



Redesigning and Implementing the Bootstrap of Large Scale Kubernetes Enterprise Infrastructure through Automated Self Contained CLI

Project 2b (T3_2000)

in the context of the examination for the
Bachelor of Science (B.Sc.)

in Computer Science (Informatik)

at the Cooperative State University Baden-Württemberg Karlsruhe

by

Yannik Schiebelhut

Submission Date:	September 19, 2022
Processing period:	July 4, 2022 - September 19, 2022
Matriculation number, Course:	3354235, TINF20B1
Training institution:	SAP SE Dietmar-Hopp-Allee 16 69190 Walldorf, Deutschland
Supervisor of the training institution:	Samed Guener
Appraiser of the Cooperative State University:	Prof. Dr. Johannes Freudenmann

Eidesstattliche Erklärung

Ich versichere hiermit, dass ich meine Project 2b (T3_2000) mit dem Thema:

*Redesigning and Implementing the Bootstrap of Large Scale Kubernetes Enterprise
Infrastructure through Automated Self Contained CLI*

gemäß § 5 der „Studien- und Prüfungsordnung DHBW Technik“ vom 29. September 2017 selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.

Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Karlsruhe, den 17. August 2022

Schiebelhut, Yannik

Sperrvermerk

Die nachfolgende Arbeit enthält vertrauliche Daten der:

SAP SE
Dietmar-Hopp-Allee 16
69190 Walldorf, Deutschland

Der Inhalt dieser Arbeit darf weder als Ganzes noch in Auszügen Personen außerhalb des Prüfungsprozesses und des Evaluationsverfahrens zugänglich gemacht werden, sofern keine anderslautende Genehmigung vom Dualen Partner vorliegt.

Abstract

- *Deutsch* -

Platzhalter

Abstract

- English -

placeholder

Contents

List of Abbreviations	VI
List of Figures	VII
List of Code Listings	VIII
1 Introduction	1
1.1 Motivation	1
1.2 Goal	1
1.3 Approach	2
2 Fundamentals	3
2.1 Go	3
2.2 Terraform	4
2.3 Kubernetes	5
2.4 Gardener	6
2.5 Amazon Web Services (AWS)	7
2.6 Jenkins	8
2.7 Vault	8
3 Conceptual Thoughts	10
3.1 AWS	10
3.2 Vault	12
3.3 Assumptions	13
4 Implementation	14
4.1 General Functionality	14
4.2 Unit Tests	14
4.3 Integration with the command-line interface (CLI)	14
5 Evaluation and Future Work	15
Literaturverzeichnis	IX

List of Abbreviations

ACL	Access Control List
API	Application Programming Interface
AWS	Amazon Web Services
CICD	Continuous Integration and Continuous Delivery
CLI	command-line interface
EKS	Elastic Kubernetes Service
HCL	HashiCorp Configuration Language
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
JSON	JavaScript Object Notation
REST	Representational State Transfer
S3	Simple Storage Service
SAML	Security Assertion Markup Language
SDK	Software Development Kit
URL	Uniform Resource Locator
VCS	Version Control System

List of Figures

2.1 Gardener architecture [11]	7
--	---

List of Code Listings

1 Introduction

1.1 Motivation

Modern enterprise infrastructure for software development often makes use of cloud computing to dynamically adapt infrastructure to the fast-paced world of agile development. The setup process of one so-called cluster is traditionally done by hand and can easily require multiple days of work to complete. Obviously, in consequence of the required man-hours, this manual deployment is rather costly and time-consuming. Also, humans are prone to error. In a manual task that big, it is very likely for unforeseeable errors to occur. Finding these mistakes can eventually take additional time.

As a conclusion, it is desired to automate as much of a clusters' deployment process as possible. There are already various tools available that can be leveraged to perform an automated deployment of a declared cluster infrastructure. But even these automatization tools require some prerequisites to run, like a technical access user with access to the necessary resources and access keys to make use of this user, which still have to be created manually or with the help of bare-bones scripts. The process of fulfilling these requirements is referred to as bootstrap.

1.2 Goal

Goal of this project is to simplify the bootstrap of a cluster by integrating the necessary functionality into a CLI which is currently developed by the supervising department. Also, the usage should be convenient and, beside providing login data for the cloud provider and credential store, minimal user input should be required to perform the bootstrap. Furthermore, the newly developed CLI is required to be able to get executed by an automated build server. The ways of user interaction have to be designed accordingly.

1.3 Approach

First, the fundamentals of the tools and services that will be worked with are introduced. Most of these tools are fixed because of the current working set of the supervising department and because the target services that have to be interacted with are clearly defined. Although, some conceptional thoughts have to be put into the appropriate choice of libraries and Application Programming Interfaces (APIs) that are used as a bridge between the programming language and the actual remote services. As an orientation for the bootstrapping procedure, an existing Python script will be leveraged. This script is checked for possible improvements and modernization potential. The newly developed procedure is then implemented as a general proof of concept. After this, unit tests will be established to prospectively ensure the structural integrity of the developed solution. Then, the solution has to be integrated with the CLI. Eventually, the developed bootstrap will be analyzed regarding economical aspects and possible weak points and a conclusion will be drawn.

2 Fundamentals

2.1 Go

Go (also known as Golang) is an open source programming language that was started at Google in 2007 and initially launched in 2009. The language was designed to face engineering challenges at Google with the goal to make it “easy to build simple, reliable and efficient software”. [1, 2] By now the compiled and statically typed language [3] is widely used and the way it approaches network concurrency and software engineering has influenced other languages to a noticeable extent. [1] Through its structure go supports programming on various levels of abstraction. For instance, one can embed Assembler or C code into a Go program or on the other hand combine groups of components into bigger, more complex components to realize abstract design patterns. [4] Nowadays, Go is a popular choice for everything related to DevOps and therefor also for the development of command line tools. [5]

Go also tries to provide its own, official solutions for common tasks in software development. When installing Go, it comes packed alongside with a formatter (which shall ensure uniform styling across all programs written in Go) and an included suite for unit testing, just to name a few examples. Furthermore, Go supports generating documentation based on comments in the source code; much alike JavaDoc. Go features an extensive standard library which depicts a good starting point for developing your own applications. In case one wants to include a third party library, this can be done via the *go get* command. It fetches the necessary resources (usually directly from a Version Control System (VCS)) and saves the modules as a dependency in the *go.mod* file. (cite go tour and go docs)

2.1.1 Cobra

Cobra is an open source library for Go. Its aim is to provide developers with an easy way to create modern CLI applications. The cobra library is being used by noticeable projects like the CLIs for Kubernetes or for GitHub. The idea behind Cobra’s intended command

schema is that commands of a well constructed CLI should read like sentences. This way, new users that are familiar with CLIs in general quickly feel native because interacting with the CLI feels more natural. In this approach, a command represents a certain action that the CLI can perform. This action then takes arguments and flags to further specify on which objects and in which way the command should take action. With Cobra, one can also easily create nested subcommands. This means that a before mentioned command can also be divided into multiple sub-actions to enable detailed handling of complex actions. Further, benefits of Cobra are, among others, the automated generation of autocomplete for the most common shells as well as the ability to automatically create man pages. [6, 7]

2.2 Terraform

Modern enterprise infrastructure for software development usually makes use of cloud computing to dynamically adapt infrastructure to the fast-paced world of agile development. These clusters are usually distributed between multiple cloud services, each of which use their own individual APIs to configure their platform. Terraform is a tool that tries to minimize the effort needed to deploy these infrastructures in the long run by automating resource management as far as possible. It allows to uniformly describe the target infrastructure in an easy to learn, machine-readable definition language and automatically takes care of deploying this infrastructure at the individual Infrastructure as a Service (IaaS) providers. This approach is also known as Infrastructure as Code (IaC). With Terraform, it is also possible to save provisioned infrastructure setups as a Terraform configuration to reuse them at a later point in time or to arbitrarily extend and adapt the configuration. For configuration, either JavaScript Object Notation (JSON) or HashiCorp Configuration Language (HCL) can be used, with HCL being the preferred way by the developing company HashiCorp because of its advanced features compared to JSON. Terraform can only unleash its full potential because of cooperations with all major software and hardware vendors and providers. HashiCorp partners with over 160 companies and services the most noticeable ones being:

- AWS,
- Atlassian,

- Cloudflare,
- Google,
- Microsoft, and
- Oracle.

The most common use cases for Terraform include general IaC, managing Kubernetes (section 2.3), multi-cloud deployment, management of network infrastructures, and management of virtual machine images. Terraform additionally integrates tightly with other HashiCorp services like Vault (section 2.7).

2.3 Kubernetes

Kubernetes (often short: k8s) is an open source solution to ease up and automate management of container based services. It follows a declarative paradigm. This means that the users just needs to describe the desired state – for example through the use of configuration files or via the Kubernetes CLI – and Kubernetes determines the steps by itself which are necessary to reach and maintain this state. Kubernetes also enables users to dynamically scale their applications and services. This means that the amount of resources, that are dedicated to an application, is adapted during runtime dependent, for example, on the current number of users. Furthermore, Kubernetes can perform load balancing and redundancy between different instances of the same service. [8, 9]

One instance of a Kubernetes system is called a cluster. A Cluster is composed of multiple nodes (which usually are virtual machines or physical servers) which run the actual applications. An Application runs inside some kind of container, internally called Pod. The interaction with a cluster is managed by the so-called *Kubernetes Master*. It is a central controlling unit. The user actually never interacts with the nodes themselves directly. [10]

2.4 Gardener

Even though there are tools that help with creating and updating single Kubernetes clusters, it is rather hard to manage many clusters. This is where Gardener comes into play. It is a Kubernetes native extension that manages Kubernetes clusters as a service, packing the performance to manage up to thousands of clusters. One key concept that is applied is so called self-hosting. This means that Kubernetes components are run inside of Kubernetes clusters and is done, because Kubernetes is the go-to way to easily manage software in the cloud. [11, 12, 13, 14]

Gardener's architecture is constructed much like Kubernetes itself although not individual Pods are managed but entire clusters. The root of all is the so-called *Garden Cluster*. It is the main interface for the Gardener administrator and hosts, among others, the Garden Cluster control plane, the Gardener dashboard, the Gardener API server, the Gardener controller manager and the Gardener scheduler. Then there are two other types of clusters, *Seed Clusters* and *Shoot Clusters*. One Seed Clusters manages the control planes (thus API server, scheduler, controller manager, machine controller etc.) of its Shoot Clusters. There is at least one Seed Cluster per IaaS provider and region. The Shoot Clusters control planes are deployed as Pods inside the Seed Cluster and can therefore be created with standard Kubernetes deployment and support rolling updates. Shoot Clusters only contain worker nodes and are the Kubernetes Clusters that actually become available to the end-user and can be ordered in a declarative way. The clusters created by Gardener are vanilla Kubernetes clusters independent of the underlying cloud provider. [13, 15] (More details of the described architecture can be seen in Figure 2.1.)

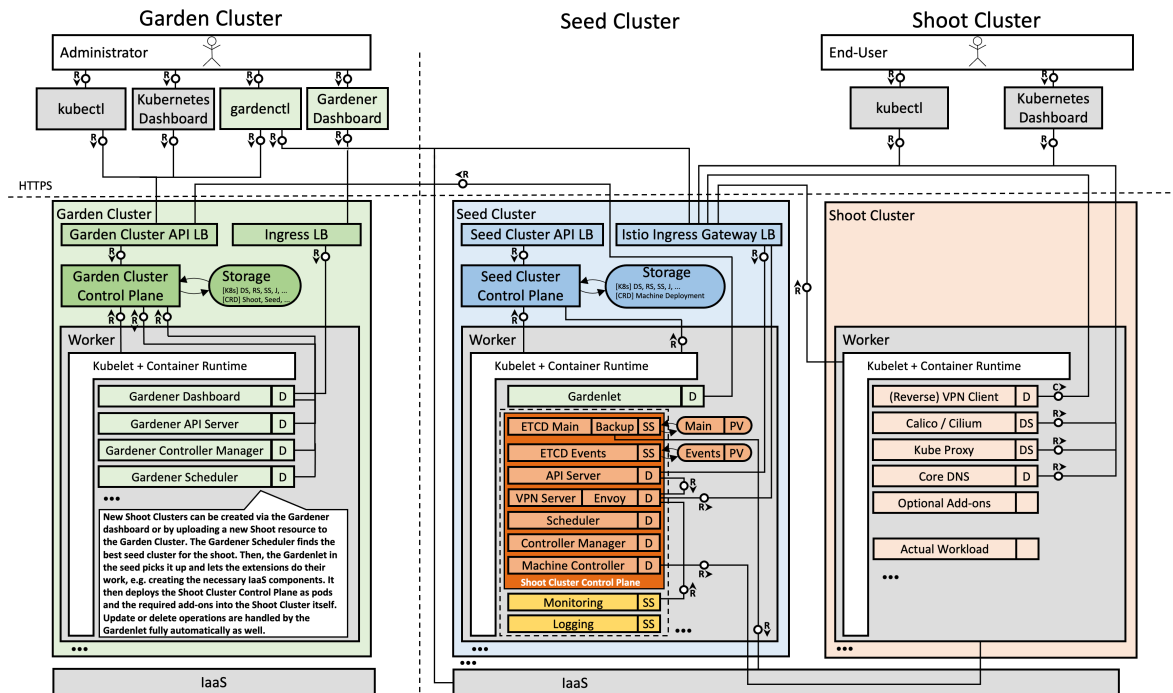


Figure 2.1: Gardener architecture [11]

2.5 AWS

AWS is a subsidiary company of Amazon that offers a cloud computing platform with various services, such as Simple Storage Service (S3) [16] or Elastic Kubernetes Service (EKS) [17]. Started in 2006, AWS nowadays runs data centers all over the world to provide scalable, reliable, and high performing services. [18, 19]

At the time of writing, AWS is the cloud provider with the biggest market share. [20] Also, most of the supervising department's clusters are currently being deployed on AWS. Because of these reasons and also due to constraints in time and complexity, the bootstrapping process worked out in this report is going to be narrowed down to deployment in an AWS environment.

2.6 Jenkins

Jenkins is a widely used open source automation server build with Java. It is a Continuous Integration and Continuous Delivery (CICD) tool aiming to save time by automating repetitive tasks like building projects, running test sets and deployment. Jenkins supports many plugins (over 1800) via its update center which give you the ability to integrate with most of the common tools in development and automate practicably any project. Jenkins can also be deployed on multiple machines to spread load and ensure quick and efficient operation. [21, 22, 23]

In context of this project, Jenkins will be used after the successful bootstrap to take care of running Terraform and performing the actual deployment.

2.7 Vault

Vault is an open source service with the primary task to provide a central control unit to manage and organize enterprise secrets. It encrypts secrets both at rest and in transit. Access to the secrets can be granted granular per user through the use of Access Control Lists (ACLs). Furthermore, vault audits access to the secrets. That means that it keeps a detailed log on whom accessed what secret at which point in time. If there was a security breach, where an unauthorized person got access to vault, this protocol can be used to tell, if a specific secret has been read by the attacker or if it is still safe to use.

Vault is designed to be highly pluggable. An instance is composed of *storage backends*, *audit log instances*, *authentication providers* as well as *secret backends*. Each of these can be impersonated by a variety of different components. This makes it possible to use different trusted authorities for attestation of identity. For example, among others LDAP, JWT, GitHub, and Radius can be used. An automated build service could very well use a different service to authenticate to vault than a human user.

Secrets and encryption are often the weak spot in applications. If a secret gets leaked and the leak stays unnoticed, attackers could gain long term access to a system. As a solution, Vault offers *dynamic secrets*. When a client requests the access credentials for a supported system, Vault creates a short-lived secret just for that specific client. Because the client is only accessing vault, it does not have to bother with key creation nor rotation

and an increased layer of security is added by not using secrets for an extended period of time. Also, if a dynamic secret gets leaked, this single secret can be revoked individually. If all clients accessing the resource used the same credentials, changing or blocking those could potentially cause an outage of the whole system.

When it comes to encryption, it can happen rather quickly that a single mistake compromises the security of the whole application. Because of this, vault offers encryption as a service. The idea is, that vault concentrates on the single task to handle credentials and encryption safely. The broad variety of applications have a different focus and are not developed with the necessary expertise to guarantee safe implementation of security measures. Vault, on the other hand, uses implementations that are audited by the open source community as well as independent experts. Those are then provided as a high level API to application developers. That way, the encryption process of data gets very easy while, at the same time, vault can handle the used encryption keys directly, and they are never actually sent to the application itself. [24]

During the bootstrap, this project is about, a technical user is created for Terraform operations. An access key is created for this user and then saved to vault. This way Jenkins then can obtain this access key and use it to run the actual cluster deployment with Terraform.

3 Conceptional Thoughts

Before implementing the bootstrap, one of the major questions is what way should be chosen for programmatically interacting with the services AWS and Vault. Both provide multiple possibilities.

3.1 AWS

When it comes to AWS, there are three obvious ways that could be chosen.

REST API Practically all required AWS functions can be accessed via its Hypertext Transfer Protocol (HTTP) API. Since Go's standard library natively includes a HTTP client, utilizing this would be a very lightweight solution. You would just have to instantiate a HTTP client object in Go. This object then already has all the required functionality to send requests to the API. An API call is made through a HTTP request with a specific method (GET, POST, PUT, DELETE etc.) to an API endpoint. This endpoint is specific to the operation you want to perform and represented by an Uniform Resource Locator (URL). Additional parameters and input data for the operation can be specified in a key value style via URL parameters, the request header, or the request body. URL parameters can be generated with string replacement and then appended to the base URL for the AWS API. The request body is a bit more complex to construct. It is basically a structure, that maps strings to basic data types or subordinate maps. This has to be constructed as a structure within Go and can then be encoded into a format supported by the HTTP client.

Generally, using the HTTP API would grant great flexibility because you construct all the requests on your own and therefore have detailed control over what happens without any additional layer of abstraction. On the other hand, since multiple different API calls are required, every single one of the needed calls would have to be manually constructed. This is a lot of work, prone to errors that are hard to debug, and has a bad influence on

the readability of the code in general because the API calls would get prevalent to the actual program logic.

AWS CLI The AWS CLI provides a very easy and intuitive interface to the user for interacting with AWS. Theoretically, it is intended to be explicitly installed on a system and to be used by a human user rather than programmatically. Anyway, Go natively provides the functionality to execute commands on system level. By this mean, also the AWS CLI could be used in the program.

But using the CLI would imply multiple drawbacks. CLIs often do not have a stable human interface and therefore the output returned by the CLI is subject to change. This is no good if the program has to parse the output and behave according to the results because the program could break easily and unnoticed just by updating the CLI. Although, in the special case of the AWS CLI the user can choose between several output formats including JSON notation, so a changing interface probably would not be of a problem. What is more of a concern is the fact that the CLI containing the bootstrap should be part of a container image packing various tools to work with clusters. The AWS CLI is entirely written in Python. If the AWS CLI should be used, Python would have to be installed into this container as well noticeably increasing the resulting image size. Also, when run locally, the Go application would have to rely on an existing installation of the AWS CLI to function correctly or check for its existence and prompt the user to satisfy the dependency manually in case it is missing. Just running the Go application executable would not be sufficient to perform the bootstrap. Because of these reasons, embedding the AWS CLI into the newly created Go CLI coordinating the bootstrap should be seen as a solution of last resort.

AWS Go SDK The AWS Software Development Kit (SDK) is a library provided by Amazon itself to interface its AWS services. It is not only available for Go but for a variety of different languages. To make use of it, during development it can be acquired with `go get` and imported into the program. In doing so, you specifically select the needed submodules minimizing the overhead. Then, the SDK's functions can be normally used inside the Go program.

One notable pain point is the partly ambiguous documentation, dependent on the part and version of the SDK. For instance, while the methods for user management have well documented error codes in version 1 of the SDK, telling you exactly what kind of errors you can expect, while version 2 – which supposedly does a better job on error handling – does not bother to take note on the possible error types, sometimes requiring in depth research to discover what you can expect. Luckily, errors are not of a big concern for this project, as near to all kinds of occurring errors just mean an unrecoverable program state and cannot explicitly be handled by the application itself. Furthermore, SDKs bring the inherent problem, that you completely rely on the provider in terms of update. If AWS changed their API while not touching the SDK, the program would stop working with no way to fix it rather than waiting for Amazon to update the rest of their codebase. On the other hand, since this is not a third party but an official SDK, one could also see an advantage in it. Staying with the example of the changed API and assuming that the SDK gets updated at the same time as the API, our codebase would simply continue to work. At the same time, you would be responsible to update a program utilizing the REST API entirely on your own. As, in this case, the SDK is released and maintained by Amazon their selves, and because of the introduced simplicity of working with an SDK rather than the API directly, this variant will be used in the following.

3.2 Vault

The aspects and options to consider for vault are very similar to those for AWS. Vault also has an HTTP api, a CLI and an own Go SDK. One noticeable difference here is that – even though the SDK is provided by the vendor itself – the documentation for the SDK is not good at all, especially in terms of login. To get some login methods running, one has to dig rather deep. Some functionality simply is not documented at all.

But the by far more important points are, that the newly created CLI by the supervising department already contains some work in progress parts that interact with Vault. It would not make much sense to reimplement key aspects that these solutions already cover. Furthermore, mixing different approaches to access Vault would be bad practice as it makes things unnecessarily complex and introduced multiple points of failure for key functionality. Because of this, Vault's HTTP API will be used in this project. This can be additionally reasoned with the advantages of HTTP APIs described in the predeceasing

section with the difference, that there are not many functions of Vault that need to be accessed despite reading and writing secrets. The programming overhead in writing these interactions manually via the HTTP client is pretty small.

3.3 Assumptions

The before mentioned container image already contains scripts to manage login to AWS. These scripts take a Security Assertion Markup Language (SAML) response and generate the file `~/.aws/credentials` out of it. This file contains sets of AWS credentials consisting of an access key ID, a session token and a secret key. These credential sets are sufficient authentication information to interface AWS. For the following implementation, the assumption is made, that this file already exists and contains a valid key set.

4 Implementation

4.1 General Functionality

4.1.1 AWS Client Struct

4.1.2 Policy Generation from File

4.1.3 Key Rotation

4.1.4 Updating Keys in Vault

4.2 Unit Tests

4.3 Integration with the CLI

5 Evaluation and Future Work

Literaturverzeichnis

- [1] Pike, R. *Using Go at Google - The Go Programming Language*. 08/2020. URL: <https://go.dev/solutions/google/> (visited on 08/02/2022).
- [2] *The Go programming language — GitHub*. URL: <https://github.com/golang/go> (visited on 08/02/2022).
- [3] Chris, K. *What is Go? Golang Programming Language Meaning Explained*. 10/2021. URL: <https://www.freecodecamp.org/news/what-is-go-programming-language/> (visited on 08/02/2022).
- [4] Maurer, C. *Objektbasierte Programmierung mit Go*. Springer Vieweg, 2021.
- [5] Van Sickle, M. *Go: Getting Started — Pluralsight*. 01/2020. URL: <https://app.pluralsight.com/library/courses/getting-started-with-go/table-of-contents> (visited on 08/02/2022).
- [6] *A Commander for modern Go CLI interactions — GitHub*. URL: <https://github.com/spf13/cobra> (visited on 08/02/2022).
- [7] *Cobra. Dev*. URL: <https://cobra.dev/> (visited on 08/02/2022).
- [8] Bloß, A. *Containerorchestrierung mit Kubernetes - Teil 4 — x-cellent technologies GmbH Blog*. 2019. URL: <https://www.x-cellent.com/blog/containerorchestrierung-mit-kubernetes-teil-4/> (visited on 07/15/2021).
- [9] *Was ist Kubernetes? — Kubernetes*. URL: <https://kubernetes.io/de/docs/concepts/overview/what-is-kubernetes/%7B%5C#%7Dwas-bedeutet-kubernetes-k8s> (visited on 07/15/2021).
- [10] *Konzepte — Kubernetes*. URL: <https://kubernetes.io/de/docs/concepts/%7B%5C-%7Dprint/> (visited on 07/15/2021).
- [11] *gardener/architecture.md at master · gardener/gardener*. URL: <https://github.com/gardener/gardener/blob/master/docs/concepts/architecture.md> (visited on 08/15/2022).
- [12] *Gardener - The Kubernetes Botanist — Kubernetes*. URL: <https://kubernetes.io/blog/2018/05/17/gardener/> (visited on 08/15/2022).

- [13] *Gardener Project Update — Kubernetes*. URL: <https://kubernetes.io/blog/2019/12/02/gardener-project-update/> (visited on 08/15/2022).
- [14] *Gardener*. URL: <https://gardener.cloud/> (visited on 08/15/2022).
- [15] *Was ist SAP Gardener?* URL: <https://www.datacenter-insider.de/was-ist-sap-gardener-a-955022/> (visited on 08/15/2022).
- [16] *Amazon Simple Storage Service S3 – Cloud Online-Speicher*. URL: <https://aws.amazon.com/de/s3/> (visited on 08/15/2022).
- [17] *Verwalteter Kubernetes-Service – Amazon EKS – Amazon Web Services*. URL: <https://aws.amazon.com/de/eks/> (visited on 08/15/2022).
- [18] *Amazon Web Services (AWS): Über uns — LinkedIn*. URL: <https://www.linkedin.com/company/amazon-web-services/about/> (visited on 08/15/2022).
- [19] *Was ist Amazon Web Services (AWS)? - Definition von WhatIs.com*. 2014. URL: <https://www.computerweekly.com/de/definition/Amazon-Web-Services-AWS> (visited on 08/15/2022).
- [20] Kumar, R. *AWS Market Share 2022: How Far It Rules the Cloud Industry?* 05/2022. URL: <https://www.wpoven.com/blog/aws-market-share/> (visited on 08/15/2022).
- [21] *Jenkins*. URL: <https://www.jenkins.io/> (visited on 08/15/2022).
- [22] *Jenkins automation server — GitHub*. URL: <https://github.com/jenkinsci/jenkins> (visited on 08/15/2022).
- [23] *What is CI/CD? — GitLab*. URL: <https://about.gitlab.com/topics/ci-cd/> (visited on 08/15/2022).
- [24] *Vault by HashiCorp*. URL: <https://www.vaultproject.io/> (visited on 08/15/2022).