Identifizierung und Sicherung von Artefakten in Infrastructure-as-a-Service Plattformen

14. Mai 2024

Fakultät für Ingenieurwissenschaften

Simon Bauer

www.hs-wismar.de

HOCHSCHULE WISMAR
UNIVERSITY OF APPLIED SCIENCES
TECHNOLOGY, BUSINESS AND DESIGN

Inhalt

1 Motivation

2 Grundlagen

3 Leitfaden

4 Evaluierung

Motivation

Motivation

1. Weite Adaption der Cloud Technologie
   - □ als eigene Infrastruktur
   - □ bestehenden Infrastruktur ergänzen
   - □ Bereitstellung von Dienstleistungen
2. Vorteile
3. Risiken: Rollen bei Cyberkriminalität

Motivation

1. Weite Adaption der Cloud Technologie
   - als eigene Infrastruktur
   - bestehenden Infrastruktur ergänzen
   - Bereitstellung von Dienstleistungen
2. Vorteile
   - finanzielle Einsparungen
   - Skalierbarkeit
   - Flexibilität
   - Schutz vor Datenverlust
3. Risiken: Rollen bei Cyberkriminalität

Motivation

1. Weite Adaption der Cloud Technologie
   - als eigene Infrastruktur
   - bestehenden Infrastruktur ergänzen
   - Bereitstellung von Dienstleistungen
2. Vorteile
   - finanzielle Einsparungen
   - Skalierbarkeit
   - Flexibilität
   - Schutz vor Datenverlust
3. Risiken: Rollen bei Cyberkriminalität
   - aktiver Part
   - passiver Part
   - als Werkzeug

Grundlagen

Grundlagen– Digitale Forensik

nach McKemmish[McK99]

1. Identification
2. Preservation
3. Analysis
4. Presentation

nach NIST [KCG06]

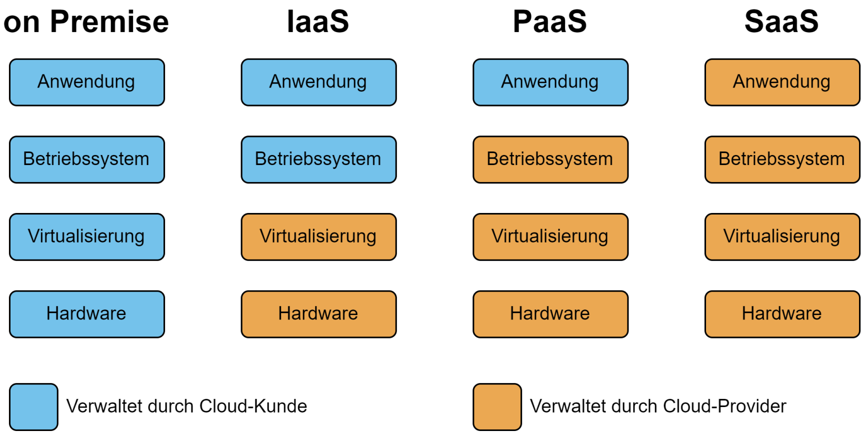
1. Collection
2. Examination
3. Analysis
4. Reporting

Grundlagen– Cloud Computing

Definition nach NIST[MG^{+}11]

- On-demand self-service
- Broad Network access
- Resource pooling
- Rapid elasticity
- Measured Service

Grundlagen– Cloud Computing



on Premise	IaaS	PaaS	SaaS
🟦 Anwendung	🟦 Anwendung	🟦 Anwendung	🟧 Anwendung
🟦 Betriebssystem	🟦 Betriebssystem	🟧 Betriebssystem	🟧 Betriebssystem
🟦 Virtualisierung	🟧 Virtualisierung	🟧 Virtualisierung	🟧 Virtualisierung
🟦 Hardware	🟧 Hardware	🟧 Hardware	🟧 Hardware

🟦 Verwaltet durch Cloud-Kunde

🟧 Verwaltet durch Cloud-Provider

Bild 1: Service Modelle

Grundlagen– Cloud Computing

Einsatzmöglichkeiten

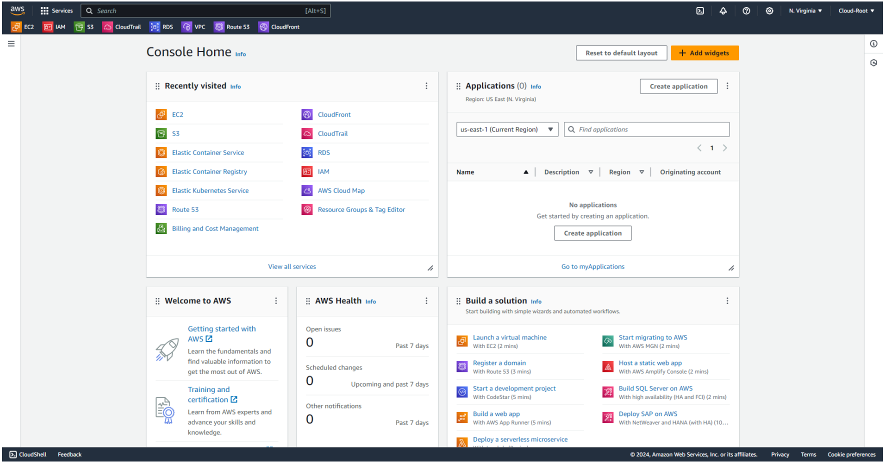
- Privat Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud

Grundlagen– Cloud Computing – Praktische Grundlagen

Interaktion IaaS nur über API möglich:

- Webinterface
- Command Line Interface
- Software Development Kits
- (per Hand)

Grundlagen– AWS Webinterface



Console Home Info

Recently visited Info

- EC2
- S3
- Elastic Container Service
- Elastic Container Registry
- Elastic Kubernetes Service
- Route 53
- Billing and Cost Management
- CloudFront
- CloudTrail
- RDS
- IAM
- AWS Cloud Map
- Resource Groups & Tag Editor

View all services

Applications (0) Info

Create application

Region: US East (N. Virginia)

us-east-1 (Current Region) ▼

Find applications

‹ 1 ›

Name ▲	Description ▽	Region ▽	Originating account

No applications

Get started by creating an application.

Create application

Go to myApplications

Welcome to AWS

Getting started with AWS

Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification

Learn from AWS experts and advance your skills and knowledge.

AWS Health Info

Open issues

0 Past 7 days

Scheduled changes

0 Upcoming and past 7 days

Other notifications

0 Past 7 days

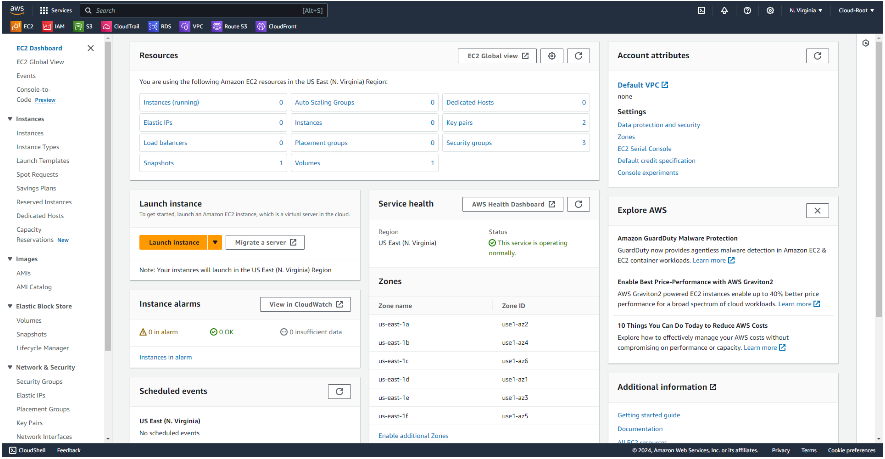
Build a solution Info

Start building with simple wizards and automated workflows.

- Launch a virtual machine – With EC2 (2 mins)
- Register a domain – With Route 53 (3 mins)
- Start a development project – With CodeStar (5 mins)
- Build a web app – With AWS App Runner (5 mins)
- Deploy a serverless microservice
- Start migrating to AWS – With AWS MGN (2 mins)
- Host a static web app – With AWS Amplify Console (2 mins)
- Build SQL Server on AWS – With high availability (HA and FCI) (2 mins)
- Deploy SAP on AWS – With NetWeaver and HANA (with HA) (10…

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Grundlagen– AWS Webinterface



EC2 Dashboard
EC2 Global View
Events
Console-to-Code Preview

▼ Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New

▼ Images
AMIs
AMI Catalog

▼ Elastic Block Store
Volumes
Snapshots
Lifecycle Manager

▼ Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces

Resources

EC2 Global view

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0	Key pairs	2
Load balancers	0	Placement groups	0	Security groups	3
Snapshots	1	Volumes	1		

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▾ Migrate a server

Note: Your instances will launch in the US East (N. Virginia) Region

Instance alarms

View in CloudWatch

⚠ 0 in alarm ✓ 0 OK ⊖ 0 insufficient data

Instances in alarm

Scheduled events

US East (N. Virginia)
No scheduled events

Service health

AWS Health Dashboard

Region: US East (N. Virginia)
Status: ✓ This service is operating normally.

Zones

Zone name	Zone ID
us-east-1a	use1-az2
us-east-1b	use1-az4
us-east-1c	use1-az6
us-east-1d	use1-az1
us-east-1e	use1-az3
us-east-1f	use1-az5

Enable additional Zones

Account attributes

Default VPC
none

Settings
Data protection and security
Zones
EC2 Serial Console
Default credit specification
Console experiments

Explore AWS

Amazon GuardDuty Malware Protection
GuardDuty now provides agentless malware detection in Amazon EC2 & EC2 container workloads. Learn more

Enable Best Price-Performance with AWS Graviton2
AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn more

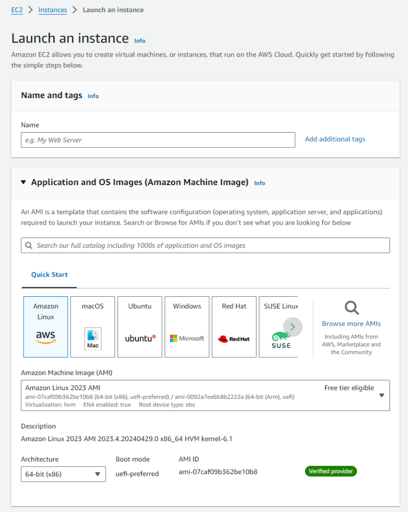
10 Things You Can Do Today to Reduce AWS Costs
Explore how to effectively manage your AWS costs without compromising on performance or capacity. Learn more

Additional information

Getting started guide
Documentation
All EC2 resources

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Grundlagen– AWS Webinterface



EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name

e.g. My Web Server

Add additional tags

▼ **Application and OS Images (Amazon Machine Image)** Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible

ami-07caf09b362be10b8 (64-bit (x86), uefi-preferred) / ami-0092a7ee6b8b2222a (64-bit (Arm), uefi)

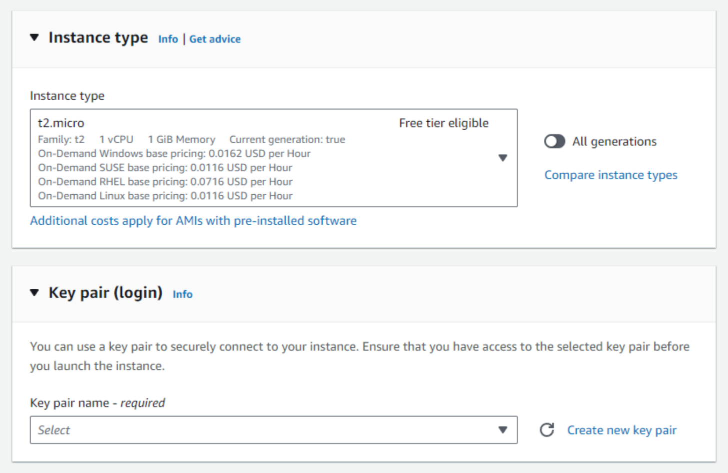
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.4.20240429.0 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	
64-bit (x86) ▼	uefi-preferred	ami-07caf09b362be10b8	Verified provider

Grundlagen– AWS Webinterface



▼ Instance type Info | Get advice

Instance type

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

○ All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) Info

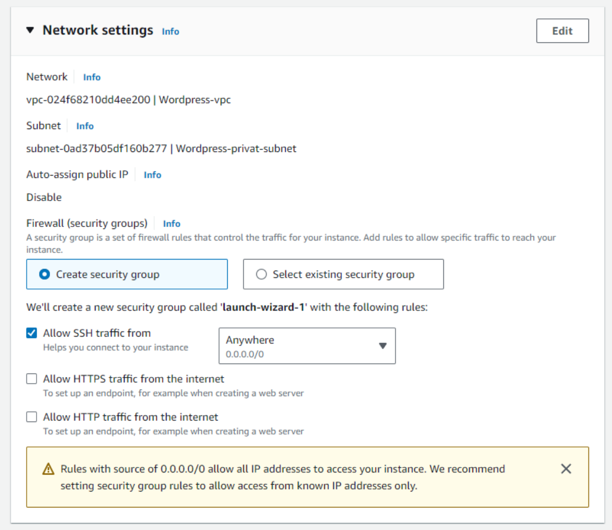
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select ▼

Create new key pair

Grundlagen– AWS Webinterface



▼ Network settings Info

Edit

Network Info

vpc-024f68210dd4ee200 | Wordpress-vpc

Subnet Info

subnet-0ad37b05df160b277 | Wordpress-privat-subnet

Auto-assign public IP Info

Disable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**launch-wizard-1**' with the following rules:

☑ Allow SSH traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0

☐ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Grundlagen– AWS Command Line Interface

```
aws ec2 run-instances --image-id ami-1 --instance-type t2.micro --region us-east-1
```

Grundlagen– AWS Command Line Interface

```
aws ec2 run-instances --image-id ami-1 --instance-type t2.micro --region us-east-1
```

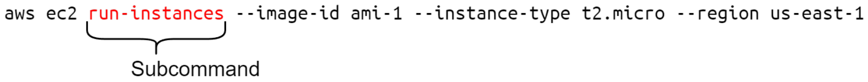
$\underbrace{\texttt{aws}}_{\text{AWS Programm}}$

Grundlagen– AWS Command Line Interface

```
aws ec2 run-instances --image-id ami-1 --instance-type t2.micro --region us-east-1
```

Command

Grundlagen– AWS Command Line Interface



```
aws ec2 run-instances --image-id ami-1 --instance-type t2.micro --region us-east-1
```

Subcommand

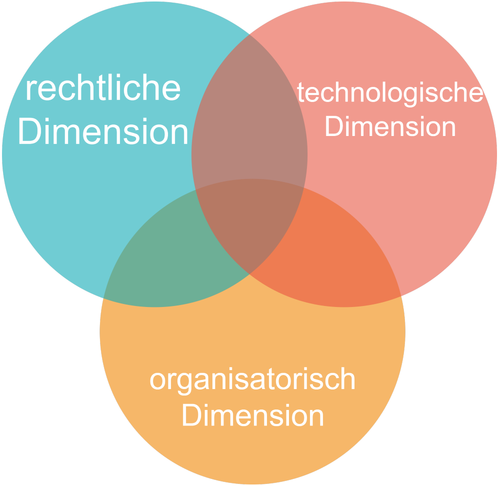
Grundlagen– AWS Command Line Interface

```
aws ec2 run-instances --image-id ami-1 --instance-type t2.micro --region us-east-1
```

Parameter

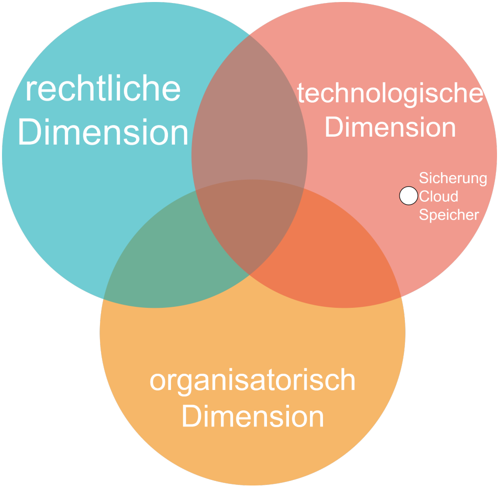
Leitfaden

Leitfaden – Herausforderungen



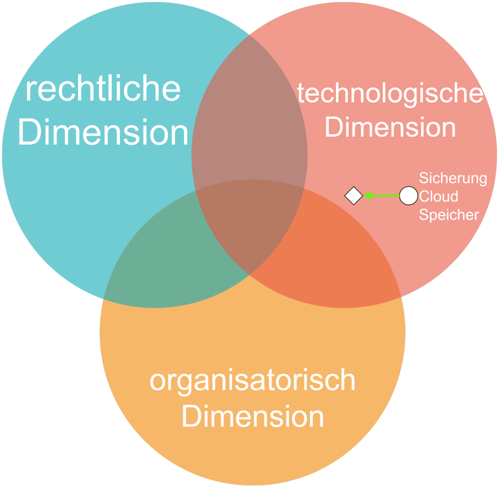
Cloud Forensik als multidimensionales Feld[RCKC11]

Leitfaden – Herausforderungen



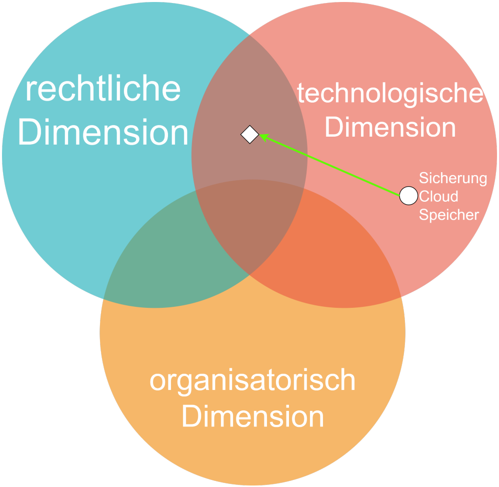
Cloud Forensik als multidimensionales Feld[RCKC11]

Leitfaden – Herausforderungen



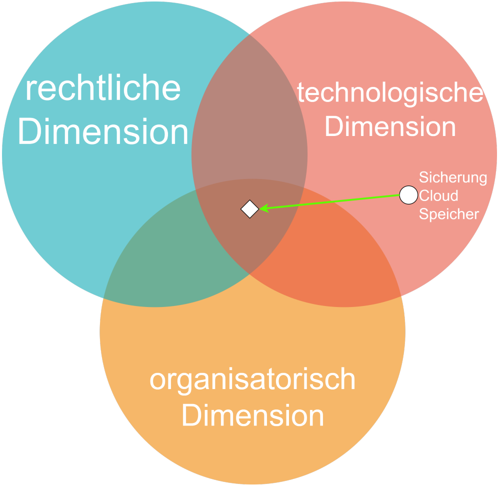
Cloud Forensik als multidimensionales Feld[RCKC11]

Leitfaden – Herausforderungen



Cloud Forensik als multidimensionales Feld[RCKC11]

Leitfaden – Herausforderungen



Cloud Forensik als multidimensionales Feld[RCKC11]

Leitfaden– Herausforderungen

Warum können klassische Methoden nicht genutzt werden?

- einhergehender Kontrollverlust
- global verteilte Daten
- kein Zutritt zu Rechenzentren
- ’Live’ Umgebung
- fehlende Schnittstellen

Leitfaden – Herausforderungen

- Log capture (Protokollerfassung)
- Live forensics
- Data integrity and evidence preservation (Beweisintegrität)
- Data Acquisition (Datensicherung)
- Data Provenance (Datenherkunft)
- Semantic Integrity (Datensemantik)

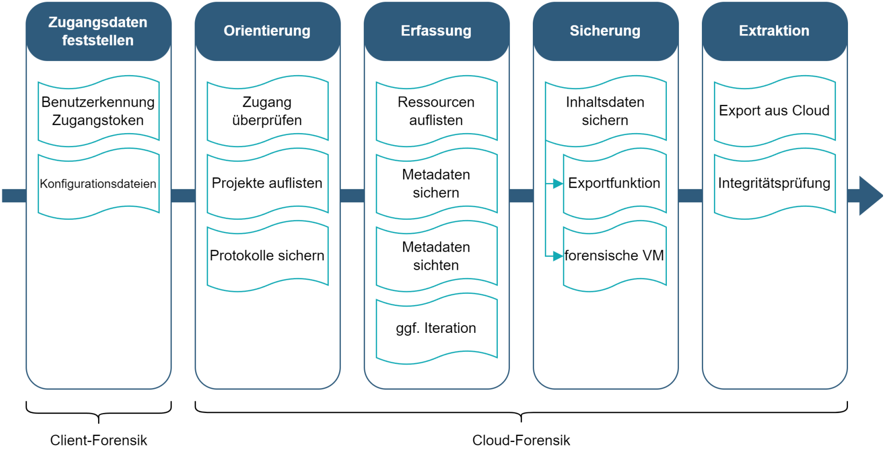
Leitfaden – bestehende Methoden

- An integrated conceptual digital forensic framework for cloud computing[MC12]
  - Iteration, wenn Cloud-Nutzung in Analyse festgestellt wird
- Remote Programmatic vCloud Forensics[MC14]
  - Beschaffen von Zugangsdaten
  - Reihenfolge der Sicherung: Logs, Metadaten, Inhaltsdaten

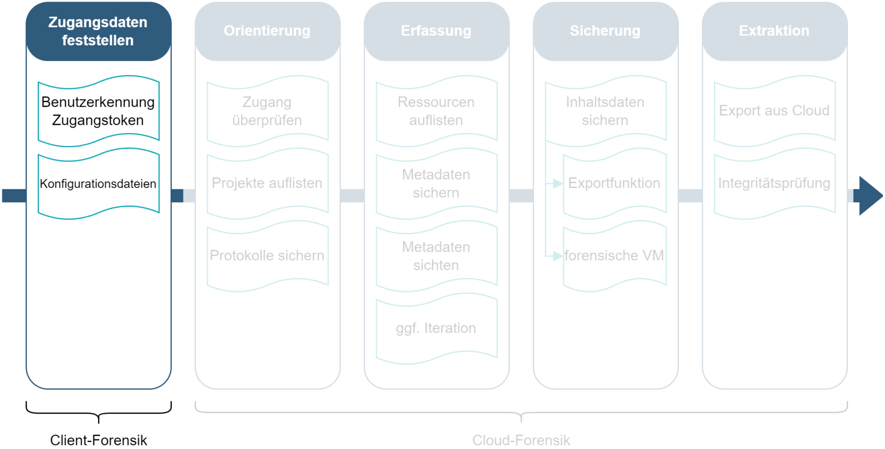
Leitfaden – bestehende Methoden

- Cloud Based Framework for Performing Digital Forensic Investigations[PWG+22]
  - Vorbereitung: rechtlicher Rahmen der Untersuchung, verfügbare Werkzeuge
  - Identifikations-Phase: Suche und Identifizierung von Beweisquellen
  - Sicherungs-Phase: Sicherung der Beweisquellen
  - Analyse-Phase: Untersuchung der gesicherten Artefakte
  - Rekonstruktions-Phase: Timeline der Ereignisse
  - Präsentations-Phase: Darstellung der Artefakte und Schlussfolgerungen

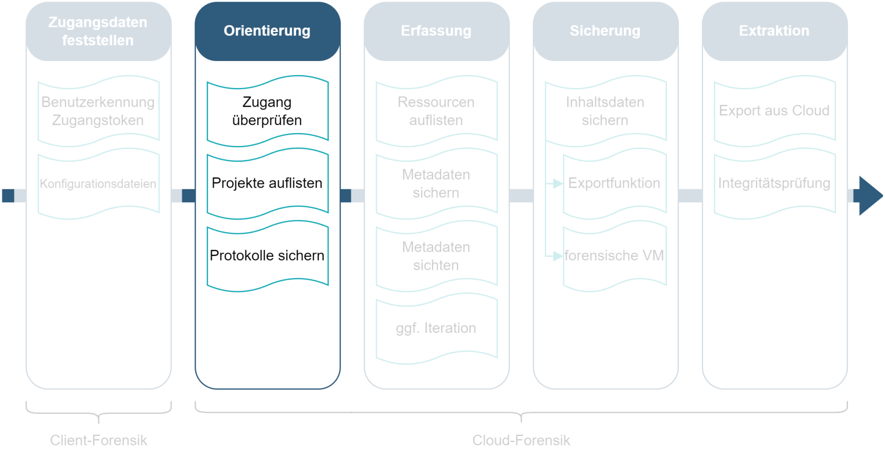
Leitfaden


Zugangsdaten feststellen
Benutzerkennung Zugangstoken
Konfigurationsdateien
Orientierung
Zugang überprüfen
Projekte auflisten
Protokolle sichern
Erfassung
Ressourcen auflisten
Metadaten sichern
Metadaten sichten
ggf. Iteration
Sicherung
Inhaltsdaten sichern
Exportfunktion
forensische VM
Extraktion
Export aus Cloud
Integritätsprüfung
Client-Forensik
Cloud-Forensik

Leitfaden


Zugangsdaten feststellen
Benutzerkennung Zugangstoken
Konfigurationsdateien
Orientierung
Zugang überprüfen
Projekte auflisten
Protokolle sichern
Erfassung
Ressourcen auflisten
Metadaten sichern
Metadaten sichten
ggf. Iteration
Sicherung
Inhaltsdaten sichern
Exportfunktion
forensische VM
Extraktion
Export aus Cloud
Integritätsprüfung
Client-Forensik
Cloud-Forensik

Leitfaden



Zugangsdaten feststellen
- Benutzerkennung Zugangstoken
- Konfigurationsdateien

Orientierung
- Zugang überprüfen
- Projekte auflisten
- Protokolle sichern

Erfassung
- Ressourcen auflisten
- Metadaten sichern
- Metadaten sichten
- ggf. Iteration

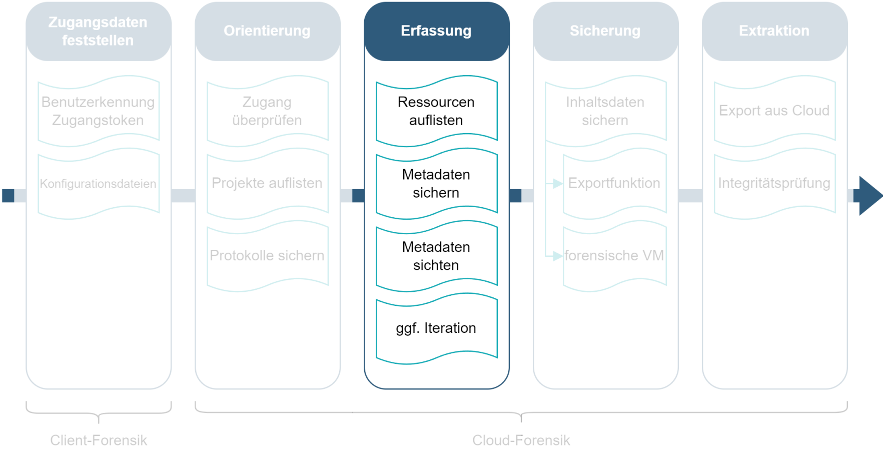
Sicherung
- Inhaltsdaten sichern
- Exportfunktion
- forensische VM

Extraktion
- Export aus Cloud
- Integritätsprüfung

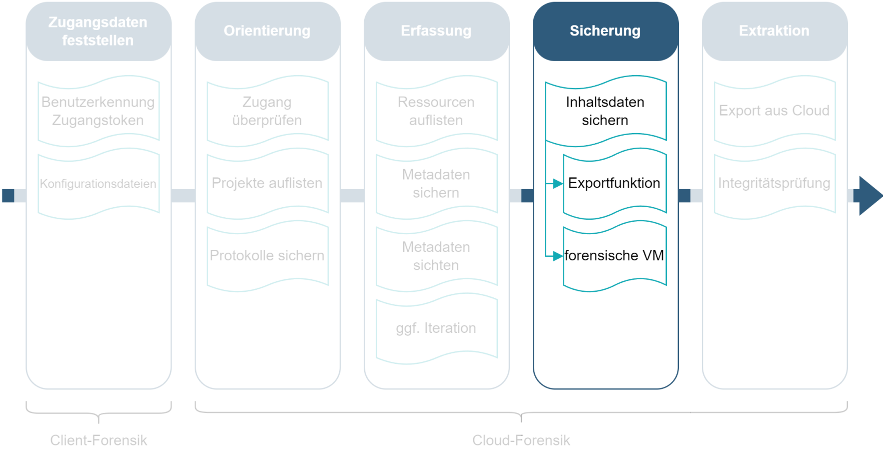
Client-Forensik

Cloud-Forensik

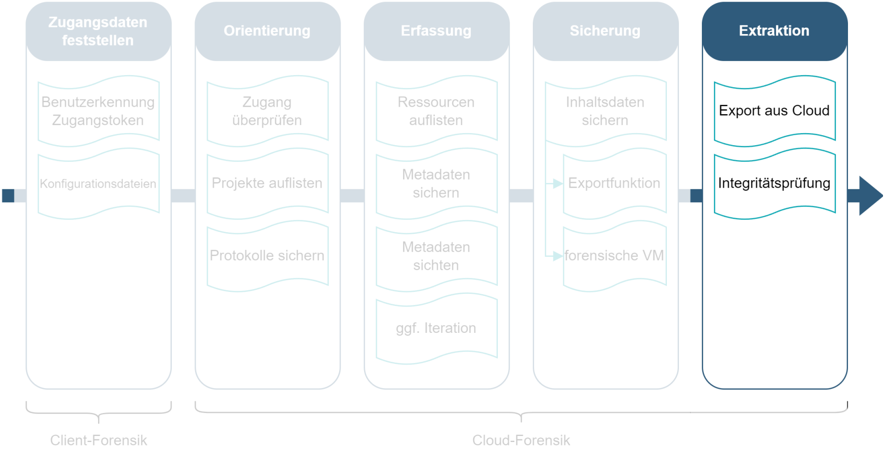
Leitfaden


Zugangsdaten feststellen
Benutzerkennung Zugangstoken
Konfigurationsdateien
Orientierung
Zugang überprüfen
Projekte auflisten
Protokolle sichern
Erfassung
Ressourcen auflisten
Metadaten sichern
Metadaten sichten
ggf. Iteration
Sicherung
Inhaltsdaten sichern
Exportfunktion
forensische VM
Extraktion
Export aus Cloud
Integritätsprüfung
Client-Forensik
Cloud-Forensik

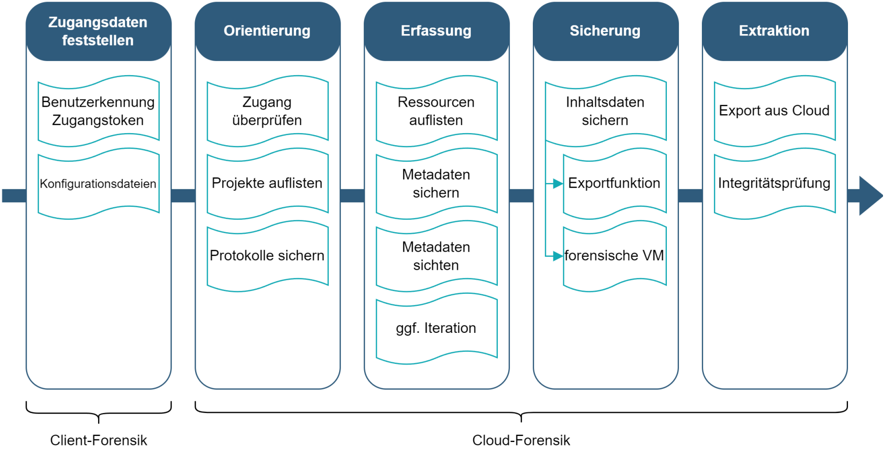
Leitfaden


Zugangsdaten feststellen
Benutzerkennung Zugangstoken
Konfigurationsdateien
Orientierung
Zugang überprüfen
Projekte auflisten
Protokolle sichern
Erfassung
Ressourcen auflisten
Metadaten sichern
Metadaten sichten
ggf. Iteration
Sicherung
Inhaltsdaten sichern
Exportfunktion
forensische VM
Extraktion
Export aus Cloud
Integritätsprüfung
Client-Forensik
Cloud-Forensik

Leitfaden


Zugangsdaten feststellen
Benutzerkennung Zugangstoken
Konfigurationsdateien
Orientierung
Zugang überprüfen
Projekte auflisten
Protokolle sichern
Erfassung
Ressourcen auflisten
Metadaten sichern
Metadaten sichten
ggf. Iteration
Sicherung
Inhaltsdaten sichern
Exportfunktion
forensische VM
Extraktion
Export aus Cloud
Integritätsprüfung
Client-Forensik
Cloud-Forensik

Leitfaden



Zugangsdaten feststellen
- Benutzerkennung Zugangstoken
- Konfigurationsdateien

Orientierung
- Zugang überprüfen
- Projekte auflisten
- Protokolle sichern

Erfassung
- Ressourcen auflisten
- Metadaten sichern
- Metadaten sichten
- ggf. Iteration

Sicherung
- Inhaltsdaten sichern
- Exportfunktion
- forensische VM

Extraktion
- Export aus Cloud
- Integritätsprüfung

Client-Forensik

Cloud-Forensik

Evaluierung

Evaluierung

- Auswahl der Cloud Service Provider

- Gestaltung der Szenarien

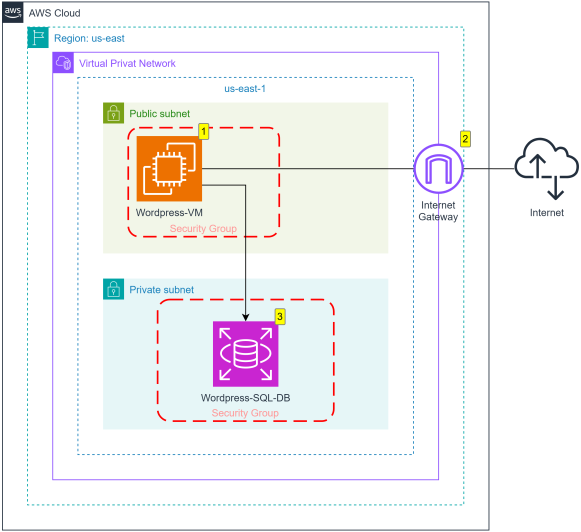
Evaluierung

- Auswahl der Cloud Service Provider
  - Amazon Web Services (AWS)
  - Microsoft Azure
  - Google Cloud Platform
- Gestaltung der Szenarien

Evaluierung

- Auswahl der Cloud Service Provider
    - Amazon Web Services (AWS)
    - Microsoft Azure
    - Google Cloud Platform
- Gestaltung der Szenarien
    - Wordpress-Anwendung mit externer Datenbank
    - statische Website mit Content Delivery Network

Evaluierung– AWS Wordpress



Evaluierung– AWS Wordpress

Orientierung

- eigener Zugang auf Berechtigungen überprüfen
- API-Protokolle exportieren

Erfassung

- Ressourcen finden
  - □ `aws resourcegroupstaggingapi get-resources`
  - □ Tag Editor
  - □ ’Brute-Force’
- Ressourcen erfassen
  - □ `aws ec2 describe-...`

Evaluierung– AWS Wordpress

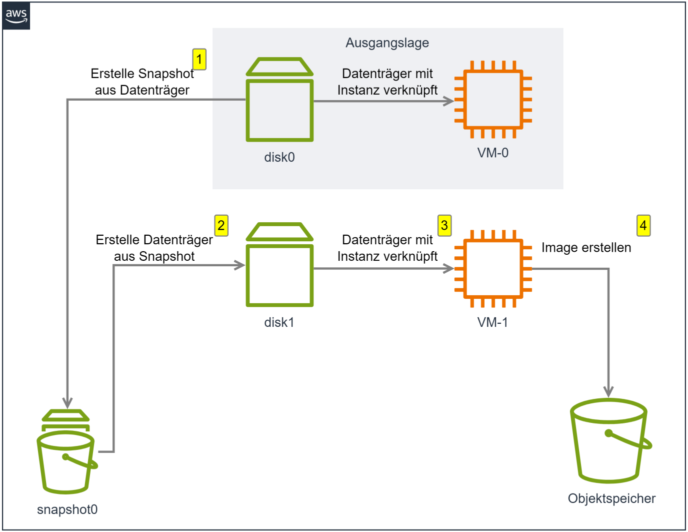
Sicherung

- Snapshot der VM erstellen: `aws ec2 create-snapshot`
- Snapshot mithilfe einer forensischen VM sichern
- Arbeitsspeicher der VM sichern: `avml`
- Datenbank sichern: `mysqldump`

Extraktion

- `aws s3 sync s3://wordpress-forensic-bucket ./s3/`

Evaluierung– AWS Snapshot sichern


aws
Ausgangslage
1
Erstelle Snapshot aus Datenträger
Datenträger mit Instanz verknüpft
disk0
VM-0
2
Erstelle Datenträger aus Snapshot
3
Datenträger mit Instanz verknüpft
4
Image erstellen
disk1
VM-1
snapshot0
Objektspeicher

Evaluierung – Zusammenfassung

	AWS	Azure	GCP
Erfassung	✗	✓	✓
forensische VM	✓	✗	✓
Objektspeicher (Hashwerte)	✗	✓	✓
Arbeitsspeicher	✗	✗	✗
Erfassung von Metadaten	—identisch—		
Sicherung von Inhaltsdaten	—komplex—		

Literatur

[KCG06] **Kent**, Karen ; **Chevalier**, Suzanne ; **Grance**, Tim:
Guide to integrating forensic techniques into incident.
In: *Tech. Rep. 800-86* (2006)

[MC12] **Martini**, Ben ; **Choo**, Kim-Kwang R.:
An integrated conceptual digital forensic framework for cloud computing.
In: *Digital investigation* 9 (2012), Nr. 2, S. 71–80

[MC14] **Martini**, Ben ; **Choo**, Kim-Kwang R.:
Remote programmatic vCloud forensics: a six-step collection process and a proof of concept.
In: *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications* IEEE, 2014, S. 935–942

[McK99] **McKemmish**, Rodney:
What is forensic computing?
Australian Institute of Criminology Canberra, 1999

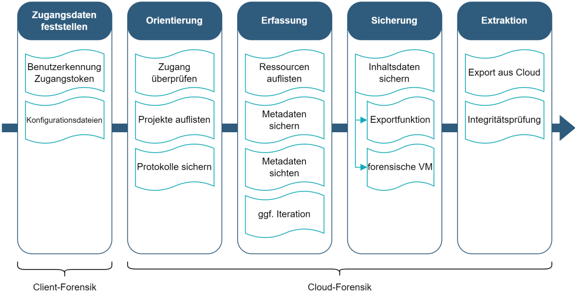
[MG+11] **Mell**, Peter ; **Grance**, Tim u. a.:
The NIST definition of cloud computing.
(2011)

[PWG+22] **Prakash**, Vijay ; **Williams**, Alex ; **Garg**, Lalit ; **Barik**, Pradip ; **Dhanaraj**, Rajesh K.:
Cloud-Based Framework for Performing Digital Forensic Investigations.
In: *International Journal of Wireless Information Networks* (2022), S. 1–23

[RCKC11] **Ruan**, Keyun ; **Carthy**, Joe ; **Kechadi**, Tahar ; **Crosbie**, Mark:
Cloud forensics.
In: *Advances in Digital Forensics VII: 7th IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, January 31–February 2, 2011, Revised Selected Papers 7* Springer, 2011, S. 35–46

Zusammenfassung

- Grundlagen
- Herausforderungen
- bestehende Methoden
- Leitfaden
- Evaluierung


Zugangsdaten feststellen
Benutzerkennung Zugangstoken
Konfigurationsdateien
Orientierung
Zugang überprüfen
Projekte auflisten
Protokolle sichern
Erfassung
Ressourcen auflisten
Metadaten sichern
Metadaten sichten
ggf. Iteration
Sicherung
Inhaltsdaten sichern
Exportfunktion
forensische VM
Extraktion
Export aus Cloud
Integritätsprüfung
Client-Forensik
Cloud-Forensik