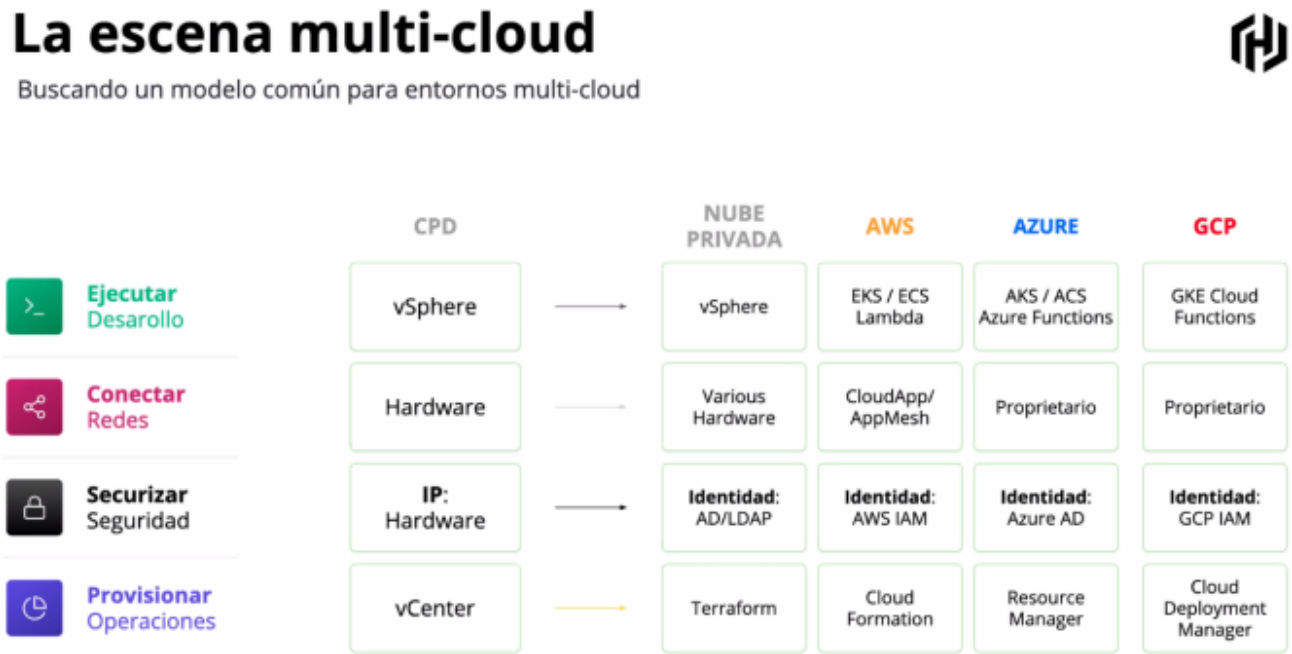
HashiCorp Taller de Vault

- ponente: Pedro Coca (gerente regional)

introducción modelo operativo cloud

- herramientas
  - vagrant
  - packer
  - terraform
  - vault
  - consul
  - nomad
- elementos infraestructura
  - conectividad
  - desarrollo
  - seguridad
  - operaciones
- transición a un mundo multi-cloud
  - sistemas de petición → auto gestión
  - llamadas API a servicios



- soluciones Hashicorp:
  - Nomad = desarrollo
  - consul = conectar
  - vault = securizar
  - terraform = infraestructura

terraform

- núcleo + proveedores (ofrecen API)

    - no solo nube pública
    - proveedores secundarios: +1000
- reutilización, control versiones, automatización
- marco de control (compliante) → terraform enterprise
    - mejores prácticas
    - políticas (as Code)

vault

- dispersión de secretos, falta de control
    - postit
    - archivo de texto
    - control de versiones
    - logs
- modelo:
    - autenticación
    - cliente
    - sistema
- centralizaión de secretos
    - más rotación, periodos más cortos
- encriptación como servicio
    - encriptar todo el tráfico de aplicación sin modificar la aplicación
- protección avanzada de datos

consul

- conectar aplicaciones
- migración de monolitos a microservicios
- middleware:
    - load-balancers
    - firewalls
- registro de apliaciones
    - ip-address → name
    - descubrimiento de servicios
- confianza cero
- service mesh
- consul intencions: definicíón control de acceso para servicios (multicloud)

nomad

- orquestrador cargas de trabajo
- contenedores o tradicionales

taller vault

info

- https://hashicorp.github.io/field-workshops-vault/slides/multi-cloud/vault-oss/#1
- https://play.instruqt.com/hashicorp/tracks/vault-basics

overview

- API
- agnóstico plataforma
- manejo de secretos centralizado
    - credenciales dinámicas de corto plazo ++
    - encriptación on-the-fly
- «castle and moat» : castillo+fosa → protección capas/perímetros
    - firewalls, reglas por IP
    - al final las credenciales se almacenaban en el código o en sitios estáticos
    - problemas modelo tradicional
        - restricciones por IP (con cada vez más IPs en danza)
        - revocación contraseña
        - rotaciones, cambios, acceso(log)
        - usuarios/aplicaciones
    - concepto de identidad
        - usarios: AD/LDAP
        - token
        - transciende los perímetros de seguridad
        - dinámico, credenciales de corto plazo, rotadas frecuentemente
        - credenciales y entidades pueden ser invalidados fácilmente
    - motores de secretos Vault
        - https://www.vaultproject.io/docs/secrets
        - https://www.vaultproject.io/docs/internals/architecture
    - alta disponibilidad
        - 3 nodos
            - en versión free, 1 activo, 2 en espera
            - no más de 8ms de diferencia entre nodos
        - vault enterprise replication
        - cluster disaster recovery