



Config Drift and Audit Solution Brief

Eliminate misconfigurations and security holes in your network with Gluware Config Drift and Audit

The Challenge

As businesses continue to digitize, the functionality and performance of the underlying network becomes more critical for success. Over time, network device configurations have continued to increase in size and complexity, making them harder to manage. Networks are also growing in size as businesses expand, and have added devices from multiple vendors for specific functionality like firewalls, load balancers, WAN optimizers and many more functions. Traditionally, these devices are manually configured by many different IT personnel, resulting in inconsistent configurations which are often not discovered until the network is audited. Operations teams regularly perform time consuming manual audits of the network to meet the requirement for various compliance organizations. Additionally, organizations may have defined a standard “policy” for configuration, but over time they are likely have drifted from these standards and are now just trying to keep the network running, minimizing cleanup while removing misconfigurations or potential security holes in the network.

The Solution Gluware® – Config Drift and Audit

Gluware Config Drift enables organizations to achieve control over their network devices and the “wild west” approach to change management taking place in most networks today.

Misconfigured devices are one of the primary causes for network outages, accounting for more than half of all network issues.

Configuration Drift provides operations with the ability to “snapshot” a known good configuration and then apply a comparison to determine if any changes have been implemented. If changes (drift) have been detected, line by line differences in the configuration are easily identified.

This becomes very powerful when an organization is able to monitor for configuration changes across all the hundreds or even thousands of multi-vendor devices in the network. If a change is approved, a new “snapshot” can be taken to promote the approved/validated configuration. If a change is not approved, it can be easily mitigated.

Benefits of Gluware® – Config Drift and Audit:

- Avoid outages caused by manual mis-configurations in the network
- Proactively detect configuration changes and quickly identify what has changed
- Detect and remediate unauthorized configuration changes across all network devices
- Reduce the risk and security vulnerability caused by out of policy configurations
- Eliminate holes in the network caused by potentially malicious configurations
- Ensure consistency of configurations across the network (QoS policy, ACL policy)
- Provide network-wide configuration audits in minutes with reporting capabilities

Features of Gluware® – Config Drift and Audit:

- Detect and remediate unauthorized configuration changes across all multi-vendor network devices
- Once verified, “Snapshot” an existing configuration as the default configuration to compare all others against
- Take periodic snapshots and compare any two snapshots, to quickly identify configuration changes
- When configuration drift is detected, the exact lines of configuration that have been changed are quickly identified
- Activity logs to determine all actions - including editable user notes
- Export Configuration Drift results which can be used for compliance reporting.