Tampere University

Olli Kortelainen

INFRASTUCTURE MANAGEMENT IN MULTICLOUD ENVIRONMENTS

Master's Thesis
Faculty of Management and Business
Professor Kari Systä
University Lecturer Anu Suominen
April 2023

ABSTRACT

Olli Kortelainen: Infrastructure management in multicloud environments
Master's Thesis
Tampere University
Master's Degree Education in Management and Information Technology
April 2023

With the increasing number of cloud service providers and data centres around the world, cloud services users are becoming increasingly concerned about where their data is stored and who has access to the data. The legal reach of customers' countries does not expand over the country's borders without special agreements that can take a long while to get. Because it is safer for a cloud service customer to use a cloud service provider that is domestically legally accountable, customers are moving to using these cloud service providers. For the case company this causes both a technical problem and a managerial problem. The technical problem is how to manage cloud environments when the business expands to multiple countries, with said countries customers requiring that the data is stored within their country. Different cloud service providers can also be heterogeneous in their features to manage infrastructure, which makes managing and developing the infrastructure even more difficult. For example, application programming interfaces (API) that makes automation easier can vary between providers. From a management point of view, different time zones also make it harder to quickly respond to any issues in the IT infrastructure when the case company employees are working in the same time zone.

The objective of this thesis is to address the issue by investigating which tools and functionalities are commonly utilized for automating IT infrastructure and are additionally supported by cloud service providers while being compatible with the specific requirements of the organization in question. The research will help the case organization replace and add new tools to help maintain the IT infrastructure. This thesis will not investigate the managerial problem of case company employees working in the same time zone. The thesis will also not research security, version control, desktop and laptop management or log collection tools or produce a code-based solution to setting up an IT environment since further research needs to be done after the tools presented in this thesis have been decided upon. The research does also not investigate every cloud service provider in every country as case company business strategies can change and the size of the thesis would grow too much.

Qualitative research method is used for this thesis and the data gathered comes from literature and articles from various source. Both literature and article review provided the theoretical aspects of this research. Data was also gathered by looking at a few countries that have companies whose business is cloud service providing and comparing the findings regarding infrastructure management and automatization.

The research is divided into five parts. The first part tries to introduce the background, research objective and structure of the research., while the second part tries to explain the theoretical background. In the third part of the research methodology is explained as what material was used and how it was gathered and descriptions of the results, fourth part analyses the results, while the fifth and final part concludes the research.

Keywords: IT, Information Technology, multicloud, multi-cloud, automation, infrastructure management

The originality of this thesis has been checked using the Turnitin OriginalityCheck service.

TIIVISTELMÄ

Olli Kortelainen: Infrastruktuurin hallinta moni pilvi ympäristössä
Diplomityö
Tampereen yliopisto
Johtamisen ja tietotekniikan maisterikoulutus
Huhtikuu 2023

Pilvipalveluntarjoajien ja datakeskusten lisääntyessä ympäri maailmaa, pilvipalvelujen käyttäjät ovat yhä enemmän huolissaan siitä, mihin heidän tietonsa on tallennettu ja kenellä on pääsy tietoihin. Asiakasmaiden laillinen ulottuvuus ei ulotu yli maan rajojen ilman erityissopimuksia, joiden saaminen voi kestää kauan. Koska pilvipalvelun asiakkaan on turvallisempaa käyttää kotimaassa juridisesti vastuullista pilvipalveluntarjoajaa, asiakkaat siirtyvät käyttämään näitä pilvipalveluntarjoajia. Tapausyritykselle tämä aiheuttaa sekä teknisen ongelman että johtamisongelman. Tekninen ongelma on pilviympäristöjen hallinnassa, kun liiketoiminta laajenee useisiin maihin, jolloin mainittujen maiden asiakkaat vaativat tietojen tallentamista omaan maahansa. Eri pilvipalveluntarjoajat voivat myös olla heterogeenisiä infrastruktuurin hallintaominaisuuksiltaan, mikä tekee infrastruktuurin hallinnasta ja kehittämisestä entistä vaikeampaa. Esimerkiksi automaatiota helpottavat sovellusohjelmointirajapinnat (API) voivat vaihdella palveluntarjoajien välillä. Johtamisen näkökulmasta eri aikavyöhykkeet määrittävät myös nopeat laitteet uudelleen IT-infrastruktuuriongelmiksi, kun yritystyöntekijät työskentelevät samalla aikavyöhykkeellä.

Tässä opinnäytetyössä pyritään ratkaisemaan ongelmaa tutkimalla, mitkä työkalut ja ominaisuudet ovat eniten käytettyjä tietotekniikan infrastruktuurin automatisoinnissa, samalla kun pilvipalveluntarjoajat tukevat niitä ja ovat yhteensopivia tapausorganisaation vaatimusten kanssa. Tutkimus auttaa tapausorganisaatiota vaihtamaan vanhentuneita työkaluja, sekä tuomaan uusia työkaluja avustamaan IT infrastruktuurin hallinnassa. Tässä opinnäytetyössä ei käsitellä samalla aikavyöhykkeellä työskentelevien tapausyritysten työntekijöiden johtamisongelmaa. Opinnäytetyö ei myöskään tutki tietoturva, versionhallinta, työasema hallinta ja lokien keräys tuotteita tai tuota koodipohjaista ratkaisua IT-ympäristön rakentamiseen, koska lisätutkimusta on tehtävä sen jälkeen, kun tässä opinnäytetyössä esitetyt työkalut on päätetty. Tutkimuksessa ei myöskään käsitellä jokaista pilvipalveluntarjoajaa kaikissa maissa, sillä tapausyritysten liiketoimintastrategiat voivat muuttua ja opinnäytetyön koko kasvaisi liikaa.

Opinnäytetyössä käytetään kvalitatiivista tutkimusmenetelmää ja kerätty aineisto on peräisin kirjallisuudesta ja artikkeleista eri lähteistä. Sekä kirjallisuus että artikkelikatsaus antoivat tämän tutkimuksen teoreettiset näkökohdat. Tietoja kerättiin myös tarkastelemalla muutamaa maata, joissa on pilvipalveluja tarjoavia yrityksiä, ja vertaamalla tuloksia infrastruktuurin hallinnasta ja automatisoinnista.

Tutkimus on jaettu viiteen osaan. Ensimmäisessä osassa pyritään esittelemään tutkimuksen taustaa, tutkimuksen tavoitetta ja rakennetta, kun taas toisessa osassa pyritään selittämään teoreettista taustaa. Kolmannessa osassa tutkimusmetodologiaa selitetään, mitä materiaalia on käytetty, miten se kerättiin sekä kuvaus tuloksista. Neljäs osa analysoinnista ja viides ja viimeinen osa päättää tutkimuksen.

Avainsanat: IT, Informaatioteknologia, multipilvi, automaatio, infrastruktuurin hallinta

PREFACE

I would like to express my thanks to Professor Kari Systä and University Lecturer Anu Suominen for guiding this thesis during the whole process. The valuable feedback and quick replies to my questions, helped immensely, when there was not much downtime between getting advice and continuing writing.

A big thanks also goes to my wife, who gave me the time to make this thesis as well as gave valuable advice on how to write and formulate the thesis.

Rajamäki, 25 April 2023

Author

Olli Kortelainen

CONTENTS

LIST OF SYMBOLS AND ABBREVIATIONS

AIOps	Artificial Intelligence for Operations
API	Application Programming Interface
APM	Application Performance Management
AWS	Amazon Web Service
CLI	Command-Line Interface
CMP	Cloud Management Platform
CSP	Cloud Service Provider
GCP	Google Cloud Platform
GUI	Graphical User Interface
HCL	HashiCorp Configuration Language
IaaS	Infrastructure as a Service
IOT	Internet of Things
IT	Information Technology
MCP	Mirantis Cloud Platform
OS	Operating System
PaaS	Platform as a Service
VM	Virtual Machine
YAML	Yet Another Markup Language

.

1. INTRODUCTION

This part of the thesis briefly introduces the research topic split into three sub-chapters. The first sub-chapter explains the background of how the research topic was discovered, the second sub-chapter covers the research objective and what concrete data will be produced, while the last sub-chapter explains the structure of the research, making it easier for the reader to follow the research.

1.1 Background

The idea for the research grew over time while the author was switching jobs. At both the old and new workplace the problem of maintaining and developing Information Technology (IT) infrastructure in multiple cloud and on-premises environments was present.

If a company sets up their Information Technology (IT) resources in various environments, the management of said resources become more difficult because of differing control interfaces like web portals, command-line interfaces (CLI), programming languages, protocols and supported automation tools. Various cloud service providers (CSP) supported tools are not necessarily homogenous with other tools and there is even some variance with the configurations of the same tools in different cloud environments (P. Raj, A, Raman: 2018). It could be simpler to invest in one CSP and learn to use the available technologies, but the case organization has one additional problem to solve. Because the case organization's customers require that the customer data is stored in the same country where the customer lives and that the data should not be accessed by anyone else but the case organisation and customer, CSPs like Amazon Web Service (AWS), Azure and Google Cloud Platform (GCP) can be legally bound to share data about customers if the service being provided uses a resource that is being managed within the USA. This both causes worry in customers not living in the USA and the case organization since legal battles can become very costly. (Punke, 2019).

The solution is thus to invest in a CSP that resides in the customers country and is bound to said country's laws. Because of customers requirements, the case organization is forced to invest in multiple CSPs in multiple countries, making it harder to maintain the IT infrastructure.

1.2 Research objective

Because of the previously mentioned problems, a solution on how to maintain and develop the multi-cloud environments need to be researched. The case company needs to fulfil the requirements of the customers, that require that data is stored within their country. By having customers also residing in other countries, the amount of new IT environments also increases and the difficulty to monitor, backup, spin up new resources and overall manage the infrastructure and its components get more difficult. The case organisations team responsible for maintaining the infrastructure is also small which makes maintaining multiple environments even more challenging. This thesis will help to find out what tools would suit best to manage multiple IT environments while also being compatible with the case organisations current and future IT requirements.

The research will investigate automation tools like Terraform and Saltstack that can help automate the IT management using code and Graphical User Interface (GUI) tools to ease the manual work required and scaling the current method of maintaining the infrastructure. The research will also help with replacing outdated tools and adding new tools to help with aspects not considered before.

1.3 Research structure

The thesis will start in section two by looking at the theory behind automating and easing the workload required to maintain and develop IT infrastructure by researching scientific literature done on the subject as well as articles written by reliable sources. In section three, the thesis explains how data was gathered and how it was used in the research while also taking a deeper look into the tools found during section two and explains how they are used. In the fourth section the thesis analyses how the tools in section four fit into the case organisations current and future IT requirements. The fifth and final section ends with discussions, conclusions and how the research could be continued.

2. CHALLENGES OF MANAGING MULTI-CLOUD IT INFRASTUCTURE

Managing IT infrastructure has always been a challenge, but with the rise of cloud computing, it has become even more complex. Multi-cloud deployments, which involve the use of two or more cloud computing systems simultaneously, have gained popularity due to their ability to provide redundancy and avoid vendor lock-in. However, using workloads across different clouds can create challenges in terms of managing costs, overseeing system management, and mitigating security risks. The impact of cloud technologies on managing multi-cloud infrastructure is an interesting topic, as cloud solutions can help organizations achieve more with less (Raj and Raman, 2018, Mulder 2020, Alonso et.al 2023).

2.1 Spreading the Infrastructure

Software applications have become increasingly complex and advanced. Integrated systems have become the norm, and it's essential for enterprise-grade applications to seamlessly integrate with third-party software components running on different systems. These days, software applications are made up of various interactive, transformative, and disruptive services that run on various devices. Additionally, there are numerous enterprises hosted in virtual and containerized environments. Furthermore, industry-specific and vertical applications (such as energy, government, telecommunications, healthcare, banking and insurance and others) are being developed and delivered via Cloud infrastructures. The future is moving towards real-time analytics and applications, which indicates that software is becoming increasingly purposeful, collaborative, and productive. Therefore, it is evident that the world is becoming more software intensive. (Raj and Raman, 2018, Alonso et.al 2023)

Due to the existence of a wide range of IT systems and business applications, distributed applications are becoming more popular as a potential solution. This method entails dividing the different parts of a software application across multiple locations to enable high availability through redundancy. The advantages of distributed applications include fault tolerance, reduced latency, independent software development, and the avoidance of vendor lock-in. As the world becomes increasingly data-driven, distributed computing

is emerging as the go-to model. The secret behind this trend is the dynamic pool of affordable servers and computers that form the backbone of the distributed systems. With the number of connected devices skyrocketing, the time of device clouds is not too far away. This means that decentralized devices will be combined in large numbers to create ad-hoc and application-specific cloud environments, where data can be collected, pre-processed, and analysed. It's evident that the future belongs to distributed computing. The centralized computing model has reached maturity and stability, but it's not sustainable due to the demand for web-scale applications. Meanwhile, the IoT, connected devices, and microservices are set to be the defining features of the next-generation internet. (Raj and Raman, 2018, Mulder 2020, Alonso et.al 2023)

2.2 The cost of spreading the infrastructure

Hybrid Clouds, which combine private and public Clouds, are increasingly popular among organizations due to their ability to offer the advantages of both Cloud types. The maturation of Cloud technology has made this pragmatic approach possible and has opened new opportunities for businesses. Hybrid Cloud allows for fast and effortless access to Cloud-based infrastructures, platforms, software, and data, while also providing robust governance and IT service management features. It enables running diverse applications in optimal environments to achieve desired benefits such as speed, scale, throughput, visibility, and control. While several Cloud providers offer capable solutions and services to expedite the setup and maintenance of Hybrid Cloud, there are numerous open-source and commercial-grade solutions and toolsets available. Additionally, service providers have devised risk-free and sustainable Hybrid Cloud frameworks.

However, establishing and maintaining a hybrid cloud environment comes with various challenges that need to be addressed, such as ensuring consistent configuration and developer experiences across geographically dispersed cloud environments, handling issues related to workload modernization, migration and IT cost management. Another significant challenge is establishing a high-performing hybrid environment that can accurately manage and monitor all its components. In multi-cloud environments, it is crucial to avoid cases where costs grow over the organization's head, where there is no clear overview of who is managing the systems, and where system sprawl introduces severe security risks. Distributed multi-cloud applications are simultaneously being run into heterogeneous and diverse cloud services (in terms of location, management systems,

technology, interfaces, etc.), whereas replicated applications do not need to coexist with more than one cloud environment. Therefore, an integrated cloud management platform (CMP) that can fully leverage the fast-evolving hybrid concept and provide maximum flexibility to businesses is essential in multi-cloud environments. (Liaqat et.al 2017, Raj and Raman 2018, Mulder 2020, Alonso et.al 2023)

2.3 Hybrid Cloud and Multi-cloud

This section provides insights into various capabilities and tools used by hybrid Cloud service providers to simplify the monitoring, measurement, and management of hybrid Cloud. It examines multiple automated solutions that address both known and unknown complexities of hybrid Cloud processes. The competitive analysis in this chapter centres on value-adding parameters that enable informed decision-making.

Selecting the right technology is paramount in today's IT landscape. The choice of implementation technologies must be strategically planned, considering not only the technologies themselves but also the methodologies to be used. However, selecting and utilizing technology without serious consideration can lead to project failures, even if sound technologies are chosen. The factors such as fitment/suitability, adaptability, sustainability, simplicity, and extensibility of technologies must be seriously considered while deciding on technologies and tools for enterprise scale, transformational, and mission-critical projects. Additionally, multi-cloud offers organizations flexibility and freedom of choice, but without a clear strategy, it can also lead to a lack of focus. It is essential to have an appropriate understanding of the concept and a design and operation strategy for such applications to avoid risks such as unpredicted costs, vendor lock-in, and other unwanted outcomes. In today's digital world, more and more businesses are realizing the importance of IT as a core activity and adopting cloud and multi-cloud strategies in their transformation process. (Raj and Raman 2018, Mulder 2020, Alonso et.al 2023)

The terms "Hybrid Cloud" and "Multi-cloud" are often used interchangeably, but they refer to different approaches to cloud computing. In a multi-cloud environment, an organization uses multiple public cloud services from various providers to achieve best-of-breed results, reduce vendor lock-in, and meet different requirements for different tasks. Multiple public clouds are often used in combination with physical, virtual, and private cloud infrastructure. (Raj and Raman 2018, Trautman 2018, Mulder 2020)

On the other hand, a hybrid cloud combines private and public clouds for the same purpose. This differs from a multi-cloud approach in two main ways. Firstly, hybrid always includes private and public clouds, while multi-cloud can include physical and virtual infrastructure and private clouds in addition to multiple public clouds. Secondly, in a hybrid cloud, the components of the private and public clouds work together, with data and processes intermingling and intersecting. In contrast, in a multi-cloud environment, the usage of each cloud service typically remains in its own silo. For example, in a hybrid cloud scenario, an application might take advantage of load balancing and application services offered by a public cloud, while keeping its database and storage within a private cloud. The application has processing capabilities that function similarly in both private and public clouds, adjusting the computational usage in each cloud based on demand and expenses. In contrast, in a multi-cloud setup, applications could either use resources solely from the public or private cloud, or access resources from both clouds independently. (Raj and Raman 2018, Mulder 2020, Alonso et al. 2023)

According to Forbes, 90% of large companies already use multi-cloud environments to run their business However, the widespread adoption of cloud services from multiple CSPs and communication service providers introduces a distinct set of obstacles for IT departments. In particular, IT teams are tasked with coordinating the onboarding, management, and delivery of IT and business services across numerous portals and suppliers. This complexity makes it challenging to maintain uniform performance, security, and governance within the multi-cloud ecosystem. (Raj and Raman 2018, Hasbe 2022, Alonso et al. 2023)

The formation and operation of a multi-cloud environment are depicted in Figure 1. This involves the utilization of multiple public Clouds in conjunction with private Clouds and traditional IT environments. To optimize their IT operations, many businesses are now using two or more public Clouds. Additionally, a popular option is the integration of private Clouds with public Clouds, which can be accomplished through the use of Cloud connectors, adapters, brokers, and other middleware solutions. These tools establish and maintain connections between multiple, geographically distributed Cloud environments. By exposing interfaces that enable other Cloud environments to connect, businesses can benefit greatly from the resources available across multiple Clouds. (Raj, Raman 2018)

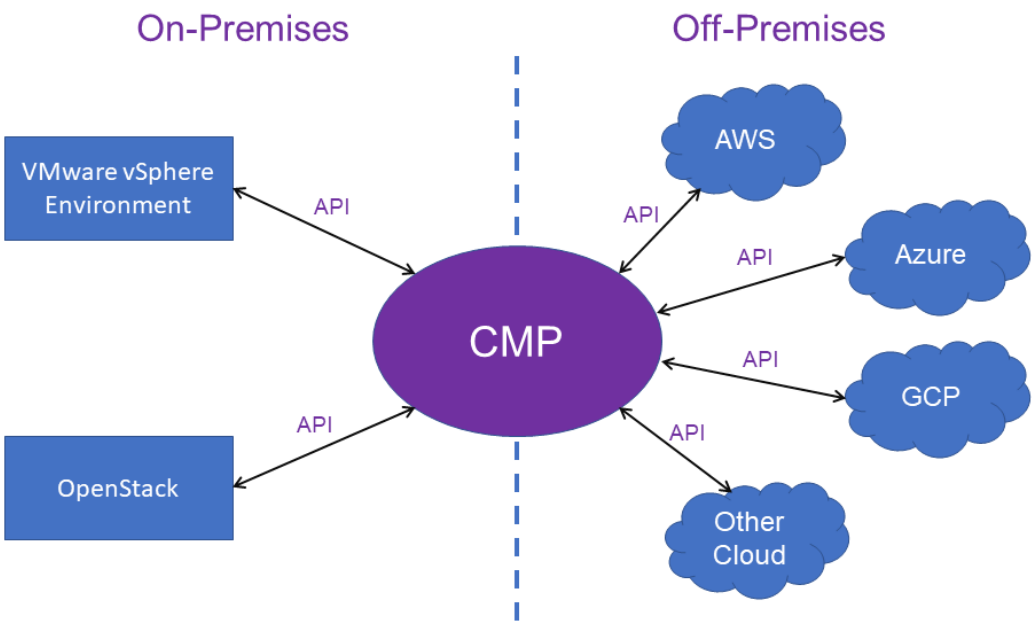

Figure 1. *Multi-Cloud Orchestration Cluster (Raman 2018)*

Multi-cloud adoption is a growing trend among organizations worldwide, driven by the benefits it provides at both tactical and strategic levels. However, several challenges come with implementing a multi-cloud approach, including:

Technical Challenges: (Raj and Raman 2018, Trautman 2018, Morehouse 2022):

- Integration/APIs: Different Cloud providers offer varying APIs to access Cloud services, making it difficult to have a single model of integration.
- Behaviour: Clouds behave differently for common actions or under specific circumstances, creating inconsistency.
- Resource sizes/types: Each Cloud provider offers varying sizes and types of compute, storage, and network resources.

Operational Challenges: (Raj and Raman 2018, Trautman 2018, Morehouse 2022)

- Testing: Deploying applications to multiple Clouds requires separate and several automated tests targeting multiple Cloud platforms.

- Operating system images: Distinct operating system (OS) images are provided by each cloud provider, complicating the execution of workloads on the same image across multiple clouds.
- Hypervisors: Various cloud providers employ diverse, and at times proprietary, hypervisors.
- Application stacks: Some cloud providers supply pre-configured application stacks, such as LAMP, Java, or .NET.
- Additional services and features: Beyond the standard compute, network, and storage resources, each cloud provider presents unique add-on services and proprietary features.
- Security capabilities: With differing access control capabilities among cloud providers, ensuring security compliance becomes challenging.
- Network capabilities: As each cloud provider has distinct methods for defining subnets, security groups, and network gateways, network planning becomes increasingly complex.
- Tool diversity: DevOps tools must keep up with the rapid changes being made to the platforms.
- Security and governance: Adhering to the rules and regulations of each Cloud service provider is necessary for full security compliance.
- Handling applications and infrastructure configurations across various cloud stacks: Cloud platforms lack a shared API, resulting in differing service definitions and billing structures.
- Technical support and expertise: Extra administrative efforts and investigation are required to identify the most suitable provider and ensure compatibility with its services.

Business Challenges: (Raj and Raman 2018, Trautman 2018):

- Cloud brokers: Having a Cloud broker is an additional cost while using multiple Clouds. More about cloud brokers in section 2.4
- Billing and pricing: Different Cloud providers offer varying pricing models, making billing and pricing management difficult.

- Skill sets and training: Different technologies and tools are being used by Cloud service providers, making education, experience, and expertise necessary for the organization.
- Planning and execution: Choosing the services that match a company's business needs, pricing, governance, and team's expertise can be challenging.

2.4 Cloud Brokers

As businesses increasingly adopt multiple cloud environments, managing and ensuring consistent performance, security, and control can become a challenge for IT teams. The availability of various cloud services from different providers, each with their own service level agreements and costs, further complicates matters. To address these challenges, cloud management and brokerage platform solutions are becoming popular. These platforms can help organizations select the best cloud services for their needs, support line of business requirements, and manage and deliver IT and business services from multiple clouds while maintaining security and performance. However, the trend towards direct procurement of cloud services by business units can lead to "shadow IT," where employees bypass corporate policies and security procedures. This occurs when enterprise IT is not closely aligned with the operational demands of specific lines of business. The use of multiple cloud environments and platforms can also increase the security risk of the organization, requiring IT to manage multiple cloud environments and services with different capabilities, processes, and costs. To effectively manage these multi-cloud environments, IT must carefully evaluate and select the appropriate cloud management tools and solutions to ensure the security and performance of their cloud infrastructure, while enabling the agility and scalability that cloud computing can provide. (Raj and Raman 2018, Alonso et.al 2023)

Cloud brokers have emerged as key players in managing the complexity of multiple Cloud ecosystems and transitioning businesses to digital enterprises. Acting as middleware, Cloud brokers act as intermediaries between Cloud service consumers and Cloud service providers.

There are three main types of Cloud brokers:

1. Cloud aggregators - These brokers package and integrate multiple service catalogues into a single user interface, allowing clients to select only the services that meet their specific business needs. This approach is more cost-effective and efficient than purchasing each service individually. As resellers, aggregators play a critical role in managing Cloud provider relationships and services and may offer additional services such as security and governance. One of their main goals is to curate a catalogue of services, providing a single point of access for business and IT services, empowering agility and portability while saving time and money. (Raj and Raman 2018, Sztukiewicz 2013, adapture.com 2023)

A few examples of cloud aggregators are:

- CloudHealth by VMware: CloudHealth by VMware is a cloud management platform that provides a centralized view of an organization's cloud environment. It allows users to optimize their cloud usage, automate cost management, and improve security and compliance. (https://www.cloudhealthtech.com/)
- CloudCheckr: CloudCheckr is a cloud management platform that provides visibility and control over cloud resources. It helps organizations to optimize cloud usage, reduce costs, and improve security and compliance. (https://cloudcheckr.com/)
- CloudBolt: CloudBolt is a cloud management platform that provides automation and orchestration of multi-cloud environments. It helps organizations to streamline IT operations, optimize cloud costs, and improve governance and compliance. (https://www.cloudbolt.io/)

2. Cloud integrators - Integrators add value by streamlining workflows in hybrid environments via unified orchestration, boosting performance and minimizing business risk. Integration serves as a function that preserves data integrity for organizations utilizing various on-demand B2B software services, SaaS, PaaS, or IaaS, as well as addressing the silos they generate. Cloud Service Integration can be intricate, necessitating efforts from brokerages, B2B vendors, and infrastructure providers. (Raj and Raman 2018, Sztukiewicz 2013)

    - Accenture: Accenture is a global professional services firm that provides consulting, technology, and outsourcing services. Its cloud integration

services help organizations to integrate and manage their cloud applications and infrastructure. (https://www.accenture.com/us-en/services/cloud/cloud-integration)

- Deloitte: Deloitte is a global professional services firm that provides audit, consulting, tax, and advisory services. Its cloud integration services help organizations to integrate and manage their cloud applications and infrastructure across multiple cloud providers. (https://www2.deloitte.com/us/en/pages/technology/solutions/cloud-integration-services.html)

- IBM: IBM is a global technology company that provides cloud computing, analytics, and cognitive computing services. Its cloud integration services help organizations to integrate and manage their cloud applications and infrastructure across hybrid and multi-cloud environments. (https://www.ibm.com/cloud/integration)

3. Cloud Intermediates - These brokers modify existing Cloud services to meet specific business needs and may even develop extra features to operate in the cloud as needed by the organization. This function is crucial for establishing a comprehensively configured cloud with heightened visibility, compliance, and integration of essential IT processes. Intermediation Cloud Service brokerage offers specialized value-added services that augment the abilities of current cloud services, such as identity or access management for multi-cloud services. (Raj and Raman 2018, Sztukiewicz 2013)

    - Cloudmore: Cloudmore is a Cloud Service Brokerage company that provides a platform for businesses to manage their cloud services from multiple vendors. Cloudmore offers features such as identity and access management, automation, and self-service capabilities. (https://www.cloudmore.com)

    - Cloud Sherpas: Cloud Sherpas is a Cloud Service Brokerage company that provides businesses with a range of services to optimize their cloud infrastructure. Cloud Sherpas offers services such as cloud migration,

managed services, and cloud integration. (https://www.cloudsherpas.com)

- Accenture Cloud Platform: The Accenture Cloud Platform is a Cloud Service Brokerage platform that provides businesses with a centralized platform for managing their cloud services from multiple vendors. Accenture Cloud Platform offers features such as service catalogue management, self-service provisioning, and cloud cost optimization. (https://www.accenture.com/us-en/services/cloud/overview)

Overall, Cloud brokers act as master orchestrators who can manage the complexity of multiple Cloud ecosystems and transform businesses into digital enterprises. Through the provision of their services, brokers empower flexibility, portability, and choice in Cloud services, while mitigating risks associated with security, governance, and integration. (Raj and Raman 2018, Sztukiewicz 2013)

2.5 Automation and Orchestration

Automation and orchestration are two key concepts in cloud computing that are often used interchangeably, but they have distinct meanings. Automation is the process of using technology to perform tasks without human intervention. In the context of cloud computing, automation can be used to launch, configure, and stop a web server, for example. (Raj and Raman 2018, McHaney 2021)

Orchestration, on the other hand, is concerned with automating multiple tasks together. In cloud computing, there are usually many tasks that need to be executed in a specific sequence in order to achieve a desired outcome. Orchestration is the process of automating these tasks in a coordinated way, ensuring that each task is performed correctly and in the right order. (Raj and Raman 2018, McHaney 2021)

Cloud orchestration is more complex than simple automation because it involves managing multiple services and ensuring high availability, failure recovery, scaling, and other factors. Without orchestration, many of the benefits of cloud computing cannot be realized. For example, the cost savings that come with cloud computing are largely due to automation and orchestration. Without these technologies, companies would need to hire more personnel to perform the same tasks manually, resulting in higher costs and slower service delivery. By automating as many processes as possible, businesses can

achieve the benefits of cloud computing at an affordable price point, making cloud services an attractive option for many organizations. (Raj and Raman 2018, McHaney 2021)

Many IT organizations currently use ad hoc automation techniques which result in disjointed automation and higher costs. Cloud orchestration, on the other hand, offers a more structured approach to maximize agility and cost savings. This allows businesses to quickly deliver new innovations and applications by coordinating processes across domains, systems, and teams. Cloud orchestration also utilizes a unified portal and IT service model with full-stack automation and monitoring, which improves the customer experience and ensures error-free delivery and continuous compliance. (Raj and Raman 2018)

To achieve this, Cloud orchestration automates the deployment of services in a Cloud environment by managing complex server systems, network solutions, storage appliances and arrays, middleware, and services. This includes managing Cloud infrastructures to allocate required resources, such as creating VMs and containers, allocating storage capacity, managing network resources, and granting access to Cloud software. By utilizing orchestration mechanisms, users can easily deploy services on servers or any Cloud platforms. (Raj and Raman 2018)

There are three main aspects to Cloud orchestration, which include resource orchestration to identify and allocate resources, workload orchestration to share workloads among resources, and service orchestration to deploy services on servers or Cloud environments. The process of Cloud orchestration is shown in Figure 2, which demonstrates how it automates services in different types of Clouds, including public, private, and hybrid Clouds. Figure 3 and 4 shows a closer view of how automation differs from orchestration but still links together. (Raj and Raman 2018)

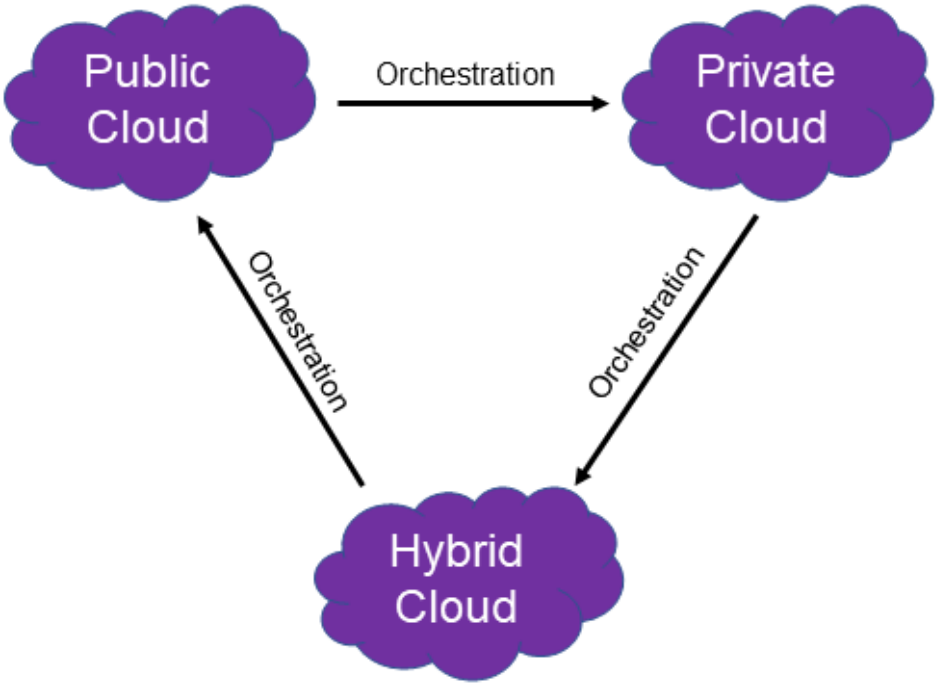

Figure 2. *Orchestration's role in formation of multi-cloud environments (Raman 2018)*

Figure 3 shows how automation in a classic IT environment works separately from other automation tasks and have no link to one another, while the IT environment in figure 4 shows a view of how orchestration links together with automation tasks. (McHaney 2021)

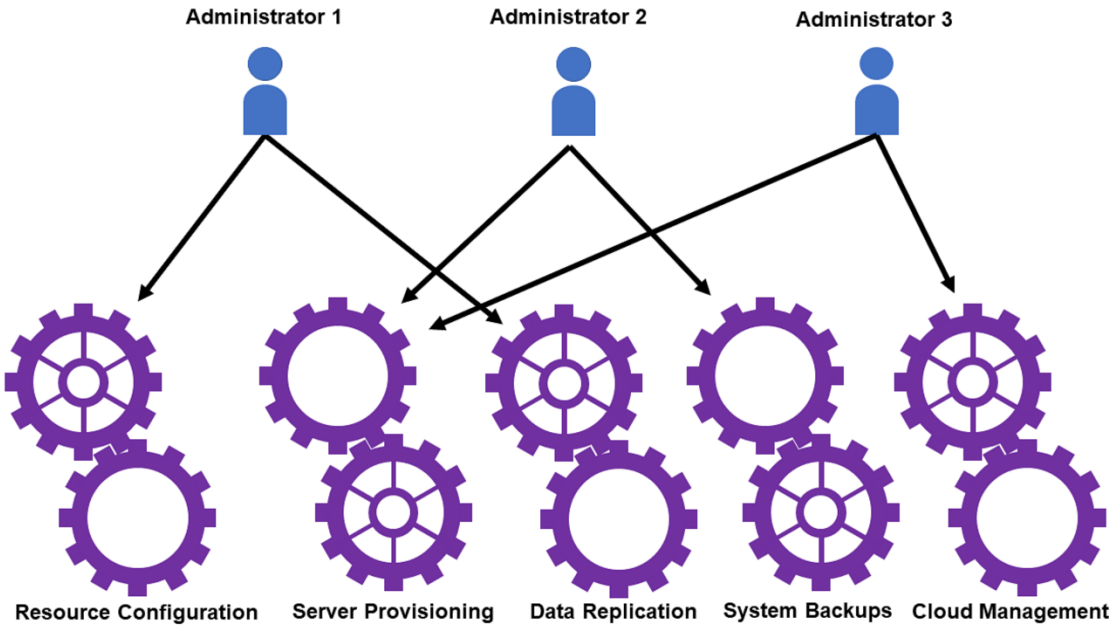

Figure 3. *Classic IT Automation (McHaney 2021)*

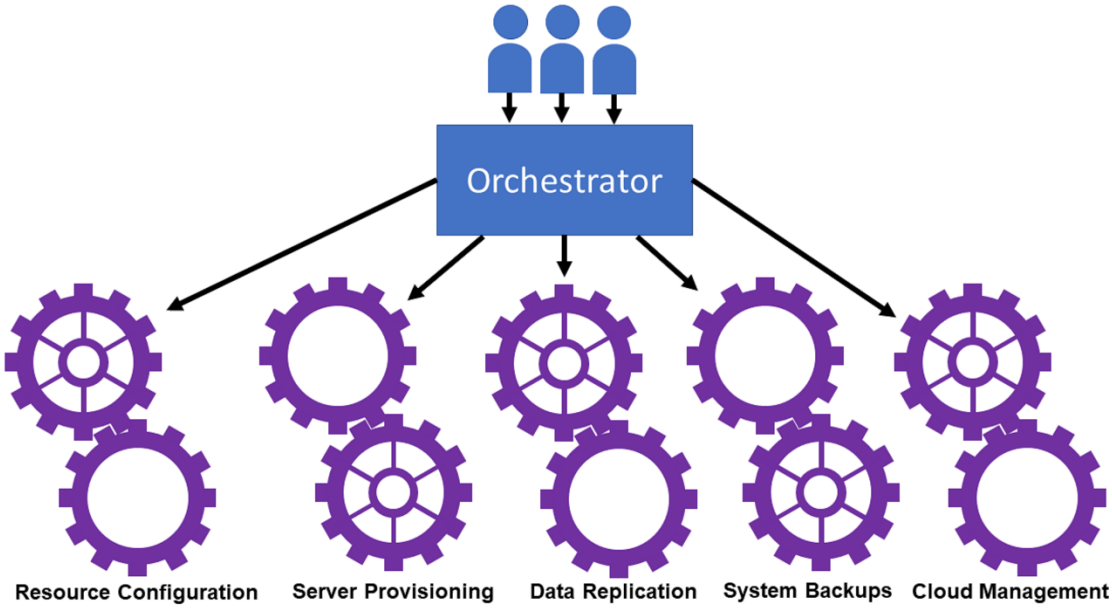

Figure 4. *Orchestration and Classic IT Automation working together (McHaney 2021)*

These tools can several Cloud providers appear as a single provider and ensure the configuration of all Cloud dependencies within a single configuration model. With the help of these tools, organizations can automatically deploy and manage multi-cloud environments. Some of the major players in this space are RightScale, Cloudify, VMware

vRealize Orchestrator, and IBM Cloud orchestrator, which provide a standard set of interfaces and capabilities across a multi-cloud environment. (Raj and Raman 2018, McHaney 2021)

Multi-cloud management platforms offer a range of capabilities, such as guiding applications through design, transition, and deployment stages, automating installation and configuration of infrastructure packages and services, provisioning application environments, developing and executing deployment plans, recommending cost-effective cloud services and providing a unified dashboard for cost tracking, monitoring the complete application stack, implementing security and governance controls to regulate environment-related activities, offering reusable blueprint templates for creating new environments, and delivering consolidated reports on instances used by the organization across multiple clouds. (Raj and Raman 2018, McHaney 2021)

2.6 Containerization

Containers and VMs have similar functions, but they are not the same. It is common for people to mix up the terms "operating system virtualization" and "operating-system-level virtualization" (which refers to containers). Containers use less memory compared to a similar VM. VMs emulate a hardware system, allowing multiple OSs to operate independently on the same physical machine. Hypervisor software emulates the necessary hardware resources (such as CPUs, memory, storage, and network) from a pool of resources, particularly in cloud environments. The hypervisor ensures that multiple VMs can share resources. As a result, VMs require more memory because each one needs a guest OS. In contrast, containers share the host OS. Although VMs may be larger and take more time to create and run compared to an equivalent container, they have the added benefit of being flexible enough to support multiple OSs from various vendors and different versions of OSs, including older ones. (McHaney 2021)

The Docker technology has caused a significant impact on the world of software. Containerization has brought about numerous advancements, many of which were previously unknown. The Docker platform, with its open-source features, has solved the long-standing issue of software portability. The elasticity of Docker containers and their ability to host a variety of microservices has made real-time scalability of business-critical applications possible, contributing to the increasing popularity of containerization. This intersection of microservices and Docker containers has brought about significant changes for software developers and system administrators. The lightweight and standardized

packaging format of Docker containers, combined with the Docker platform, has made software deployment more efficient and faster. (Raj and Raman 2018, McHaney 2021)

Containers package software, along with configuration files, dependencies, and required binaries, enabling them to work in any operating environment. There are several benefits to using containers, including environment consistency, faster deployment, and isolation. Containers enable consistency in applications, processes, and microservices, making testing and debugging less cumbersome and more efficient. Containers are lightweight and can start and stop in a few seconds, which helps with faster creation, deployment, and high availability. Additionally, containers running on the same machine using the same resources are isolated from one another, which prevents processes running within one container from affecting processes running in another container or in the host system. This isolation can be further enhanced by using isolated containers that have their own kernel and leverage virtualization mechanisms to provide stronger isolation, such as Intel's Clear Containers or HyperHQ's Hyper. (Raj and Raman 2018, McHaney 2021)

To address the challenge of transitioning legacy applications from virtual machines (VMs) to containers, a hybrid solution has emerged in the form of unified platforms. These platforms, such as Mirantis Cloud Platform (MCP) 1.0, allow workloads to be split between containers, VMs, and non-virtualized resources to achieve optimal performance and cost-efficiency. MCP 1.0 includes OpenStack, Kubernetes, and OpenContrail, allowing these components to work together to support legacy application stacks in various stages of transformation. This approach enables organizations to leverage the best aspects of each workload type, resulting in a flexible and efficient hybrid cloud environment. (Raj, Raman 2018)

2.7 Devops

Cloud computing is going through significant changes, and one of the emerging trends is the growing popularity of DevOps. DevOps is a software development methodology that emphasizes collaboration, communication, and integration between development and operations teams. It involves automating the software delivery process and using

tools and practices to enable continuous integration and delivery (CI/CD). DevOps aims to create a culture of collaboration and shared responsibility, where developers and operations work together to deliver high-quality software more quickly and reliably. The goal of DevOps is to increase the speed and efficiency of software delivery, while also improving quality and reducing the risk of failures in production. However, to take full advantage of DevOps, organizations need to consider the challenges of multi-cloud application deployment. In the current multi-cloud era, it is crucial to address several problems, such as finding DevOps tools that can deploy application code quickly and reliably to multi-clouds. Traditional engineering teams often work in silos that allow counterproductive practices to persist, leading to long release cycles, missed deadlines, and low product quality. DevOps, on the other hand, bridges organizational gaps to deliver greater value for both internal and external customers by removing strict division of responsibility and enabling collaboration and automation. (Raj and Raman 2018, Trautman 2018, McHaney 2021)

Enterprises increasingly use cloud-native and cloud-enabled applications hosted on multiple cloud environments, and DevOps tools must be able to adapt dynamically to these environments without human intervention. To support multi-cloud deployment and delivery, the DevOps processes and tools need to be enhanced to include security and governance aspects, such as logging, tagging, and cloud governance concepts. To achieve a complete DevOps automation solution, infrastructure automation is crucial in a hybrid cloud. A model-based approach that accounts for an application's various dependencies and a policy-based approach that naturally complements model-based automation is recommended. Additionally, a workflow-driven orchestration and lifecycle management approach helps coordinate tasks centrally. DevOps needs a central location where all workflows can be defined, maintained, monitored, and shared, with a unified view for collaboration and a common perspective on all applications and services being managed. Any DevOps automation solution should work with existing solutions and leverage them for tasks they are best suited to, enabling reuse of existing automation. Finally, organizations must select model-based, workflow-driven automation tools that integrate well with their chosen cloud management framework. (Raj and Raman 2018, Trautman 2018)

In a multi-cloud deployment, the same code set and accompanying data are selected for a target platform during staging. The application then undergoes platform-specific testing, shown in figure 5, to identify any issues that may arise when using the unique features of each cloud platform. For instance, the testing engine verifies that provisioning

aligns with the target platform and checks for issues that could affect performance or prevent the application from running on the target platform.

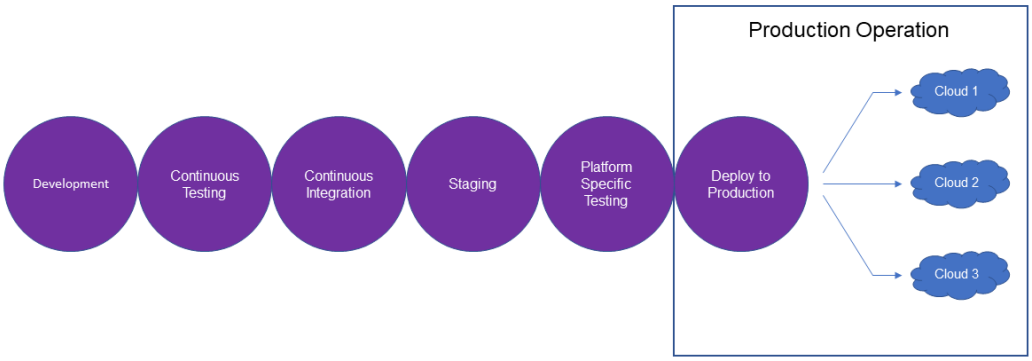

Figure 5. *Multi-Cloud environment continuous deployment (Raman 2018)*

Ideally, a well-designed system automates issue resolution or flags them for manual correction by the developer. After correcting any issues, the application must go through platform-specific testing again. (Raj and Raman 2018)

Once all platform-specific issues are resolved, the application proceeds to the deployment to production stage, where it is packaged for deployment to each target cloud platform. The application is deployed to a machine instance within a private or public cloud and subjected to continuous operations, which include monitoring, management, resource governance, service governance/catalogue, and security. (Raj and Raman 2018)

2.8 Multi-cloud management through predictive analytics

As multi-cloud environments become more complex, IT organizations will have to provide business users and developers with a consolidated approach to multiple cloud services. This will include contract management, spending optimization, SLA enforcement, and regulatory compliance. Effective management of complicated multi-cloud environments is critical for achieving digital transformation. Cloud management platforms are typically an excellent choice for providing unified automation, monitoring, and analytics

across multiple clouds. Additionally, leveraging Artificial Intelligence for Operations (AIOps) can help optimize the multi-cloud platform. AIOps analyses the health and behaviour of workloads end-to-end, providing advice for optimization and discovering issues cross-platform, from the perspective of the application and even the business chain. (Raj and Raman 2018, Mulder 2020).

As Cloud computing becomes more complex, predictive analytics can help predict resource consumption rates, costs, and availability. Due to the deployment of software applications and data sources on various Clouds, predictive analytics can project and forecast future events based on historical and real-time data patterns and trends. Predictive analytics are used for predicting and managing the cost of Cloud services, preventing server and network failures, and managing customer experiences. To maximize the benefits of predictive analytics in a multi-cloud environment, data must be at the centre of everything. Data is the gravity that holds all the business applications together and drives every business decision. Predictive analytics can proactively manage IT resources, ensure meeting licensing and service-level agreement requirements, and predict bottlenecks and process entanglements. Therefore, a refined data strategy and accessible and flexible data storage are essential to make the most of business analytics. Removing data silos inside each Cloud is necessary to make a collection of Cloud services work holistically for the business (Raj and Raman 2018, Mulder 2020).

3. TOOLS

Section two of the thesis researched various topics and best practices to use, while managing an IT infrastructure. From that research five main topics of tools arose that are investigated in more detail below of this section and further analysed from the case company's perspective in section four. This section also explains how the data for various tools were gathered and how the tools are used. The five main topic areas are:

- Resource provisioning tools: These tools are used to automate the process of deploying and managing resources such as servers, storage, and networking equipment.
- Configuration management tools: These tools help IT teams manage and automate the configuration of servers, applications, and other IT resources.
- Monitoring tools: These tools provide visibility into the performance and health of IT resources, allowing IT teams to identify and resolve issues before they impact users.
- Orchestration tools: These tools are used to automate and streamline complex workflows and processes across different IT systems and resources. Orchestration tools enable IT teams to automate tasks such as resource provisioning, application deployment, and configuration management, as well as enable integration and automation between different systems and applications.
- Backup and recovery tools: These tools help IT teams protect data and applications by creating backups and providing mechanisms for recovering from data loss or system failures.

The tools reviewed in this section were chosen by using Googles search engine with the keyword "*Top 10 IT [topic]*" i.e "*Top 10 IT resource provisioning tools*". From the search results, the five topmost websites related to the search query where chosen. If the website had a sorting system for the tools, the tools were sorted according to popularity. If the website did not have a way to sort the tools or the filter did not have a filter for popularity, tools were picked based on how it could be interpreted that the website author ranked the tools. The tools were then chosen by calculating the total sum of point based on their ranking. The top five tools were chosen to keep the thesis from growing too much. Environment specific tools like Microsoft owned Bicep and AWS CloudFormation are not included in the review, since these tools cannot be used in other environments,

which defeats the purpose on this thesis research. The description of the tools was gathered from the tool developer's websites.

3.1 Resource provisioning

Efficiently provisioning and managing IT resources is a critical task for any organization. Resource provisioning tools help automate the process of provisioning and managing resources such as servers, storage, and networking equipment. These tools can save time and reduce the risk of errors in the provisioning process, as well as enable organizations to quickly and easily scale their IT infrastructure as needed.

Resource provisioning tools

Popularity \ Website	Xenonstack.com	spectralops.io	biplus.com.vn	spacelift.io	medium.com
10 (Highest popularity)	Terraform	Terraform	Terraform	Terraform	Brainboard
9	Ansible	Spectralops	Chef	Ansible	Ansible
8	Chef	Chef	Ansible	Pulumi	Kubernetes
7	Puppet	Puppet	Puppet	Spacelift	Jenkins
6	SaltStack	SaltStack	SaltStack	AWS CloudFormation *	Chef
5	(R)?ex	Vagrant	(R)?ex	Azure Resource Manager *	Puppet
4	Vagrant	Pulumi	Vagrant	Google Cloud Deployment Manager *	SaltStack
3	AWS CloudFormation *	AWS CloudFormation *	AWS CloudFormation *	-	Vagrant
2	Azure Resource Manager *	Azure Resource Manager *	Azure Resource Manager *	-	Attune
1 (Lowest popularity)	Google Cloud Deployment Manager *	Google Cloud Deployment Manager *	Google Cloud Deployment Manager *	-	Pulumi

* Environment specific tool skipped and moved to the end of list

Figure 6. *Resource provisioning tools ranking*

In figure 6 the resource provisioning tools have been ranked, based on the opinion of the website content creator or if no opinion on popularity was given, the placement on the ranking table was chosen based in order of appearance on the website.

3.1.1 Terraform

Terraform, developed by HashiCorp, is an open-source Infrastructure as Code (IaC) tool. It allows the definition and management of infrastructure as code, offering a secure and dependable method for creating, modifying, and versioning infrastructure. Terraform enables the creation and management of resources across various cloud providers such as AWS, Google Cloud, Azure, and many others, as well as on-premises data centers.

Some common use-cases for Terraform include setting up virtual machines, configuring networks, deploying container orchestration platforms like Kubernetes, and automating the provisioning of serverless applications.

Using Terraform, infrastructure is defined as a set of declarative configuration files in HashiCorp Configuration Language (HCL) or JSON format. These files outline the desired state of your infrastructure, comprising the resources, their configurations, dependencies, and relationships. Terraform is responsible for provisioning, updating, and decommissioning resources to match the desired state.

Terraform offers several advantages over traditional infrastructure management approaches. First, it allows version control of infrastructure like any other software code, enabling tracking of infrastructure changes over time, collaboration with others, and rolling back changes when necessary. Second, it facilitates safe and predictable infrastructure changes, minimizing manual errors and reducing downtime risks. Third, it encourages the reuse of infrastructure code, enabling the creation and management of infrastructure as a set of reusable modules. This makes it easier for users to apply consistent configurations across multiple environments, such as development, staging, and production.

Terraform has a large and active community, with numerous third-party providers and modules available to enhance its functionality. It integrates well with other tools and services, such as Ansible, Jenkins, and GitLab, making it a popular choice for DevOps teams and infrastructure engineers. (Hashicorp 2023)

3.1.2 Ansible

Ansible, developed by Red Hat, is an open-source automation tool for managing and provisioning IT infrastructure. Written in Python, it operates via SSH or PowerShell protocols. Ansible allows automation of repetitive tasks, management of complex deployments, and streamlining of infrastructure operations. Some common use-cases for Ansible include automating server provisioning, configuring network devices, managing user accounts, and deploying security updates. Its core uses a straightforward, declarative language called Yet Another Markup Language (YAML) to define the desired state of infrastructure. Users write playbooks in YAML that detail tasks to be executed on a set of target hosts. These playbooks can install packages, configure servers, deploy applications, and more. Ansible utilizes modules to perform these tasks, which are reusable code snippets that can be shared and extended.

A key benefit of Ansible is its agentless nature, meaning no software installation is required on target hosts. Instead, Ansible uses SSH or PowerShell to communicate with hosts and execute the required tasks. This makes it compatible with various operating systems and cloud providers. It allows seamless integration with other tools and platforms, such as Terraform, Jenkins, and GitLab. Ansible provides a broad range of features, making it a potent tool for automation. These include:

• Idempotence: Ansible ensures that the desired state of infrastructure is maintained even when the playbook is run multiple times.

• Ad-hoc commands: Ansible's ad-hoc mode allows running quick, one-time commands on a set of hosts.

• Roles: Users can organize playbooks into reusable roles, which can be shared and extended across the organization.

• Ansible Galaxy: Ansible Galaxy is a community-driven hub for sharing roles and collections.

• Variables: Ansible enables the definition of variables that can be used to parameterize your playbooks.

• Templates: Ansible's templating engine allows you to create dynamic configuration files that can be customized for each host. This feature is particularly useful for managing configuration drift and enforcing consistent settings across your infrastructure.

In summary, Ansible is a robust automation tool that can help simplify and streamline your IT operations. Its agentless architecture, simple syntax, and vast community make it a popular choice for DevOps teams and IT professionals. (Ansible 2023)

3.1.3 Chef

Chef, developed by Chef Software, is an open-source configuration management tool used for automating the deployment and management of infrastructure. Written in Ruby, it uses a domain-specific language called Chef DSL to describe the desired state of infrastructure. Chef allows you to automate software installation and configuration and manage the provisioning of infrastructure across multiple cloud providers and on-premises data centers. Some common use-cases for Chef include automating server configurations, managing application deployments, maintaining security policies, and ensuring compliance across your infrastructure. Chef is based on the concept of Infrastructure as Code (IAC). Users write code describing the desired state of infrastructure, and Chef

ensures that the environment conforms to this state. This code is organized into cookbooks, which are collections of recipes and resources detailing how to configure specific aspects of infrastructure.

A key benefit of Chef is its adaptability, allowing management of a wide range of infrastructure, from small applications to large, complex environments. Chef offers a variety of built-in resources and plugins to manage server configurations, databases, and network devices. It also allows for seamless integration with popular cloud providers like AWS, Azure, and Google Cloud Platform.

Chef is designed to be extensible, allowing users to create custom resources and plugins to expand Chef's functionality and integrate with other tools in their environment. Chef also integrates well with other DevOps tools, such as Jenkins, Git, and Docker. Another key advantage of Chef is its ability to handle complex deployments, offering features such as role-based management that enable grouping hosts by function and applying configurations to all hosts in a specific role. This is particularly useful for managing large-scale environments with varying requirements across different hosts. Chef also includes an auditing feature for tracking infrastructure changes over time, which helps maintain visibility and accountability in your infrastructure management processes.

In conclusion, Chef is a powerful configuration management tool that can help automate your infrastructure and simplify your operations. Its flexibility, extensibility, and support for complex deployments make it a popular choice for DevOps teams and infrastructure engineers. (Chef 2023)

3.1.4 Puppet

Puppet, developed by Puppet Labs, is an open-source configuration management tool used to automate the deployment and management of IT infrastructure. Written in Ruby, it employs a declarative language called Puppet DSL to describe the desired state of infrastructure. Puppet enables users to automate software installation and configuration and manage the provisioning of infrastructure across various cloud providers and on-premises data centers. Some common use-cases for Puppet include automating patch management, configuring network devices, managing user accounts, and enforcing security policies. As with Chef, Puppet is based on the concept of IAC. Users write code describing the desired state of infrastructure, and Puppet ensures that the environment conforms to this state. This code is organized into modules, which are collections of manifests and resources detailing how to configure specific aspects of infrastructure.

A key benefit of Puppet is its emphasis on scalability and repeatability. Puppet enables the management of large, complex environments with ease, using features such as node classification to group hosts by function and apply configurations to all hosts in a particular group. This allows for efficient management of diverse infrastructure environments and ensures consistency in configuration across multiple hosts. Puppet also offers a robust reporting system for tracking infrastructure changes over time, providing insights into the state of your infrastructure and facilitating audits and compliance efforts. Puppet is designed to be extensible, allowing users to create custom resources and plugins to expand Puppet's functionality and integrate with other tools in their environment. Puppet also integrates well with other DevOps tools, such as Jenkins, Git, and Docker.

Another key advantage of Puppet is its ability to handle cross-platform environments. Puppet offers a variety of built-in resources and plugins to manage infrastructure across multiple operating systems and cloud providers. This makes it an ideal choice for organizations with heterogeneous environments, as it simplifies management and reduces the need for multiple tools.

In conclusion, Puppet is a powerful configuration management tool that can help automate your infrastructure and simplify your operations. Its scalability, repeatability, and support for cross-platform environments make it a popular choice for DevOps teams and infrastructure engineers. (Puppet 2023)

3.1.5 SaltStack

SaltStack, also known as Salt, is an open-source configuration management and automation tool used to manage IT infrastructure. Developed by SaltStack, it is written in Python and employs a domain-specific language called Salt State to describe the desired state of your infrastructure. With SaltStack, you can automate software installation and configuration, as well as manage the provisioning of infrastructure across multiple cloud providers and on-premises data centers. Some common use-cases for SaltStack include automating server configurations, managing application deployments, enforcing security policies, and orchestrating complex workflows.

As with Chef and Puppet, SaltStack is based on the idea of IAC. You write code that describes the desired state of your infrastructure, and SaltStack takes care of applying that code to your environment to ensure that it remains in the desired state. This code is organized into Salt States, which are collections of states and modules that describe how to configure a particular aspect of your infrastructure. One of the key benefits of SaltStack is its speed and scalability. SaltStack uses a client-server architecture that enables it to

manage large, complex environments with ease. It also provides features such as parallel execution and remote execution, which allow you to manage infrastructure across multiple systems simultaneously, improving efficiency and reducing deployment times.

SaltStack is designed to be extensible. You can write your own custom modules and plugins to extend SaltStack's functionality and integrate it with other tools in your environment. Additionally, SaltStack integrates well with other tools in the DevOps toolchain, such as Jenkins, Git, and Docker.

Another key benefit of SaltStack is its support for event-driven automation. SaltStack provides an event bus that allows you to trigger actions based on changes to your infrastructure, such as scaling up or down based on demand. This enables you to create dynamic, responsive systems that can adapt to changing conditions and requirements, minimizing manual intervention and reducing operational overhead.

Overall, SaltStack is a powerful configuration management and automation tool that can help you simplify your operations and reduce the time and effort required to manage IT infrastructure. Its speed, scalability, and support for event-driven automation make it a popular choice for DevOps teams and infrastructure engineers. (Revankar 2018)

3.2 Configuration management

In order to maintain consistent performance and stability in IT environments, configuration management is essential. Configuration management tools help IT teams manage and automate the configuration of servers, applications, and other IT resources. By automating configuration management, these tools can reduce the risk of errors and ensure that all IT resources are configured to the organization's standards.

Configuration management tools					
Popularity \ Website	upguard.com	softwaretestinghelp.com	theqalead.com	G2.com	itoutposts.com
10 (Highest popularity)	CFEngine	CFEngine	SysAid	Github	Ansible
9	Puppet	Chef	ManageEngine ServiceDesk Plus	CloudBees	Terraform
8	Chef	Rudder	Comindware Tracker	ServiceNow	Chef
7	Ansible	Bamboo	ManageEngine Service Desk Plus	Ansible	Vagrant
6	SaltStack	Puppet	ServiceNow	SaltStack	TeamCity
5	Docker	Ansible	Jira Service Management	Chef	Puppet
4	PowerShell DSC	SaltStack	Octopus	Codenvy	Octopus
3	TeamCity	Juju	Pointel CMS	TeamCity	SaltStack
2	Juju	Team City	Micro Focus Configuration Management System	Terraform	AWS Config *
1 (Lowest popularity)	Rudder	Octopus Deploy	Ansible	Bamboo	Microsoft Endpoint Manager *
* Environment specific tool skipped and moved to the end of list					

Figure 7. *Configuration management tools ranking*

In figure 7, configuration management tools have been ranked, based on the opinion of the website content creator or if no opinion on popularity was given, the placement on the ranking table was chosen based in order of appearance on the website. Although Ansible, Chef, Puppet and SaltStack are primarily configuration management tools, they can also be used to provision resources. The mentioned tools were already covered in the previous section (3.1) and are thus not covered here.

3.2.1 CFEngine

CFEngine is an open-source configuration management and automation solution employed to manage IT infrastructure. Developed by CFEngine AS, it is written in C and utilizes a declarative language known as CFEngine Policy to define the desired state of your infrastructure. CFEngine enables you to automate software installation and configuration while managing infrastructure provisioning across multiple cloud providers and on-premises data centers. Some common use-cases for CFEngine include automating system updates, managing user accounts, enforcing security policies, and monitoring compliance with regulatory standards. At its core, CFEngine is founded on the concept of self-healing systems. You create code that outlines the desired state of your infrastructure, and CFEngine ensures its application to maintain that state. CFEngine is designed to continuously monitor your infrastructure and automatically rectify any discrepancies from the desired state.

A key advantage of CFEngine is its emphasis on scalability and efficiency. Utilizing a client-server architecture, CFEngine can easily manage extensive, intricate environments. Features such as parallel execution and delta reporting facilitate the efficient management of infrastructure across numerous systems simultaneously, reducing the time required for deployments and ensuring consistent configurations across your infrastructure. CFEngine is also designed to be adaptable, allowing you to create custom policies and plugins to extend its functionality and integrate it with other tools in your environment. Moreover, CFEngine seamlessly integrates with other DevOps tools, including Jenkins, Git, and Docker.

CFEngine also supports policy-driven automation, providing a robust policy language for crafting complex policies that automate a wide array of tasks, from basic software installation and configuration to comprehensive security compliance checks. This enables you to create sophisticated, automated workflows that can respond to changing conditions and requirements, minimizing manual intervention and reducing the risk of human error.

In summary, CFEngine is a potent configuration management and automation solution that can streamline operations and minimize the time and effort needed to manage IT infrastructure. Its focus on self-healing systems, scalability, and policy-driven automation make it a favored choice for DevOps teams and infrastructure engineers. (CFEngine 2023)

3.3 Monitoring

To ensure optimal performance and availability of IT resources, monitoring tools provide visibility into the performance and health of IT resources. These tools allow IT teams to identify and resolve issues before they impact users, as well as track performance over time and plan for capacity needs. Monitoring tools are critical for ensuring the reliability and availability of IT resources.

Monitoring tools					
Popularity \ Website	gartner.com	sematext.com	softwaretestinghelp.com	trustradius.com	betterstack.com
10 (Highest popularity)	Paessler PRTG	Sematext Monitoring	Datadog	LogicMonitor	Better Uptime
9	OpManager	Elastic Stack	Auvik	Splunk	Dynatrace
8	Zabbix	Prometheus	Nagios	Auvik	Zabbix
7	Datadog	Zabbix	Paessler PRTG	ScienceLogic SL1	Elastic Stack
6	SolarWinds	SolarWinds	Zabbix	New Relic	New Relic
5	Nagios XI	N-able RMM	Checkmk	SolarWinds	AppDynamics
4	Dynatrace	Datadog	Progress WhatsUp Gold	AppDynamics	Site24x7
3	SCOM	OpManager	OpManager	-	Datadog
2	Progress WhatsUp Gold	Paessler PRTG	Infopulse	-	Prometheus
1 (Lowest popularity)	VMware vRealize Operations *	Nagios	Dynatrace	-	Sematext
* Environment specific tool skipped and moved to the end of list					

Figure 8. *Monitoring tools ranking*

In figure 8, monitoring tools have been ranked, based on the opinion of the website content creator or if no opinion on popularity was given, the placement on the ranking table was chosen based in order of appearance on the website.

3.3.1 Zabbix

Zabbix is an open-source monitoring and alerting solution that tracks IT infrastructure health and performance. Users can monitor real-time server, application, network device, and other IT resource performance. Developed by Zabbix SIA, the C-based solution employs a robust agent-based architecture for data collection. Custom dashboards facilitate infrastructure health and performance visualization, while customiza-ble alerts, notifications, and event correlation help rapidly identify and address issues. Some common use-cases for Zabbix include monitoring resource utilization, tracking application performance, identifying network bottlenecks, and predicting infrastructure capacity requirements.

A key advantage of Zabbix is its adaptability and scalability, capable of monitoring tens of thousands of devices and supporting distributed monitoring for resources across various locations and data centers. Zabbix's extensibility enables integration with other tools. Its monitoring capabilities include network, application, and perfor-mance monitoring, supporting various data collection methods, such as SNMP, JMX, IPMI, and custom scripts. Additionally, Zabbix's anomaly detection features can help identify unusual behavior and potential security threats, allowing you to proactively address issues before

they escalate. Zabbix also offers automation support through a powerful API for monitoring and alerting task automation, along with templates for new re-source monitoring configuration.

Overall, Zabbix is a potent monitoring and alerting solution ensuring IT infrastructure health and performance, making it a popular choice among DevOps teams and infrastructure engineers for its flexibility, scalability, and automation support. (Zabbix 2023)

3.3.2 Datadog

Datadog is a cloud-based monitoring and analytics platform offering real-time insight into IT infrastructure health and performance. Users can monitor server, application, database, and other IT resource performance, as well as track metrics, logs, and traces. Developed by Datadog Inc., this platform aims to optimize operations and en-hance service reliability. Custom dashboards and alerts enable infrastructure health and performance monitoring, while anomaly detection, forecasting, and correlation analysis features facilitate rapid issue identification and resolution. Some common use-cases for Datadog include monitoring application performance, identifying and diagnosing infrastructure issues, optimizing resource usage, and tracking system security.

Datadog's key advantage is its focus on cloud-native technologies, offering out-of-the-box support for AWS, GCP, Azure, and popular container technologies such as Kubernetes and Docker, ensuring seamless infrastructure performance monitoring re-gardless of deployment location. Its monitoring capabilities encompass infrastructure, application, and network monitoring, and it integrates with numerous third-party tools for easy integration.

Datadog also emphasizes collaboration, with shared dashboards, alerts, and note-books for effective team collaboration and knowledge sharing. APIs and integrations with popular communication tools like Slack and PagerDuty allow real-time team communication and collaboration.

In summary, Datadog is a powerful monitoring and analytics platform that helps or-ganizations optimize operations and enhance service reliability. Its cloud-native tech-nology focus, collaboration support, and broad monitoring capabilities make it a popu-lar choice for DevOps teams and infrastructure engineers. (Datadoghq 2023)

3.3.3 Paessler PRTG

Paessler PRTG is a network monitoring solution that enables businesses to monitor and manage their IT infrastructure in real-time. Developed by Paessler AG, it provides a comprehensive set of tools for monitoring servers, applications, and network devic-es. With PRTG, you can create custom dashboards to monitor the performance of your infrastructure. Some common use-cases for Paessler PRTG include monitoring network performance, identifying and diagnosing infrastructure issues, optimizing resource usage, and ensuring system reliability.

It provides a wide range of sensors, allowing you to monitor metrics such as CPU usage, memory usage, network traffic, and more. Additionally, PRTG provides customizable alerts and notifications, enabling you to quickly respond to any issues that arise. One of the key benefits of PRTG is its simplicity and ease of use. It is designed to be user-friendly and provides a straightforward interface that enables you to quickly set up and configure monitoring for your infrastructure. Additionally, it is highly scala-ble and can monitor networks of any size.

PRTG provides a wide range of monitoring capabilities, including network monitoring, server monitoring, application monitoring, and database monitoring. It also provides support for a wide range of protocols, in-cluding SNMP, WMI, and SSH. Another key benefit of PRTG is its affordability. It pro-vides a range of pricing options that are tailored to the needs of small and medium-sized businesses, making it an accessible solution for organizations with limited IT budgets.

Overall, PRTG is a powerful network monitoring solution that provides a comprehen-sive set of tools for monitoring and managing IT infrastructure. Its simplicity, scalabil-ity, and affordability make it a popular choice for small and medium-sized businesses looking to improve the performance and reliability of their networks. (Paessler 2023)

3.3.4 SolarWinds

SolarWinds is a network and systems management software provider that offers a wide range of solutions designed to help businesses manage and monitor their IT in-frastructure. Their suite of products includes network management, systems man-agement, database management, and IT security solutions. SolarWinds provides a variety of tools to help businesses manage their networks, including network perfor-mance monitoring, network configuration management, and network traffic analysis. Some common use-cases for SolarWinds include optimizing network performance, improving network security, managing system resources, and protecting against cyber threats.

Their solutions are designed to help businesses optimize their network performance and improve their overall network security. One of the key benefits of SolarWinds is its focus on simplicity and ease of use. Its solutions are designed to be user-friendly, with a straightforward interface that makes it easy to manage and monitor your net-work. Additionally, SolarWinds provides comprehensive reporting and analytics tools, enabling you to easily identify network issues and take corrective action.

Another key benefit of SolarWinds is its scalability. Its solutions are designed to grow with your business, making it easy to add new devices and capabilities as your net-work evolves. Additionally, SolarWinds provides flexible licensing options, enabling you to choose the solutions that best meet your needs and budget.

SolarWinds also provides a wide range of IT security solutions, including security information and event management (SIEM) solutions, intrusion detection and preven-tion systems (IDPS), and vulnerability management solutions. These solutions are designed to help businesses protect their networks from cyber threats and keep their data safe.

Overall, SolarWinds is a comprehensive network and systems management software provider that offers a range of solutions designed to help businesses optimize their IT infrastructure. Its focus on simplicity, scalability, and IT security make it a popular choice for businesses of all sizes.

3.3.5 Auvik

Auvik is a cloud-based network management solution that provides businesses with the tools they need to manage and monitor their IT infrastructure. It offers a compre-hensive suite of features, including network mapping, device discovery, and configu-ration management. With Auvik, businesses can easily identify network issues and take corrective action. It provides real-time network monitoring and alerts, enabling businesses to quickly respond to any issues that arise. Additionally, Auvik provides comprehensive reporting and analytics tools, giving businesses the insight they need to optimize their network performance. Some common use-cases for Auvik include network mapping, device management, configuration management, and real-time monitoring.

One of the key benefits of Auvik is its simplicity and ease of use. It is designed to be user-friendly, with a straightforward interface that makes it easy to manage and moni-tor your network. Additionally, Auvik is highly scalable, making it easy to add new de-vices and capabilities as your network grows.

Auvik also provides a range of integrations with third-party tools and services, ena-bling businesses to extend their network management capabilities. It provides support for a

wide range of protocols, including SNMP, WMI, and SSH, making it easy to mon-itor a variety of devices and systems. Another key benefit of Auvik is its affordability. It offers flexible pricing options that are tailored to the needs of small and medium-sized businesses, making it an accessible solution for organizations with limited IT budgets.

Overall, Auvik is a powerful cloud-based network management solution that provides businesses with the tools they need to manage and monitor their IT infrastructure. Its simplicity, scalability, and affordability make it a popular choice for businesses looking to optimize their network performance.

3.4 Orchestration

As IT environments become more complex, managing and automating workflows across different systems and resources becomes increasingly important. Orchestration tools en-able IT teams to automate tasks such as resource provisioning, application deployment, and configuration management, as well as enable integration and automation between different systems and applications. By automating these tasks, organizations can reduce the risk of errors and save time and effort.

Orchestration tools

Popularity \ Website	networkworld.com	G2.com	theqalead.com	devopscube.com	testsigma.com
10 (Highest popularity)	ActiveBatch	Mirantis	Cyclr	Kubernetes	Jenkins
9	Ansible	Kubernetes	Cloudify	OpenShift	Ansible
8	BMC	Aptible	Ansible	Hasicorp Nomad	Docker
7	Chef	SaltStack	CloudHealth	Docker Swarm	Kubernetes
6	MicroFocus	OpenShift	Cloudbolt	Rancher	Nagios
5	Puppet	Helios	BMC	Mesos	New Relic
4	Resolve	Apache Mesos	AWS CloudFormation	Google Container Engine (GKE)*	AppDynamics
3	Terraform	Platform9 Managed Kubernetes (PMK)	IBM Cloud Orchestrator	Google Cloud Run*	Splunk
2	Microsoft System Center	Centurion	Puppet	AWS Elastic Kubernetes Service (EKS) *	ELK (Elasticsearch, Logstash, Kibana)
1 (Lowest popularity)	VMware vRealize Automation	Shippable	Microsoft Azure Automation	Amazon EC2 Container Service (ECS) *	Zabbix

* Environment specific tool skipped and moved to the end of list

Figure 9. *Orchestration tools ranking*

In figure 9, orchestration tools have been ranked, based on the opinion of the website content creator or if no opinion on popularity was given, the placement on the ranking table was chosen based in order of appearance on the website. Ansible was already covered in section 3.1, and thus not covered here.

3.4.1 Kubernetes

Kubernetes is an open-source container orchestration platform that automates the deployment, scaling, and management of containerized applications. Developed by Google and now maintained by the Cloud Native Computing Foundation (CNCF), Kubernetes allows developers to manage containerized workloads and services more efficiently. The platform provides features like self-healing, load balancing, and rolling updates, which help maintain application stability and ensure high availability. Some common use-cases for Kubernetes include container orchestration, deployment automation, application scaling, multi-cloud management, and service discovery.

One of the key advantages of Kubernetes is its ability to manage complex, multi-container applications. Its architecture relies on a declarative approach, where users describe the desired state of their applications, and Kubernetes automatically takes care of deploying and maintaining that state. Kubernetes also supports a variety of storage options, including block, file, and object storage, ensuring seamless integration with various infrastructure providers.

Kubernetes is highly extensible, allowing users to build custom resources and controllers, which extend the platform's functionality. Additionally, Kubernetes has a vast ecosystem of third-party tools and integrations, which help improve monitoring, security, and other aspects of container management.

Overall, Kubernetes is a powerful container orchestration platform that simplifies the deployment and management of containerized applications. Its robust features, extensibility, and vast ecosystem make it a popular choice among DevOps teams and infrastructure engineers.

3.4.2 OpenShift

OpenShift is a container orchestration platform developed by Red Hat, built on top of Kubernetes. It simplifies the deployment, scaling, and management of containerized applications while providing additional features and enhancements to the core Kubernetes platform. OpenShift includes support for various programming languages, frameworks, and databases, enabling developers to build and deploy applications using their preferred tools and technologies. Some common use-cases for OpenShift include hybrid cloud deployments, microservices management, multi-tenancy support, and application modernization.

A key advantage of OpenShift is its comprehensive approach to application development and deployment. The platform includes built-in support for Continuous Integration and

Continuous Deployment (CI/CD) pipelines, enabling teams to automate their development processes and reduce time-to-market. OpenShift also provides a powerful web console and command-line interface, making it easy for developers and administrators to manage their applications and infrastructure.

OpenShift focuses on security and compliance, integrating features like container image scanning, role-based access control, and network segmentation. The platform supports a variety of authentication mechanisms, including OAuth, LDAP, and SAML, ensuring seamless integration with existing identity management systems.

In summary, OpenShift is a feature-rich container orchestration platform that extends Kubernetes, offering a comprehensive solution for deploying and managing containerized applications. Its support for CI/CD, security features, and seamless integration with various tools and technologies make it a popular choice for DevOps teams and infrastructure engineers. (OpenShift 2023)

3.4.3 BMC

BMC Helix ITSM is a comprehensive IT service management solution developed by BMC Software. It streamlines the delivery of IT services, enabling organizations to automate processes, enhance collaboration, and improve overall service quality. With BMC Helix ITSM, organizations can manage incidents, problems, changes, releases, and assets more effectively, resulting in improved IT service delivery and customer satisfaction. Some common use-cases for BMC Helix ITSM include IT helpdesk management, service catalog management, IT asset management, and knowledge management.

One of the key benefits of BMC Helix ITSM is its cognitive capabilities, powered by artificial intelligence and machine learning. These features enable organizations to automate repetitive tasks, reduce manual effort, and accelerate issue resolution. BMC Helix ITSM also provides a modern user interface and supports multiple channels for service requests, such as chatbots, email, and mobile applications, improving the user experience.

BMC Helix ITSM is highly customizable and extensible, allowing organizations to tailor the solution to their specific needs and integrate it with their existing tools and systems. The platform also supports a variety of deployment options, including on-premises, public cloud, and hybrid cloud environments.

In summary, BMC Helix ITSM is a powerful IT service management solution that helps organizations streamline their IT processes, improve service quality, and enhance customer satisfaction. Its cognitive capabilities, customizability, and support for multiple deployment options make it a popular choice for IT service management professionals.

3.4.4 Jenkins

Jenkins is an open-source automation server that helps organizations automate various aspects of their software development processes, including building, testing, and deploying applications. Developed by Kohsuke Kawaguchi and now maintained by the Jenkins community, it is written in Java and supports a wide range of plugins and integrations, allowing teams to build custom pipelines and automation workflows. Some common use-cases for Jenkins include automated build and testing, deployment automation, environment provisioning, artifact management, and parallel execution of tasks.

A key advantage of Jenkins is its extensibility. With thousands of available plugins, organizations can tailor Jenkins to their specific needs and integrate it with their existing development tools and systems. Jenkins supports various version control systems, build tools, and testing frameworks, making it a flexible solution for a variety of software development environments.

Jenkins focuses on improving collaboration and efficiency in development teams. Its built-in support for Continuous Integration (CI) and Continuous Delivery (CD) helps teams automate their development processes, identify issues early, and reduce time-to-market. Jenkins also provides a user-friendly web interface and comprehensive reporting capabilities, enabling teams to monitor the progress of their builds and deployments.

In conclusion, Jenkins is a versatile automation server that helps organizations streamline their software development processes and improve collaboration among team members. Its extensibility, support for CI/CD, and wide range of plugins and integrations make it a popular choice for software developers and DevOps professionals. Additional use-cases include code quality analysis, automated notifications, and integration with issue tracking systems. (Jenkins 2023)

3.5 Backup and recovery

Data protection is a critical task for any organization, and backup and recovery tools help ensure that data and applications are protected from data loss or system failures. These tools create backups of data and provide mechanisms for recovering from data loss or

system failures, reducing downtime and minimizing the risk of data loss. Backup and recovery tools are essential for ensuring business continuity and data availability.

Backup and recovery tools					
Popularity \ Website	peerspot.com	G2.com	gartner.com	softwareadvice.com	predictiveanalyticstoday.com
10 (Highest popularity)	Veeam Backup & Replication	IDrive Online Backup	Veeam Backup & Replication	Altaro VM Backup	Acronis
9	Zerto	Acronis Cyber Backup	Dell Data Protection Suite	Backblaze	vCenter Server
8	Commvault Complete Data Protection	Acronis Cyber Protect Cloud	Cohesity	BackupVault	3scale
7	Rubrik	CrashPlan	Rubrik Security Cloud	Cohesity	R-Studio
6	N-able Cove Data Protection	Druva Data Resiliency Cloud	Druva Data Resiliency Cloud	Datto SIRIS	Microsoft System Center
5	Nakivo	MSP360 Managed Backup	Commvault Backup & Recovery	G Cloud	NetWorker
4	Cohesity DataProtect	Veeam Data Platform Foundation	Veritas NetBackup Software	Keepit	Avamar
3	Veritas NetBackup	Unitrends Backup and Recovery	NAKIVO Backup & Replication	NinjaOne	Veeam
2	-	Redstor Backup and Archiving	Acronis Cyber Protect	Skyvia	NAKIVO
1 (Lowest popularity)	-	Veritas Backup Exec	Veeam Availability Suite	SyncBackPro	CloudBerry
* Environment specific tool skipped and moved to the end of list					

Figure 10. *Backup and recovery tools ranking*

In figure 10, backup and recovery tools have been ranked, based on the opinion of the website content creator or if no opinion on popularity was given, the placement on the ranking table was chosen based in order of appearance on the website.

3.5.1 Veeam Backup & Replication

Veeam Backup & Replication is a robust data protection solution developed by Veeam Software. It delivers reliable backup, replication, and recovery capabilities for virtual, physical, and cloud-based workloads. Veeam Backup & Replication is designed to help organizations safeguard their critical data and ensure business continuity. Some common use-cases include disaster recovery, long-term data retention, and granular recovery of individual files or objects.

A primary advantage of Veeam Backup & Replication is its versatility. The solution supports various environments, including VMware vSphere, Microsoft Hyper-V, Nutanix AHV, and major public clouds like AWS, Azure, and Google Cloud Platform. This flexibility allows organizations to protect their workloads, regardless of their infrastructure choices.

Veeam Backup & Replication emphasizes simplicity and ease of use. With its intuitive interface and powerful automation capabilities, organizations can streamline their data protection processes and reduce the time and effort required to manage backups and recoveries. Veeam also offers advanced features such as Instant VM Recovery, enabling organizations to minimize downtime and restore services rapidly.

In summary, Veeam Backup & Replication is an efficient data protection solution that helps organizations ensure the safety and availability of their critical data. Its versatility, ease of use, and advanced recovery features make it a popular choice for IT professionals and data center managers. (Veeam 2023)

3.5.2 Cohesity DataProtect

Cohesity DataProtect is a comprehensive data protection platform developed by Cohesity. It offers organizations a unified solution for safeguarding their data across multiple environments, including on-premises, cloud, and edge locations. Cohesity DataProtect simplifies data protection processes, helping organizations minimize risk and optimize their operations. Key use-cases include disaster recovery, compliance management, and analytics-driven data protection.

A key strength of Cohesity DataProtect lies in its ability to consolidate multiple data protection capabilities into a single platform. This includes backup, replication, and recovery for a wide range of workloads, such as virtual machines, databases, and file systems. Cohesity DataProtect's unified approach helps organizations streamline their data protection strategies and reduce complexity.

Cohesity DataProtect also emphasizes rapid recovery and reduced downtime. With features like instant mass restore and global deduplication, organizations can accelerate their recovery processes and minimize the impact of data loss incidents. Cohesity DataProtect's scalability ensures that organizations can protect their data efficiently as their needs grow.

In conclusion, Cohesity DataProtect is a comprehensive data protection platform that helps organizations safeguard their valuable data and optimize their operations. Its unified approach, rapid recovery capabilities, and scalability make it an attractive choice for IT professionals and data protection specialists. (Cohesity 2023)

3.5.3 Acronis Cyber Backup

Acronis Cyber Backup, developed by Acronis International GmbH, is a powerful data protection solution designed to secure critical data across diverse environments, including physical, virtual, and cloud-based systems. Acronis Cyber Backup helps organizations maintain business continuity and minimize the risk of data loss. Common use-cases include bare-metal recovery, granular restore, and migration between different hypervisors or cloud platforms.

One notable advantage of Acronis Cyber Backup is its comprehensive support for various platforms, such as Windows, Linux, macOS, VMware, Hyper-V, and popular public clouds like AWS and Azure. This extensive compatibility ensures that organizations can protect their data regardless of the underlying infrastructure.

Acronis Cyber Backup focuses on ease of use and efficiency. With a user-friendly interface and automation capabilities, organizations can simplify their backup and recovery processes. Acronis also offers advanced features like Active Protection, which safeguards data from ransomware attacks and other threats.

In summary, Acronis Cyber Backup is a versatile data protection solution that helps organizations secure their critical data and maintain business continuity. Its platform compatibility, user-friendly design, and advanced security features make it a popular choice for IT professionals and data protection experts. (Acronis 2023)

3.5.4 Rubrik

Rubrik is a modern data management platform developed by Rubrik, Inc. It offers a unified solution for backup, recovery, and data governance across on-premises, cloud, and edge environments. Rubrik helps organizations simplify their data protection strategies and optimize their operations. Use-cases for Rubrik include ransomware recovery, automated data lifecycle management, and policy-driven data retention.

A key benefit of Rubrik is its ability to consolidate multiple data management functions into a single platform. Rubrik supports a wide range of workloads, including virtual machines, databases, and applications, providing organizations with a comprehensive data protection solution that reduces complexity.

Rubrik also emphasizes rapid recovery and minimal downtime. With features like Live Mount and global deduplication, organizations can accelerate recovery processes and minimize the impact of data loss incidents. Rubrik's scalability ensures efficient data protection as organizations grow and their needs evolve.

In conclusion, Rubrik is a comprehensive data management platform that helps organizations safeguard their data and optimize their operations. Its unified approach, rapid recovery capabilities, and scalability make it an appealing choice for IT professionals and data protection specialists. (Rubrik 2023)

3.5.5 Druva Data Resiliency Cloud

Druva Data Resiliency Cloud, developed by Druva Inc., is a cloud-native data protection and management solution designed to secure and manage data across various environments, including endpoints, data centers, and cloud workloads. Druva Data Resiliency Cloud enables organizations to maintain business continuity and reduce the risk of data loss. Notable use-cases include remote office/branch office (ROBO) protection, endpoint data protection, and eDiscovery support.

One of the main strengths of Druva Data Resiliency Cloud is its cloud-native architecture, which leverages the scalability and flexibility of public clouds like AWS. This allows organizations to protect their data efficiently, regardless of their infrastructure choices or locations.

Druva Data Resiliency Cloud places an emphasis on simplicity and ease of use. With a centralized management console and automation capabilities, organizations can streamline their data protection processes and reduce the time and effort required to manage backups and recoveries. Druva also offers advanced features such as ransomware detection and compliance monitoring, ensuring robust security and adherence to regulatory requirements.

In summary, Druva Data Resiliency Cloud is an efficient data protection and management solution that helps organizations secure their critical data and maintain business continuity. Its cloud-native architecture, ease of use, and advanced security features make it a popular choice for IT professionals and data protection experts. (Druva 2023)

4. TOOL ANALYSIS

In this chapter, we present a comprehensive analysis of various tools utilized in the management and optimization of IT infrastructure. These tools play a vital role in enhancing the efficiency, security, and reliability of modern technology environments. The following sections delve into the specifics of five essential categories of tools: resource deployment, configuration management, monitoring, orchestration, and backup and recovery. By examining the features, benefits, and potential drawbacks of each tool within these categories, this analysis aims to provide a better understanding of their respective roles and contributions to the overall IT infrastructure management process. Through this evaluation, we hope to support decision-makers in selecting the most suitable tools to meet their organization's unique needs and requirements.

4.1 Resource deployment and configuration management tool analysis

In Sections 3.1 and 3.2, we explored various resource deployment and configuration management tools, including Terraform, Ansible, Chef, Puppet, SaltStack, and CFEngine. While these tools serve distinct purposes, they often share overlapping functionalities, primarily in resource provisioning and configuration. The most significant difference lies in the computer languages they employ. This section aims to analyze these tools by examining their respective strengths and weaknesses, assisting the case organization in making an informed decision on the most suitable tool for their needs.

Terraform, utilizing its proprietary HCL language, boasts easily-readable state files and consistency among various providers. Providers, such as CSPs, develop their own Terraform interface, which they register with the Terraform registry. However, a potential drawback arises if a CSP or hypervisor vendor does not support Terraform, rendering the tool inapplicable for certain environments. Moreover, Terraform's focus on IaC makes it a powerful choice for organizations looking to standardize and version their infrastructure configurations.

Both Ansible and SaltStack use YAML as their default language for defining resource states, with the option to switch to Python. This flexibility is advantageous for the case organization, as their application natively supports Python. These tools' capabilities are only limited by the APIs provided by the CSP or hypervisor vendors. Furthermore, Ansi-

ble's agentless architecture and ease of use make it an attractive choice for organizations seeking rapid deployment and reduced management overhead. On the other hand, SaltStack's event-driven automation and real-time reporting features provide enhanced visibility and control over infrastructure management.

Puppet and Chef resemble Ansible and SaltStack in many ways, but their proprietary languages, Ruby-based DSL for Puppet and Ruby for Chef, require users to have prior experience with the tools, which may pose a barrier to entry for some organizations. However, Puppet's robust cross-platform support and Chef's powerful cookbooks and recipes model offer valuable features that cater to diverse infrastructure requirements.

CFEngine, the oldest tool among them, uses its own domain-specific language called the CFEngine Policy Language. It is a lightweight and highly scalable solution suitable for managing large-scale infrastructures. However, it has a steeper learning curve compared to the other tools and might not be the best choice for organizations looking for simplicity and ease of use.

After careful analysis, it appears that both Ansible or SaltStack would be a suitable choice for the case organization when selecting a resource deployment and configuration management tool. Both options offer flexibility, ease of use, and compatibility with the organization's existing Python-based infrastructure, making them strong contenders in this competitive landscape. Ultimately, the decision between Ansible and SaltStack may come down to factors such as the organization's existing skillset, desired automation features, and integration requirements with their existing toolset.

4.2 Monitoring tool analysis

In Section 3.3, we examined various monitoring tools, including Zabbix, Datadog, Paessler PRTG, Solarwinds, and Auvik. These tools provide organizations with insights into the health and performance of their IT infrastructure. In this section, we will analyze each tool to determine its strengths and weaknesses, ultimately aiding the case organization in selecting the most suitable monitoring solution for their needs.

Zabbix is an open-source monitoring tool with a powerful agent-based architecture. It offers flexibility and scalability, making it suitable for environments with tens of thousands of devices. Zabbix supports a wide range of monitoring capabilities, including network, application, and performance monitoring. However, its open-source nature may require more in-house expertise to manage and maintain, as well as the need to invest time and resources into customizing and configuring the tool to fit the organization's specific requirements.

Datadog is a cloud-based monitoring and analytics platform that excels in providing real-time visibility into the health and performance of IT infrastructure. It offers comprehensive support for cloud-native technologies, making it an ideal choice for organizations utilizing AWS, GCP, Azure, Kubernetes, or Docker. Datadog also fosters collaboration through shared dashboards, alerts, and notebooks. One potential downside of Datadog is its pricing model, which may be cost-prohibitive for smaller organizations, as well as the potential for vendor lock-in due to its cloud-based nature.

Paessler PRTG is an all-in-one monitoring solution that simplifies infrastructure management by consolidating multiple monitoring tools into a single platform. It provides a user-friendly interface and a wide range of sensors for monitoring various aspects of IT infrastructure. However, PRTG's reliance on Windows-based servers may be a limitation for organizations that predominantly use non-Windows environments, and its scalability may not be as strong as some of the other options available.

Solarwinds is a comprehensive suite of monitoring and management tools that cater to diverse IT environments. Its modular architecture allows organizations to choose the specific tools they need, enabling a tailored monitoring solution. The main drawback of Solarwinds is its complex licensing and pricing structure, which may be challenging for organizations to navigate, as well as the possibility of having a steeper learning curve due to the wide array of available tools and features.

Auvik is a cloud-based network management solution focused on providing real-time network visibility and automation. It offers network topology mapping, inventory management, and device configuration backups. Auvik's cloud-based nature ensures easy deployment and low maintenance. However, its primary focus on network management may leave organizations looking for a more comprehensive monitoring solution wanting, as it lacks the broader scope of monitoring features found in some of the other tools discussed.

In conclusion, each monitoring tool offers unique benefits tailored to different organizational needs. When selecting the appropriate tool, the case organization should consider factors such as the size of their infrastructure, cloud-native technology adoption, ease of use, and budget constraints. By analyzing these factors in conjunction with the strengths and weaknesses of each tool, the case organization can make a well-informed decision that best supports their monitoring requirements.

4.3 Orchestration tools analysis

In Section 3.4, we explored various orchestration tools, including Kubernetes, OpenShift, BMC, Jenkins, and Ansible. These tools help organizations manage, deploy, and scale their applications and infrastructure efficiently. In this analysis, we will consider the specific needs of the case organization, which mainly uses Debian and VMs, with a goal to transition to Docker containers.

Kubernetes is an open-source container orchestration platform that automates deployment, scaling, and management of containerized applications. It is a powerful tool for organizations looking to adopt containerization and is compatible with Docker containers. However, Kubernetes has a steep learning curve and may require significant time and effort to master, especially for smaller organizations with limited resources, and its integration with existing systems may be complex.

OpenShift, built on Kubernetes, is an enterprise-grade container orchestration platform that offers additional features such as developer tools, integrated CI/CD pipelines, and enhanced security. OpenShift supports Debian and is well-suited for organizations transitioning to Docker containers. The main disadvantage of OpenShift is its cost, as it is a commercial product with a subscription-based pricing model, which may be a barrier for smaller organizations or those with budget constraints.

BMC provides a suite of IT management and orchestration tools that can be tailored to the specific needs of an organization. While BMC offers comprehensive support for managing VMs and traditional infrastructure, its support for containerization and Docker may not be as mature as Kubernetes or OpenShift. This could be a limiting factor for the case organization's future plans, as it may not fully align with their containerization goals.

Jenkins is an open-source automation server that simplifies the process of building, testing, and deploying applications. While it is primarily known for its CI/CD capabilities, Jenkins can also be used for orchestration tasks. It supports Debian and integrates well with Docker. However, Jenkins is not specifically designed for container orchestration, and its functionality in this area may be limited compared to Kubernetes or OpenShift, making it less suitable for organizations with a strong focus on containerization.

Ansible is a versatile automation tool that can be used for configuration management, application deployment, and orchestration. It supports Debian and can manage VMs, as well as work with Docker containers. One downside of using Ansible for container orchestration is that it may not offer the same level of scalability and advanced features as Kubernetes or OpenShift, and its primary strength lies in configuration management rather than container orchestration.

In conclusion, the case organization should consider its current infrastructure and future plans when selecting an orchestration tool. If the primary focus is on containerization and transitioning to Docker containers, Kubernetes or OpenShift may be the most suitable choices. However, if the organization requires a more versatile tool that can handle various aspects of IT management and orchestration, Ansible or Jenkins may be a better fit. Ultimately, the organization must weigh the benefits and limitations of each tool in the context of their specific needs and resources.

4.4 Backup and recovery tools analysis

In Section 3.5, we explored various backup and recovery tools, including Veeam Backup & Replication, Cohesity DataProtect, Acronis Cyber Backup, Rubrik, and Druva Data Resiliency Cloud. These tools provide critical data protection, backup, and recovery solutions to ensure business continuity and minimize downtime.

Veeam Backup & Replication is a comprehensive data protection solution that supports virtual, physical, and cloud environments. It offers fast, flexible, and reliable backup and recovery for VMs and containers. While Veeam is a popular choice for many organizations, it may require additional investment in storage and backup infrastructure, which could be a concern for organizations with limited resources or tight budgets.

Cohesity DataProtect is a modern data protection solution that consolidates backup and recovery for various environments, including VMs, physical servers, and containers. Its web-scale architecture and policy-based automation make it an efficient choice for organizations. However, Cohesity's pricing structure may be a concern for organizations with budget constraints, as the cost of the solution could impact the overall return on investment.

Acronis Cyber Backup is a versatile backup and recovery solution that supports a wide range of platforms, including Debian, VMs, and containers. Its easy-to-use interface and advanced features, such as ransomware protection, make it a valuable option. One potential drawback of Acronis is that its container support may not be as extensive as some other solutions, which could limit the organization's ability to fully leverage containerization in their environment.

Rubrik is a cloud data management platform that provides backup, recovery, and data protection across physical, virtual, and containerized environments. Its policy-driven automation and instant recovery capabilities make it an attractive choice for modern IT environments. Rubrik's primary downside is its cost, as it may be more expensive than

other solutions in the market, potentially putting it out of reach for smaller organizations or those with strict budgetary constraints.

Druva Data Resiliency Cloud is a cloud-native backup and recovery solution that protects data across VMs, physical servers, and containers. Its as-a-service model reduces complexity and eliminates the need for additional hardware investments. However, Druva's reliance on cloud infrastructure may be a concern for organizations with strict data residency or compliance requirements, as they may need to ensure their data remains within specific geographic boundaries or adhere to specific regulatory standards.

In conclusion, the case organization should evaluate each backup and recovery tool based on factors such as support for VMs, containerization readiness, ease of use, scalability, and budget. By carefully considering these factors and weighing the pros and cons of each solution, the organization can select the most suitable backup and recovery tool to safeguard their critical data and ensure a smooth transition to containerized environments.

5. CONCLUSIONS

In conclusion, this thesis has explored the challenges and solutions associated with infrastructure management in multicloud environments, particularly in the context of an organization with diverse customer requirements. The main findings revealed that the selection of appropriate tools depends on the organization's specific needs, in-house expertise, and budget constraints. The implications of these findings suggest that organizations must carefully plan and assess their requirements before committing to any specific tools. The research did not help with replacing outdated tools as tools like Zabbix and SaltStack that are in use in the case organization, are still valid. However, the research helped to realize that the case organization is missing a dedicated backup tool and even though not yet relevant, orchestration tools to manage both classic VM environments as well as container environments.

While this study has provided valuable insights, it acknowledges its limitations, such as not addressing security tools, log collection, version control, and desktop and workstation management tools. Future research could expand on these areas, as well as explore the transition from VMs to Docker containers within the case organization, and the integration of backup and orchestration tools in the infrastructure management process.

Overall, this research has shed light on the complexities of infrastructure management in multicloud environments, emphasizing the need for a strategic and adaptable approach to selecting and utilizing the appropriate tools. As organizations continue to face evolving customer demands and regulatory requirements, a robust and flexible infrastructure management strategy will be essential for success in an increasingly competitive and globalized IT landscape.

REFERENCES

[1] P. Raj, A. Raman, Software-defined cloud centers: operational and management technologies and tools, 2018

[2] M. Punke, AWS and the CLOUD act, 2019. Available: https://aws.amazon.com/blogs/security/aws-and-the-cloud-act/

[3] S. Hasbe, 90% Of Companies Have A Multicloud Destiny: Can Conventional Analytics Keep Up?, Accessed 25.3.2023, Available: https://www.forbes.com/sites/googlecloud/2022/03/04/90-of-companies-have-a-multicloud-destiny-can-conventional-analytics-keep-up/?sh=5a446c3f5d89

[4] J. Mulder, Multi-Cloud Architecture and Governance, 2020, Available: https://learning.oreilly.com/library/view/multi-cloud-architecture-and/9781800203198/B16298_01_Epub_AM.xhtml#_idParaDest-17

[5] J. Alonso, L. Orue-Echevarria, V. Casola, A. Isabel Torre, M. Huarte, E. Osaba, J Lobo, Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review, 2023

[6] M. Liaqat, V. Chang, A. Gani, S. Hafizah Hamid, M. Toseef, U. Shoaib, R. Liaqat Ali, Federated cloud resource management: Review and discussion, 2017, Available: https://www.sciencedirect.com/science/article/pii/S1084804516302387

[7] J. Morehouse, The Challenges of Multi-Cloud Management and How Observability Helps Solve Them, 2022, Available: https://orangematter.solarwinds.com/2022/10/06/multi-cloud-management-challenges/

[8] adapture.com, Accessed 3/2023, Available: https://adapture.com/key-benefits-using-cloud-aggregators/

[9] M. Sztukiewicz, What is a cloud broker?, 2013, Available: https://www.ibm.com/blogs/cloud-computing/2013/01/17/cloud-broker/

[10] P. Trautman, Designing and building a Hybrid cloud : deliver automation, visibility, and management consistency in a multi-cloud world, 2018, Available: https://learning.oreilly.com/library/view/designing-and-building/9781492036937/

[11] R. McHaney, Cloud technologies: an overview of cloud computing technologies for managers, 2021.

[12] G. Singh, Infrastructure as Code (IaC) Tools to Boost Your Productivity in 2023, January 2023, Accessed 1.4.2023, Available: https://www.xenonstack.com/blog/infrastructure-as-code-tools

[13] U. Shamay, Top 10 Infrastructure as Code (IaC) Tools to Know in 2022, August 2021, Accessed 1.4.2023, Available: https://spectralops.io/blog/top-10-infrastructure-as-code-iac-tools-to-know-in-2022/

[14] B. Xuân Hiền, Top Infrastructure As Code Tools (IaC) For 202, February 2023, Accessed 1.4.2023, Availiable: https://biplus.com.vn/infrastructure-as-code-tools/

[15] S. Ninawe, 7 Most Useful Infrastructure as Code Deployment Tools, December 2023, Accessed 1.4.2023, Available: https://spacelift.io/blog/infrastructure-as-code-tools

[16] M. Tyson, IT Automation: 10 Alternatives To Terraform, October 2022, Accessed 1.4.2023, Available: https://medium.com/@mike_tyson_cloud/it-automation-10-alternatives-to-terraform-286107def5ad

[17] K. Sen, Top 10 Configuration Management Tools You Need to Know About, May 2022, Accessed 2.4.2023, Available: https://www.upguard.com/blog/configuration-management-tools

[18] Software Testing Help, 11 BEST Software Configuration Management Tools (SCM Tools In 2023), March 2023, Accessed 2.4.2023, Available: https://www.softwaretestinghelp.com/top-5-software-configuration-management-tools/

[19] J. Boog, 10 Configuration Management Tools The Experts Love, March 2023, Accessed 2.4.2023, Available: https://theqalead.com/tools/configuration-management-tools/

[20] G2, Best Configuration Management Software, Accessed 2.4.2023, Available: https://www.g2.com/categories/configuration-management?utf8=%E2%9C%93&order=popular

[21] D. Vishnyov, Top-10 DevOps Configuration Management Tools, Accessed 2.4.2023, Available: https://itoutposts.com/blog/devops-configuration-management-tools/

[22] Gartner, IT Infrastructure monitoring tools reviews and ratings, Accessed 2.4.2023, Available: https://www.gartner.com/reviews/market/it-infrastructure-monitoring-tools

[23] E. Qadah, 15 Best IT Infrastructure Monitoring Tools & Software [2023 Comparison], Accessed 2.4.2023, Available: https://sematext.com/blog/infrastructure-monitoring-tools/

[24] Software Testing Help, Top 11 Infrastructure Monitoring Tools And Services For 2023, March 2023, Accessed 2.4.2023, Available: https://www.softwaretestinghelp.com/infrastructure-monitoring-tools-and-services/

[25] Trustradius, IT Infrastructure Monitoring Tools, Accessed 2.4.2023, Available: https://www.trustradius.com/it-infrastructure-monitoring#toprated

[26] Betterstack, 10 Best Infrastructure Monitoring Tools in 2023, Accessed 2.4.2023, Available: https://betterstack.com/community/comparisons/infrastructure-monitoring-tools/

[27] T. Ferrill, 10 top automation and orchestration tools, June 2022, Accessed 2.4.2023, Available: https://www.networkworld.com/article/3663441/10-top-automation-and-orchestration-tools.html

[28] G2, Best Container Orchestration Software, Accessed 2.4.2023, Available: https://www.g2.com/categories/container-orchestration?utf8=%E2%9C%93&order=popular

[29] E. Onukwube, 10 Best Cloud Orchestration Platforms In 2023, March 2023, Accessed 2.4.2023, Available: https://theqalead.com/tools/best-cloud-orchestration-platforms/

[30] B. Wilson, 16 Best Container Orchestration Tools and Services, January 2022, Accessed 2.4.2023, Available: https://theqalead.com/tools/best-cloud-orchestration-platforms/https://devopscube.com/docker-container-clustering-tools/

[31] K. Devaraj, Top 10 DevOps Orchestration Tools to Know and Master in 2023, January 2023, Accessed 2.4.2023, Available: https://testsigma.com/blog/devops-orchestration-tools/

[32] Peerspot, Best Backup and Recovery Software, Accessed 2.4.2023, Available: https://www.peerspot.com/categories/backup-and-recovery-software

[33] G2, Best Backup Software, Accessed 2.4.2023, Available: https://www.g2.com/categories/backup

[34] Gartner, Enterprise backup and recovery software solutions reviews and ratings, Accessed 2.4.2023, Available: https://www.gartner.com/reviews/market/enterprise-backup-and-recovery-software-solutions

[35] P. Buttan, Top 10 Backup Software, September 2022, Accessed 2.4.2023, Available: https://www.softwareadvice.com/resources/top-backup-software/

[36] Predictiveanalyticstoday, TOP 10 BACKUP SOFTWARE, Accessed 2.4.2023, Available: https://www.predictiveanalyticstoday.com/top-backup-software/

[37] Hashicorp, What is Terraform?, Accessed 2.4.2023, Available: https://developer.hashicorp.com/terraform/intro

[38] Ansible, How Ansible works, Accessed 2.4.2023, Available: https://www.ansible.com/overview/how-ansible-works

[39] Chef.io, Platform Overview, Accessed 2.4.2023, Available: https://docs.chef.io/platform_overview/

[40] Puppet, Introduction to Puppet, Accessed 2.4.2023, Available: https://www.puppet.com/docs/puppet/6/puppet_overview.html

[41] M. Revankar, What is SaltStack?, October 2018, Accessed 2.4.2023, Available: https://saltproject.io/whats-saltstack/

[42] Cfengine, What is CFEngine and Why?, Accessed 2.4.2023, Available: https://docs.cfengine.com/docs/master/overview-what-is-cfengine-and-why.html

[43] Abbix, What is Zabbix, Accessed 2.4.2023, Available: https://www.zabbix.com/documentation/current/en/manual/introduction/about

[44] Datadoghq, Getting Started in Datadog, Accessed 2.4.2023, Available: https://docs.datadoghq.com/getting_started/application/

[45] Paessler, PRTG Manual: Welcome to PRTG, Accessed 2.4.2023, Available: https://www.paessler.com/manuals/prtg/introduction

[46] Solarwinds, Main website, Accessed 2.4.2023, Available: https://www.solarwinds.com/

[47] Kubernetes.io, Main website, Accessed 13.4.2023, Available: https://kubernetes.io/

[48] redhat.com, Main website, Accessed 13.4.2023, Available: https://www.redhat.com/en/technologies/cloud-computing/openshift

[49] BMC Helix ITSM, Main website, Accessed 13.4.2023, Available: https://www.bmc.com/it-solutions/bmc-helix-itsm.html

[50] Jenkins.io, Main website, Accessed 13.4.2023, Available: https://www.jenkins.io/

[51] Veeam, Main website, Accessed 13.4.2023, Available: https://www.veeam.com/

[52] Cohesity, Main website, Accessed 13.4.2023, Available: https://www.cohesity.com/products/dataprotect/

[53] Acronis, Main website, Accessed 13.4.2023, Available: https://www.acronis.com/en-us/products/cyber-protect/backup/

[54] Rubrik, Main website, Accessed 13.4.2023, Available: https://www.rubrik.com/

[55] Druva, Main website, Accessed 13.4.2023, Available: https://www.druva.com/