aws PARTNER Advanced Tier Services

binbash®

Building a Secure AWS Landing Zone and VPN Foundation for Cloud Migration

Executive Summary

HiCap is an AI-driven technology company focused on building advanced data and intelligence platforms to support scalable, high-performance workloads. As part of its growth strategy, HiCap planned to migrate its runtime platform from Microsoft Azure to AWS. At the time of engagement, HiCap already had an existing AWS POC account used for early experimentation, which needed to be integrated into a production-ready AWS Organization.
To support this transition, HiCap partnered with binbash, an AWS Advanced Consulting Partner, to design and deploy a secure AWS Landing Zone, integrate the existing POC account, and establish a private VPN access layer, all aligned with AWS Well-Architected best practices.

Customer Challenge

HiCap faced the challenge of scaling beyond early experimentation while maintaining security, governance, and operational efficiency. Key challenges included:

- An existing standalone AWS POC account that lacked centralized governance, security controls, and cost visibility.
- The need to import and standardize that POC account within a broader multi-account AWS Organization.
- Secure access requirements for internal services and future Kubernetes workloads.
- The need to move fast with POCs while ensuring the environment could later be hardened for production.
- Limited internal capacity to design a multi-account AWS foundation following AWS best practices.

HiCap engaged binbash to transform its early AWS footprint into a well-governed, scalable cloud foundation without disrupting existing POC work.

hicap

Hicap is an AI capacity management platform that helps teams run top foundation models at lower cost and higher throughput. It provides rate-limit-free inference, instant model switching across OpenAI, Anthropic and Gemini, and reserved GPU capacity for faster performance. With drop-in SDK compatibility, clear cost visibility and strong security, Hicap simplifies scaling AI.

binbash has helped accelerate our compliance goals by building our secure AWS foundation and infrastructure automation. The team has also helped accelerate our application deployments by integrating with our teams. Thanks to binbash, we've reduced deployment times, fewer compliance issues,

JAVIER CEVALLOS
CTO & CO-FOUNDER

aws PARTNER Advanced Tier Services

binbash®

Solution

binbash designed and implemented a fully Infrastructure-as-Code (IaC) AWS Landing Zone, using Terraform and the binbash Leverage™ reference architecture, while importing HiCap's existing POC account into the AWS Organization.

This approach allowed HiCap to:

- Preserve ongoing POC workloads.
- Immediately benefit from centralized security, identity, and cost governance.
- Prepare the environment for future production-grade platforms such as Amazon EKS.

Key AWS Services and Technologies

- AWS Organizations to establish a structured multi-account model and import the existing POC account.
- AWS Identity Center (SSO) for centralized authentication and role-based access.
- Amazon VPC, Route 53, and VPC Peering for shared networking and DNS resolution.
- AWS CloudTrail, IAM Access Analyzer, KMS, and VPC Flow Logs for security and auditing.
- AWS Budgets and CloudWatch Billing Alarms for cost control.
- Amazon EC2 with Pritunl VPN to provide secure private access to internal AWS resources.

Architecture Overview:

A multi-account AWS Organization where an existing POC account was imported and standardized alongside newly created Dev and Prod accounts, with centralized security, shared networking, and a hardened VPN access layer.

Key Components of the Solution

- **AWS Organization with Imported POC Account**
  - Imported HiCap's existing apps-poc account into the AWS Organization.
  - Applied Service Control Policies (SCPs) and security baselines without disrupting active workloads

.

- **Identity & Access Management**
  - Centralized authentication using AWS Identity Center (SSO).
  - Least-privilege permission sets consistently applied across all accounts.

- **Networking & DNS**
  - Shared VPC architecture with controlled VPC peerings.
  - Route 53 private and public hosted zones for internal and application services.
  - Network design aligned with future EKS deployments.

- **Security Baseline**
  - Organization-wide CloudTrail for auditing.
  - IAM Access Analyzer for exposure detection.
  - Customer-managed KMS keys in every account.
  - Secure defaults for IAM, S3, EBS, and MFA.

- **Private Access via VPN**
  - Pritunl VPN deployed in the shared account.
  - MFA-enabled access to private subnets, internal tools, and APIs.
  - Reduced public exposure of development and POC environments.

- **Cost Governance**
  - Centralized billing through the management account.
  - Budgets and alerts to track actual and forecasted spend.

Results

- Seamless integration of an existing AWS POC account into a governed AWS Organization.
- Immediate security and governance improvements without interrupting active experimentation.
- Faster path from POC to production, enabled by standardized accounts and networking.
- Reduced operational risk through centralized auditing, encryption, and access controls.
- Improved cost visibility across all AWS environments.

Key Milestones

- **AWS Organization Setup & POC Account Import**
  - Created AWS Organization and Organizational Units.
  - Imported HiCap's existing POC account into the organization.
- **Identity & Security Baseline**

binbash®

- Configured AWS Identity Center (SSO).
- Enabled CloudTrail, IAM Access Analyzer, and encryption across all accounts.

- **Shared Networking & DNS**
  - Deployed shared VPCs, peerings, and Route 53 hosted zones.
  - Integrated POC, Dev, and Prod environments into the shared network.
- **VPN Deployment**
  - Provisioned EC2 instance and configured Pritunl VPN with MFA.
  - Enabled secure private access to internal AWS resources.
- **Knowledge Transfer**
  - Delivered documentation and walkthrough sessions.
  - Enabled HiCap's team to manage and extend the platform independently.

Metrics

- Infrastructure automation: ~100% of core resources managed via Terraform.
- POC continuity: 100% — no disruption to existing workloads during account import.
- Security coverage: Centralized logging, encryption, and access controls across all accounts.
- Cost efficiency: 100% of Landing Zone costs covered via AWS Startup funding.

Conclusion

By partnering with binbash, HiCap successfully evolved from an isolated AWS POC into a secure, scalable, and well-governed multi-account AWS environment. The decision to import and standardize the existing POC account allowed HiCap to maintain development velocity while gaining the benefits of enterprise-grade cloud governance.

Built following the AWS Well-Architected Framework and accelerated by binbash Leverage™, the solution positioned HiCap to confidently scale its workloads, adopt Kubernetes and production platforms, and continue its cloud migration with a strong and future-proof foundation.