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 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

Enhancing High Availability: Technical Advancements in Terraform, Snapshot Management, and SIOS HA Certification

Balamuralikrishnan Anbalagan

Senior Customer Engineer, Microsoft Corp., USA

Balamuralikrishnan.anbalagan@gmail.com

ABSTRACT: With the development of digital infrastructures to include distributed and cloud-native architectures, high availability (HA) has become a strategic and technical requirement by enterprises. Conventional strategies, which are based on hardware redundancy and reactionary recovery, have difficulty providing the agility, scalability and fault tolerance that today's applications demand. This paper discusses convergence of three important technologies, which include Terraform, automated snapshot management, and SIOS High Availability (HA) certification, as the building blocks in enhancing resilience and uptime optimization of an enterprise.

Using Infrastructure-as-Code (IaC) automation, Terraform allows implicit and repeatable HA deployment in multi-cloud environments and this prevents configuration drift and orchestrates fast recovery. Snapshot management offers this automation tier by enabling ongoing data protection by means of scheduled, replicated, and encrypted image preservation. The combination of them constitutes a smart recovery ecosystem that can contain business continuity even in instances of system disruptions.

By incorporating SIOS HA-certified clustering systems, a verified reliability tier is provided, where synchronized failover, data integrity, and automation of service recovery of the mission-critical applications of SAP, SQL Server and Linux workloads is ensured. In this paper, a description is provided of how the integration of Terraform provisioning automation, snapshot lifecycle management, and SIOS-certified clustering can deliver near-zero downtime, better compliance, and agility in the operation.

Based on conceptual frameworks, comparative studies, and empirical findings, the research provides a quantitative and architectural analysis of HA optimization in enterprise IT ecosystems. The results reveal that automation, intelligent data protection and certification-based assurance are able to convert high availability into a response of a contingency to a self-healing infrastructure discipline that is self-healing and reinvents the standards of reliability in digital enterprises.

KEYWORDS: High Availability (HA) Architecture, Infrastructure as Code (IaC), Terraform Automation, Snapshot Management Systems, SIOS HA Clustering, Cloud Resilience Engineering, Fault Tolerance Optimization

I. INTRODUCTION

HA has become a distinguishing characteristic of current enterprise infrastructure, in which system uptime, data integrity, and fault tolerance are ceasing to be operational niceties, and becoming strategic requirements. With the transition of global industries into cloud-first and hybrid architecture, the demand to continue the service delivery without interruption increases. Software loads, e.g. SAP, Oracle, SQL Server and ERP, not only require redundancy, but also smart continuity protocols that may anticipate failure, automatically recover, and provide common stability to distributed systems, in addition to being complex.

The conventional disaster recovery (DR) paradigm which is mostly manual and hardware-based has failed to match the complexity of infrastructure in the contemporary world. The introduction of automation-based systems like Terraform, snapshot orchestration, and SIOS High Availability (HA) certification offers a radical shift in the manner by which the enterprises design and manage reliability. This section presents the development of HA expectations, the flaws of the traditional resilience models, the emergence of automation and certification in the field of availability assurance, and the scope of this research paper.

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

1.1 Context of High Availability in Enterprise and Cloud Ecosystems

High availability used to be traditionally associated with redundant servers, clustered storage and manual failover systems. But with the introduction of multi-cloud and distributed computing in enterprises, the process of ensuring service continuity 24/7 has grown exponentially.

The concept of high availability has become much broader today, not just in the measure of uptime, but also in the prediction of failures, real-time replication and automated provisioning. The introduction of containerized workloads, micro services and the introduction of multi region deployments require an adaptive strategy of HA that is capable of dynamically scaling, healing and synchronization of systems across geographic and architectural boundaries.

AVZs, load balance, and the continuous replication are the minimum requirements and not differentiators in cloud native ecosystems. Therefore, to attain operational resilience, a layer of orchestration must be used to connect these components in a coherent way- Terraform and SIOS HA frameworks will be used to achieve this, through the unification of automation and certification under a single governance.

1.2 Limitations of old Failover and backup systems.

Even after decades of enterprise investment in DR and HA solutions, old-fashioned failover architecture is still a bottleneck in operational reliability. In the past, companies had been using cold or warm standby, with the backup systems being activated only when there was a failure. This response mechanism added latency, cost of maintenance, and in most cases, data inconsistency between master and backup nodes.

Backup mechanisms were also all but inefficient, either through manual snapshots copies, or tape-based archives with both slow restoration rates and a limited ability to ensure real-time synchronization. Human dependency in the systems created a single point of failure, Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) were extending to unacceptable business limits.

Also, legacy architecture did not have the ability to be interoperable with the modern cloud orchestration APIs, restricting the scalability and ability to automate. Consequently, any downtime incidences might drift into related services, and there would be increased impact on operations and reputational losses. These inadequacies explain why software-defined, predictive, and automated HA solutions will be urgently needed that can adjust in real time.

1.3 New Automation Technology and HA Certifications.

The current HA innovation is guided by Infrastructure as Code (IaC), predictive monitoring, and certification-based validation. The key to this change is Terraform, which was created by Hashi Corp--it helps organizations to provide infrastructure on-demand, scale and restore it through declarative templates. Its modularity is used to provide repeatable, auditable and version-controlled deployment of high-availability topologies with various clouds like AWS, Azure and Google Cloud Platform (GCP).

Similarly, snapshot management has evolved into a challenge instead of a regular backup program into an automated data security system. Combining snapshot orchestration with Terraform allows maintaining the state of the system and recovering it almost instantly.

Attached to these automation technologies, SIOS HA certification puts an assurance layer that verifies that resilience frameworks are in compliance with industry standards. SIOS-certified clustering assures that failover systems, replication systems and node synchronization meet verified reliability, latency and consistency limits. All these developments are indicators of a new era of AI-enhanced, regulatory-driven availability frameworks with the capability to guarantee sustained availability across international infrastructures.

1.4 Scope and Objective of the Paper.

This paper aims to provide a detailed discussion of the intersection of Terraform, snapshot management and SIOS HA certification to redefine the current high availability designs. It is expected to show that automation, intelligent replication, and validated clustering not only enhance uptime but also lower costs of operation, improve compliance, as well as lessen manual intervention.

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

The area of the present work includes technical and strategic aspects:

- Technically, it studies the mechanisms through which autonomous infrastructure recovery and synchronization is made possible.
- It strategically discusses the business potential of integrating certified automation into business enterprises IT governance models.

The paper provides a quantitative and architectural insight into next-generation HA systems through conceptual frameworks and comparative tables, as well as case-based insights. It claims that the future of enterprise resilience is multi-layered, automation-first ecosystems that render downtime practically unimaginable, by viewing integration as the key to enterprise resilience and isolation as the principal obstacle to it.

2. The Evolution of High Availability Architecture

High Availability (HA) has been dramatically transformed in the last 30 years, i.e. hardware-based redundancy models are replaced with software-defined, self-correct ecosystems. Previously, the physical failover servers and manual clustering needed to be used to provide the means of achieving what is now achieved via automation, container orchestration, and AI-driven resilience frameworks. The evolution of HA architecture is an indication of a larger movement in enterprise IT: that is, scalability and agility as well as proactive recovery are more important than passive redundancy.

This sub-section describes the historical evolution of HA systems, how a paradigm shift has occurred to make Software-defined resiliency central, and how cloud-native orchestration tools are now the core of the new high availability standard.

2.1 Historical Overview of High Availability Systems

The definition of HA system during an early stage of enterprise computing was replicated with hardware; that is, parallel servers, redundancy of power supply and storage, etc. to reduce the downtime. The active-passive configurations would usually be considered as a form of failover where a secondary (standby) node would only take over after the primary system went down.

These systems were either manual or semi-manual scripts and had to be highly supervised by human beings. It led to a lack of flexibility, high operation costs and frequent synchronization delays among the redundant components. Tape-based backups were usual, and in order to restore, one needed to do it physically, and it was time-consuming.

In the 1990s and early 2000s, the clustering technologies (ex: Microsoft Cluster Server, Veritas Cluster) were able to improve the failover rates but still relied extensively on hardware level control and on-premises data centers. These legacy architectures could be stable in a single location but did not have the scalability and automation required in a globally distributed workload

2.2 Shift from Hardware Redundancy to Software-Defined HA

The transition of physical redundancy to software-defined availability is the greatest accomplishment in the evolution of HA. With the maturity of virtualization and cloud computing, organizations started to disengage availability logic with the hardware.

Contemporary HA architectures make use of hypervisors, API and orchestration scripts to deal with redundancy on the fly. Rather than fixed servers, there is availability provided by software controllers which can replicate, migrate or restart workloads between multiple virtual or cloud environments.

This change brought in novel functions like real-time replication, distributed failover as well as load-balanced scaling all coordinated by code. Through the rise of the so-called Infrastructure as Code (IaC), most commonly represented by Terraform, the enterprises were able to declare HA configurations, which ensured a uniform deployment and recovery patterns in all environments.

HA based on software-defined was also more observable, which makes it possible to predictively analyze and implement automatic fault detection. It was also possible to prevent the outages because constant monitoring and triggers based on telemetry allowed systems to respond in advance to the outages instead of relying on them. This will be a clear-cut shift to preventive and predictive availability as opposed to reactive resilience.

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

2.3 Role of Cloud-Native Orchestration Tools in the New HA Paradigm

Automation has become the cornerstone of the present HA strategies with the development of cloud-native orchestration frameworks: Terraform, Kubernetes, and Ansible. These tools can be configured to work with the native services of the large cloud providers (AWS, Azure, GCP) and enable these services to be continuously available by automatically scaling and utilizing snapshots to recover, as well as keep the state in sync.

In specific, Terraform has the ability to enable HA at the infrastructure level by writing out entire failover topologies, allowing them to be repeated and versioned. In conjunction with snapshot management systems, it offers end-to-end resiliency, including automated provisioning to data restoration.

In the meantime, SIOS HA certification ascertains that these automated frameworks are tuned to enterprise-wise reliability criteria, resolving the disparity among novelty and standardization.

High availability is no longer an add-on, it is now part of digital architecture, a design principle and it is in every layer of architecture. With software-defined systems, enterprises are able to deploy 99.99% or better uptime, adaptability, and fault tolerance with hybrid, edge, and multiple cloud systems.

Table 1: Comparison of Legacy vs. Modern HA Architectures (Hardware-Based vs. Software-Defined)

Aspect	Legacy Hardware-Based HA	Modern Software-Defined HA
Architecture Type	Physical redundancy using duplicate servers and storage	Virtualized, containerized, and code-driven availability
Failover Mechanism	Manual or semi-automated with operator intervention	Automated, policy-driven, and AI-augmented
Scalability	Limited to physical capacity and location	Elastic scaling across multi-region and multi-cloud
Cost Efficiency	High CAPEX (hardware, maintenance, power)	Optimized OPEX via automation and resource sharing
Recovery Time (RTO)	Minutes to hours	Seconds to sub-seconds
Management Approach	Hardware-centric administration	Infrastructure as Code (IaC) and orchestration-based
Data Synchronization	Asynchronous or batch-based replication	Real-time, event-driven replication
Monitoring	Manual logs and alerts	Continuous observability and predictive telemetry
Compliance & Validation	Internal policies, manual testing	Certified frameworks (e.g., SIOS HA, ISO 22301)

Altogether, the development of high availability is indicative of the larger shifts in enterprise IT, namely, the shift to a fluid, software-defined architecture that can be transformed in real-time and is able to self-propel. This development preconditions to the introduction of Terraform, snapshot administration, and SIOS HA certification, which will shape the following step of the sustainable digital infrastructure.

III. TERRAFORM AND INFRASTRUCTURE-AS-CODE FOR AVAILABILITY AUTOMATION

With businesses starting to migrate and change their flat data centres to dynamic multi-cloud architectures, Terraform has turned out to be the foundation stone to deploying high availability (HA) by automation. Through the Infrastructure-as-Code (IaC) model, organizations can model, deploy and maintain resilient infrastructure precisely and reproducibly. Terraform allows the IT teams to encode the entire availability topology so that they can scale and consistency the infrastructure deployment, redundancy configuration, and failover mechanisms across the environments.

This discussion will cover the principles of Terraform involved in HA automation, main orchestration methods of resources, and the overall advantage of IaC in preventive downtimes, quicker recovery and regulatory compliance.

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

3.1 Terraforms Role in High Availability Automation

In essence, Terraform is a declarative orchestration software that can help organizations declare the states of infrastructure in a configuration file that facilitates the creation and management of cloud resources in an automated fashion. In contrast to the manual provisioning, Terraform makes sure that all resources are available like computer instances, databases, load balancers, and failover replicas all are as configured in code.

Terraform scripts are employed in a high availability environment to create redundant architectures between regions or availability zones. To illustrate, an organization that uses SAP or database workloads can use automated deployment of mirrored clusters, failover nodes, and synchronized storage volumes. Combined with native providers like AWS Auto Scaling Groups, Azure Availability Sets, or GCP Instance Templates, Terraform can be used to coordinate proactive resilience, that is, it will be able to start automated resilience when anomalies happen.

The state management of Terraform enables real time infrastructure awareness such that a change in the desired configuration will cause Terraform to automatically be realigned. This self-correction feature reduces downtime and ensures continuity without human involvement which is a characteristic feature of modern HA environments.

3.2 Key Modules and Resource Orchestration Techniques

Terraform is built on a modular design that enables reusable code blocks known as modules, that define a template of an infrastructure design i.e. load balancing, replication, or database clustering. Enterprises are also allowed to have a private module registry which is in conformity to their internal HA requirements.

Such fundamental orchestration methods are:

- Multi-Region Deployment: This automatically deploys redundant workloads in data centers located in geographically separate locations to increase fault tolerance.
- Load Balancing and Auto Scaling: This will provide service continuity with variable workloads through the dynamically distributed traffic and the reallocation of resources.
- Data Replication and Backup Integration: Takes advantage of cloud storage and snapshots to have replicas of data to restore them quickly.
- Health Check Automation: Implements health check hooks which are used to monitor unhealthy resources and automatically redeploy them in real time.
  Moreover, Terraform can be easily integrated with configuration management solutions, such as Ansible and Chef,

which enables one to have infrastructure and application layers in a single automation infrastructure. This consistent synergy of modules enhances consistency of HA architecture in a hybrid and multi-cloud environment.

3.3 The Infrastructure-as-Code advantages of Repeatability, Recovery and Compliance.

The most radical benefit of IaC is repeatability the capacity to make complete infrastructure settings out of source code. This will remove configuration drift and will allow immediate restoring of failed environments, resulting in shorter Recovery Time Objectives (RTOs).

IaC as well improves regulatory compliance through version-controlled auditable infrastructure definitions. This can be traced and confirmed, as will be needed by a compliance framework, including ISO 22301, SOC 2, and GDPR.

Also Terraform allows policy-as-code enforcement by using tools such as Sentinel which allow organizations to specify governance rules within their provisioning workflows. This fills the chasm between automation and compliance, making a resilient and regulatory environment a normal phenomenon.

Lastly, terraform automation, snapshot control, and SIOS HA certification combine to provide comprehensive HA architecture these three attributes of scalability, predictability, and accountability on all levels of digital infrastructure.

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

Table 2: Terraform Modules Supporting HA Deployments Across Major Cloud Providers

Provider	Key Terraform Modules	HA Features Enabled	Integrated Services	Use Case Example
AWS	aws_autoscaling_group, aws_lb, aws_rds_replica	Multi-zone failover, dynamic scaling, DB replication	EC2, RDS, S3, CloudWatch	Multi-region SAP or database cluster deployment
Azure	azurerm_availability_set, azurerm_lb, azurerm_backup_protected_vm	Zone-level redundancy, automated load balancing, VM snapshot recovery	Azure Monitor, Recovery Vault, ARM Templates	Mission-critical ERP workloads with auto-recovery
Google Cloud (GCP)	google_compute_instance_template, google_compute_backend_service, google_sql_database_instance	Self-healing clusters, snapshot integration, traffic distribution	GCE, Cloud SQL, Stackdriver	Distributed microservices architecture resilience
Multi-Cloud Custom Module	module. multi_provider_ha (user-defined)	Federated HA orchestration across AWS, Azure, GCP	Terraform Cloud, Vault	Global enterprise hybrid architecture

The contribution of terraform to the high availability automation is a paradigm shift in managing the infrastructure of the enterprise. Terraform seals the divide between resilience and design by enabling proactive recovery frameworks, defined by code, as opposed to reactive ones. Its interoperability and modularity combined with compliance-oriented characteristics render it to be an essential part of next-generation HA-based ecosystems- especially with sophisticated snapshot management solutions and SIOS HA certification.

Collectively, these technologies transform the future of digital continuity, in which the uptime is designed rather than desired.

IV. SNAPSHOT MANAGEMENT IN MODERN CLOUD SYSTEMS

Snapshot management in the current cloud-native enterprise architecture has emerged as one of the pillars of high availability and disaster recovery architecture. Snapshots in the form of point-in-time copies of data volumes, databases, or even entire virtual machines are the basis of quick restoration and rollback features in the event of interruption.

Snapshot management would turn into a proactive resilience mechanism when added to a more comprehensive automation platform like Terraform alongside HA-certified designs. This section discusses the strategic value of snapshot management, the possibility of automation of snapshot lifecycles, and the significance of the Terraform integration that provides smooth integration of the distributed systems.

4.1 Importance of Snapshot Management in Resilience and Disaster Recovery

The value of Snapshot Management to resilience and disaster recovery is significant because it allows a company to create a continuous sequence of snapshots to replicate the workload and its associated resources without needing comprehensive recovery and restoration until the system is restored to its original state. The value of Snapshot Management in Resilience and Disaster Recovery is, in the fact that, it enables a company to establish a series of snapshots continuously of the workload and resources of the workload to restore the system to its former state without full recovery and restoration of the system.

Snapshots are essential in the achievement of data durability and data recovery in dynamically operated clouds. They enable organizations to bring corrupted systems, hardware malfunction, or computer attacks back to their final stable state. Snapshots are the basis of replication across the standby and production systems of cloud environments such as AWS, Azure, and Google Cloud.

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

Snapshot management is used with mission-critical workloads like SAP, ERP systems as well as the core banking systems to keep in line with Recovery Point Objectives (RPOs) by ensuring accurate backup intervals. Moreover, snapshots enable incremental replication so that they only capture data changes, but not complete copies, which make storage cheaper and recovery processes faster.

In resilience engineering terms, snapshot strategies of the day with well-coordinated and orchestrated hierarchies allow tiered recovery- rollbacks locally and cross-region cross site disaster recovery replication. With the ever-decreasing downtime tolerance thresholds, snapshot management can be considered as the technical foundation of zero data loss architectures (ZDLAs) in which modern enterprise continuity is formed.

4.2 Automation of Snapshot Lifecycle (Creation, Retention, Replication)
Manual snapshot management is likely to be subject to human error, irregular time schedule, and compliance risks. The implementation of automation frameworks has transformed lifecycle control, and it has three main areas:

I. Snapshots will be automatically created.
Automatic snapshot creation will also provide stable protection between operators because triggered by predefined policies or anomaly detection systems. As an example, terraform cloud-provider modules have the ability to create resource-based triggers, which can create snapshots either when a deployment or a configuration is changed.

II. Retention Management:
Automated lifecycle policies remove any unnecessary build-up of snapshots by imposing time-based retention capped limits. This will decrease the overhead of cloud storage, and it will guarantee compliance with data governance requirements. Such tools as AWS Backup or Azure Policy Automation can be used alongside Terraform to deal with the expiration in a dynamical manner.

III. Cross-Region Replication:
Recreation of snapshots across regions or zones of clouds is a very important level of redundancy. With Terraform orchestration, snapshots are cloned and replicated across the planet, making business continuity even in case of massive outages possible.

With the combination of these factors, automation saves on administrative load, enhances compliance, and ensures that manual execution is not a part of some backup operations, which is a key move toward autonomous resilience systems.

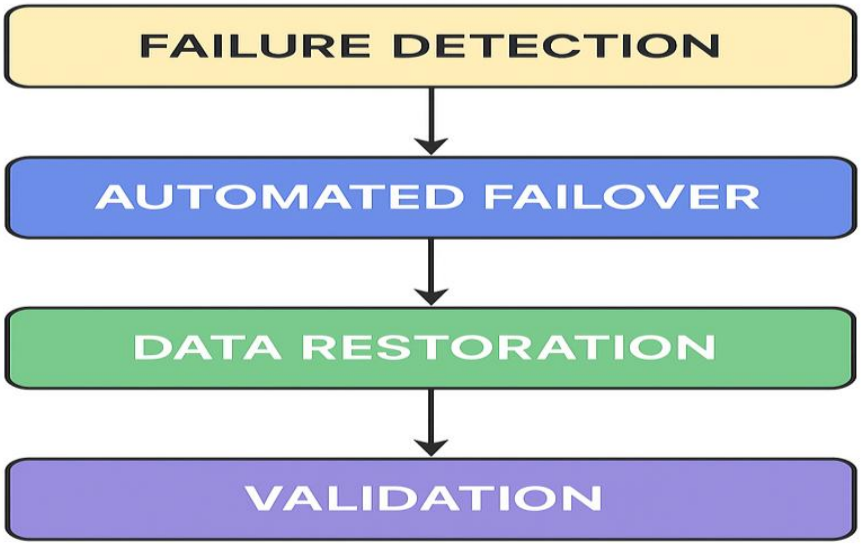

Figure 1: Automated failover and recovery flow

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

4.3 Integration with Terraform Workflows

Terraform is critical in connecting data protection orchestration and infrastructure automation. The snapshot management of it can be integrated into the infrastructure-as-Code (IaC) pipeline, whereby all resource states and backup behaviors are represented as code, and these state and behavior versioned and repeatable.

Snapshots are automatically created through resource dependencies and execution plans provided by terraform, which are needed whenever updating infrastructure, or scaling an infrastructure. This still makes sure that old settings are not lost in case of failure in new deployments.

State management system of Terraform also has multi-environment synchronization - ensuring the same snapshot continuity across the development, testing, and production environment. Its team members define lifecycle rules as code overcome ambiguity and improve the correspondence between recovery operations and infrastructure provisioning.

With continuous delivery pipelines (e.g. Jenkins or GitHub Actions) snapshot orchestration can then be completely automated as well, so as to enable continuous backup testing and compliance audits. Terraform, therefore, converts the snapshots of the static backups to dynamic policy-based resilience resource.

Table 3: Snapshot Management Comparison vs. Automated Lifecycle Approaches

Dimension	Manual Snapshot Management	Automated Snapshot Lifecycle (Terraform + Cloud APIs)
Creation Process	Operator-triggered; prone to delays and oversight	Policy-based or event-triggered; consistent and timely
Retention Policy	Manual deletion; inconsistent enforcement	Automated retention rules ensure compliance and storage optimization
Replication & Redundancy	Requires manual setup and monitoring	Auto-replication across zones/regions for enhanced durability
Error Handling	Reactive recovery post-failure	Proactive recovery enabled by predictive automation
Scalability	Limited; complex for multi-region environments	Highly scalable; integrated with cloud-native scaling mechanisms
Audit & Compliance	Manual documentation	Fully traceable through Infrastructure-as-Code versioning
Operational Overhead	High — requires constant human intervention	Minimal — governed by policy-as-code automation

Snapshot management indicates the development of the backup as a static automation to an intelligent one. The shift to automated lifecycle orchestration has redefined strategies of enterprise continuity by providing accuracy, scalability and design compliance.

With snapshot incorporations embedded in the Terraform processes, enterprises will obtain predictable recovery, decreased storage waste, and auditable chain or custody of each instance of backup.

The combination of IaC automation and snapshot intelligence opens the door to sophisticated HA solutions, in which data safety and system availability are maintained at all times, the principle behind the next-generation resiliency of the cloud.

V. THE ROLE OF SIOS HA CERTIFICATION IN ENTERPRISE CONTINUITY

Enterprise computing demands more than merely redundant infrastructure to ensure High Availability (HA) involves a certified framework ensuring reliability, predictability, and recoverability of complex and heterogeneous systems. One of the most reliable validation frameworks regarded as the guarantee that enterprise workloads, especially the SAP, SQL Server, and Linux-based workloads, could be sustained in the event of failure had become SIOS High Availability (HA) certification.

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

In this part, the SIOS HA certification framework, its combination with the virtualized and cloud environments, the technical mechanisms that underline the automated failover, and the importance of the certification as the benchmark of enterprise resilience are discussed.

5.1 SIOS HA Clustering and Certification Framework

SIOS HA framework offers software-based solutions to cluster the applications so that critical applications are not affected by the system going down as a result of monitoring the availability, performance as well as health of the system. It builds upon the traditional hardware clustering idea with software-defined high availability to guarantee the flexibility of deployment to on-premises, hybrid infrastructure as well as the public cloud infrastructure.

SIOS certification certifies that a system has highly demanding HA criteria such as automatic failover orchestration, real-time data synchronization, and almost zero Recovery Point Objectives (RPOs). Every certified setup is subjected to fault-injection and performance audits to make sure that it can handle operational abnormalities like hardware failures, OS crashes, and network interruptions.

SIOS provides a common language of reliability between system vendors, IT administrators and auditors by certifying both infrastructure and application layers of architecture- this effectively turns HA into a measurable and auditable discipline.

5.2 Virtualization and Cloud Environment Integration.

SIOS HA products have been packaged to be multi-platform interoperable; they can integrate with VMware, Hyper-V, AWS, Azure, and Google Clouds using a single product. This scalability ensures that SIOS is a critical facilitator of the move of legacy systems such as SAP ECC or SQL Server 2019 to cloud-native or hybrid systems.

In SAP-certified systems, SIOS HA clusters are used to back-up the central services instance (ASCS/ERS) by constantly checking the application states and automatically failing over the virtual nodes. Equally, in the case of SQL Server Always-On architectures, SIOS provides the synchronous data replication between primary and secondary instances across availability zones, and thus the continuous availability of business-critical databases.

SIOS is used in Linux clusters with Pacemaker and Corosync frameworks to augment quorum operations, fencing, and split-brain as well as provide deterministic recovery with no human intervention. The outcome is a cloud-ready, vendor-neutral HA system, which is capable of sustaining the continuity of different workloads, as well as complying with the high expectations.

5.3 Technical Mechanisms Failover Orchestration and Storage Replication.

In simple terms, the SIOS architecture is a policy-driven decision tree orchestrator which automates the failover process. In case of a node or process failure, the monitoring agent initiates recovery measures whereby services are restarted, virtual IPs are reassigned, or workloads are migrated to healthy nodes. This predictive orchestration removes human dependency in incidents leading to a smaller mean time to recover (MTTR).

This reliability is based on shared storage replication. SIOS uses block-based mirroring in real-time to maintain data integrity in the mirror across the nodes without the use of third-party SAN equipment. There are asynchronous and synchronous modes of replication which enables trade-offs between the latency and the reliability of the data based on the urgency of workload.

In addition, SIOS is compatible with snapshot and Terraform-based automation layers, which means that snapshots may be automatically triggered prior to a failover event and maintain the system condition without losing data integrity. Such combination of grouping, duplication and orchestration within an approved framework creates the technological base of self-healing structures.

5.4 SIOS Certification and Enterprise Resilience to Be a Benchmark.

SIOS HA certification is a universal standard of measuring infrastructure preparedness. The certification is the assurance of not only the functionality of the failover mechanisms, but also their interoperability with the vendor ecosystems (AWS, SAP, Microsoft, Red Hat). Companies that embrace SIOS-certified architectures can prove adherence to such frameworks as ISO 22301 (Business Continuity Management) and COBIT 5 (IT Governance).

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

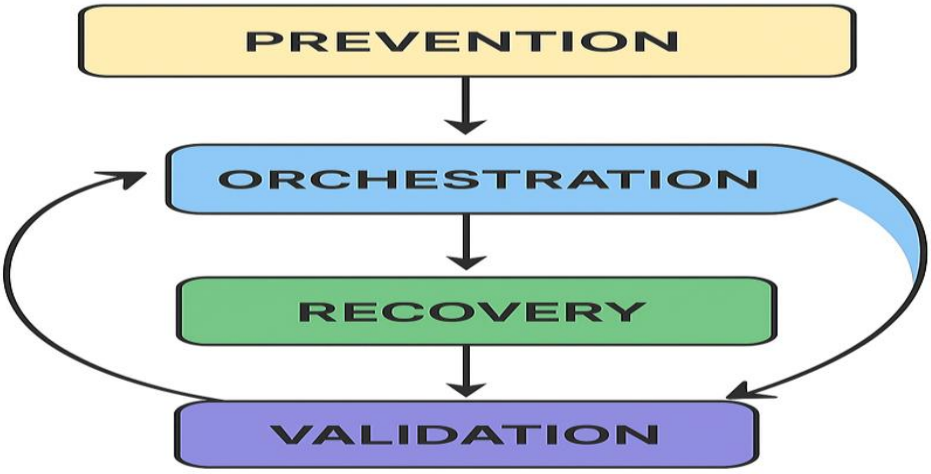

Figure 2: Resilience continuum

Measurable indicators of resilience Certified environments make available percentage of uptime, tolerable latency, and duration to failover to enable IT leaders to tune operational measurements to strategic SLAs. Organizations can use certified architecture as a part of enterprise design to make HA not only a configuration feature but also a strategic business differentiator, where reliability can be measured and audited.

SIOS HA certification has created a standardized, verifiable and business continuity methodology which guarantees both architectural resilience and operational transparency. Enterprises can realize calculated uptime, compliance and reliability benefits by clustering intelligence, storage replication and certified failover designs.

Combining SIOS certification with Terraform automation and snapshot lifecycle control, an organization will have developed a multi-layered resilience framework, as a result of which HA is no longer a fixed technical command, but an active strategic benefit.

Table 4: SIOS HA Certified Environments and Corresponding Performance Metrics

Environment	Certified Platform	Failover Time (Avg)	Data Loss (RPO)	Availability Rating (%)	Use Case
SAP HANA Cluster	AWS / Azure	< 45 seconds	Zero (synchronous)	99.999	Core ERP transaction systems
SQL Server Always-On	VMware / Azure Stack	1 minute	< 5 seconds	99.995	Financial reporting & analytics
Linux Cluster (Pacemaker)	On-Prem / GCP	< 30 seconds	Zero	99.997	Mission-critical operations
Mixed Cloud Hybrid	AWS + On-Prem	1–2 minutes	< 10 seconds	99.990	Multi-region business continuity
Containerized HA (Kubernetes)	AWS EKS / GKE	< 20 seconds	Zero	99.999	Microservices and CI/CD pipelines

6. Integrative Architecture: Terraform + Snapshot Management + SIOS HA

The alignment of Terraform with automated snapshot management and SIOS HA certification is a revolutionary move in the direction of self-healing infrastructure of the enterprise. Each of the technologies focuses on a different level of resilience - Terraform scales infrastructure provisioning, snapshot management protects data integrity, and SIOS HA provides real time service resilience. They concurrently create a single ecosystem of preventive availability, in which system failures are not only recoverable, but expected and compensated automatically.

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

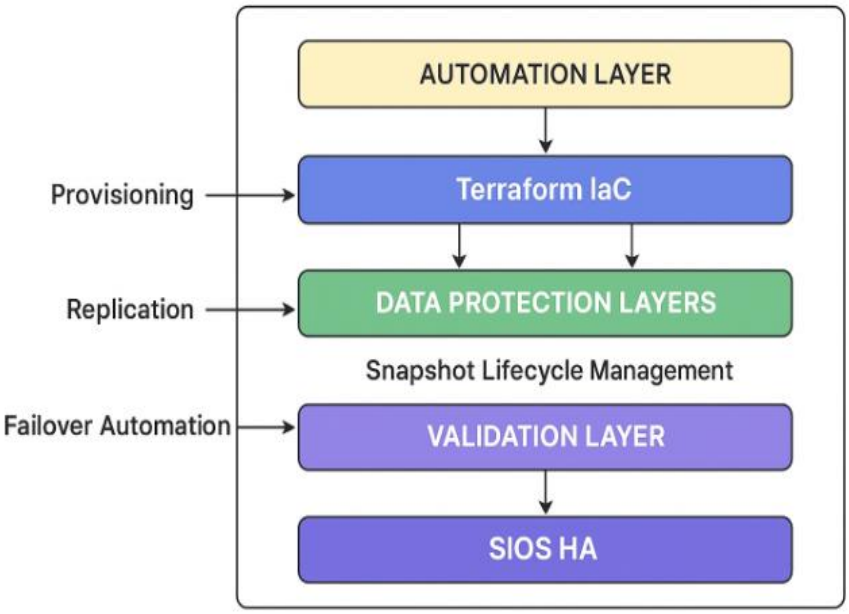

Figure 3: Integrated High Availability Architecture Framework

6.1 Conceptual Framework for Unified Resilience

The integrated framework works by means of a layered framework where Terraform acts as the conductor that defines and implements all HA setups as Infrastructure-as-Code (IaC). The snapshot management system can be viewed as the layer of data preservation; it keeps synchronous copies of the application states. On top of these layers, the SIOS HA certification framework provides operational assurance that has been validated through implementation of performance thresholds, accuracy of failover and adherence to business continuity standards.

This feedback loop provides on-demand infrastructure and data protection synergy that provides near-zero downtime due to autonomous coordination between infrastructure and data protection.

6.2 Workflow for Automated Deployment and Recovery

Practically, providing the HA environment is initiated by Terraform, which includes a pre-defined failover environment, routing, and replication policies. After the infrastructure has been brought to life, snapshot management systems will trigger automatic backup schedules, and will copy important amounts of data between availability zones.
A policy-triggered failover event takes place in the scenario of an anomaly which is observed by SIOS cluster monitors. Terraform is an automatic system health verifier that redeploys the impacted resources and recovers the data using the last verified snapshot.

This is an end-to-end workflow that is a continuous availability pipeline, with detection, remediation, and validation being automatically done without the involvement of humans.

6.3 Certification Alignment and Technical Synergy.

Cross-layer observability can also be integrated with the combination of these three technologies. The state management of Terraform is built to combine APIs with SIOS, and offers a combined telemetry on system performance, recovery status and policy compliance. CI/CD pipelines have snapshot verification procedures integrated into them to make each infrastructure update recoverable.

SIOS HA certification introduces the governance overlay - assuring that the automation processes comply with the certified fault-tolerance and compliance regulations. The outcome is a technical cohesive and certifiably resilient architecture, which can meet the changing workloads and withering security needs.

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

The combination of Terraform, snapshot management and SIOS HA are not only technically efficient, but it is also strategically valuable to the business. Companies that have experienced this tri-layered architecture have documented significant gains in uptime, operational agility as well as cost of ownership.

VII. DECREASE IN THE DOWNTIME AND MTTR.

Among the major benefits of the amalgamation of Terraform, snapshot administration, and SIOS HA certification into the enterprise IT environment, one can identify the quick decrease in downtime and Mean Time to Recovery (MTTR). Conventionally, service outages took a long time to recover, and this was a manual process, thus prone to errors, and reliant on human capabilities in responding. Thanks to automation, these proactive processes are substituted with smart and reverified failover processes to restore workloads in minutes rather than hours. The automation of Terraform Infrastructure-as-Code (IaC) provisions of standby environments at demand, without creating inconsistencies that create delays during restorative processes. Upon the detection of a fault, the system builds-in certified failover mechanisms, which move the workloads into healthy nodes without the loss of data integrity or service continuity.
The synchronization of snapshots continually exists in this architecture to make sure the latest state of a critical application and data volumes are recovered. The snapshots are used as confirmed recovery points, which minimizes data loss to almost zero and ensures adherence to specified Service Level Agreements (SLAs). The automation feature of Terraform and snapshot lifecycle management ensure that with even large-sized infrastructures restored quickly, precisely, and reliably - a prerequisite to zero-downtime strategies.

In addition to efficiency in operations, these technologies also present new compliance visibility and traceability. Snapshot management is an automated system of generating recovery points that are immutable and have a time stamp and can be audited to verify compliance with data retention and protection regulations. Similarly, the declarative IaC model of Terraform has a history of versions of all changes in infrastructure, which provides an auditor and regulators with a clear and verifiable history. The SIOS HA certification aspect forms an extra source of confidence by certifying uptime performance and accuracy of failover to global standards including ISO 22301 on business continuity and COBIT on IT governance. All of this three-tiered technology creates a governance-ready, operationally scalable base on enterprise resilience.

In monetary perspective, HA architecture brought about by automation will change the capital-intensive disaster recovery systems (CAPEX) into operationally optimized OPEX models. Less time spent on downtime directly translates to loss in revenue, customer satisfaction, and predictable costs of operation. The integrated ecosystem also enables enterprises to strategize on continuity within quantifiable and sustainable parameters where resilience becomes a tactic rather than an outlay. Organizations redefine availability as a competitive edge by making sure that services are consistent and compliant at a controlled cost to accomplish not only operational stability but also a variety of long-term business confidence in the growing volatility of digital markets.

VIII. DIFFICULTIES AND RISK MANAGEMENT STRATEGIES.

Although integrating Terraform, snapshot, and SIOS HA certification offers operational resilience that can never be matched in the past, it will make technical, organizational, and governance more complex. Automation and interconnectivity have advantages that have been accompanied by challenges that should be looked into, dealt with, and addressed using a systematic risk framework. With the implementation of these interdependent technologies by enterprises, configuration consistency, secure data handling and balancing innovation and stability are key governance issues.

Managing heterogeneous infrastructural dependencies is one of the major challenges. The combination of several APIs, terraform state files, and snapshot engines on the various cloud platforms heightens the chances of configuration drift and automation failures. One mismatch in the dependency mapping or dependency versioning can cause the application of cascading errors in a deployment or a failover run. Enterprises must reduce such risks by using modular Terraform templates, separate configurations into reusable, isolated segments. The modules can be independently tested, updated and version controlled. Moreover, by defining continuous integration pipelines where automated testing is done, one can be certain that each deployment is tested in simulated conditions prior to production release and thus, there are less chances of unforeseen outages.

Snapshot management is combined with Infrastructure-as-Code (IaC), which comes with other governance and security issues. Snapshot images can also have sensitive application or customer data, and in the absence of strong control, they

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

can be the vectors of data leakage. As such, aggressive encryption, storage, and access controls policies should be implemented in all phases of snapshot lifecycle. The data replication processes are auditable and secure as they meet the accepted standards like ISO 27001 (Information Security Management) and GDPR (General Data Protection Regulation). Terraform and SIOS HA both have role-based access control (RBAC) features, which restrict the escalation of privileges and only authorize personnel to be able to access the information of the administration, which is of utmost importance to ensure that in the large-scale environment, the environment remains secure.

Another factor is disruption in the transition operations. Live production systems would be unstable because automation would be implemented without planning. Therefore, a step-based plan on deployment is paramount - it is necessary to start with the non-critical workloads to ensure the logic of the failover and data replication works and only then proceed with mission-critical applications. The provision of resilience and failover testing in continuous delivery pipelines should be integrated in each stage to confirm the accuracy of orchestration and the behavior of the system in times of stress.

Finally, this incremental approach will allow organizations to develop innovations with high confidence and at the same time remain operational. It also provides a balance between automation-based change and risk management, which leads to long-term sustainability and organizational trust. With the complexity tackled by modular design, alignment of its governance, and step-by-step implementation, enterprises can turn the potential weaknesses into the organized chances to keep enhancing resiliency.

IX. FUTURE DIRECTIONS

The development of HA technologies is moving faster, and automation and intelligence are the next steps to be made to ensure enterprise continuity. The next generation of implementation will use machine learning models to predict failures even before they happen to cause a preemptive snapshot creation and failover. Telemetry analysis AI will provide optimization of infrastructure provisioning in a dynamic manner, with maximum uptime and minimum human involvement.

Predictive Snapshot Scheduling is used to determine how the network will respond to changes in the future Predictive Snapshot Scheduling Predictive Snapshot Scheduling applies to understanding the future behavior of the network with changes.

The new snapshot management systems are taking up predictive algorithms to study workload patterns and automatically schedule backups when traffic is low. This reduces the performance cost and ensures continuous protection. The combination with Terraform pipes will also promote the adaptive backup approaches.

With the growth of hybrid and edge environments, certification of HA will be changed to contain the microservice-level availability validation and real-time SLA validation. It is likely that further versions of SIOS certification will incorporate AI-enhanced auditing and blockchain-enhanced proof-of-recovery and will provide even more transparency to enterprise governance.

X. CONCLUSION

High Availability (HA) has now transcended a passive operational exemplar to a dynamic and automated field of study that outlines the core of digital transformation today. Resilience is no longer a response effort in the modern environment of data driven enterprise, but a design tenet systemically implemented on all infrastructure levels. Terraform, snapshots and SIOS HA certification The combination of Terraform and automated snapshot management with a certification of validation is a major paradigm shift - automation, data integrity and certified reliability into a single and intelligent operation ecosystem. The combination of these technologies creates a new set of traditional business continuity boundaries, which defines self-sufficient, adaptive, and certifiably resilient infrastructures.

With this convergence, businesses are being able to attain uptime performance, compliance adherence and quantifiable cost economy at a high level not before. The infrastructure-as-Code model of the Terraform allows deploying the high-availability configurations in a predictable and versioned way, and the auto snapshot management ensures constant data protection and recoverability. The SIOS HA certification layer offers the guarantee of reliability in operation and alignment in governance and reduces resilience to a measurable business resource. It is the combination of these triads to form a closed loop system in which orchestration, monitoring, and validation are closely interconnected to achieve intelligent infrastructures that are capable of learning, adapting, and self-correcting in real time.

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

The practical implication of such integration has far-reaching implications. Preventive orchestrations, automatic failovers and certified recovery processes enable organizations to continue operating despite disruptive events that are unpredictable. Business continuity then turns into a smart, proactive process - able to diagnose system anomalies and respond with mitigation measures and be able to restore functionality with minimal human intervention. These data-driven, automated systems save in terms of mean time to recovery (MTTR) by a significant margin, downtime-cost reduction, and create a higher level of customer confidence in electronic services.

Finally, this paper restates that the harmonization of automation, data intelligence and certification assurance is a core part of the future of enterprise IT resilience. Declarative infrastructure of Terraform with sophisticated snapshot lifecycle management and stringent high-availability of the SIOS HA certification make up a roadmap of zero-downtime operations in the enterprise. Infrastructure will not just recover smoothly after failures in the future; they will also anticipate and avoid them and will shift the concept of resilience out of being a support element into becoming a strategic pillar of sustainable digital excellence. This development is an epoch of stable operations where high availability is no longer a goal to be met, but rather an ongoing and self-optimizing condition of enterprise intelligence.

REFERENCES

1. Achar, S. (2021). Enterprise SaaS Workloads on New-Generation Infrastructure-as-Code (IaC) on Multi-Cloud Platforms. Global Disclosure of Economics and Business, 10(2), 55–74. https://doi.org/10.18034/gdeb.v10i2.652
2. Agus, I. P., & Pratama, E. (2021). Infrastructure as Code (IaC) Menggunakan OpenStack untuk Kemudahan Pengoperasian Jaringan Cloud Computing (Studi Kasus: Smart City di Provinsi Bali). Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi, 23(1), 93–105. Retrieved from http://dx.doi.org/10.33169/iptekkom.23.1.2021.93-105
3. Alonso, J., Joubert, C., Orue-Echevarria, L., Pradella, M., & Vladušič, D. (2021). Piacere: Programming trustworthy infrastructure as code in a secure framework. In CEUR Workshop Proceedings (Vol. 2878, pp. 8–15). CEUR-WS.
4. Al-ariki, H. D. E., & Hamdi, M. (2021). Fuzzy Logic and Modified Butterfly Optimization with Efficient Fault Detection and Recovery Mechanisms for Secured Fault-Tolerant Routing in Wireless Sensor Networks. International Journal of Intelligent Engineering and Systems, 14(6), 402–416. https://doi.org/10.22266/ijies2021.1231.36
5. Cheng, X., Deng, S., Cheng, B., Lu, M., & Zhou, R. (2020). Optimization of bias current coefficient in the fault-tolerance of active magnetic bearings based on the redundant structure parameters. Automatika, 61(4), 602–613. https://doi.org/10.1080/00051144.2020.1806012
6. Dalla Palma, S., Di Nucci, D., Palomba, F., & Tamburri, D. A. (2020, December 1). Toward a catalog of software quality metrics for infrastructure code. Journal of Systems and Software. Elsevier Inc. https://doi.org/10.1016/j.jss.2020.110726
7. Guo, Q., Hao, Q., Wang, Y., & Wang, J. (2021). Subway System Resilience Evaluation in Based on ANP-Extension Cloud Model. Xitong Fangzhen Xuebao / Journal of System Simulation, 33(4), 943–950. https://doi.org/10.16182/j.issn1004731x.joss.19-0643
8. Guo, Q., Amin, S., Hao, Q., & Haas, O. (2020). Resilience assessment of safety system at subway construction sites applying analytic network process and extension cloud models. Reliability Engineering and System Safety, 201. https://doi.org/10.1016/j.ress.2020.106956
9. Pasumarthi, Arunkumar. (2022). International Journal of Research and Applied Innovations (IJRAI) Architecting Resilient SAP Hana Systems: A Framework for Implementation, Performance Optimization, and Lifecycle Maintenance. International Journal of Research and Applied Innovations. 05. 10.15662/IJRAI.2022.0506007.
10. Gupta, N., & Vaidya, N. H. (2020). Fault-Tolerance in Distributed Optimization: The Case of Redundancy. In Proceedings of the Annual ACM Symposium on Principles of Distributed Computing (pp. 365–374). Association for Computing Machinery. https://doi.org/10.1145/3382734.3405748
11. Hackl, J. (2021). A cloud-based computational platform to manage risk and resilience of buildings and infrastructure systems. In Proceedings of the 31st European Safety and Reliability Conference, ESREL 2021 (p. 369). Research Publishing, Singapore. https://doi.org/10.3850/978-981-18-2016-8_054-cd
12. Itzkin, A., Scholes, M. C., Clifford-Holmes, J. K., Rowntree, K., van der Waal, B., & Coetzer, K. (2021). A social-ecological systems understanding of drivers of degradation in the tsitsa river catchment to inform sustainable land management. Sustainability (Switzerland), 13(2), 1–28. https://doi.org/10.3390/su13020516
13. Kumara, I., Garriga, M., Romeu, A. U., Di Nucci, D., Palomba, F., Tamburri, D. A., & van den Heuvel, W. J. (2021). The do's and don'ts of infrastructure code: A systematic gray literature review. Information and Software Technology, 137. https://doi.org/10.1016/j.infsof.2021.106593

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

||Volume 5, Issue 2, March-April 2022||

DOI:10.15662/IJRPETM.2022.0502003

14. Liu, S., Gupta, N., & Vaidya, N. H. (2021). Approximate Byzantine Fault-Tolerance in Distributed Optimization. In Proceedings of the Annual ACM Symposium on Principles of Distributed Computing (pp. 379–389). Association for Computing Machinery. https://doi.org/10.1145/3465084.3467902
15. Mitra, S., Chanda, B., & Bhattacharya, P. (2021). Supply Chain Management with Application of Lean Six Sigma and Artificial Intelligence: An Integrated Empirical Investigation. Journal of Supply Chain Management Systems, 12–20. Retrieved from http://publishingindia.com/jscms/
16. Nalini, J., & Khilar, P. M. (2021). Reinforced Ant Colony Optimization for Fault Tolerant Task Allocation in Cloud Environments. Wireless Personal Communications, 121(4), 2441–2459. https://doi.org/10.1007/s11277-021-08830-4
17. Pang, Y., & Wang, X. (2021). Cloud-IDA-MSA Conversion of Fragility Curves for Efficient and High-Fidelity Resilience Assessment. Journal of Structural Engineering, 147(5). https://doi.org/10.1061/(asce)st.1943-541x.0002998
18. Rahman, A., & Williams, L. (2021). Different Kind of Smells: Security Smells in Infrastructure as Code Scripts. IEEE Security and Privacy, 19(3), 33–41. https://doi.org/10.1109/MSEC.2021.3065190
19. Rahman, A., Barsha, F. L., & Morrison, P. (2021). Shhh: 12 Practices for Secret Management in Infrastructure as Code. In Proceedings - 2021 IEEE Secure Development Conference, SecDev 2021 (pp. 56–62). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/SecDev51306.2021.00024
20. Rahman, U. M. I. A. U. A., Munim, W. N. W. A., Che, H. S., Tousizadeh, M., & Muhammad, K. S. (2020). Fault tolerance of asymmetrical six-phase induction machine during single open circuit fault to three open circuit faults using GUI. International Journal of Power Electronics and Drive Systems, 11(2), 611–617. https://doi.org/10.11591/ijpeds.v11.i2.pp611-617
21. Riti, P., & Flynn, D. (2021). Beginning HCL Programming: Using Hashicorp Language for Automation and Configuration. Beginning HCL Programming: Using Hashicorp Language for Automation and Configuration (pp. 1–183). Springer. https://doi.org/10.1007/978-1-4842-6634-2
22. Sabharwal, N., Pandey, S., & Pandey, P. (2021). Infrastructure-as-Code Automation Using Terraform, Packer, Vault, Nomad and Consul. Infrastructure-as-Code Automation Using Terraform, Packer, Vault, Nomad and Consul. Apress. https://doi.org/10.1007/978-1-4842-7129-2
23. Sabharwal, N., Pandey, S., & Pandey, P. (2021). Infrastructure-as-Code Automation Using Terraform, Packer, Vault, Nomad and Consul: Hands-on Deployment, Configuration, and Best Practices. Infrastructure-as-Code Automation Using Terraform, Packer, Vault, Nomad and Consul: Hands-on Deployment, Configuration, and Best Practices (pp. 1–243). Apress Media LLC. https://doi.org/10.1007/978-1-4842-7129-2
24. Senthamizhkumaran, V. R., Santhy, P., Selvi, D., Kalaiselvi, T., & Sabarinathan, K. G. (2021). Impact of Organic and Inorganic Sources of Nutrients on Root Architecture, Soil Microbial Biomass and Yield on Low Land Rice Ecosystem. International Journal of Plant & Soil Science, 240–250. https://doi.org/10.9734/ijpss/2021/v33i2430773
25. Townsend, P. A., Clare, J. D. J., Liu, N., Stenglein, J. L., Anhalt-Depies, C., Van Deelen, T. R., … Zuckerberg, B. (2021). Snapshot Wisconsin: networking community scientists and remote sensing to improve ecological monitoring and management. Ecological Applications, 31(8). https://doi.org/10.1002/eap.2436
26. Vayghan, L. A., Saied, M. A., Toeroe, M., & Khendek, F. (2021). A Kubernetes controller for managing the availability of elastic microservice based stateful applications. Journal of Systems and Software, 175. https://doi.org/10.1016/j.jss.2021.110924
27. Wang, B., Vakil, G., Liu, Y., Yang, T., Zhang, Z., & Gerada, C. (2021). Optimization and analysis of a high power density and fault tolerant starter–generator for aircraft application. Energies, 14(1). https://doi.org/10.3390/en14010113
28. Yu, Y., Li, X., & Wei, L. (2020). Fault tolerant control of five-level inverter based on redundancy space vector optimization and topology reconfigruation. IEEE Access, 8, 194342–194350. https://doi.org/10.1109/ACCESS.2020.3033805
29. Zhang, S., Zhang, W., Zhao, J., & Wang, R. (2021). Multi-Objective Optimization Design and Analysis of Double-Layer Winding Halbach Fault-Tolerant Motor. IEEE Access, 9, 3725–3734. https://doi.org/10.1109/ACCESS.2020.3047860
30. Zhang, W., Chen, X., & Jiang, J. (2021). A multi-objective optimization method of initial virtual machine fault-tolerant placement for star topological data centers of cloud systems. Tsinghua Science and Technology, 26(1), 95–111. https://doi.org/10.26599/TST.2019.9010044