Welcome

DCO COBRA and SOSSEC - CYBER TALK
October 1, 2020

Presents - HashiCorp

and

Infrastructure as Code, Security as Code, and
Policy as Code for Implementing a Cloud Operating Model

Speakers Include:

James Nyika
HashiCorp, Solutions Architect

Louis Alberne
HashiCorp, Army Account Director
US Army

The Cloud Operating Model at the Edge

FY 2021

Louis Albuern - lalbuern@hashicorp.com

James Nyika - jnyika@hashicorp.com

UNCLASSIFIED
About HashiCorp

Leading Cloud Infrastructure Automation

Our software stack enables the provisioning, securing, connecting and running of apps and the infrastructure to support them.

We unlock the cloud operating model for every business and enable their digital transformation strategies to succeed.

Founded | Employees | Funding
---|---|---
2012 | 1000+ | 349M

#4 Forbes Cloud 100 List - [https://www.forbes.com/cloud100/#4b6f3eab5f94](https://www.forbes.com/cloud100/#4b6f3eab5f94)
A generational transition is underway

Proprietary & Varied Infrastructure
“Static”

- Proprietary Custom Designed Networks and Compute
- Dedicated Fixed Infrastructure

Army Tactical Data Center (Cloud Model)
“Dynamic”

Commodity Hardware Running Cloud Stacks and Mission Kits

Big Data Platforms In the Cloud
The 4 essential elements of distributed infrastructure

D0 - Operations
Provision infrastructure

D1 - Security
Secure infrastructure and applications

D2 - Development
Run/Deploy applications on Infrastructure

D3 - Connect
Infrastructure and applications
## Adopting Capabilities to thrive

### Challenge
What tools are available to help you manage the challenges of working in a distributed infrastructure environment?

### Default Solution
Use the tools provided by each CSP or ISV to manage the challenge in their environments.

### DEDICATED
- **Run Development**: vSphere
- **Connect Networking**: Hardware
- **Secure Security**: IP: Hardware
- **Provision Operations**: vCenter

### MULTI CLOUD
- **vSphere**: vSphere
- **EKS / ECS**: Various Hardware
- **Identity: AD/LDAP**: Identity: AD
- **Cloud Formation**: Terraform
- **AWS**: AWS
- **Azure**: Azure
- **GKE Cloud Functions**: GKE Cloud Functions
- **CloudApp/AppMesh**: CloudApp/AppMesh
- **Identity: AWS IAM**: Identity: AWS IAM
- **Resource Manager**: Resource Manager
- **Identity: Azure AD**: Identity: Azure AD
- **GKE Cloud Functions**: GKE Cloud Functions
- **Proprietary**: Proprietary
- **Cloud Dep. Manager**: Cloud Dep. Manager

### PHYSICAL
- VMs

### CLOUD NATIVE
- CONTAINERS

### SERVERLESS
- SERVICES

### EDGE
- DEVICES
Challenge
How can we consistently and quickly provision infrastructure in our predefined multi-infrastructure providers in Garrison, Regional Cyber Center or at the Tactical Edge?

Example: Provisioning Infrastructure

GEF on VMWARE

GDP/DDS on RED HAT
Best practice approaches

### Challenge
What tools are available to help you manage the challenges of working in a distributed infrastructure environment?

### BEST Solution
Leverage a **COMMON ENTERPRISE CAPABILITY** that can provision, secure, connect and deploy across ALL the environments you are mandated to use.

<table>
<thead>
<tr>
<th>PHYSICAL</th>
<th>VMs</th>
<th>CONTAINERS</th>
<th>SERVICES</th>
<th>DEVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="App Server" /></td>
<td><img src="image" alt="Vms" /></td>
<td><img src="image" alt="Containers" /></td>
<td><img src="image" alt="Services" /></td>
<td><img src="image" alt="Devices" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Orchestration</th>
<th>Networking</th>
<th>Security</th>
<th>Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nomad</td>
<td>Consul</td>
<td>Vault</td>
<td>Terraform</td>
</tr>
</tbody>
</table>
Infrastructure as Code (IaC) vs Click-Ops

Increase Agility

With Infrastructure as Code the manual effort involved in provisioning infrastructure (Click-Ops) is significantly reduced. Code can be reused and modified as many times as necessary.

Infrastructure as Code:
Enabler for objective of Time Dominance for Multi-Domain Operations

Click-Ops:
Provisioning infrastructure through Point and Click GUI's or custom scripts is slow, error-prone, and inefficient
Provisioning Infrastructure

Solution
Terraform Enterprise Infrastructure as Code (IaC) provides:

- Out of the box provisioners for infrastructure providers you use today (OpenStack/VMware)
- Integration with Config Mgmt Tools
- Single Declarative Language
- Human Readable
- Machine Parsable
- Support Policy As Code
Securing Infrastructure

Challenge
How do we manage credentials for across all the provisioned resources centrally, securely and reliably?

- Dynamic Credential Provisioning
- Rotate Credentials
- App Credentials
Securing Infrastructure

Solution
Utilize a flexible credentials/secrets manager designed for the new cloud operating model
Deploy Applications or Mission Kits

Challenge
How do we **consistently and efficiently** deploy applications across the fleet of infrastructure we have provisioned and secured?
Deploy Applications or Mission Kits

Solution
Use an orchestrator and scheduler like Nomad to provision pre-built kits, containers or legacy applications consistently and resource efficiently on your infrastructure.

INTEL APPS

Enterprise Apps

Mission Apps

HARDENED IMAGES
FROM IMAGE REPO

NOMAD DEPLOYS

kubernetes
Connecting Applications

Challenge
Can we overlay a logical SERVICE network over the field network to provide a service registry and better manage East-West traffic?
Connecting Applications

Solution
We can use a SERVICE NETWORKING CAPABILITY like Consul to create:

- A Service Registry with Health Checks
- Configure MUTUAL TLS (mTLS) between services and applications without altering them
- Dynamically reconfigure routers, switches and firewalls between services to allow them to adapt to the new requirements
Notional Use Case: Deployment to Tactical Edge

1. **IaC/VCS Repository**
   - OROCK
   - GITLAB
   - DRUID
   - CI/CD Pipeline

2. **Load DRUID QEMU Images**
   - Intermittent

3. **Deployment of GDP/GEF Module**
   - FORGE
   - GDP/GEF/Armory

4. **Hashicorp Vault Dynamic Credentials Generated**
   - Intermittent

4a. **Hashicorp Terraform Provisioned Tactical Kit Infrastructure in Openstack or KVM/RHV**

5. **Deploy Tactical Kit Applications to Infrastructure with Hashicorp Nomad**

6. **Tear Down Tactical Kit Infrastructure. Retain Data for Analysis**

**Intermittent**

**TACTICAL INTEL KIT**

**EDGE/DDS**
Cyber Mission Infrastructure Support

Mission Partners

Big Data Platform

Fort Gordon / GDP/GEF
FORGE SOUTH
(Innovation)

RCC CONUS / GDP/GEF

ARMORY

RCC Europe / GDP/GEF

Fort Belvoir / GDP/GEF
FORGE North
(Innovation)

CAMP ROBERTS / DDS/CPT/Tactical Kit
Data Plane

Control Plane

Policy As Code

Sentinel

Policy Enforcement Point

At IaC Provisioning
At Authentication
At Secret Access
At Access
At Authentication
At Authentication
At Access

DCO Tools
ACAS
HBSS
Splunk / SIEM
IPS/IDS
QRadar

Army Policies
DoD PKI
NIST 800.53
NIST 800-207
Active Directory
RMF
Continuous ATO

Security Teams
Compliance Teams

Users/
Mission
Owners
Warfighters

Enterprise
Resources
Containers, VMs
BareMetal
Apps

Enterprise
Resources
Containers, VMs
BareMetal
Apps
Hashicorp Enterprise Solutions Remediates Cloud Migration Challenges

EXAMPLE ENTERPRISE JOURNEY TO UNLOCK A CLOUD OPERATING MODEL

Solutions
- Nomad
- Consul
- Vault
- Terraform

Containers Orchestration
- Service Registry & Discovery
- Network Middleware Automation

Heterogeneous Workload Orchestration
- Service Mesh
- Encryption as a Service
- Advanced Data Protection

Innovate

Establish

Standardize

Innovate
What: Provides the foundation for cloud infrastructure automation using infrastructure as code for provisioning and compliance in the cloud operating model

- Multi-Cloud Compliance & Management to provision and manage any infrastructure with one workflow
- Self-Service infrastructure for users to easily provision infrastructure on-demand with a library of approved infrastructure modules
- Provision Infra and 3rd party software dependencies
  - Firewalls, Load Balancers, Analytic/Monitoring tools
Vault: Security Automation

Provides the foundation for cloud security that uses trusted sources of identity to keep secrets and application data secure in the cloud operating model.

- **Secrets management** to centrally store and protect secrets across clouds and applications.
- **Data encryption** to keep application data secure across environments and workloads.
- **Advanced Data Protection** to secure workloads and data across traditional systems, clouds, and infrastructure.
- **Integrates with Multiple Authentication Sources** to include Active Directories, AWS IAM, Azure AD, Okta, etc.
- **Participates in Zero Trust security** by requiring Authentication of Identity for machines and users.
Consul: Network Automation

Provides the foundation for cloud network automation as a central service registry for service-based networking in the cloud operating model

- **Service registry & health monitoring** to provide a real-time directory of all services with their health status
- **Network middleware automation** with service discovery for dynamic reconfiguration as services scale up, down or move
- **Zero Trust network with service mesh** to enable identity-based security enforced at the endpoints via sidecar proxies
- **Real time integration with underlying network** to dynamically open/close ports and update routing tables as infrastructure changes and workloads move
Nomad: Application Automation

Provides the foundation for cloud application automation by enabling workload orchestration in the cloud operating model

☑ Container Orchestration for deploying, managing and scaling containerized applications

☑ Legacy Application Orchestration to containerize, deploy and manage legacy apps on existing infrastructure

☑ Batch Workload Orchestration to enable ML, AI, data science and other intensive workloads in high performance computing (HPC) scenarios

☑ Orchestrates any Application to include Bare Metal, Virtual Machines, .NET apps, JAR, Containers, etc
Call to Action

What can you do as a next step

- **Talk to us** for a deeper dive into any one of these topics, use cases or to discuss a challenge you are having. HashiCorp is a Partner First company

- **Consider a free hands-on webinar** to learn more about the world of possibilities:
  
  [https://www.hashicorp.com/events/](https://www.hashicorp.com/events/)

- **Ask more questions** - reach out to us for answers about how our other customers are overcoming challenges like yours

- **Recommended Reading - Terraform: Up and Running by Yevgeniy Brikman**
  
  - Chapter 1 is available online (O’Reilly Publication)
  - [https://www.oreilly.com/library/view/terraform-up-and/9781491977071/ch01.html](https://www.oreilly.com/library/view/terraform-up-and/9781491977071/ch01.html)

Louis Albuerne - [lalbuerne@hashicorp.com](mailto:lalbuerne@hashicorp.com)
SOSSEC Membership is Required for Award on PEO EIS, DCO
Cyberspace Operations Broad Responsive Agreement (COBRA)
Other Transaction Agreement (OTA)

Benefits of Joining the SOSSEC Consortium

✔ Opportunity to perform work under seven (7) OTAs for the Air Force, Army and National Geospatial-Intelligence Agency
✔ Opportunity to build members’ business base by applying their technologies/expertise to meeting urgent DoD requirements
✔ Simple, streamlined process to compete for DoD work
✔ Average 60 days from requirements definition to award
✔ Flexible treatment of intellectual property
✔ OTA access to any DoD user with approval of OTA customer

Go to www.sossecinc.com and click on the JOIN NOW Tab to access the membership application. The process is simple and rapid. There is no joining fee, and the membership fee is $500 per year. Membership is open to Industry (traditional, nontraditional, small business), not for profit and academic institutions that share the values of the SOSSEC Consortium.

Questions about SOSSEC COBRA OTA contact: eaguirre@sossecinc.com
Q&A

Louis Albuerne | lalbuerne@hashicorp.com

www.hashicorp.com