Deutsche Telekom IT GmbH

Enabling a secure AWS adoption

About Deutsche Telekom IT GmbH

DTIT is the internal IT service provider of Deutsche Telekom AG. DTIT is responsible for the design, development and operation of all its owned and transferred IT systems supporting business processes at Deutsche Telekom AG. DTIT creates user-friendly web portals with intelligent self-service functions to create the basis for an integrated, cross-channel customer experience with the Telekom Magenta brand.

> T-Systems helped us to accelerate public cloud adoption for applications of Deutsche Telekom by implementing a secure AWS landing zone adapted to our rigorous security requirements.
>
> **Torsten Jester**
> Sr. Manager DTIT Cloudhub

Executive Summary

Starting in 2018, DTIT is undergoing an IT transformation program aiming to increase adoption of agile methods and forms digital hubs to enable the full range of public cloud capabilities for internal applications. The main challenge in the highly regulated Telco business are the comprehensive security requirements and standards, including Deutsche Telekom's rigorous own

In the project we wanted to build a secure and compliant platform for the applications by combining the advanced AWS-native automation and security services with the best practices and standards of Deutsche Telekom for secured system and network operation. Since T-Systems has a proven track record of delivering solutions complying with challenging security requirements while preserving the agility of the public cloud, they were contacted by DTIT as a partner to support and accelerate their project.

The Challenge

- **Challenge 1:** Build up an AWS landing zone which allows DTIT to provide isolated AWS environments for the internal applications while staying in control of security and compliance.
- **Challenge 2:** Federate Telekom's Active Directory with AWS to allow central management of identity pool and single-sign on into AWS for Telekom employees in a way that is compliant with the security policies and standards of Deutsche Telekom AG.
- **Challenge 3:** Build up a highly secure, centrally managed network environment that is ready for connection with the corporate network. Provide hardened deployment templates for the projects

Security on AWS

Amazon Web Services (AWS) places security at the heart of every offering to help you fully realize the speed and agility of the cloud. AWS integrates comprehensive security controls, superior scaling, visibility, and automated security processes into its cloud infrastructure to enable a secure foundation on which you can build. The Shared Responsibility Model (SRM) makes it easy to understand your choices for protecting your unique AWS environment, and it provides you with access to resources that can help you implement end-to-end security quickly and easily. Choose from the many cloud-ready software solutions offered by AWS and AWS Security Competency Partners to meet the highest standards of data security in the cloud.

Why T-Systems as a partner

T-Systems has a proven track record of delivering solutions complying with challenging security requirements while preserving the agility of the public cloud.

T-Systems offers

- comprehensive Cloud consulting and engineering for AWS across the whole application stack
- specific Cloud security expertise, including AWS certified security specialists.
- security reviews of existing applications running on AWS (according to the security pillar of the AWS well-architected framework)
- highly automated security and compliance assessments of a whole AWS environment
- and managed services with a strong focus on security and compliance leveraging the latest and greatest security and compliance tools for AWS and pro-active 24x7 support including integration with Telekom security operation center (SOC)

T · · Systems ·

Let's power
higher performance

DTIT selected T-Systems for those reasons as well as their in-depth knowledge and experience around the Telekom security requirements.

The Solution

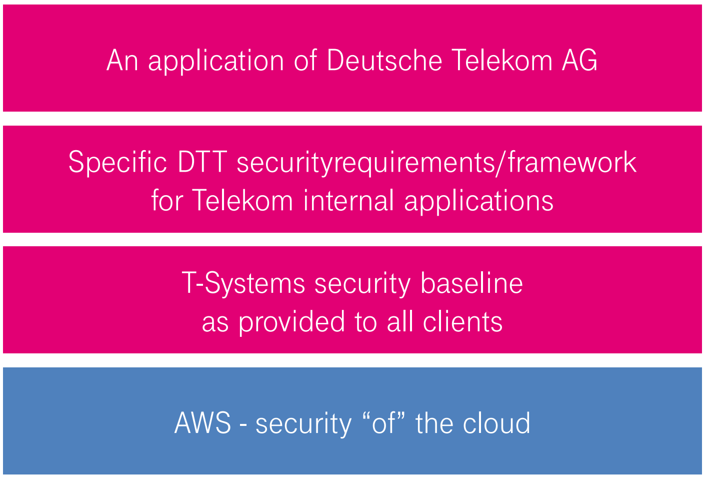
1. Landing Zone

T-Systems set up a dedicated AWS Organization for DTIT. The security baseline on the accounts is a combination of the standard security baseline of T-Systems and an additional layer realizing the specific requirements of the client. The T-Systems baseline was deployed from a central SecOps account of T-Systems. It enabled the ability to encrypt and decrypt S3 Data Storage based on a classification tag and using deployed KMS keys. It also ensured that structured IAM roles and password policies exist, multi-factor authentication is enforced and proper logging (CloudTrail) is in place and accessible for forensics as well as audits. Region restrictions were applied using service control policies (SCP), which ensures geographic containment according to client requirements. T-Systems also employs a rigorous and auditable process for root-level access. Other AWS Services such as CloudFormation, CloudWatch and CodePipeline were also central in building, deploying and enabling this cloud native solution following policy as code and CI/CD paradigm. The solution delivered by T-Systems has passed the rigorous Telekom Privacy and Security Assessment.

This solution has enabled the DTIT AWS DevOps team to work seamlessly, in an enterprise-grade, pre-configured and hardened AWS environment and focus on the specific requirements. T Systems then advised and supported DTIT to define, build and expand on top of that their own security baseline in a highly automated way (using CloudFormation Stacksets, Step Functions and Lambda, deployed from code from the corporate gitlab environment). Part of the DTIT security baseline are GuardDuty, encryption of all data at rest using KMS as well as a dedicated logging and monitoring stack. T-Systems also implemented a secure interface (using API Gateway) so that a new AWS account for DTIT can be ordered and deployed automatically via a central cloud management portal.

2. Active Directory Federation

One of the most important things for security is a secure identity foundation. It is a recommended security best practice for enterprises of all sizes to limit the number of different identities/users required for each employee using federation. Main reason is, besides end-user convenience, that it solves the so-called mover/leaver problem.


An application of Deutsche Telekom AG

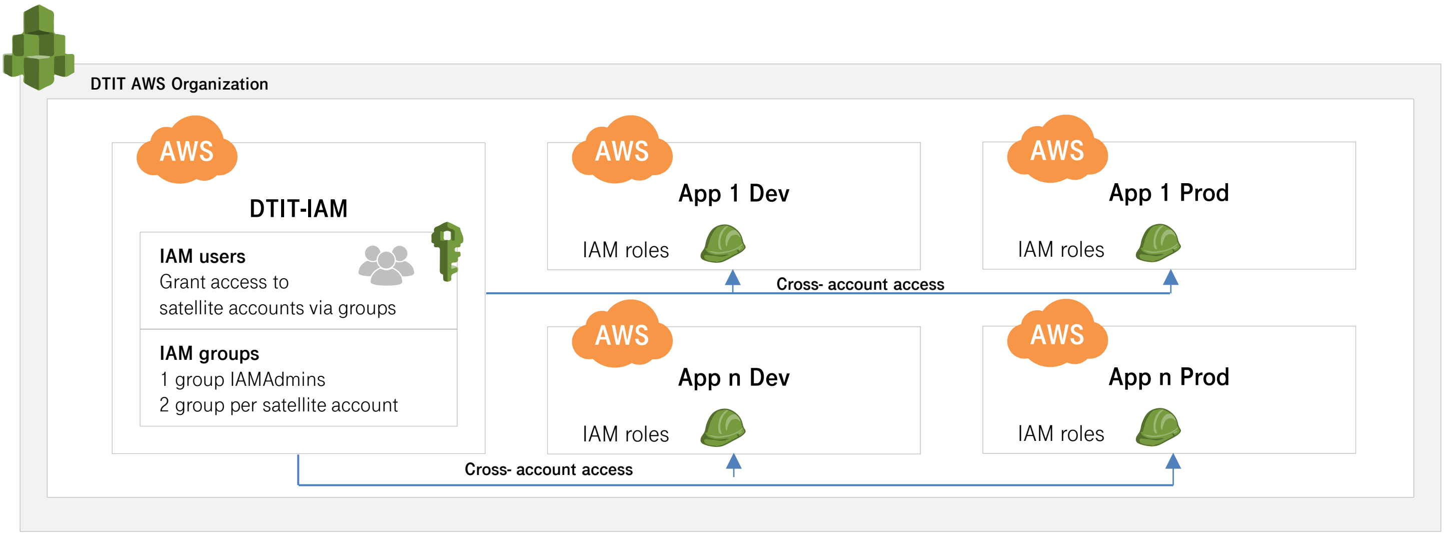
Specific DTT securityrequirements/framework
for Telekom internal applications

T-Systems security baseline
as provided to all clients

AWS - security “of” the cloud

That’s why T-Systems has been asked to support DTIT to design and set up a user management for AWS. We started as an interim solution with a central user management using IAM in a dedicated user management account. We deployed roles to the project accounts facilitating cross-account trust relationships.

In parallel T-Systems prepared the federation with Telekom Active Directory via the corporate ADFS farm in order to actually benefit from the corporate user pool and avoid setting up a separate rigorous isolated user management for AWS. ADFS is the solution used in most enterprises to enable single-sign-on with SaaS solutions and the cloud. In our scenario the ADFS serves as so-called SAML2.0 (security assertion markup language) provider for AWS. The high-level setup is quite straightforward and described in detail here. In summary, the client internally receives a SAML token from ADFS, which he/she can then use to get temporary credentials from AWS and sign in to his/her AWS account. The permissions for environments are controlled via groups in the Active Directory and on ADFS side a so-called relying party trust with AWS needs to be established. The most challenging part of that activity was to define the solution on the client side (concept), get the approvals, do the testing and go live with the change. But T-Systems also automated the rollout of the identity provider and roles on the AWS side and integrated the solution with the corporate group management application and processes.



Let’s power
higher performance

3. Secure Central Network

Concerning networking, T-Systems designed a highly secure, centrally managed network environment that is ready for connection with the corporate network (see the T-Systems direct connect case for DTIT). That way, AWS features like VPC endpoints and VPC sharing have been used as well as the other typical features required for network security such as NACL and Security Groups. T-Systems also created hardened deployment templates for the projects to simplify the usage of the centrally managed network environment. In addition, a more secure default VPC is being rolled out to whitelisted regions in order to simplify the getting started with AWS for new projects. All networks are managed as code (CloudFormation templates) in the central DTIT gitlab.

Results and Benefits

- **Benefit 1:** Saving time by setting up a T-Systems landing zone and baseline for AWS. That way DTIT could focus on their specific requirements and adding value for internal applications.
- **Benefit 2:** DTIT profits from the expertise of T-Systems in implementing security solutions on AWS. That way, the specific security requirements could be implemented faster and cloud-native capabilities leveraged wherever possible.
- **Benefit 3:** Higher level of security and better user experience by implementing federation with corporate Active Directory via ADFS.
- **Benefit 4:** Centrally managed shared networks as well as templates for isolated networks to facilities fast innovation and prototyping but also integration with corporate backend systems as required for Go Live of solutions.

Next Steps

T-Systems will continue support our client DTIT and the Telekom applications, e.g. by performing consulting, well-architected reviews and managed services for Containers (EKS, ECS).

About APN Partner

With a footprint in more than 20 countries T-Systems is one of the world's leading vendor independent provider of digital services headquartered in Europe. The Deutsche Telekom subsidiary offers one-stop shopping: from secure operation of legacy systems and classical ICT services, transition to cloud-based services as well as new business models and innovation projects in the Internet of Things. T-Systems is an Advanced Consulting Partner of AWS.

Your Contact

Denise Becker
denise.becker@t-systems.com
www.t-systems.com/aws

Published by

T-Systems International GmbH
Hahnstraße 43d
60528 Franfrut am Main, Germany