Security on AWS

A Update and Overview

Bertram Dorn
Specialized Solutions Architect for Security and Compliance

30. Juni 2016
Agenda:

• AWS
• AWS Services
• Sicherheits Standards
• Technische Compliance
• DPA
Consumer Business

Tens of millions of active customer accounts

13 countries:
US, UK, Germany, Japan, France, Canada, China, Italy, Brazil, Mexico, India, Spain, Australia

Seller Business

Sell on Amazon websites

Use Amazon technology for your own retail website

Leverage Amazon’s massive fulfilment centre network

IT Infrastructure Business

Web-scale cloud computing infrastructure for developing, deploying & operating applications

Over 1 million registered customers in over 190 countries
On demand

Pay as you go

Uniform

Available

Cloud
What is DevOps?

**Software development lifecycle**

**delivery pipeline**

**build** → **test** → **release**

**plan** → **monitor**

**feedback loop**

**DevOps** = efficiencies that speed up this lifecycle
Monolith development lifecycle

developers

app

delivery pipeline

build

test

release
Microservice development lifecycle

- Developers
- Services
- Delivery pipelines

(build) → (test) → (release)
Service-Oriented Architecture (SOA)

Single-purpose

Connected through APIs

Highly decoupled

“Microservices”
## DevOps Practices

<table>
<thead>
<tr>
<th>DevOps Best Practices</th>
<th>Tools, Methods, Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure as Code</td>
<td>• CloudFormation -&gt; Compute/Storage/Network/Database/Messaging</td>
</tr>
<tr>
<td>IT Automation</td>
<td>• AutoScaling, Events, Logging</td>
</tr>
<tr>
<td>Continuous Integration</td>
<td>Code Pipeline</td>
</tr>
<tr>
<td>Continuous Deployment</td>
<td>• Code Deploy</td>
</tr>
<tr>
<td>Version Control Integration</td>
<td>• Code Commit</td>
</tr>
<tr>
<td>Monitoring and Logging</td>
<td>• CloudTrail, CloudWatch, Elasticsearch, SEIM approaches</td>
</tr>
</tbody>
</table>
AWS CodeDeploy

• Easy and reliable deployments
• Scale with ease
• Deploy to any server
Connect to best-of-breed tools
Accelerate your release process
Consistently verify each release
AWS CodeCommit

- Use standard Git tools
- Scalability, availability, and durability of Amazon S3
- Encryption at rest with customer-specific keys
Evolution of DevOps from Agile

Business Case
Requirements
Use Case
Features
Plan
Go to market

Business
Agility

Agile Development
- Iterative development
- Scrum, sprints, stories
- Velocity

Design
Code
Refactor
Unit Test
Bug Fix
Deploy

Developers (application)

DevOps
- Continuous Integration
- Continuous Deployment
- IT Automation
- Application Management

Provision
Configure
Orchestrate
Deploy
Report
Monitor

IT Operations (infrastructure)

Business Agility

IT Agility
What is AWS?

Deployment & Administration

Application Services

Compute  Storage  Database

Networking

AWS Global Infrastructure
AWS Global Footprint

Region

An independent collection of AWS resources in a defined geography

A solid foundation for meeting location-dependent privacy and compliance requirements
Example AWS Region

Mesh of Availability Zones (AZ) and Transit Centers

**Redundant** paths to transit centers

Transit centers connect to:
- Private links to other AWS regions
- Private links to customers
- Internet through peering & paid transit

Metro-area DWDM links between AZs

82,864 fiber strands in region

AZs <2ms apart & usually <1ms

25Tbps peak inter-AZs traffic
AWS Global Footprint

Availability Zone

Designed as independent failure zones

Physically separated within a typical metropolitan region
Example AWS Availability Zone

- 1 of 33 AZs world-wide
- All regions have 2 or more AZs
- Each AZ is 1 or more DC
  - No data center is in two AZs
  - Some AZs have as many as 6 DCs
- DCs in AZ less than ¼ ms apart
Example AWS Data Center

- Single DC typically over 50,000 servers & often over 80,000
- Larger DCs undesirable (blast radius)
- Up to 102Tbps provisioned to a single DC (inter DC not intra)
Shared Responsibility

- Managed by AWS
  - Cloud Service Provider Controls
    - Optimized Network/OS/App Controls
    - Service-specific Controls
    - Cross-service Controls
- Managed by Customer
  - Security in the Cloud
  - Security of the Cloud

Request reports at: aws.amazon.com/compliance/#contact

ISO 27000, ISO 9001, AICPA SOC, FedRAMP, FISMA, FIPS, ITAR, HIPAA

Security in the Cloud

Security of the Cloud
The main AWS Compliance Frameworks of today

Certificates:

- ISO 27000
- MPAA
- ISO 9001

Programmes:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI DSS Level 1</td>
<td>HIPAA</td>
</tr>
<tr>
<td>SOC 1/ ISAE 3402</td>
<td>FedRAMP (SM)</td>
</tr>
<tr>
<td>SOC 2</td>
<td>DoD CSM Levels 1-2, 3-5</td>
</tr>
<tr>
<td>SOC 3</td>
<td>DIACAP and FISMA</td>
</tr>
<tr>
<td>ISO 9001</td>
<td>ISO 27001</td>
</tr>
<tr>
<td>IRAP (Australia)</td>
<td>MTCS Tier 3 Certification</td>
</tr>
<tr>
<td>FIPS 140-2</td>
<td>ITAR</td>
</tr>
<tr>
<td>CJIS</td>
<td>MPAA</td>
</tr>
<tr>
<td>CSA</td>
<td>G-Cloud</td>
</tr>
<tr>
<td>FERPA</td>
<td>Section 508 / VPAT</td>
</tr>
</tbody>
</table>
Point-in-time, or continuous compliance assessments?
Scope

- By Service (not only Datacenter)
- By Region
- By Certification
- Global
- Scalable
Dedicated Security Services

- Tenant Isolation
- Deep Network Security
- Scaling Crypto Services
- Detailed Monitoring
- Access Control
  - Mandatory
  - Fine Grade
  - MFA Possible

SECURITY & COMPLIANCE

- Identity Management
- Access Control
- Key Management & Storage
- Monitoring & Logs
- Configuration Compliance
- Web application firewall
- Assessment and reporting
- Resource & Usage Auditing

Deployment & Administration

Application Services

Compute  Storage  Database

Networking

AWS Global Infrastructure
Setup

Auftragsdatenvereinbarung
Inclusive
Technische und Organisatorische Massnahmen
Report of Independent Accountants

To the Board of Directors of Amazon Web Services, Inc.

We have examined management’s assertion that Amazon Web Services, Inc. (AWS), during the period October 1, 2015 through March 31, 2016, maintained effective controls to provide reasonable assurance that:

- the Amazon Web Services System was protected against unauthorized access, use, or modification to meet AWS’ commitments and system requirements
- the Amazon Web Services System was available for operation and use to meet AWS’ commitments and system requirements

based on the criteria for security and availability in the American Institute of Certified Public Accountants’ TSP section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy updated as of March 2016. This assertion is the responsibility of AWS management. Our responsibility is to express an opinion based on our examination.
Security Possibilities

**Lift and Shift**
- Integrate standards
- Replicate

**Transparency**
- Monitor Every Activity
- Transparent Data Flows
- No Hidden IT Cost Driven Awareness
- Automatic Alarming

**Scale and Innovate**
- Use Cloud Security
- Scale Out Services as Code
- Continuous Deployment
- Continuous Security

**Permanent Monitoring/Audit**
- Automatic Reaction
- Permanent Monitoring
- Integrated Audit
- Security - DevOps
Certifications/Audits: **Scope**
Features Overview
Network Security

Choose and combine a bunch of build in network related options:

- Build in firewall features (Security Groups and NACL’s)
- Virtual Private Cloud
- Transport Encryption (IPsec and TLS)
- Dedicated Network Connection (Direct Connect)
- Cypher Suites with Perfect Forward Secrecy
- Managed NAT Gateways
- WebApplicationFilters
Virtual Private Cloud Security Layers

- **Virtual Private Gateway**
- **Internet Gateway**
- **Availability Zone A**
  - **Security Group**
  - **Subnet 10.0.0.0/24**
  - **Network ACL**
  - **Routing Table**
- **Availability Zone B**
  - **Security Group**
  - **Subnet 10.0.1.0/24**
  - **Network ACL**
  - **Routing Table**

**Lockdown at instance level**
**Isolate network functions**
**Lockdown at network level**
**Route restrictively**
Access Control

Allow only authorized administrators and applications access on AWS resources

- Multi-Factor-Authentication (MFA)
- Fine granular access to AWS object in S3-Buckets/SQS/SNS and others
- API-Request Authentication
- Geo-Restrictions
- Temporary access tokens through STS
Monitoring and Logging

Get an overview about activities on your AWS resources

- Asset-Management and -Configuration with AWS Config
- Compliance Auditing and security analytics with AWS CloudTrail
- Identifications of configuration challenges through TrustedAdvisor
- Fine granular logging of access to S3 objects
- Detailed informations about flows in the network through VPC-FlowLogs
- Rule based config checks and actions with AWS Config Rules
- Filter and monitoring of HTTP access to applications with WAF functions in CloudFront
Encryption

Security is the first priority for AWS

- Encryption of your data at rest with AES256 (EBS/S3/Glacier/RDS)
- Centralized (by Region) managed Key-Management
- IPsec tunnels into AWS with the VPN-Gateways
- Dedicated HSM modules in the cloud with CloudHSM
IAM Overview
Identity and Access Management

- Users & Groups
Identity and Access Management

• Users & Groups
• Unique Security Credentials
Identity and Access Management

- Users & Groups
- Unique Security Credentials
- Temporary Security Credentials
Identity and Access Management

- Users & Groups
- Unique Security Credentials
- Temporary Security Credentials
- Policies & Permissions
Identity and Access Management

- Users & Groups
- Unique Security Credentials
- Temporary Security Credentials
- Policies & Permissions
- Roles
Identity and Access Management

- Users & Groups
- Unique Security Credentials
- Temporary Security Credentials
- Policies & Permissions
- Roles
- Multi-factor Authentication
Vielen Dank

Bertram Dorn
Root Accounts Do Not Need Access Keys

Root Accounts Do Normally Not Log In
Best Practices

- Lock away your AWS account access keys
- Create individual IAM users
- Use groups to assign permissions to IAM users
- Grant least privilege
- Configure a strong password policy for your users
- Enable MFA for privileged users
- Use roles for applications that run on Amazon EC2 instances
- Delegate by using roles instead of by sharing credentials
- Rotate credentials regularly
- Remove unnecessary credentials
- Use policy conditions
- Keep a history of activity
What type of events should I monitor for?

- You can monitor any specific event recorded by CloudTrail and receive notification from CloudWatch
- Monitor for security or network related events that are likely to have a high blast radius
- Popular examples based on customer feedback
  1. Creation, deletion and modification of security groups and VPCs
  2. Changes to IAM policies or S3 bucket policies
  3. Failed AWS Management Console sign-in events
  4. API calls that resulted in authorization failures
  5. Launching, terminating, stopping, starting and rebooting EC2 instances
- Fully defined and pre-built CloudFormation template to get started
Receive email notifications of specific API activity
Demo: Kibana
Data at Rest: **Simplified**
Securing Data at Rest

- Amazon RDS
- Redshift
- Amazon EBS
- Glacier
- Amazon S3

- AES-256 key
- KMS integration
- Easy one-click encryption

Encryption

Encrypt this volume
Securing Data at Rest

- AES-256 key
- Each object is encrypted
- Each key is encrypted with a master key
- Master key is rotated regularly
- KMS integration
Securing Data at Rest

- AES-256 key
- Performed on EC2 host
- Snapshots
- KMS integrated
- Each Volume gets its DataKey
- DataKey is encrypted with MasterKey
Securing Data at Rest

> AES-256 key
> Logs, backups, and snapshots
> Read replicas
> Active and backup
> CloudHSM (Oracle TDE only)
> KMS integration
Securing Data at Rest

- AES-256 key
- Data blocks
- Metadata
- Active and backup
- CloudHSM integration
- 4-tier encryption architecture
Securing Data at Rest

- Hardware Security Module
- Single tenancy
- Private key material never leaves the HSM
- AWS provisioned, customer managed