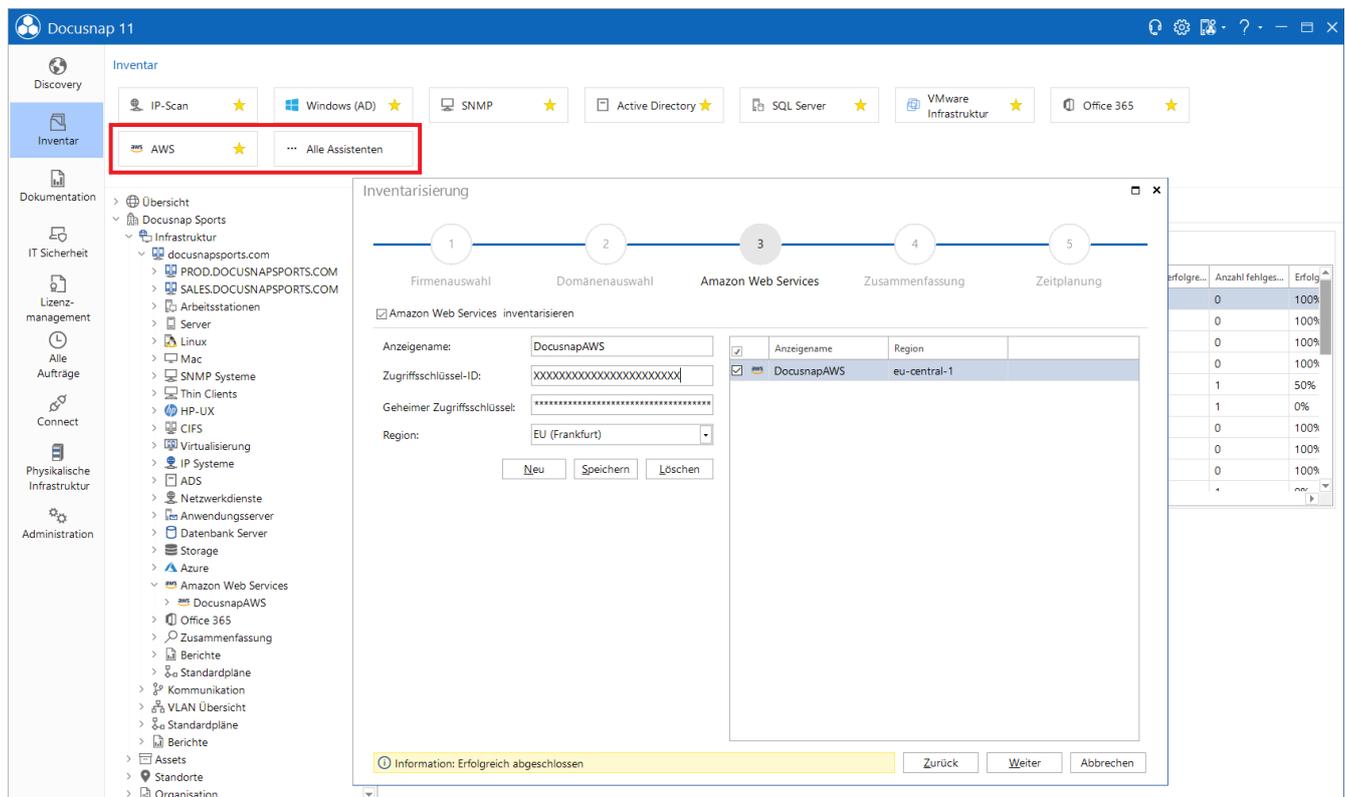


Abbildung 10 - Die erstellen Schlüssel werden im Assistenten eingetragen

Nach erfolgreicher Speicherung sehen Sie über **Weiter** eine Kurzzusammenfassung und können im letzten Schritt definieren, ob Sie die Inventarisierung zeitgesteuert einplanen möchten.

ABBILDUNGSVERZEICHNIS

ABBILDUNG 1 - AWS INVENTARISIERUNGSASSISTENT.....	5
ABBILDUNG 2- DIE KONFIGURATION DER RICHTLINIEN UND BENUTZER FINDET IM BEREICH IAM STATT.....	6
ABBILDUNG 3 - DIE RICHTLINIENVERWALTUNG DER AMAZON WEB SERVICES	7
ABBILDUNG 4 - „RICHTLINIE PRÜFEN“ FÜHRT SIE ZUM NÄCHSTEN SCHRITT DER KONFIGURATION.....	8
ABBILDUNG 5 - ABSCHLUSS DER RICHTLINIENKONFIGURATION	9
ABBILDUNG 6 - BENUTZERVERWALTUNG DER AMAZON WEB SERVICES	10
ABBILDUNG 7 - FESTLEGUNG DER BENUTZERDETAILS FÜR DEN INVENTARISIERUNGSACCOUNT	11
ABBILDUNG 8 - ZUWEISUNG DER ERSTELLTEN RICHTLINIEN FÜR DIE DOCUSNAP INVENTARISIERUNG.....	12
ABBILDUNG 9 - NACH ABSCHLUSS DER BENUTZERERSTELLUNG ERHALTEN SIE IHRE SCHLÜSSEL	13
ABBILDUNG 10 - DIE ERSTELLEN SCHLÜSSEL WERDEN IM ASSISTENTEN EINGETRAGEN.....	14

VERSIONSHISTORIE

Datum	Beschreibung
04.10.2019	Version 1.0 – Beschreibung des Inventarisierungsmoduls „Amazon Web Services“
22.04.2020	Version 2.0 - Überarbeitung des HowTos für Docusnap 11
