

Hybrid Multi-Cloud Blueprint Factory

Degree programme :

Managing secure operating system blueprints in a complex hybrid multi-cloud environment is challenging. This thesis provides a unified solution that addresses the challenges of maintaining and synchronizing blueprints across cloud providers by using cloud-agnostic approaches and technologies. This new pipeline, called the Blueprint Factory, streamlines the blueprint release process and enhances security measures.

Introduction

Johnson & Johnson (JNJ) runs Linux and Windows workloads in a hybrid multi-cloud environment called CLOUDx, which consists of multiple virtual public clouds and on-premises clouds. The backbone of CLOUDx compute service offering is its blueprints, or golden images, which ensure the secure and consistent deployment of new instances. However, maintaining and synchronizing these blueprints across different cloud providers is challenging and requires significant manual effort. The current fragmented CLOUDx Blueprint Framework presents JNJ with several significant challenges that range from time-consuming blueprint refreshes and inconsistent release cycles to platform discrepancies.

Objectives

The thesis must address these challenges by providing a unified pipeline that automates and streamlines the creation, testing and the management of CLOUDx OS blueprints while significantly enhancing security measures. The pipeline must use cloud-agnostic technologies to ensure compatibility across the different cloud providers. A modular design should allow the easy integration of new hosting platforms or operating systems, minimizing the need for changes to the pipeline itself and enabling rapid adaptation to new requirements.

Methods

The thesis started with a comprehensive analysis of the existing tools and scripts used to create and publish blueprints. Each step of the process was carefully examined to identify potential tools, resulting in informed decisions about the most appropriate tools for implementation.

An „everything as code“ methodology was adopted to ensure that all attributes required to create, test, and release blueprints are maintained in a configuration repository. The pipeline was developed in stages,

with each module representing a distinct phase of the blueprint release process.

Prior to production release, the pipeline underwent rigorous testing and qualification using pre-defined test cases to ensure its reliability and effectiveness.

Results

The CLOUDx Blueprint Factory consists of two Jenkins pipelines. The main Blueprint Factory pipeline uses Packer to create blueprints for AWS, Azure, Azure-China (21Vianet), GCP, and on-premises environments. Terraform is used to provision the test infrastructure for each blueprint, while the release process for each cloud platform is managed by custom Python scripts. To ensure compliance with JNJ's security configuration standards, functional testing is performed using Chef Inspec. In addition, TrendMicro and Nexpose are used to perform malware and security scans before the test infrastructure is decommissioned during the cleanup phase.

The second pipeline, known as the orchestrator, executes the Blueprint Factory for each hosting platform and OS combination across DEV, QA, and Production environments. Automated gates ensure that the pipeline does not move to the next environment until the previous one has been successfully completed. In addition, a manual gate is included prior to production execution to ensure proper change control.



Ramon Zumstein
MAS Information Technology
ramon.zumstein@gmail.com

