Guardian

Configuration Drift in the Clouds

Why Change Management, Configuration Management and Drift Management matter even more in the cloud.

Executive Summary

Cloud adoption brings speed and elasticity—but also the risk of **configuration drift**. In dynamic, multi-cloud environments, even small, untracked changes accumulate and degrade security, compliance, reliability, and cost control. Effective cloud governance requires modernised change enablement, Infrastructure as Code (IaC), continuous drift detection, and automated remediation orchestration. This whitepaper outlines cloud-neutral practices and compares three complementary approaches: **Guardian by Cloudhouse**, **Azure Policy**, and **AWS Config**.

Introduction

Cloud platforms are inherently dynamic: resources are created, modified, and retired at high velocity across providers. In this context, configuration drift—divergence between actual configuration and the approved baseline—becomes inevitable without policy-driven guardrails and automation. Traditional change management remains relevant but must evolve into progressive change enablement that integrates with developer workflows and cloud-native tooling.

The Problem: Drift and Its Consequences

Configuration drift occurs when infrastructure or system settings diverge from their intended state over time—often due to manual console changes, emergency fixes, or conflicting automations. **Consequences include:**

Security risks from misconfigured permissions or unpatched systems.

Compliance failures that jeopardise regulatory obligations.

Operational instability, where undocumented changes lead to outages, circa 70% of network failures stem from configuration errors (Uptime Institute, 2023).

Importantly another consequence of configuration drift aligns with the financial impact to the business, misconfigurations or changes in configuration can have unforeseen impacts on the billing for cloud services used by the business. If unplanned, unapproved changes get implemented, this can cause significant uplift in costs for running services which, in turn, has a natural knock-on effect to the charges passed from the cloud provider to the customer. For many, staying on top of the cost of cloud utilization is a focus.

Why Change Enablement Still Matters

Cloud-native architectures increase the number and frequency of changes. Rather than abandoning governance, organisations should automate it: codify policies, integrate approvals with CI/CD, and use tooling that continuously validates and reconciles the estate to the baseline while preserving agility.

Solution Pillars: Governance and Automation

To tame the chaos, organisations need three pillars:

Infrastructure as Code (IaC):
Treat configurations as version-controlled artefacts. IaC ensures a single source of truth and enables reproducibility.

Continuous Drift Detection:
Continuously evaluate configurations against baseline policies and desired state across clouds.

Implementation and alignment with Change Policy:
Use policy effects or automation runbooks to restore compliance, and reconcile changes with service management workflows.

Tool Comparison: Which Approach Fits Your Estate?

Capability	Guardian	Azure Policy	AWS Config
Primary Purpose	Unified drift management and forensic traceability across multi-cloud	Policy enforcement & compliance for Azure resources	Configuration recording and compliance evaluation for AWS resources
Resource Inventory	Discovers and unifies multi-cloud estate	Azure Resource Graph integration	Continuous configuration recorder for AWS
Configuration History	Full forensic change traceability	Activity logs and compliance snapshots	Time-ordered configuration timeline
Drift Detection & Compliance	Continuous drift detection across providers	Policy definitions evaluate compliance	Config rules and conformance packs
Remediation	Automated reconciliation integrated with ITSM	DeployIfNotExists/Modify effects	SSM Automation for remediation
Ease of Use	Intuitive UI, minimal technical overhead	Requires deep Azure knowledge	Requires AWS-specific expertise
Integration	ServiceNow, Freshservice, CI/CD pipelines	Azure Monitor, Defender, pipelines	AWS Systems Manager, CloudFormation
Reporting	Unified dashboards and audit evidence	Compliance dashboard per resource/policy	Compliance status and timelines

How does Guardian by Cloudhouse help?

Guardian is designed for multi-cloud realities, offering a unified view across providers without requiring deep platform-specific expertise. Unlike Azure Policy and AWS Config, which are tied to their ecosystems and assume technical familiarity, Guardian provides an intuitive interface and clear workflows accessible to both technical and non-technical teams. It simplifies drift detection and remediation, reducing complexity and accelerating compliance. By integrating with ITSM tools such as ServiceNow and FreshService along with CI/CD pipelines, Guardian ensures change reconciliation is seamless, transforming audits into continuous evidence generation. For organizations seeking simplicity, visibility, and agility across clouds, Guardian is the stronger choice.

Guardian interrogates your **Azure, AWS or GCP** accounts to ensure that all elements of your services are accounted for and then proceeds to add them into its management framework enabling detailed monitoring of configuration across your elements and forensic traceability of change within them. Including increases in resource utilisation a key symptom of latent configuration drift.

With the promise of extreme flexibility comes the challenge of tracking and verifying the ongoing churn of change in the cloud environment. If you attempt to apply traditional manual methods to this environment your **Change Management team** would easily be overwhelmed. Firstly by having to work through the load of **Change approvals**, then having to reconcile those completed changes with the actual environment post change implementation.

How does Guardian by Cloudhouse help?

As you can imagine with the volume and rate of change within cloud estates this easily becomes a problem that is hard to address purely with manual effort. This is where **Guardian's ability** to integrate with **key Service Management tools** enables you to bring cloud estates into your existing governance framework.

servicenow
freshservice
bmc
ivanti

Automatically reconciling the changes occurring with those approved via your processes and tooling such as **ServiceNow** or **FreshService**. Highlighting those that are out of band, where changes have not been approved and importantly where changes are expected but have not been implemented or deployed successfully.

Guardian operates at scale providing native support for the key cloud services supporting your business needs and providing seamless support with a unified approach no matter the services you make use of in your cloud infrastructure.

Crucially, we transform the audit experience. **Automated evidence capture**, **consistent policy enforcement**, and **real-time configuration visibility** replace the scramble for screenshots and human-assembled reports. Instead of auditing being a disruptive, retrospective exercise, integrated tooling enables **continuous audit readiness,** giving stakeholders **trustworthy proof of compliance** at any point in time.
Working with large scale organisations **Cloudhouse** has brought order to chaos reigning in the wild west of cloud implementations and providing the key transparency and visibility into these complex large-scale implementations which previously had remained opaque and been ungovernable.

Agility Secured, Compliance Simplified.

Benefits of Doing It Right

Security hardening by eliminating misconfigurations.

Regulatory compliance through continuous enforcement.

Operational resilience by reducing outages linked to undocumented changes.

Cost optimisation by preventing resource sprawl.

Conclusion

Cloud environments amplify the risks of configuration drift. The principles of change enablement that safeguarded traditional infrastructures are not obsolete, they’re indispensable.
By combining governance, automation, and proactive monitoring, IT leaders can transform cloud operations from chaos to control, ensuring security, compliance, and operational excellence.

References
Gartner (2025). Cloud Adoption Trends Report.
IDC (2024). Governance in Cloud Environments Study.
Uptime Institute (2023). Network Outage Analysis.
AWS, HashiCorp, Cloudhouse (2024). Drift Management Tools Documentation.