ctac

Using Terraform to Automate Cloud Enclave Clients

Using Terraform to Automate Cloud Enclave Clients

Customer Overview:

The ideal customer of a Terraform project is any Public Sector Agency operating in AWS Cloud. CTAC manages each of our federal customers using multi-tenant Cloud Enclaves. Our clients require highly secure, isolated environments to manage sensitive data and workloads while still maintaining centralized control and compliance. They rely on us to manage an integrated orchestration system to streamline operations and monitoring of their infrastructure. To support their cloud security needs, many of these organizations leverage Kion, a cloud operations platform that integrates seamlessly with AWS. The solution we provide is tailored to leverage both Kion and Terraform, which together have become a defining part of our internal operations and client solutions.

Challenge and Need:

Prior to the implementation of this solution, clients and cloud consultants faced several hurdles in managing their AWS Cloud environments. Modern best-practice cloud infrastructure presents several key challenges: the isolation of environments means many accounts to manage, insight into spending across numerous projects and accounts is fragmented, and maintaining security and compliance across this complex base can require significant engineering. To address these issues, CTAC's goal is to provide a unified solution that allows clients to access and manage their resources from a single point, with seamless integration between different environments. Guaranteeing consistent security, performance, and ease of use across multiple AWS accounts is essential for improving the operational efficiency of our clients. Standardized templates and modules crafted to customer specifications allows account-factory style provisioning with minimal configuration.

Solution Implemented:

CTAC offers a comprehensive solution using Terraform and Kion, providing clients with a single sign-on (SSO) experience and automated infrastructure provisioning. The technical and operational processes involved are as follows:

1. Account Creation & Integration:

- We provision new AWS accounts for tenants and incorporate them into the AWS Organizations structure with consolidated billing.
- Each new account is associated with a Kion project, where project and team resources and permissions are managed.
- Kion provides its own high level OU structure for enforcing permissions, project isolation, compliance, and different FISMA security levels

2. Terraform Implementation:

- We use Terraform to define and provision infrastructure in a consistent and modular way. This allows us to apply the same configuration to different projects, accounts, and environments, including but not limited to networking, security groups, databases, compute resources, and other essential infrastructure components.
- Through Terraform's infrastructure-as-code (IaC) capabilities, the process is highly automated, eliminating manual interventions and reducing human error.

3. Modular & Consistent Environment:

- Terraform modules are used to ensure that infrastructure was provisioned consistently across different projects. This modular approach enables our clients to scale easily, and maintain standard security policies across all environments.
- The integration of Terraform within Kion provides a consolidated dashboard that displays real-time status across all accounts, improving visibility and management efficiency for the clients.
- Terraform modules allow enclave-wide configurations to be managed in a single place and easily modified as needs evolve over time while eliminating "configuration drift."

4. Operational Workflow:

- Daily operations include policy updates, provisioning and decommissioning of resources (e.g., EC2 instances), and managing cloud resources as needed.
- Terraform allows us to manage the entire lifecycle of cloud resources, ensuring that security standards are consistently applied across all environments.

5. Security & Access Management:

- We leverage Zscaler as a Zero-Trust solution for secure remote access to resources, tightly integrating with Okta for secure single sign-on (SSO) and Active Directory to provide clients with seamless, secure access to their AWS resource without the need for multiple sets of credentials.
- This significantly improves access management and reduces the overhead of managing multiple AWS accounts and projects.

Results and Benefits:

The implementation of Terraform provides measurable improvements across several key areas:

1. Security & Compliance:

- Consistent Security Standards: By using Terraform to enforce consistent policies across multiple accounts, security configurations are uniformly applied across all environments.

- The integration of SSO via Zscaler + Okta simplifies access control and enhances security for users managing multiple accounts.

2. **Operational Efficiency:**

- The modular approach of Terraform leads to greater consistency and predictability in resource provisioning. Clients no longer have to manually configure infrastructure components for each account.
- Automated infrastructure provisioning and lifecycle management reduce manual intervention, resulting in time savings and more efficient resource management.

3. **Time & Cost Savings:**

- With the consolidated Kion dashboard, clients can easily monitor budgets and track savings across all projects. The time saved from not having to manually manage resources or credentials is substantial.
- Clients experience faster deployment times and a reduction in operational overhead by using Terraform's infrastructure-as-code approach.

4. **Centralized Management:**

- Kion replaces several native AWS tools, consolidating management into a single, holistic interface. Clients now have easy SSO access to their AWS accounts and resources without the need for managing separate credentials. User access is simplified, identities are centralized, access and roles are easily audited.
- Tracking and documenting changes in infrastructure via Terraform + Git enhances transparency and allows for efficient change management.

5. **Scalability:**

- The modular, IaC approach enables clients to scale their infrastructure quickly and consistently. They can replicate infrastructure across environments or projects with minimal effort, while ensuring that all environments adhere to the same security and performance standards.

Conclusion:

By leveraging Terraform, we are able to deliver a streamlined, efficient, and secure cloud orchestration solution for our AWS Cloud Enclave clients. This solution eliminates the need for clients to manage account specific credentials, simplifies security through account consolidation and SSO, and automates infrastructure provisioning and compliance scanning. Ultimately, it provides measurable improvements in security, operational efficiency, and cost savings.