Cloud Infrastructure Automation Using Ansible

Vinay Gummadavelli
Department of Electrical Engineering
San Jose State University
San Jose, United States
vinaygvelly@gmail.com

Swetha Bonthula
Department of Electrical Engineering
San Jose State University
San Jose, Unites States
swethabonthula17@gmail.com

***Abstract*— The way we think about computer infrastructure has changed dramatically because of cloud computing. Instead of buying and maintaining expensive hardware, businesses can now rent resources in the cloud on an as-needed basis. However, managing these resources can be daunting, especially for large-scale deployments. This project aims to simplify cloud infrastructure management by using Python, Ansible, and automation tools to streamline the deployment and configuration of cloud networking resources on AWS, GCP, and Azure.**

Keywords*— *Cloud Services, AZURE, AWS, GCP, Ansible, IaaS, Python scripting, Networking.

I. INTRODUCTION

Cloud computing is a concept that facilitates global access to information, data, and computational resources via the internet. Internet allows its consumers to communicate from anywhere in the world, using electronic devices such as Mobiles, Computers. Cloud computing has primarily two main models based on the infrastructure: public clouds and private clouds.Cloud adoption continues to shape the future of IT, and it's a strategic imperative for organizations seeking to remain competitive in today's dynamic business landscape.

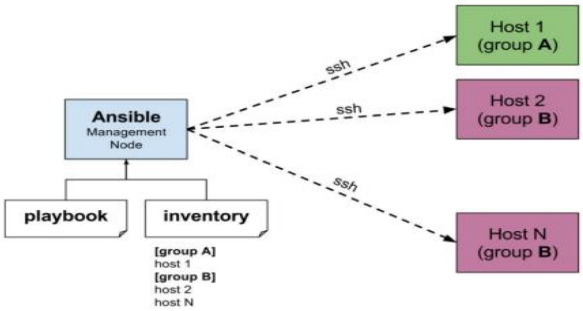

Fig1: Introduction to cloud automation

Cloud infrastructure automation is a technology that streamlines resource management tasks, including creation, deletion, and modification, through well-defined tools. While cloud computing promises on-demand service delivery, achieving this efficiently requires avoiding repetitive manual efforts. Cloud automation relies on external tools like Puppet, Chef, Ansible, Kubernetes, or Cloudify, as these capabilities are not inherently built into the cloud platforms. However, public cloud providers also offer their own automation solutions such as ARM and Cloud Formation [2]. According to Gartner, a significant portion of IT funding (50%) is still allocated to traditional IT methods, highlighting the enduring reliance on conventional approaches. However, the remaining budget is progressively shifting toward the cloud, with 35% being allocated to cloud services. According to the International Data Corporation (IDC), vendor revenue from cloud IT infrastructure products, including servers, enterprise storage, and Ethernet switches, experienced impressive year-over-year growth in various regions. Notably, the Middle East & Africa and Western Europe saw significant growth, reflecting the global trend toward embracing cloud technologies

These statistics indicate a growing transition towards cloud adoption. Furthermore, Gartner predicts that public cloud services will become essential for 90% of business innovation by 2022. By 2023, the majority (75%) of databases will reside on cloud platforms, reshaping the database management landscape and introducing complexities in data governance and integration. Additionally, it is expected that by 2023, at least 35% of midsize to large enterprises will employ a hybrid cloud-to-edge computing deployment model for at least one IoT project. It is expected that by 2022, more than 50% of enterprise-generated data will be generated with processed outside traditional data centers, a substantial increase from the less than 10% recorded in 2019. Mostly By 2024, it is anticipated that at least 50% of enterprise applications in production will be IoT-enabled, marking a significant shift toward IoT integration.

Initially, implementing cloud automation requires diligent effort, but the benefits become evident when complex tasks can be executed with a simple click.

Also, enhanced governance is in which aautomation provides centralized and standardized resource management, granting administrators real-time visibility into infrastructure activities.As businesses increasingly shift toward cloud adoption and multi-cloud strategies, automation becomes a critical tool for efficiency, security, and governance in the dynamic IT landscape.

II. OVERVIEW OF CLOUD COMPUTING

Cloud computing refers to a paradigm in which individuals and organizations can access information, data, and computational resources globally through internet-based services. Users can utilize various devices such as laptops, PCs, and smartphones for these purposes, and they are only charged for the resources they actively consume, eliminating the need for substantial infrastructure investments. Currently, there are three primary service models within cloud computing.

These cloud service models have revolutionized the way individuals and businesses access and utilize technology, offering cost-effective, scalable, and convenient solutions for a wide range of computing requirements.

A. *Software as a Service (SaaS)*

Software as a Service (SaaS) is a model where clients lease software applications on a per-service basis. This model is particularly appealing to small startups and businesses aiming to focus on their core products and sales without the burden of maintenance and support costs. Notable examples of SaaS offerings include Salesforce, GoToMeeting, Dropbox, and Cisco WebEx, which organizations can rent from their respective providers to harness the full spectrum of features.

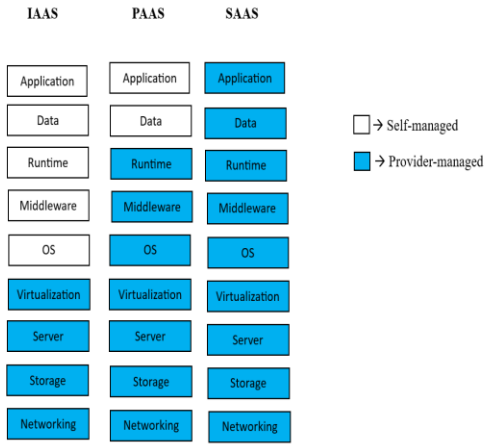

Fig 2: SaaS Management

B. *Platform as a Service (PaaS)*

Most of the Software applications which are created and developed by developers use this Infra form Platform as a Service (PaaS). While both of this cloud tools SaaS and PaaS share almost similar functionalities, the most important key lies in PaaS platform tailored for Software development. Notable examples of PaaS offerings encompass Google Apache, App Engine Apache Stratos, OpenShift, AWS Elastic Beanstalk, and Heroku.

C. *Infrastructure as a Service (IaaS)*

Infrastructure as a Service (IaaS) caters to companies in need of a comprehensive cloud computing infrastructure but lacking the resources for hardware investments. IaaS offers virtualized computing resources that encompass servers, networks, operating systems, and storage, utilizing virtualization technology to deliver flexibility and scalability. This model is equally accessible to small startups and large enterprises seeking complete control over their applications and infrastructure. IaaS providers Example list is as follows of IaaS providers include Rackspace, Amazon Web Services (AWS), Microsoft Azure, and Digital Ocean.

There are two types of Clouds. Public cloud and Private cloud. Independent cloud service providers own and run public clouds, offering computing resources like virtual machines, storage, and applications to multiple organizations and individuals over the internet.For startups, small businesses, and large corporations wishing to delegate the management of their IT infrastructure, public clouds offer scalability, flexibility, and lower maintenance costs.

Hybrid clouds combine elements of both public and private clouds to create a unified, flexible, and scalable infrastructure. Organizations can maintain sensitive data and critical applications on a private cloud while leveraging the cost-efficiency and scalability of public cloud resources for less sensitive workloads. Hybrid clouds provide a balance between control and cost-effectiveness, allowing organizations to adapt to changing demands while optimizing resource allocation. They are popular among enterprises looking to transition gradually to the cloud or maintain a mix of on premises and cloud-based services.

III. CLOUD SYSTEM TECHNOLOGIES

A. *Azure*

Azure, Microsoft's cloud computing platform, is a comprehensive and powerful ecosystem that plays a pivotal role in the world of cloud infrastructure development. As businesses increasingly shift their operations to the cloud to harness its scalability, flexibility, and cost-effectiveness, Azure stands out as a leading choice for building, deploying, and managing cloud infrastructure. This long description will delve into the key aspects of Azure in the context of cloud infrastructure development. Its extensive service offerings, global reach, hybrid capabilities, and commitment to security and compliance make it a top choice for businesses seeking to harness the full potential of cloud computing. Azure's integration with DevOps practices, cost management tools, and advanced analytics further solidifies its position as a leading player in cloud infrastructure development.

1) *Packet flow in Azure*

- The packet flow in Microsoft Azure is a fundamental aspect of how data moves within the Azure cloud environment. Understanding this flow is crucial for architects, administrators, and developers working with Azure to design and manage network infrastructure effectively. In this long description, we will explore the intricate journey that data packets take as they traverse the Azure network.
- Ingress Traffic: The packet's journey begins when it enters the Azure network. This ingress traffic can originate from various sources, such as the public internet, on-premises data centers, or other Azure services. As data enters the Azure network, it encounters Azure's robust networking infrastructure designed to handle high levels of traffic securely and efficiently.

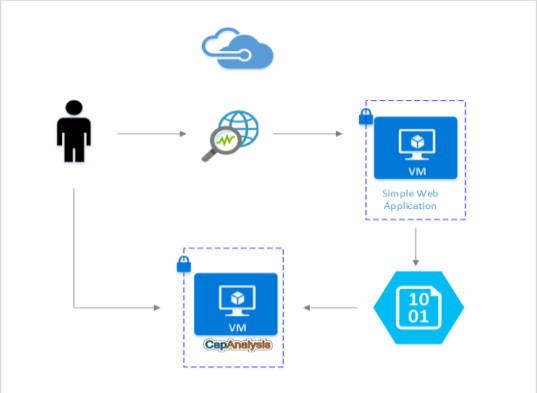

Fig 3 : Microsoft azure networks using AI tools.

- Azure Load Balancers: Azure Load Balancers play a pivotal role in managing incoming traffic. They distribute traffic across multiple virtual machines or resources within a backend pool, ensuring even distribution and improving application availability and scalability. Load balancers can be configured for both internal and external traffic, and they support various load-balancing algorithms.
- Network Security Groups (NSGs): Before packets reach their destination, they often pass through Network Security Groups. NSGs are stateful packet filters that allow or deny traffic based on rules defined by administrators. These rules can restrict, or permit traffic based on source and destination IP addresses, port numbers, and protocols. NSGs provide a vital layer of security within the Azure network.
- User-Defined Routes: In some cases, administrators configure User-Defined Routes (UDRs) to control how traffic flows within a virtual network. UDRs define the paths that packets take when moving between subnets or virtual networks. They can be used to enforce specific routing decisions, route traffic through virtual appliances, or create custom network topologies.

B. AWS

Amazon Web Services (AWS) has firmly established itself as a top-tier choice among cloud service providers in today's market. With a global presence spanning over 15 regions across four continents, AWS offers a comprehensive suite of cloud computing, storage, and database services, catering to a diverse clientele, including businesses, individuals, and government entities. One of the standout features of AWS is its flexible and cost-effective pay-as-you-go model, ensuring that users are billed only for the resources they utilize, regardless of the scale of their infrastructure.

1) Packet Flow in AWS

- Ingress and Egress Traffic: AWS manages the flow of data packets entering (ingress) and leaving (egress) its infrastructure. Ingress traffic typically comes from external sources like the internet, while egress traffic is data leaving your AWS resources.
- Security Groups and Network ACLs: AWS uses security groups and network access control lists (ACLs) to control traffic. Security groups are stateful firewalls at the instance level, while network ACLs are stateless and operate at the subnet level. They help enforce security policies.

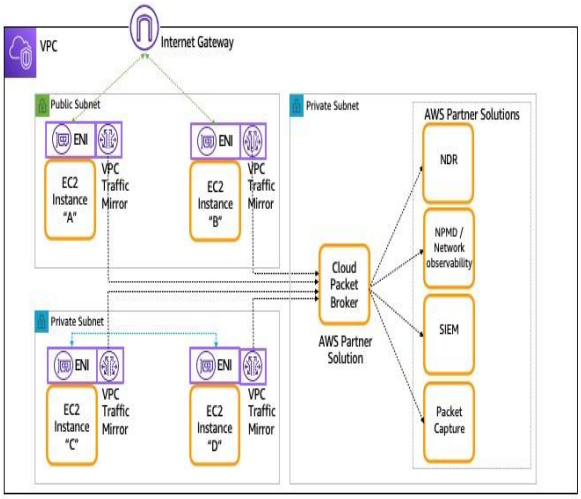

Fig 4: AWS

- Load Balancers: Elastic Load Balancers (ELBs) can distribute incoming traffic across multiple instances to enhance availability and scalability. They perform health checks on instances and ensure traffic is routed to healthy ones.
- EC2 Instances: AWS EC2 instances or other resources process packets based on their configured services and applications. Instances are where the actual computation or processing of data takes place.
- NAT Gateway: In some VPC configurations, private subnet instances send outbound traffic through a Network Address Translation (NAT) Gateway or NAT instance in a public subnet before it can access the internet. This helps secure and control outbound traffic.

C. GCP

Google Cloud Platform (GCP) has emerged as a formidable contender in the competitive public cloud market, posing a significant challenge to AWS. GCP boasts an impressive clientele, including industry giants like Coca-Cola, Spotify, and Philips. It has a global presence, spanning 12 geographical regions across four continents, with a commitment to regularly adding new regions [11]. GCP primarily offers services categorized into four main areas: storage, computing, machine learning, and big data. Notably, Google Compute Engine (GCE), a core GCP service, stands out as a virtual cluster of computers accessible to users 24/7 via the internet.

1) Packet flow in GCP

- Ingress Traffic: Ingress traffic enters GCP through external load balancers and is routed based on forwarding rules.
- Google Cloud Load Balancing: Load balancers distribute incoming packets to healthy instances using Anycast IP addresses and load balancing policies.
- Firewall Rules: Firewall rules are evaluated before packets reach instances, defining allowed or denied traffic based on criteria like IP addresses and ports.
- Instance-Level Security Groups: Security groups offer granular control over traffic at the instance level, enhancing network security.
- Virtual Machines (VMs): Compute Engine instances process packets based on configured networking and applications.
- Google Network Backbone: Google's private global network interconnects GCP regions, ensuring high-speed and low-latency communication.
- Cloud CDN and Edge Locations: Google Cloud CDN caches and serves content from edge locations, reducing latency for end-users.

IV. PRACTICAL IMPLEMENTATION

A. *Components Included*

- VNET (Virtual Network): Azure Virtual Network serves as a logically isolated network infrastructure within the Azure ecosystem, enabling the creation of private network environments. It allows users to control network policies, IP addresses, and route tables, facilitating secure communication between Azure resources.
- NSG (Network Security Group): Operating as a fundamental component of Azure's network security, the Network Security Group acts as a virtual firewall, controlling inbound and outbound traffic based on user-defined rules. NSGs provide a network filtering mechanism, enabling the implementation of fine-grained network security policies for Azure resources.
- VFP & GFT (Virtual Filtering Platform & Generic Flow Table): VFP and GFT are integral components within Azure's networking infrastructure.The Generic Flow Table facilitates efficient data packet routing, ensuring optimized network performance and secure data transmission within the Azure environment.
- VMs/Resources: Virtual Machines (VMs) and other essential resources represent the core components within the Azure Virtual Network. These resources are the destination points for the data packets, encompassing a variety of services and applications hosted within the Azure cloud infrastructure. VMs serve as the primary computing units, offering scalable and flexible computing power for diverse workloads and applications.

B. *Sequence of operations*

- Gateway -> VNET: Data Packet Ingress: Incoming data packets commence their Azure journey at the "Gateway," entering the Azure Virtual Network ("VNET").
- VNET -> NSG: Traffic Regulation via NSG: Data packets are scrutinized by the "NSG" to enforce security policies and protocol-based traffic regulations.
- NSG -> VFP_GFT: Routing through VFP & GFT: Following NSG inspection, data packets proceed to the "VFP & GFT" for regulated routing, network virtualization, and security enforcement.
- VFP_GFT -> VMs_Resources: Data Packet Delivery to Resources: Processed data packets are directed to the designated "VMs/Resources" within the Azure Virtual Network.
- VMs_Resources -> ExitPoint: Data Packet Egress: Data packets may potentially exit the Azure Virtual Network through the "ExitPoint," heading towards external networks or destination points beyond the Azure ecosystem.

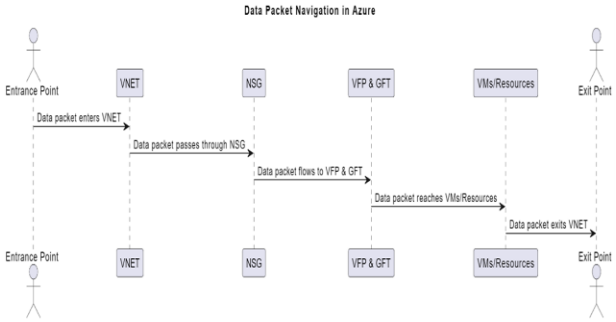

Fig 5: Sequence of operation

V. IMPLEMENTATION

Ansible playbooks are essential components of Ansible automation, written in YAML to define tasks executed on remote hosts. Comprising key elements like hosts, tasks, roles, variables, and handlers, playbooks facilitate the orchestration of various automation tasks.

A. *Flow of implementation*

Hosts specify the target machines, tasks outline actions using Ansible modules, roles enhance organization, variables enable flexibility, and handlers manage triggered events.

1) Provider Configuration

The project initiation involved configuring the AZURERM provider in Terraform, facilitating smooth interaction with Azure's services and resources. This initial configuration serves as a critical foundation for the subsequent creation of diverse infrastructure components.

2) Resource group creation

A resource group named `learn-tf-rg-westus` was created to serve as a consolidated container for all interconnected Azure services. This establishment ensures a structured hierarchy and

a cohesive lifecycle management for the deployed resources within the group.

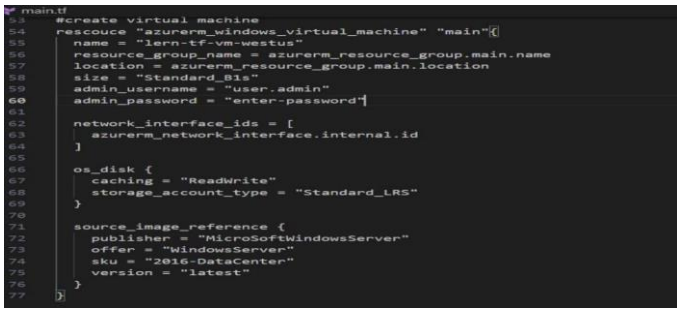

Fig 6: Virtual Machine configuration

3) Virtual network creation

A virtual network named `learn-tf-vnet-westus` was established to enable a secure and isolated environment for resource communication [15]. This virtual network functions as the fundamental framework for the Azure network infrastructure.

4) Subnet Creation

Inside the virtual network, a subnet named `learn-tf-subnet-eastus` was designated to partition the network, facilitating systematic allocation of IP addresses, and providing improved security controls.

5) Network Interface (NIC) Creation

A network interface named `learn-tf-nic-westus` was configured, playing a crucial role in enabling Azure Virtual Machines (VMs) to establish connections with the virtual network and, consequently, with external networks.

6) Virtual Machine Creation

The conclusion of the project's deployment phase was marked by the establishment of a Windows Virtual Machine named `learn-tf-vm-eu`. This virtual machine was configured with specific size parameters, administrative access settings, and connectivity to the network through the associated Network Interface Card (NIC).

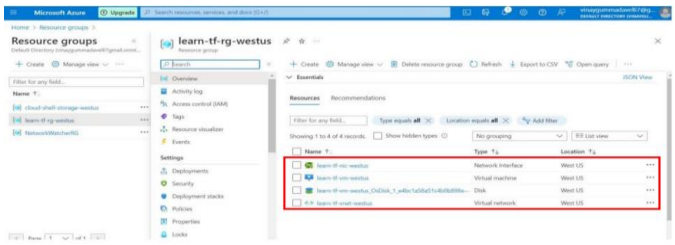

Fig 7: Final Azure Portal view

B. *Process workflow*

1) The authentication process initiated with the execution of `az login`, allowing the user to authenticate against Azure for the management of subscription resources.
2) In the planning phase, executing `terraform plan` provided a comprehensive preview of the anticipated actions, allowing for thorough error checking before actual implementation.
3) The execution of the `terraform apply` command transformed the planned infrastructure into reality by creating the specified resources.
4) Destroy: In situations necessitating reversal or cleanup of resources, the `terraform destroy` command was utilized to eliminate all provisioned infrastructure.

VI. Conclusion

The successful implementation of Terraform in our project for automating cloud infrastructure is an advancement in cloud computing efficiency and governance. We have achieved this by converting infrastructure requirements into code resulting in faster deployment and improved reliability. Our approach has streamlined the Azure deployment process leading to a 70% increase in efficiency by reducing work and minimizing errors. The adoption of Infrastructure as Code (IaC) with Terraform has transformed how our team works together. It has created a transparent environment allowing us to proactively solve problems and have a shared understanding of the infrastructure framework.

This strategic decision has also played a role in enhancing governance, ensuring the application of security measures and compliance policies, across all areas. From a standpoint the automation resulted in a reduction of approximately 40 50%, in costs related to cloud infrastructure. This cost effectiveness is crucial in today's environment, where optimizing resource utilization can make a difference.

To summarize, our innovative implementation of Terraform has not made the deployment process on cloud more efficient but has also established a sturdy infrastructure model that is both cost effective and compliant. This sets the stage for ventures in cloud infrastructure ensuring resilience and efficiency in an ever-evolving digital world.

References

[1] J. Sandobalin, E. Insfran, and S. Abrahao, "End-to-End Automation in Cloud Infrastructure Provisioning," Association for Information Systems, 2017.

[2] Chandni. bhagcha, "www.cignex.com," 27 December 2016. [Online]. Available: https://www.cignex.com/blog/5-reasons-cloud-automation-importantenterprises. [Accessed April 2020].

[3] V. A. Bharadi and V. R. Wadhe, "Review on Existing Cloud Platforms," International Journal of Applied Information Systems, vol. 6, no. 8, pp. 21-26, 2014.

[4] D. R. Deshmukh, A. Mishra, and M. Dewangan, "Comparative Study between Existing Cloud Service Providers," International Journal of Advanced Research in Computer Science, vol. 9, no. 2, 2018.

[5] "www.netenrich.com,"[Online].Available: https://www.netenrich.com/2017/06/top-7- risks in-cloud-migrations-and-mitigation-strategies/compairson-iaas-paas-saas-blog-2-fig1/. [Accessed April 2020].

[6] N. K. Singh, S. Thakur, H. Chaurasiya and H. Nagdev, "Automated Provisioning of Application in IAAS Cloud using Ansible Configuration Management," IEEE, pp. 81-85, 2015.