



AWS

Inventarisierung der Amazon Web Services (AWS)

TITEL	AWS
AUTOR	DocuSnap Consulting
DATUM	12.12.2023
VERSION	3.0 gültig ab 21.12.2022

Die Weitergabe, sowie Vervielfältigung dieser Unterlage, auch von Teilen, Verwertung und Mitteilung ihres Inhaltes ist nicht gestattet, soweit nicht ausdrücklich durch die itelio 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 itelio GmbH. All rights reserved.

INHALTSVERZEICHNIS

1. Einleitung	4
2. Voraussetzungen	5
3. Richtlinien erstellen	5
4. Benutzer konfigurieren	6
5. Inventarisierung der AWS in DocuSnap	7

1. Einleitung

Der Scan der Amazon Web Services liefert die Möglichkeit, Kernbereiche Ihrer AWS Infrastruktur zu inventarisieren:

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

Für die AWS Inventarisierung sind zwei Assistenten in DocuSnap verfügbar. Der Unterschied der Assistenten liegt in der Ablage der inventarisierten Daten.

- AWS
 - Daten sind unterhalb der Cloud Infrastruktur – Tenant Domäne zu finden
- AWS – Legacy
 - Daten sind unterhalb der Infrastruktur - Domäne - Azure zu finden

Damit alle Daten der Cloud Inventarisierungen in der Cloud Infrastruktur zu finden sind, empfehlen wir die Verwendung der Assistenten, die nicht als Legacy bezeichnet sind:

- Microsoft 365
- Azure Service
- AWS

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. Voraussetzungen

Für die AWS Inventarisierung werden Richtlinien für jeden der zu inventarisierenden Kernbereiche benötigt. Die Richtlinien werden anschließend einem Benutzer, für den Programmgesteuerten Zugriff zugewiesen. Diese Zuordnung aktiviert eine Zugriffsschlüssel-ID und einen Geheimen Zugriffsschlüssel.

Für die Erstellung der Richtlinien wird ein entsprechend berechtigter Benutzer benötigt:

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

Für die eigentliche Inventarisierung werden die folgenden Daten, pro Region, benötigt:

- Anzeigename
- Zugriffsschlüssel-ID
- Geheimer Zugriffsschlüssel
- Region

3. Richtlinien erstellen

Für jeden Kernbereich / Service, den Sie verwenden und mit DocuSnap inventarisieren möchten, wird eine eigene Richtlinie benötigt. Sie benötigen also bis zu 7 Richtlinien für:

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

Melden Sie sich in Ihrer AWS Konsole und öffnen Sie

- Services - IAM
- Richtlinien – Richtlinien erstellen

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, z. B. EC2
- **Aktionen**
Die in **EC2** zulässigen Aktionen werden auf Zugriffsebene **Auflisten** sowie **Lesen** gesetzt.
- **Ressourcen**
Es wird empfohlen, die Aktionen über **Alle Ressourcen** der Services zu berechtigen.

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.

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.

4. Benutzer konfigurieren

Die zuvor erstellten Richtlinien werden nun einem Benutzer zugewiesen. Wechseln Sie innerhalb von AWS erneut in die

- **Services - IAM** – und wählen Sie nun **Benutzer – Benutzer hinzufügen**

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

- Vergeben Sie einen eindeutigen **Benutzernamen**
- Wählen Sie den Zugriffstyp: **Programmgesteuerter Zugriff**

Im nächsten Schritt weisen Sie die erstellten Richtlinien dem Benutzer zu – wählen Sie

- Vorhandene Richtlinien direkt anfügen
- 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.

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!

5. Inventarisierung der AWS in Docusnap

Starten Sie den AWS Inventarisierungs-Assistenten:

- Discovery – Alle Assistenten – AWS
- Inventar – Alle Assistenten – AWS
- Alle Aufträge – Alle Assistenten – AWS

Wählen Sie die gewünschte Firma und Tenant-Domäne aus.

Im Anzeigenamen sollten Sie den Namen des Benutzers angeben, für den Sie daraufhin die

- Zugriffsschlüssel-ID
- Geheimer Zugriffsschlüssel
- und Region

hinterlegen.

ABBILDUNGSVERZEICHNIS

ES KONNTEN KEINE EINTRÄGE FÜR EIN ABBILDUNGSVERZEICHNIS GEFUNDEN WERDEN.

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
21.12.2022	Version 3.0 – Überarbeitung des HowTos für Docusnap 12
