Executive summary

This case study describes the integration of an AWS Landing Zone with a configuration management database (CMDB) that T-Sys- tems has recently implemented for our client Deutsche Telekom IT (DTIT). The central CMDB of DTIT is used for Service Asset and Configuration Management and has a lot of interfaces to other sys- tems, like the interface with the security management system or IT service management tool. It contains Configuration Items (CIs) such as networks, applications, databases and virtual machines. Specifically, every application can be associated to a list of cloud environments, which link to a specific cloud tenant like an AWS account. As a result of this project, all cloud resources in scope and their relationships can be properly represented. The project has been implemented using DevOps practices such as infrastructure as code, CI/CD and automated testing, logging and monitoring as well as an AWS serverless architecture.

The challenge

In order to fulfil DTITs requirements, every AWS account of the client needs to be linked with an application represented in the CMDB. Also, for a selected set of cloud services new resources need to be registered in the CMDB. Automation is needed to reduce manual effort and avoid configuration drift. The integration generally is required for getting master data related to AWS ac-counts (like incident assignment group, contacts, cost codes etc.), handling of ITIL process such as incident resolution and integration with other security-related systems such as the DTIT’s central vul-nerability management. In addition, the agility of the cloud must be dealt with, as resources can be ramped up and shut down in a matter of seconds - unlike in the past where e.g. virtual machines existed in the database for extended periods of time.

About Deutsche Telekom IT

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 sup- porting business processes at Deutsche Telekom AG. DTIT creates user-friendly web portals with intelligent self-service functions as a basis for an integrated, cross-channel custo-mer experience with the Telekom Magenta brand. DT IT is in the middle of a large-scale transformation program, adopt- ing cloud as well as agile methods such as the Scaled Agile Framework.
Solution architecture

We implemented a decoupled application architecture for making it highly available and easy to evolve. So, an interface was established with DTIT’s AWS account management API (AWS account factory) and processes which support CRUD (create, read, update, delete) operations on master data of AWS accounts. As integration layer and back-end we have been using lambda-functions subscribed to SNS topics via SQS. That way we get a convenience layer and much simpler interface with the CMDB, which is specific to AWS and can be invoked from within AWS in an easier way (permissions, network etc.). There are lambda functions for all the needed operations on CMDB (register account, delete account, update application allocation, validate application id etc.) that are provided and ready to be called by other processes including account creation or decommissioning.

The benefits

As a result of this solution, our customer DTIT’s AWS Landing Zone is now integrated with their CMDB. Cloud resources are registered and as they are properly linked to applications and respective master data a lot of use cases have become possible or can be achieved in an easier way, from incident response to vulnerability scanning, from cost allocation to validations and data analysis. Also, the integration with Telekom’s Cyber Defense Center is utilizing this integration, so that in case of a security incident all data is available for analysis and countermeasures can be triggered quickly. Note that due to the growing number of completed AWS projects by T-Systems we have a repository of standard project templates and pre-configurations that helps us bring the best practices from previous projects into new engagements. While different clients use different CMDB tools we created this solution in a way that most of it can be re-used.

About the partner

With a footprint in more than 20 countries, T-Systems is one of the world’s leading vendor-independent providers 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 a trusted AWS partner for many clients including Deutsche Telekom, setting up their landing zones, networks and supporting more and more hubs and applications in adopting AWS. T-Systems also is an accredited AWS managed service provider and advanced consulting partner with a growing list of competencies.

Contact

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Germany
Email: referenzen@t-systems.com
Internet: www.t-systems.com

Published by

T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main
Germany