International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 2, March-April 2023||

DOI:10.15662/IJRPETM. 2023.0602004

Cloud Infrastructure Automation and Role-Based Access Governance in Azure Kubernetes Services

Suresh Pairu Subramanyam

Technical Manager, Full Stack Development, Columbus, OHIO, USA

ABSTRACT: Cloud solutions are making inroads on the learning curve; the need for automated infrastructure admin and good security admin is nothing new. But to get this scalable, container orchestration service securely and compliant to production and then sustain it will be challenging.Getting access and controlling access to this scalable, container orchestration service shouldn't be too hard – Azure Kubernetes Service (AKS) – and it'll be possible to comply with strict security needs. It explains in detail how in an AKS deployment, cloud RBAC is deployed and configured—with a lot of infrastructure automation, which can greatly facilitate deployment—and why it offers fine-grained access management. The objective of the study is to have the automatic provisioning of AKS clusters, and creation of dynamically generated RBAC policy applying path of Infrastructure as Code (IaC). Consistent environment configuration and least-privilege access along the framework is offered with Azure Resource Manager (ARM) templates, Terraform scripts and Kubernetes infrastructure capabilities called Role Based Access Control (RBAC). The field test has definitely demonstrated its ability to decrease the chances of manual configuration mistakes, shorten deployment cycles and increase the security of unauthorized access. The capabilities of the free version are live pattern auditing and it boosts a whole slew of other patterns such as the Azure identity management pattern, Azure Active Directory (AD). Key learnings were the necessity for a holistic view in the roadmap to operations to automation as it relates to a cloud first approach, and the need for more agility and being more security-effective from operations. In this study, they actually brought a viable idea to the businesses that have the chance to deploy and optimise AKS without having to violate any of their policies and rules for security.

KEYWORDS: Azure Kubernetes Service, Cloud Infrastructure Automation, Role-Based Access Governance, RBAC, Infrastructure as Code, Security Compliance, Azure Active Directory

I. INTRODUCTION

Planning, development and implementation of information systems for sure has been impacted. With its tightly coupled and inflexible deployment of the architecture, monolithic architecture therefore has problems in terms of scalability, resilience and agility. Because they are cloud-native, can be scaled up, and deployed with the microservices and containerization approach, they are able to be spun-up and to scale applications and respond to changing needs in a timely manner. It's quite similar to the industry standard, with really nice scaling, fail/restart and some sort of service discovery in the containers. The fully-managed service for K8s in the cloud is Azure Kubernetes Service (AKS), helping enterprise to concentrate on developing their programs and innovation whereas Azure takes care of the cloud companies.

While there are lots of efficiency's there are others issues in the implementation of AKS such as managing the infrastructure with scale. The clusters are configured manually, and can contain configuration inconsistencies, be misconfigured or have security level mismatches or issues within or between clusters.Creating networking policies, access controls and clusters manually can result in inconsistencies and misconfigurations between and/or within clusters or with security issues. The need to automate cloud infrastructure has increased for complex reasons and with some of the new complexities of enterprise use. Automation isn't just an automated machine that only deploys for “speed deployments”, it also is a repeatable or predictable deployment type one that will be devoid of human input or human error. Version and deploy resources in the cloud, using Infrastructure as Code (IaC) that can be in Terraform, Azure Resource Manager (ARM) templates, Ansible or other programs. They help ensure uniformity of deployment – from dev through to production – they allow you to scale up your system fast and easily, and intuitively integrate and seamlessly provide continuous delivery/continuous integration (CI/CD) Pipelines.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 2, March-April 2023||

DOI:10.15662/IJRPETM. 2023.0602004

Getting and using them in a compliant and secure manner to Kubernetes resources is not a challenge anymore – except for Automation. That's because in the cloud-native world, there are many users, services and service accounts affecting a cluster role-playing. If misconfigured, it may be that some of their potentially valuable workload can be accessed without them being authorised to do so, which could lead to a security issue. Role Based Access Governance (RBAG) is based on Kubernetes Role Based Access Control (RBAC) and works with Azure Active Directory (AAD) that allows you to automate the principle of least privilege. RBAG can help ensure that cluster resources can only be accessed, modified and deleted by those who have been granted granular access and permissions for the cluster, which in turn helps to keep the cluster secure and consistently compliant with regulations. Governance also has a significant role to report access activity and is also part of compliance with audit, monitoring and audit reporting of other Industry Standards Compliances (including ISO 27001, SOC 2 and GDPR Compliances).

A cloud infrastructure automation and RBAG ensures that any organisation can avoid the pitfalls of having a less efficient and less secure infrastructure. The clusters could be quickly provisioned and configured – using an appropriate automation method – and access policies could be applied on all clusters – and monitored using RBAG. These merge to lower the risk of misconfiguration, curb insider hazard as well as conserve amount of time for administration to deal with vibrant cloud conditions. Also, automated access governance is scalable, which enables businesses to easily scale as they grow and expand their access policies. With IaC and the ability to apply access controls via RBAC, a secure and compliant ‘operational posture' can be achieved without taking a hit in terms of the speed and agility offered by IaC.

Since there isn't a Cloud-native deployment solution available today, the authors in this study suggest a simple solution that they can demonstrate an easy integration of theAKS automation experience in a role based governance solution to address this challenge. It is able to enforce rbac policies that clearly define the roles of different groups of users, for example service-accounts, administrators, developers etc., to be followed during cluster provisioning, storing namespaces and persistent storage. Azure Active Directory integration is perfect for adding additional layers of identity management and as part of authentication and authorization processes. Further, the framework can be applied to test and audit the events in real time, detect events that are not typically recorded, observe the rules and govern the governance process.

Multiple studies indicate that cloud-based infrastructures, as far as scaling is concerned, are facing some problems. Inconsistencies and errors in the manual configurations, due to wrong configurations, can make the system collapse, which can result in unpredictable behaviour, security issues and an undesirable collapse of the system. But an inappropriate level of access control governance can result in loss of data and/or privilege escalation. While there is work that has focused on automation of Kubernetes itself, or on RBAC policies (or groups), there hasn't really been much that focused on holistic automation and (RBAC policies / groups) across AKS in enterprise use cases. This research does follow this goal – developing a methodological approach which is integrated, with the purpose of increasing the operational efficiency as well as security and complexity-less compliance management.

It's a study with both a technical dimension to optimize the study, and a higher dimension. The second distinction vendors can make is based on security concerns deployment has towards cloud capabilities.The next area of differentiation is for vendors to accept automation of deployments across multiple cloud environments that have security issues. Optimizing infrastructure, along with freed up human time and resources, that would have been used manually managing their clusters can be reinvested in other important aspects of their IT team's jobs, for example, optimizing applications, tuning up performance boosts, innovating, etc. Strong role-based access governance, however, will make it possible to achieve all these efficiencies, while maintaining the integrity, compliance and security of data. It discusses adhering to the following elements of the current needs of companies as elements of the framework proposed: resilience adducing capacities, scalability and operational excellence.

Finally, the new cloud infrastructure automation feature, along with role-based access governance is a big step in the Azure Kubernetes Services. IaC can be employed to automate provisioning, access control, sanitation using RBAC and Azure Active Directory can be used to provide an operationally agile, and a security compliant experience. This research not only provides a framework to tackle many issues pertaining to the management of AKS, but also an approach to easily leverage in enterprise scale deployments that are scalable, auditable and secured. Next, the "Why" for design of the framework, testing and potential implications of a framework in the Cloud-based computing paradigm will be discussed.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 2, March-April 2023||

DOI:10.15662/IJRPETM. 2023.0602004

Current Challenges in Cloud Infrastructure Automation and Access Governance in AKS

1. Complexity in Cluster Configuration

One of the difficulties on Azure Kubernetes Services (AKS) is the complexity of the configuration of the clusters. Easy as it may be to deploy Kubernetes with AKS, administrators will face a myriad of layering interdependencies to ease management of the various aspects of their deployment, such as node pools, networking, storage and security policies. The manual configuration provides numerous opportunities for inaccuracies, incorrect configurations and human errors, using this may lead to inefficiencies or downtime. In addition, it is more challenging to get multiple cluster configuration consistent at the time of scaling or adding cluster. One part of this complexity triggers the necessity to have a solid automation plan to deploy and manage them automatically, while preserving the operation and security policies defined.

2. Security and Access Management Challenges

Another aspect to consider is obtaining access security to AKS clusters. While Kubernetes relies on Kubernetes Roles Based Access Control (RBAC) to control access rights, many times the definition of the right role for an administrator, developer and/or service account can be challenging and prone to inaccuracies. Incorrectly configured RBAC policies can allow for the unintended granting of privileges with a risk of unauthorized access, data leakage or privilege escalation and improperly scoped roles can also allow privileges to be granted that are at odds with the policy's intent. However when it comes to connecting to Azure Active Directory (AAD) there is yet another aspect that has to be as correctly configured as possible, and that is seamless when working with multiple clusters and namespaces: identity mapping, group management, Single Sign-On (SSO).

3. Monitoring and Compliance Limitations

Having a large and/or multi-tenant AKS deployment is hard to monitor and audit. This is because the amount of tools on offer to provide metrics or logs to Azure is immense – Azure Monitor, Prometheus, Grafana and so much more – however, it really could be a nightmare to get from a stream of data to actionable insights, and then staying updated on changes to compliance requirements. If there is a set of unusual actions or policy violations, it will be difficult to see them in real-time and if there is a self-service remediation system, unless the system has an advanced warning capability. Compliance in the form of continuous auditing, reporting and logging actions is required by standards like the ISO27001, GDPR and SOC2 and are a time consuming manual process for operations.

4. Scalability and Operational Overhead

With growing number of applications being used by the organisations, it is increasingly difficult to manage operations to execute efficiently and securely. If automation and governance isn't put in place, then other areas of potential failure can be created, such as using nodes and other namespaces, or interweaving CI/CD pipelines. As Manual Reconciliation becomes more expensive to operate, it has a variety of issues with cluster setups and security configuration with clusters. Between many of the businesses are really enthusiastic about AKS can be utilized in manufacture workloads, it's another essential element that as soon as you're going to manufacturing workloads it cannot fail to scale back and great governance.

Framework for Cloud Infrastructure Automation and Role-Based Access Governance in Azure Kubernetes Services

CIA and RBAG should follow each other in AKS to optimize and manage security and compliance. It can be leveraged for automatic cluster provisioning, cluster configuration in standardisation and fine granular cluster (organisation unit level) access control for security policy consistency and audit of organisation unit audit trail. If it is deployed without any obstacles, deployment frictionless, or if one uses the deployment Azure native orchestation tools, coupled with an Azure Active Directory (AAD) and Azure RBAC framework for centralized identity management, the deployment and governance experience is smooth, leading to less redundant work, more operation reliability and greater security level.

1. Objectives of the Framework

The basic goal of the "automated deployments" in the framework, is to ensure for AKS clusters that they can be automatically deployed and maintained as much as reasonably possible to reproduce in other environments. The consistent enforcement of policy is also important, especially protocols such as network policy, storage configuration and namespace isolation which are applied automatically to minimize the risks of being mis-applied within the system or the chances of an operational discrepancy. It not only provides 'granular access control' granular access control based on 'RBAC policy, user level and exact permission to users, administrators and service users' treatments' with the consequence that the users will have ‘least-privilege access', it also offers ‘RBAC policy, user level and exact permission to users, administrators and service users' treatments'. The framework also allows for systems to be in place

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 2, March-April 2023||

DOI:10.15662/IJRPETM. 2023.0602004

for for real-time auditing: Systems are set up to record and track all system activity, aiding compliance and audit. The clusters are dynamically scalable and extensible: They can be scaled up when necessary – and additional components can be added to the cluster without impacting the cluster governance or cluster security that includes seamless CI/CD integration. Last but not least, it helps you integrate the rest of Azure cloud products/services (Azure automations, Azure identity services and Azure monitoring services) seamlessly with the rest of your Azure cloud solutions and manage the entire Azure cloud environment as per the current enterprise cloud design.

II. FRAMEWORK ARCHITECTURE

The presented model is comprised of four different layers, each with a unique responsibility that works together to ensure it is operable as an entire system as well as to maintain a flow of automation and governance. This converts to a familiar, predictable and efficient orchestration of both AKS clusters and cloud resources, via the Automation layer, which is aware of provisioning and configuration. The governance layer allows for role based access control, plays a part in enterprise policy enforcement, and enforces enterprise identities (roles, systems, applications and enterprises), making access permissions explicit and easily verifiable without compromising enterprise security needs. The monitoring and auditing layer checks on-going compliance, user activity, system performance parameters, provides a system activity view while in operation, tracks where the system's operating activity is coming from and keeps a compliance trail of all system activity. The last piece that brings together AKS clusters and CI/CD pipelines, enterprise identifying systems and alerting is the integration layer.Last but not least, an interface that allows the AKS clusters to be included in any CI/CD pipelines, enterprise identity systems and alerts to enable coordination of automated process activities with enterprise activities. These layers are available as a base to solve problems in the cloud-native operating environment, such as with operations, security and governance.

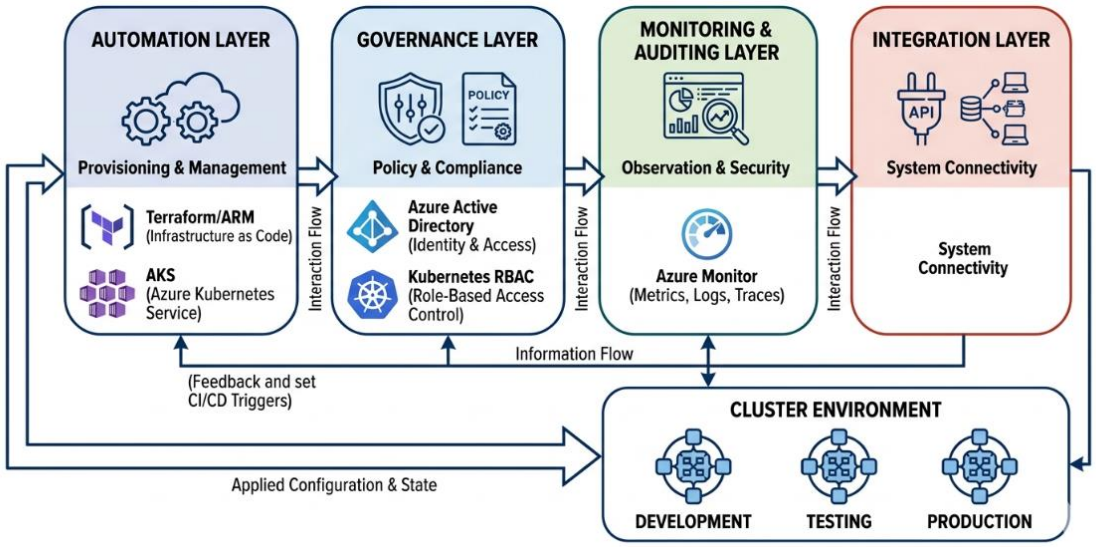

Figure 1: Conceptual Architecture of the Framework

2.1 Automation Layer

The automation layer is heavily integrated with the framework and automates the AKS deployment to enable faster and repeatable deployment of AKS. There are tools such as Infrastructure as Code (IaC) (e.g. Terraform, ARM templates) that can be used to assist in determining the configuration of the cluster, including node pools, networking, storage provisioning and etc., and be repeatable, version controlled, and managed with rich infrastructure codes. AKS computes, memory, network and storage parameters are provisioned via scripts, thus making it easier to automate and steer clear of human mistakes which could be different for dev/ test/ production clusters; and keeping the same parameter configurations across all cluster types (dev/ test/ production). The automation aspects also feature automatic separation of workloads by teams and projects, with each workload getting its own Kubernetes namespace, in Kubernetes. Network policies control internamespace communication, and ensure that the messages are kept safe. Continuous integration and continuous deployment (CI/CD) integration allows the integration of Azure DevOps or Github Action workflows dynamically provision resources when needed, trigger/App deployment, and/or implement

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 2, March-April 2023||

DOI:10.15662/IJRPETM. 2023.0602004

testing protocol on the fly when software deployment into an environment with consistency & operational low risk software deployment is required.

2.2 Governance Layer

See how the governance layer runs to make sure a secure policy is adhered to and Azure AD and policy definitions are used to manage access via RBAC in Kubernetes. This is where the concept of these roles (cluster administrator, namespace administrator, developer and read-only auditor) and their respective permissions comes into play. It enables user and groups provisioned in Microsoft Azure Active Directory (AAD) to be correlated with these roles then impose a common identity based policy known as single sign-on (SSO). The framework ensures compliance at subscription level, resource level, via Azure Policy integration, cluster configuration and allowed namespaces, resource quotas, network isolation and much more. On top of that, Azure Key Vault allows for adding sensitive data like certificates, api keys and connection strings which can be stored in Azure Key Vault and which are automatically added to the workloads. Granting role based access governance at multiple levels provides transparent permissions, under control of the organization and compliant to internal/entity level regulations as well as external ones which also gives reduced risk as no one can enter into the app or its data at the server without authorization.

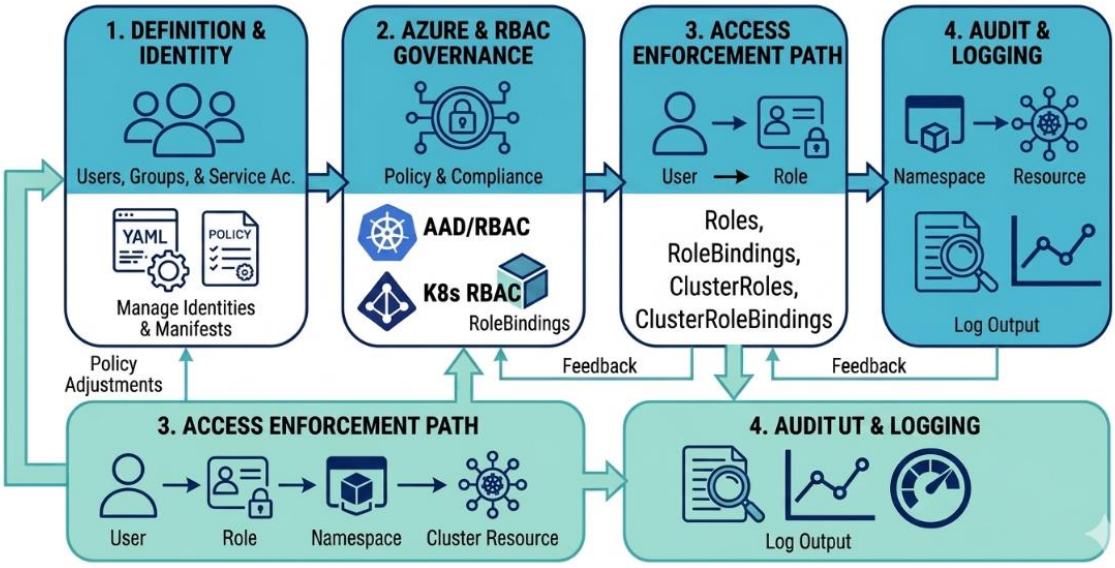

Figure 2: Role-Based Access Governance Flow

2.3 Monitoring and Auditing Layer

The monitoring and auditing layer aimed in providing the up-to-the-minute view of the functioning performance and governance compliances. Any time the user performs an admin specific activity or any specific user activity related to the cluster: Adding/Removing clusters, Deployments, clusters modifications, roles modifications, etc. should be captured in Azure Monitor and the Kubernetes audit log. Azure Security center will provide you real-time threat detection, visibility into how people are accessing your services and resources without permission, and/or if any are there policies violate. The predefined dashboards create reporting on RBAC assignment and assignment compliance to RBAC assignments' policies or support auditing and compliance with policies or regulations, like ISO 27001, SOC2 or GDPR, etc. Prometheus + Grafana provides the ability to monitor clusters, manage cluster capacity and proactively manage cluster performance and improve metrics collection. Reliability and consistency when used – understanding behaviours and security positions at a system-wide level leading to a self-healing and auditable system.

International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 2, March-April 2023||

DOI:10.15662/IJRPETM. 2023.0602004

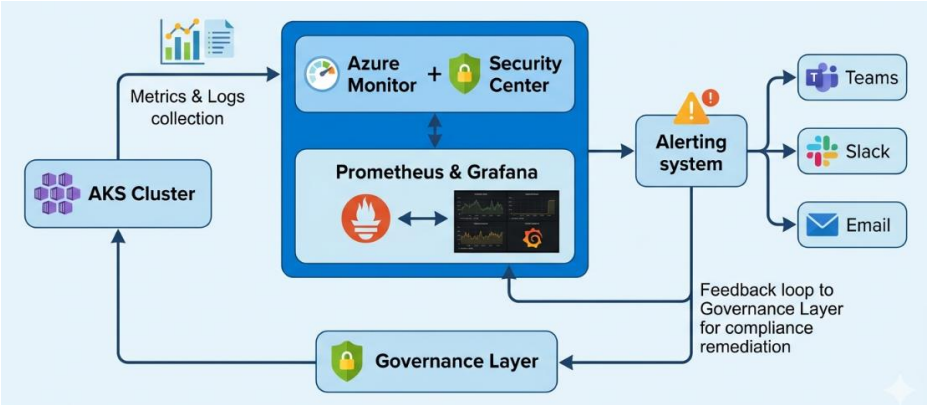

Figure 3: Monitoring and Auditing Flow

2.4 Integration Layer

The integration layer makes it possible to seamlessly integrate the automated, governed AKS environment in an enterprise workflow. AI triggered CI/workflows for code commit makes it a breeze to create courses for container images, to deploy and ensure them to adhere to the RBAC policy. An on hand collaboration tool like Microsoft teams, Slack and email notification to keep all stakeholders informed of critical events, failures and any policy violation will keep everyone in the operation informed. These provide 3rd party security monitoring and/or analytics applications (e.g. for Aqua Security, Sysdig or Datadog) to be integrated to see even more about the security of the containers and clusters. Through those integrations, the flexibility of the organization (or whatever's being integrated) is attained and these don't affect resilience, governance or security.

III. IMPLEMENTATION WORKFLOW

Uses the framework in actual practice with an operational workflow of phases and the various steps in the process. The definition phase includes scripts coded using the Terraform language and yaml manifests for capturing the requirements, roles, policies and namespaces just before automated deployment. Provisioning is the running of provisioning scripts which create the AKS clusters, networking parameters, namespaces and provision persistent storage. RBAC roles and policies are identified and during Governance, AAD Users/ Groups are mapped to Kubernetes Roles which offer access control. When deploying the application it will deploy to the above pre-defined namespaces as default and all the access policies will be applied on Application. Monitoring constantly collects performance metrics and logs, as part of the internal auditing and security monitoring / performance evaluation. The framework also includes policies and ways to automatically switch the tools to the corrective course of action if a policy is violated, or a tool is released to a non-compliant environment, thereby ensuring increased alerts and/or corrective actions while remaining in an automized, compliant and operationally resilient environment. This workflow will give them a means of syncing access between the clusters, and will roll it out throughout the AKS cluster lifecycle.

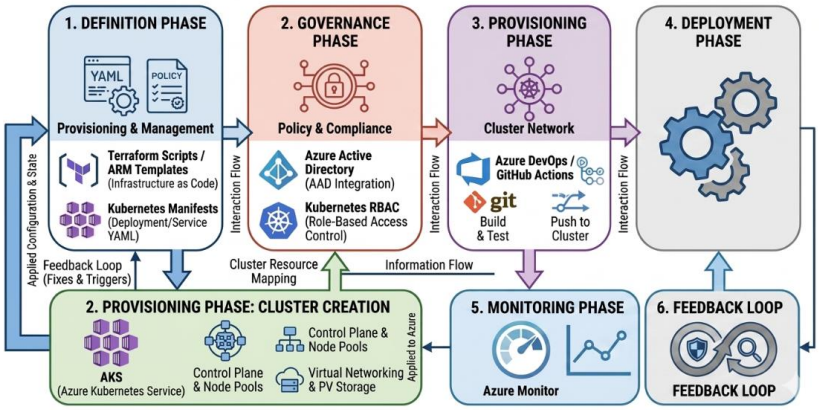

Figure 4: AKS Cluster Automation Workflow

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 2, March-April 2023||

DOI:10.15662/IJRPETM. 2023.0602004

IV. ADVANTAGES OF THE PROPOSED FRAMEWORK

There are a number of important benefits offered by the framework. IaC helps to achieve deployability and configuration drift giving consistency in actual operations. The RBAG attack surface minimisation and least privilege access enforcement results in overall better security. It is designed to be scalable (e.g. it can support larger workloads via provisioning additional clusters and it can be reduced (e.g. it can support smaller workloads even within the cluster by removing cores from clusters), while providing automated cluster provisioning and policy operations within the cluster itself. The process is done in an ongoing manner with monitoring and logging—it is auditible, with proof of compliance. Integration-Friendly design enables smooth integration with the CI/CD pipelines, Identity Management and enterprise security solutions. The framework also provides added convenience in setting up, as well as in administering and monitoring good working practices making any manual action unnecessary and closing the door against human error. All play an important role in providing cloud agility with good cloud security governance.

V. TOOLS AND TECHNOLOGIES

The framework built on a number of technologies which are available on Azure - “Transitions” is the list of open sourced technologies. Azure Kubernetes Service (AKS) serves as the managed Kubernetes orchestrator, a hassle-free method to deal with the management of clusters and procedures. This policy is defined using Infraestructure as Code (using Terraform or ARM) and deployed/reproducible and enforced using fine-grained access control using the Kubernetes RBAC. Azure Active Directory provides the means of domain management and integration with SSO with the view of having a common set of policies across the enterprise. Azure Key Vault securely stores sensitive data and provides a way to securely inject it to workloads. Logging, monitoring and threat detection capabilities of Azure Monitor and Security Center. Use collection and visualization of metrics (with the help of Prometheus and Grafana) in order to better understand the operations. Using automated deployment procedures, and perhaps showcasing exemplary tools such as Azure Devops and GitHub Actions, can improve otherwise substandard continuous delivery pipelines, and of course focus on rules of governance too. The technologies are intensively working together in developing an Ecosystem to manage the Cloud infrastructure and is planning to work on a Holistic Access Governance Model for AKS.These technologies, working hand in hand, will provide a fully extensible and smooth technology for managing applications in the cloud infrastructure as well as provide Identity Strong access control in AKS environments.

Evaluation of Framework Performance in AKS Automation and Governance

1. Metrics for Performance Assessment

To measure the performance of the proposed framework, the following measurements, both operational and security may be used along with compliance measures. Operational efficiency: Deployment of cluster take less time and there will be lesser percentage of uniformity in the cluster with no error(s) in the cluster deployment. The effectiveness of automation is defined as the number of times the deployments can be repeated between the development, test and production environments, with infrastructure matches to the Infrastructure as Code (IaC) specifications. Security and Governance metrics will be around enforcing access control – how many times has access been denied and shouldn't have been denied, how many times has access been granted and shouldn't have, adherence to access control policies and effectiveness of access policies across Azure Active Directory. The dependent attribute in the conformance can be the ability to generate audit logs or you can generate a conformance report, or you can endorse policy constraints to be applied on namespaces, resources or resources in namespaces. All these show different aspects of how the framework is at work and how effective it is (or is not) in each area would be welcome if an organisation had some idea of what was working and what was not.

2. Operational Efficiency Analysis

Parts of the Azure Knowledge onboarding content (ARM templates and Terraform templates) were used for the automated cluster deployments in the testing. The results show that it took much less time to deploy clusters than was traditionally the case, as the cluster was provisioned and configured in a few seconds. When we automatically generate our Namespace, police the network and allocate resources, there were virtually no issues between stages related to configuration. The final remaining part – ‘final integration capability with CI/CD' – allowed them to deploy and test the apps automatically making them more effective. Thus this was an automated way to remove the human error, improve cluster reliability and demonstrate AKS cluster management's ability to effectively streamline cloud operations when operating at scale.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 2, March-April 2023||

DOI:10.15662/IJRPETM. 2023.0602004

3. Security and Governance Effectiveness

Measuring security based on enforcing the RBAC policies and the policies' ability to limit accesses per principle of least privilege. One role-assignment was assigned for each role and role assignment via central management (Azure Active Directory) was not explicitly allowed for any of the roles. All activity log events (both user and administration events) were tracked and all events recorded and abnormally performed events tracked periodical. To ensure compliance with the policies the organisation has, all policies related to namespaces, network policies and resource quotas were enforced using Azure Policy. Overall, the framework was able to address the potential security concerns, deliver on accountability and create an audit-log of who was accessing AKS clusters, making it effective within the setting up of good access control governance in AKS clusters.

4. Scalability and Compliance Evaluation

Dynamic scaling, simulation of growth in numbers of dynamic namespaces had been carried out to accommodate the growth in the number of clusters (namespace). The scaling operations are delicately run through successful implementation of both the policies as indicated in the framework as well as no people inclusion. Using the compliance process, logging, Dashboard and real time alerts were used as compliance checking tools to ensure that ISO 27001 complied and other regulatory compliance guidelines were followed. Predefined dashboards offered transparency in the RBAC assignment, and reporting and alerting on Policy violations and timely remediation, were quick. These assessments provide proof and justification that the framework can be effectively applied in a secure, compliant and scalable fashion in a cloud-native environment.

5. Summary of Performance Outcomes

The evaluation on framework for using the same confidence can lead towards significant improvement in the efficiency of the operation in the environment AKS along with that in the security & compliance field as well. Automated provisioning—provisioned devices are provisioned the same manner each time, with no fails; and Built-in RBAC and Azure AD Governance— gives Least Privilege for access to provisioning, and provides auditability of provisioning actions. They are also very easy to integrate with CI/CD and can be easily scaled up, thus further enhancing the agility of operations. The cluster monitoring and auditing functions bring transparency of clusters operation and compliance to the enterprises, and construct a secure and compliant cloud ecosystem. These are performance metrics that show how fit the framework is to be deployed in enterprise scenarios to ensure stable execution, security from threats and compliance in the system.

VI. CONCLUSION AND FUTURE WORK

There are many varying alternative cloud-native architectures that reveal the need for an enterprise-wide efficient and effective operating model that is secure as well – in the cloud. The Azure Kubernetes Services (AKS) area of the study provided insight into the scalable, secure and regulatory-compliant cloud deployments that automation and role based access governance (RBAG) of cloud infrastructure can be a powerful means of achieving. The proposal framework will build from the IaC approaches which aim to do the following: streamline cluster provisioning, remove human error and accelerate cluster deployment using the metaphysical method. When enabled with Azure Active Directory, Azure Kubernetes RBAC enforces and follows the policy of least privilege, delivers auditability and can minimize risk of unauthorized access to the system. Coordinated operation communication between the various operational processes and security policies will flow smoothly across the four levels of hierarchy – Automation Layer, Governance Layer, Monitoring Layer & Integration Layer – and efficiency and compliance goals will be supported.

If adopted the use of this concept of performance would significantly reduce provisioning time, remove inconsistencies in the provisioning process, increase provisioning robustness and create conformity of provisioning to organisational/regulatory provisioning standards. For Compliance and Security, logging, monitoring and dashboards can help to keep everyone on the same page when it comes to the behaviour of a system and can also mean it is much easier to remediate – whilst at the same time increasing the workload of a system means it is easier to manage it. Furthermore, integration with CI/Cd enables App deployment on Enterprise grade with faster and safer app deployment to other environments without compromising on the governance and security put in place.

Resuarchers could continue to work on the model to modify and/or enhance a variety of features to increase its usefulness. In the future, another evolution may be an anomaly detection feature equipped with the algorithms of AI-ML that can be utilized in advance to detect suspicious activities or misconfigurations in AKS clusters. The other path is to hybrid and multi-cloud, where a single control and automation can be achieved across multiple cloud environment. These, which are out of time today like policy-as-code tools and access control models, could even assist adaptation to

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 2, March-April 2023||

DOI:10.15662/IJRPETM. 2023.0602004

the needs of the organization. Moreover, this performance evaluation (for the degenerate CASE, with high load and high density of tenants) can metaphorically throw light on the optimum utilization of resources from the application's perspective, and its scalability. Finally compliance solutions can be integrated and compliance processes can be automated, which makes auditing compliance easily, and decreases the compliance overhead.

Lastly, the dialogue that happened in October, inside the cloud is helpful because it allows you to see a blueprint of how you could work with automating cloud infrastructure with Azure Kubernetes Service and a role based governance model. The future events and capabilities with regards to governance via cloud would be scalable thanks to the inclusion of a repeatable provisioning, strict control of access and surveillance via centralized tracking. The research contained in this thesis provides a work vector and a concrete solution with regard to the enterprise component, as well as a good foundation for more research and development of automated and secure orchestration in the cloud.

REFERENCES

[1] Microsoft, "Azure Kubernetes Service (AKS) Entra ID Authorization," Microsoft Docs, 2022. [Online]. Available: https://learn.microsoft.com/en-us/azure/aks/entra-id-authorization.
[2] Trend Micro, "Enabling Azure RBAC for Kubernetes Authorization," Trend Micro Knowledge Base, 2021. [Online]. Available: https://trendmicro.com/trendaivisiononecloudriskmanagement/knowledge-base/azure/AKS/enable-azure-rbac.html.
[3] Cloud Native Computing Foundation, "Cloud Native Computing Foundation Overview," 2022. [Online]. Available: https://en.wikipedia.org/wiki/Cloud_Native_Computing_Foundation.
[4] IBM, "What Is Cloud Computing?," IBM, 2021. [Online]. Available: https://www.ibm.com/think/topics/cloud-computing.
[5] Microsoft, “Best practices for Azure Kubernetes Service (AKS),” Microsoft Docs, Aug. 23, 2024. [Online]. Available: https://learn.microsoft.com/en-us/azure/aks/best-practices.
[6] National Institute of Standards and Technology, “Role Based Access Control | CSRC,” NIST, Nov. 21, 2016. [Online]. Available: https://csrc.nist.gov/projects/role-based-access-control.
[7] IBM, “What Is Role-Based Access Control (RBAC)?,” IBM, 2022. [Online]. Available: https://www.ibm.com/think/topics/rbac.
[8] Microsoft Q&A, “Authentication and Authorization in AKS Cluster?”, Microsoft Learn Q&A, Sep. 20, 2022. [Online]. Available: https://learn.microsoft.com/en-us/answers/questions/1015449/authentication-and-authorization-in-aks-cluster-be.
[9] Microsoft Tech Community, “Best practices to harden your AKS environment,” Microsoft Blog, Oct. 29, 2022. [Online]. Available: https://techcommunity.microsoft.com/blog/azuredevcommunityblog/best-practices-to-harden-your-aks-environment/3665659.
[10] Cloud Security Alliance, “Kubernetes Security Best Practices: Definitive Guide,” Cloud Security Alliance Blog, Mar. 3, 2022. [Online]. Available: https://cloudsecurityalliance.org/blog/2022/03/03/kubernetes-security-best-practices-definitive-guide