

ACME Corp: Challenges and Solutions

Enhancing Service Discovery and Resilience Across AWS & Azure Clouds

Joji Varghese

Nov'2023

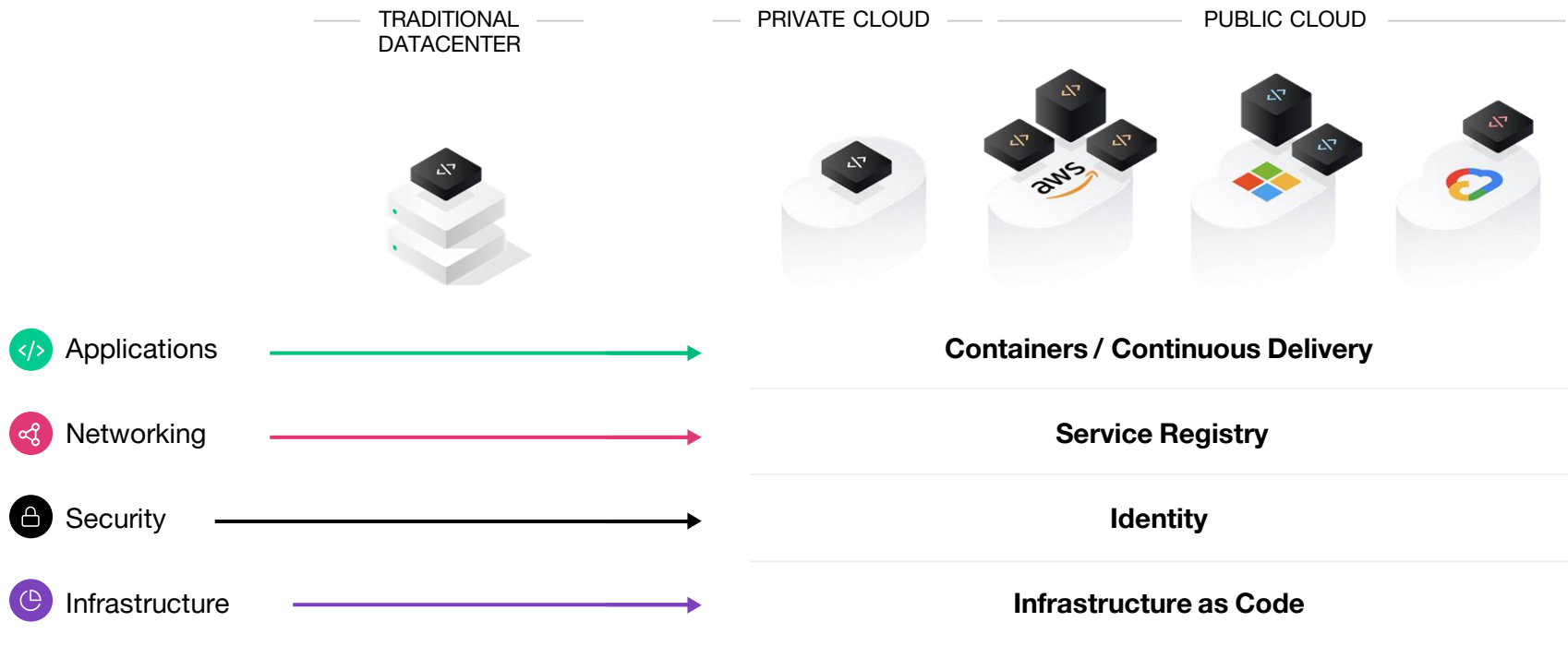
Agenda



- HashiCorp Introduction
- ACME Corp Requirements and Challenges
- HashiCorp Solution Recommendation
- Demo
 - Consul demo – Resiliency and Access Control
- Summary and Next Steps

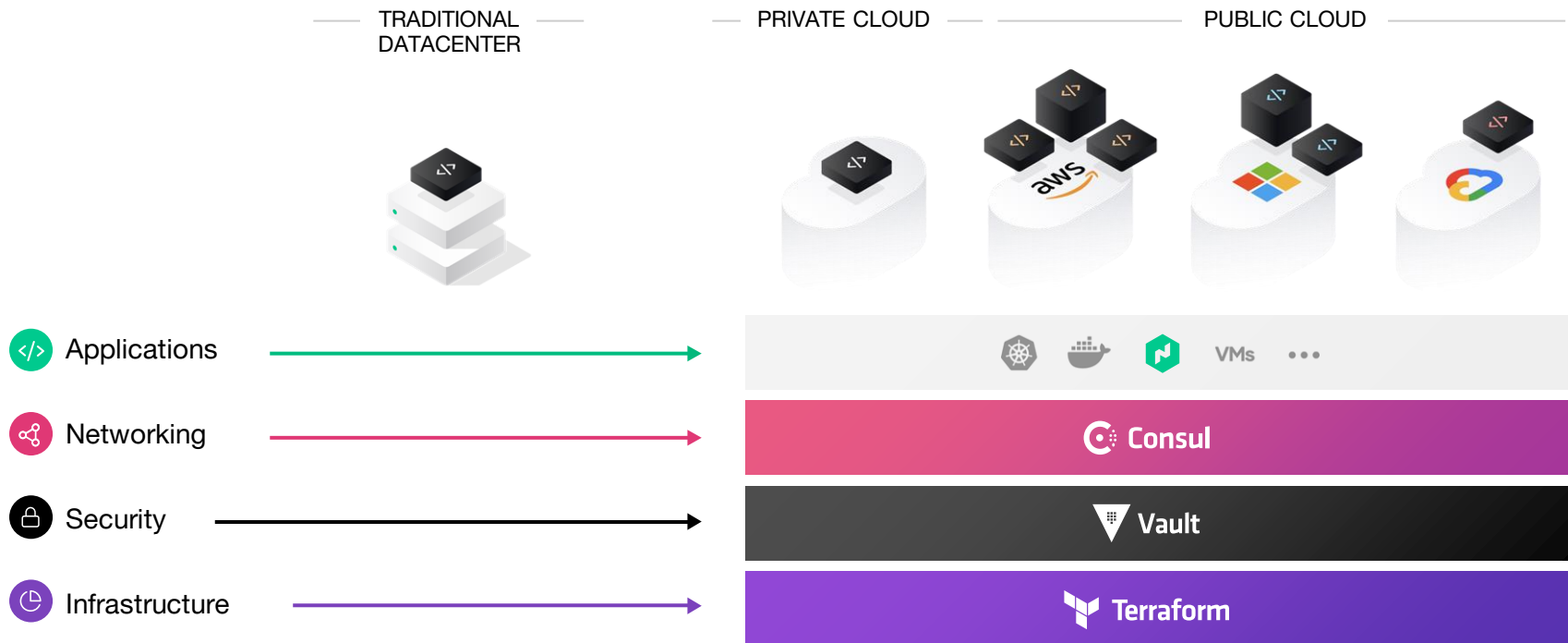


Challenge: Dynamic infrastructure introduces new **control points** at each layer





Solution: **Unified interfaces** to simplify and accelerate cloud adoption





ACME Corp Requirements and Challenges

- ACME Corp: A leading SaaS-based Business Intelligence application provider
- Revenue Significance: The **BI application** accounts for over 85% of ACME's revenue
- Current Infrastructure: **Hundreds of microservices** on AWS EKS clusters
- Key Challenges:
 - Need for a robust service discovery solution
 - Securely connecting microservices
 - Exploring alternate service discovery solutions
 - Ensuring higher availability post recent AWS outages: Considering Azure as a potential platform
 - Seeking a scalable solution with fastest time to market



HashiCorp Solution using Consul on AKS

- 1. Service Discovery & Mesh:**
 - **Consul** provides seamless service discovery for ACME's hundreds of microservices.
 - **Consul** secures service-to-service communication, crucial for ACME's BI application.
- 2. Scalability:**
 - **Consul** clusters can easily scale to accommodate ACME's growing workload.
 - **Consul** will ensure the BI application performs optimally, supporting ACME's revenue generation.
- 3. Multi-Cloud Capability:**
 - **Terraform** with **Consul** eases deployment across AWS and Azure.
 - Addresses ACME's need for higher availability and disaster recovery post recent AWS outages.
- 4. Fast Time to Market:**
 - Quick setup and integration of **Consul** with AKS, meeting ACME's requirement for a fast-to-market solution.
- 5. Secure Communication:**
 - **Consul** provides automatic TLS encryption and identity-based authorization for secure microservices communication.
 - **Consul** addresses ACME's need for a secure connection between microservices with access control using Intentions.



HashiCorp Solution using Consul across roles

CIO:

- Consul ensures business continuity with multi-cloud resilience.
- Promotes vendor diversity with a multi-cloud approach.
- Enhances operational efficiency via a unified service mesh.
- Provides scalability and flexibility with a service mesh architecture.

Cloud Architect:

- Enables seamless cross-cloud networking with Consul mesh gateways.
- Manages dynamic service discovery and mesh configuration.
- Facilitates infrastructure as code for repeatable, controlled deployments.

DevOps Engineer:

- Consul automates CI/CD, enhancing update efficiency.
- Ensures encrypted microservices communication with sidecars.
- Supports integrated tools for comprehensive monitoring and observability.

SRE (Site Reliability Engineer):

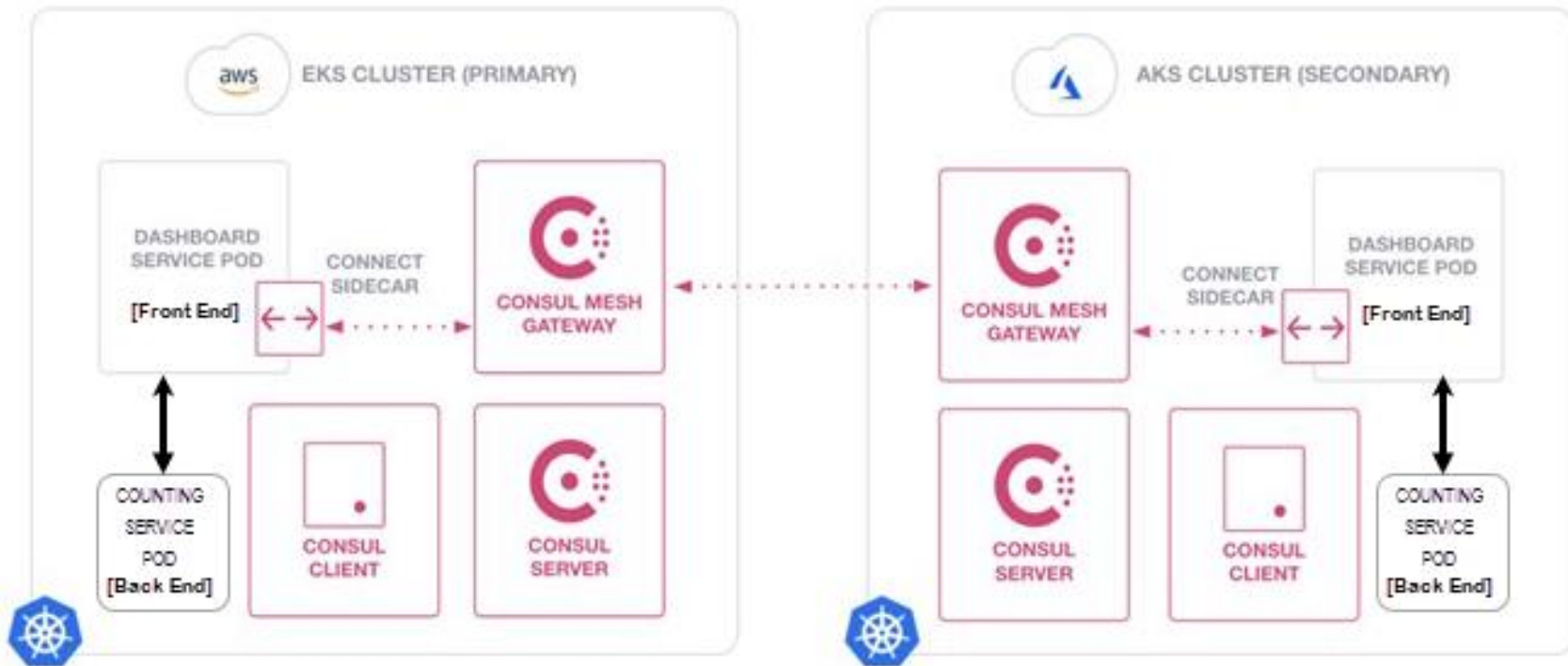
- Guarantees reliability and uptime with strategic traffic rerouting.
- Helps meet SLOs with consistent, cloud-spanning performance.
- Offers robust DR with multi-cloud cluster failovers.
- Enables dynamic scaling for efficient capacity planning.



HashiCorp Solution using Consul and other products

- 1. Multi-Cloud Capability with Terraform and Consul:**
 - Terraform enables infrastructure as code for easy deployment across AWS and Azure.
 - Consul's multi-cloud capability ensures higher availability and disaster recovery.
- 2. Service Discovery & Mesh with Consul:**
 - Seamless service discovery for ACME's microservices architecture.
 - Secure service-to-service communication with Consul's service mesh.
- 3. Scalability with Nomad and Consul:**
 - Nomad's simple and flexible workload orchestrator scales with ACME's growing workload.
 - Consul ensures optimal performance and scalability of service discovery as workload grows.
- 4. Fast Time to Market with Vagrant and Consul:**
 - Vagrant provides development environments to quickly test and deploy microservices.
 - Consul's quick setup and integration with AKS accelerates time to market.
- 5. Secure Communication with Vault and Consul:**
 - Vault secures microservices communication with secrets management.
 - Consul ensures automatic TLS encryption and identity-based authorization.

Bridging Multi-Cloud Environments with Consul – Demo layout



Consul demo – Resiliency and Access Control

Objective 1: Configure **Consul on AWS EKS and Azure AKS** to enable multi-cloud service discovery and connectivity.

Live Demonstration with Code review:

Terraform installation and configuration of Consul using Helm. Setup of federated Consul datacenters across AWS and Azure.

Objective 2: Showcase **seamless communication** between a two-tier application deployed across AWS and Azure.

Live Demonstration with Code review:

Deploy and demonstrate a two-tier application setup with Consul service registration and communication across federated Consul datacenters.

Objective 3: Showcase **application resilience** by maintaining service continuity during a backend failure (figure next page).

Live Demonstration with Code review:

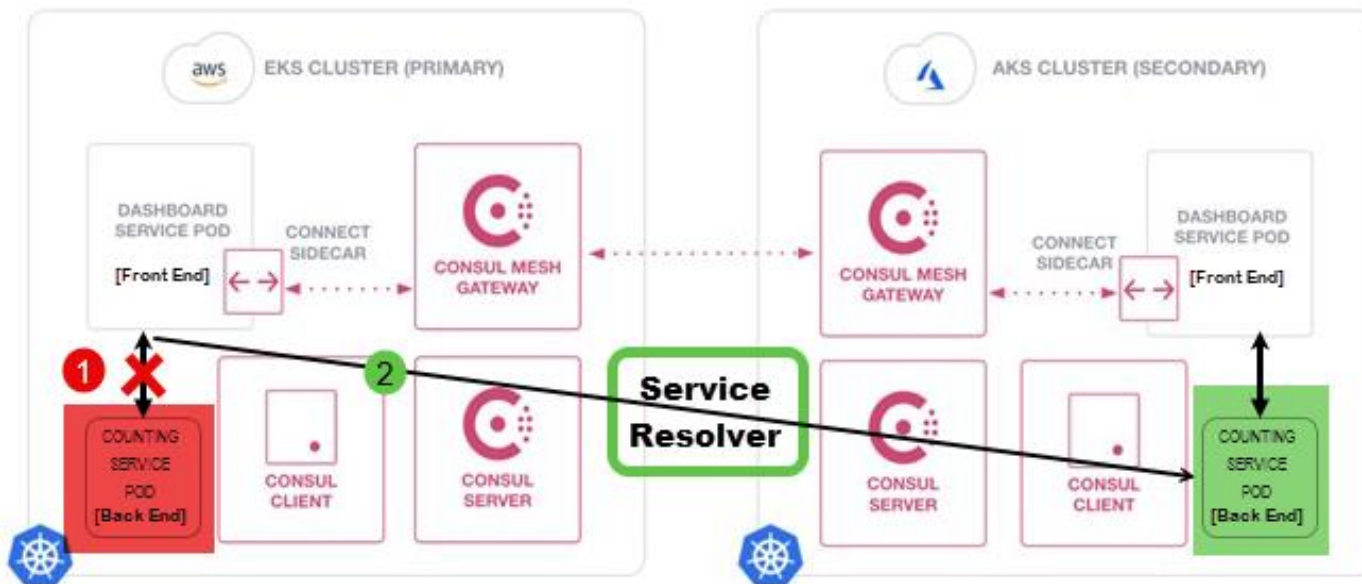
Using Consul's Service Resolver demonstrate real-time failover by simulating a backend outage in the primary datacenter and observing uninterrupted service on the dashboard app.

Objective 4: Showcase service-to-service communication, **allowing or denying requests** between a static client and server.

Live Demonstration with Code review:

Execute live changes to Consul Service Intentions, observing allowed and then denied communication between services, illustrating real-time traffic control.

Resiliency failover using Consul's Service Resolver



1. Scale down Counting service to 0 effectively removing EKS back-end
2. With Service Resolver deployed, EKS front-end dashboard now connects to the working AKS Counting service



Summary and Next Steps



Summary

Every action we take moves us in some direction.



Next Steps

Vision is a point much farther than a single action can take us.