

Unlocking the Cloud Operating Model with Alibaba Cloud

Achieving the fastest
path to value in a modern,
multi-cloud datacenter



Table of Contents

Executive Summary	3
“Go China” and Regional Considerations	4
Transitioning to a Multi-Cloud Datacenter	5
Implications of the Cloud Operating Model	6
Unlocking the Cloud Operating Model on Alibaba Cloud	9
Multi-Cloud Infrastructure Provisioning with Terraform	11
Multi-Cloud Security with Vault	14
Multi-Cloud Service Networking with Consul	18
Multi-Cloud Application Delivery with Nomad	21
Industrialized Application Delivery Process	24
HashiCorp & Alibaba Cloud: Better Together	25
Appendix: Seven Steps to the Alibaba Cloud	26

Executive Summary

To thrive in an era of multi-cloud architectures, driven by digital transformation, enterprise IT must evolve from ITIL-based gatekeeping to enabling shared self-service processes for DevOps excellence.

For most enterprises, digital transformation means delivering new business and customer value more quickly, and at a very large scale. The implication for enterprise IT, then, is a shift from cost optimization to speed optimization. The cloud is a critical part of this shift, as it's required in order to rapidly deploy on-demand services at unlimited scale.

To unlock the fastest path to value in the cloud, enterprises must industrialize the application delivery process across each layer of the cloud: embracing the cloud operating model and tuning people, processes, and tools to take advantage of it.

This white paper lays out the advantages of implementing the cloud operating model with HashiCorp and Alibaba Cloud, and offers suggestions on how to successfully deploy it.

“Go China” and Regional Considerations

Notably, organizations seeking to navigate these industry changes in China and in Asia more broadly face some specific challenges, but Alibaba Cloud offers uniquely valuable expertise and perspective for these efforts.

Born and raised in China, Alibaba Cloud understands both the complexities and opportunities of the Chinese market. This helps ensure that Alibaba Cloud customers have access to outstanding “Go China” solutions. (For more on how Alibaba Cloud services can be tailored for the Chinese market, check out Alibaba’s [China Gateway](#).)

Further, as a native Asian Infrastructure-as-a-Service (IaaS) service provider, Alibaba Cloud is well positioned to accelerate enterprise success in Asia. (For more information on Alibaba Cloud’s place in the Asian IT ecosystem, check out its [Asia Accelerator](#) offerings.)

Transitioning to a Multi-Cloud Datacenter

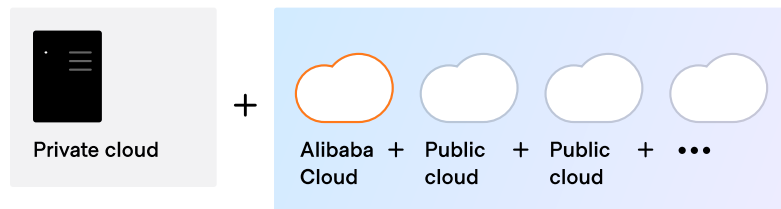
The transition to cloud and multi-cloud environments is a generational transition for IT. This transition means shifting from largely dedicated servers in a private datacenter to a pool of compute capacity available on demand. While most enterprises began with one cloud provider, there are good reasons to use services from others. Inevitably, most Global 2000 organizations will use more than one cloud provider. In fact, 90% of large enterprises are already multi-cloud according to the 2021 [HashiCorp State of Cloud Strategy Survey](#).

Traditional datacenter “Static”



Dedicated infrastructure

Modern datacenter “Dynamic”



SYSTEMS OF RECORD ← → SYSTEM OF ENGAGEMENT

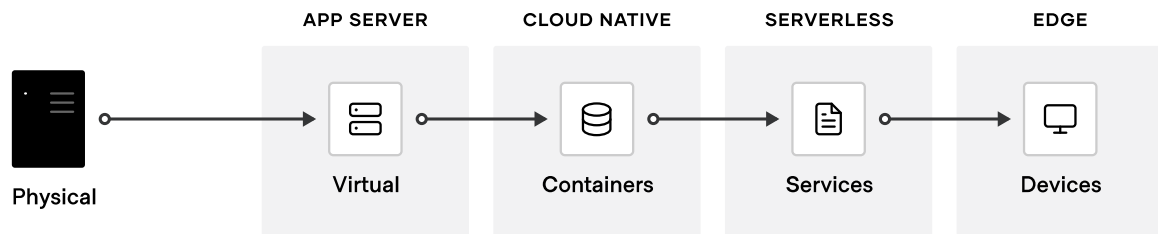
The cloud presents an opportunity for speed and scale optimization of new “systems of engagement” — the applications built to engage customers and users. These new apps are the primary interface for customers to engage with a business, and are ideally suited for delivery via the cloud, as they tend to:

- Have dynamic usage characteristics, needing to quickly scale loads up and down by orders of magnitude.
- Support fast development and iteration. Many of these new systems are central to how the organization engages its customers, so development teams need to quickly release enhancements in response to competitors and user feedback.

For most enterprises though, these systems of engagement must connect to existing “systems of record” — the organization’s core business databases and internal applications, which often continue to reside on infrastructure in existing datacenters. As a result, enterprises end up with a hybrid model — a mix of multiple public and private cloud and on-premises environments.

The challenge for most enterprises, then, is how to use the cloud to consistently deliver these applications while ensuring the least possible friction across the various development teams.

Compounding this challenge, the underlying primitives have changed from manipulating virtual machines in a self-contained environment to working with a variety of cloud resources in a shared environment. Enterprises must deal with competing operational models as they work to maintain their existing estate while also developing the new cloud infrastructure.







For cloud computing to deliver on its promises, enterprises need consistent workflows that can be reused at scale across multiple cloud providers. This requires:

- Consistent instruction sets for provisioning
- Identity for security and network connections
- Privileges and rights that support enterprise role-based access controls (RBACs)

Implications of the Cloud Operating Model





The essential implication of the transition to the cloud is the shift from “static” infrastructure to “dynamic” infrastructure: from a focus on configuration and management of a static fleet of IT resources to provisioning, securing, connecting, and running dynamic resources on demand.

	Static	Dynamic
 Run	Dedicated infrastructure	→ Scheduled across the fleet
 Connect	Host-based, static IP	→ Service-based, dynamic IP
 Secure	High trust, IP-based	→ Low trust, identity-based
 Provision	Dedicated servers, homogeneous	→ Capacity on-demand, heterogeneous

This implies a number of changes in approach at each layer of the stack:

- **Provision.** The infrastructure layer transitions from running dedicated servers at limited scale to a dynamic environment where organizations can easily adjust to increased demand by spinning up thousands of servers and scaling them down when not in use. As architectures and services become more distributed, the sheer volume of compute nodes increases significantly.
- **Secure.** The security layer transitions from a fundamentally “high trust” world enforced by a strong perimeter and firewall to a “low trust” or “zero trust” environment with no clear or static perimeter. As a result, the foundational assumption for security shifts from being IP-based to identity-based access to resources. This shift is highly disruptive to traditional security models.
- **Connect.** The networking layer transitions from being heavily dependent on the physical location and IP address of services and applications to using a [dynamic registry of services for discovery](#), segmentation, and composition. An enterprise IT team does not have the same control over the network, or the physical locations of compute resources, and must think about service-based connectivity.
- **Run.** The runtime layer shifts from deploying artifacts to a static application server to deploying applications with a scheduler atop a pool of infrastructure provisioned on demand. In addition, new applications become collections of dynamically provisioned services and packaged in multiple ways: from virtual machines to containers.

Additionally, each cloud provider has its own solution to these challenges. For enterprise IT teams, these shifts in approach are compounded by the realities of running on hybrid- and multi-cloud infrastructures and the varying tools each technology provides.

	Static		Dynamic	
	DEDICATED	→	PRIVATE CLOUD	ALIBABA CLOUD
 Run Deployment	vSphere	→	vSphere	ACK/function compute
 Connect Networking	Hardware	→	Various hardware	Service mesh (ASM)
 Secure Security	IP: hardware	→	Identity: AD/LDAP	Identity: IDaaS
 Provision Operations	vCenter	→	Terraform	Resource orchestration service


To address these challenges, teams must ask some key questions around three core questions:

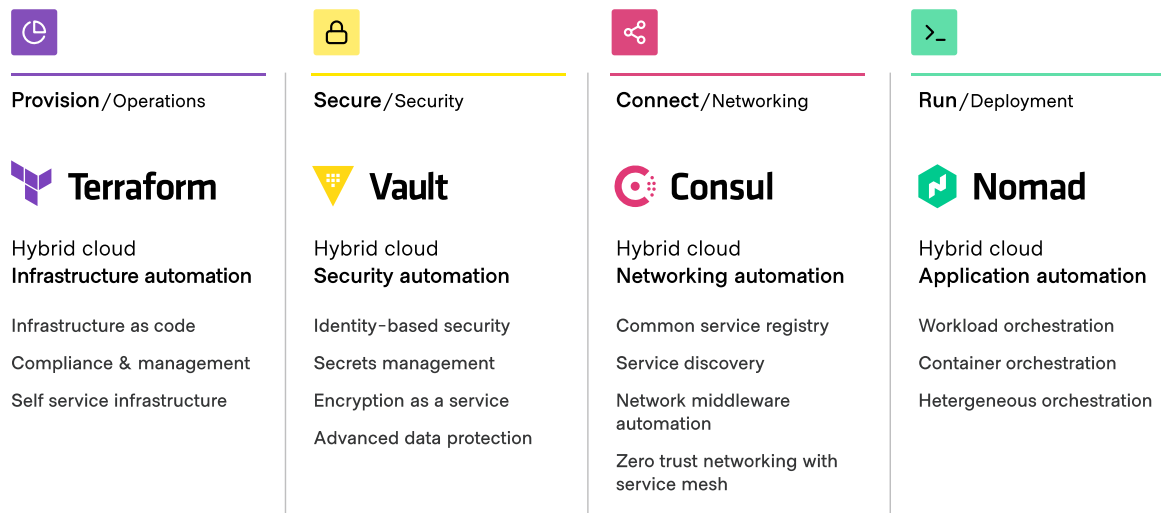
- **People.** How can we enable teams to thrive in a multi-cloud reality, where skills must be applied consistently regardless of the target environment?
- **Process.** How do we position central IT services as a self-service enabler of speed instead of a ticket-based gatekeeper of control, while retaining compliance and governance?
- **Tools.** How do we best unlock the value of the available capabilities of the cloud providers to boost customer and business value?

Unlocking the Cloud Operating Model on Alibaba Cloud

The implications of the cloud operating model impact enterprise teams across infrastructure, security, networking, and applications. In response, enterprises are establishing central shared services — centers of excellence — to deliver the dynamic infrastructure necessary at each layer for successful application delivery.

As teams deliver on these shared services for the cloud operating model, IT velocity increases. The greater cloud maturity an organization has, the faster its velocity.

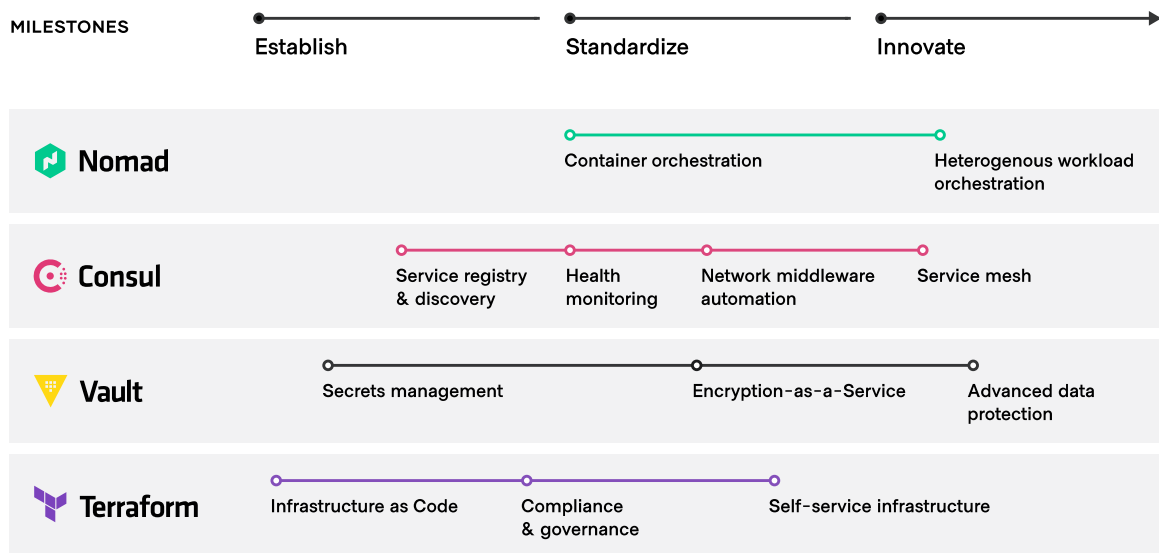
Expanding use of the HashiCorp Stack increases maturity and velocity for our customers 



The typical journey to unlock the cloud operating model comprises three major milestones:

- 1. Establish the cloud essentials.** At the beginning of the cloud journey, the immediate requirements are provisioning the cloud infrastructure — typically by adopting infrastructure as code and ensuring it is secure by implementing a secrets-management solution. These are the bare necessities to build a scalable, dynamic, and futureproof cloud architecture.
- 2. Standardize on a set of shared services.** As cloud consumption grows, enterprises need to implement and standardize on a set of shared services to take full advantage of the cloud’s advantages. This can introduce challenges around governance and compliance as setting access control rules and tracking requirements becomes increasingly important.
- 3. Innovate using a common logical architecture.** Fully embracing the cloud and depending on cloud services and applications as the primary systems of engagement, creates a need for a common logical architecture. This requires a control plane that connects with the extended ecosystem of cloud solutions and provides advanced security and orchestration across services and multiple clouds.

Example enterprise journey to unlock a cloud operating model

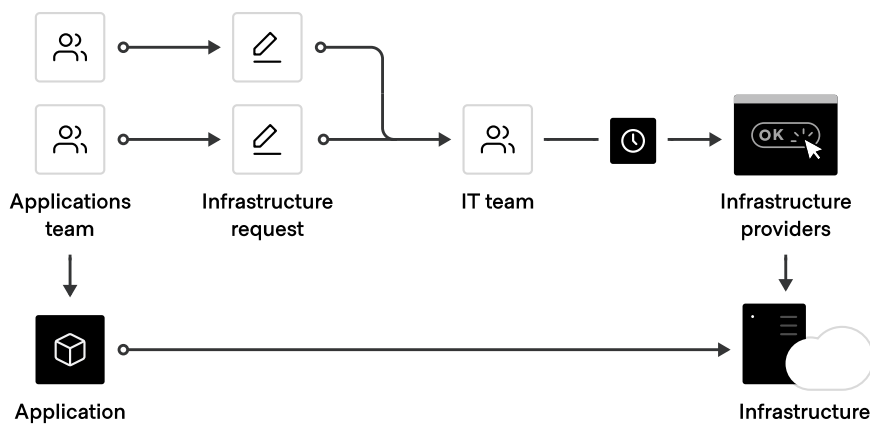


Multi-Cloud Infrastructure Provisioning with Terraform

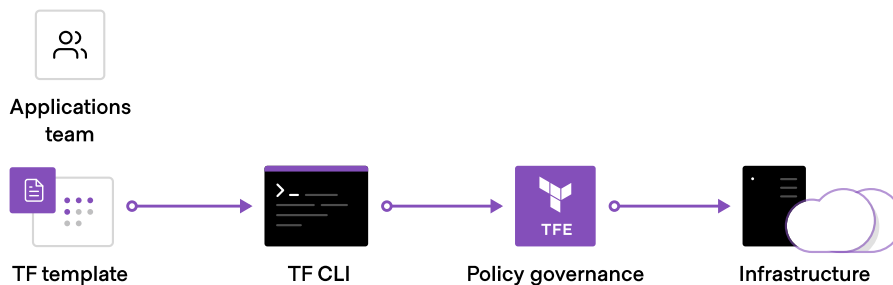
The foundation for adopting the cloud is infrastructure provisioning. [HashiCorp Terraform](#) is the world's most widely used cloud provisioning product. It can be used to provision infrastructure for any application using an ever-growing array of providers for popular platforms and technologies.

To create shared services for infrastructure provisioning, IT teams should start by implementing reproducible infrastructure as code practices, and then layering on compliance and governance workflows to ensure appropriate controls.

Before Terraform



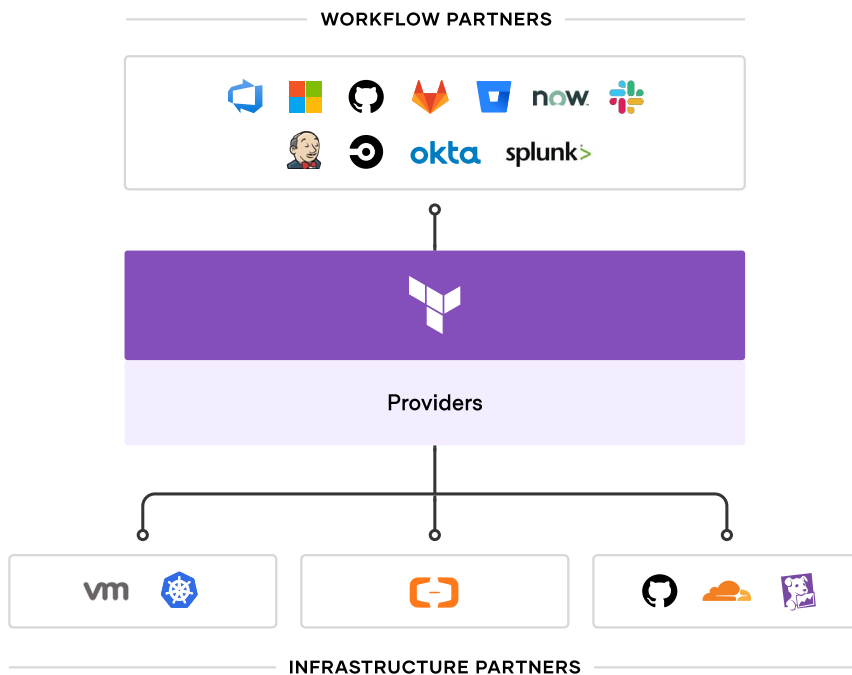
After Terraform



Reproducible Infrastructure as Code

The first goal of a shared service for infrastructure provisioning is to enable the delivery of reproducible infrastructure as code, providing DevOps teams a way to plan and provision resources inside CI/CD workflows using familiar tools.

DevOps teams can create Terraform templates that express the configuration of services from one or more cloud platforms. Terraform integrates with all major configuration-management tools to allow fine-grained provisioning following the provisioning of the underlying resources. Finally, templates can be extended with services from many other software providers, monitoring agents, application performance monitoring (APM) systems, security tooling, DNSs, content delivery networks, and more. Once defined, the templates can be provisioned as required in an automated way. That makes Terraform the lingua franca and common workflow for teams provisioning resources across public and private clouds.



For self-service IT, the decoupling of the template-creation process and the provisioning process greatly reduces the time taken for any application to go live, since developers using pre-approved templates no longer need to wait for operations approval.

Compliance and Management

Most teams also need to enforce policies covering the type of infrastructure created, how it is used, and which teams get to use it. [HashiCorp's Sentinel](#) policy as code framework provides compliance and governance without requiring a shift in the overall team workflow. Sentinel is also defined as code, enabling collaboration and comprehension for DevSecOps.

Without policy as code, organizations typically resort to ticket-based review processes to approve changes. This can make developers wait weeks or longer to provision infrastructure. Policy as code solves this by splitting the definition of the policy from the execution of the policy.

Centralized teams codify policies enforcing security, compliance, and operational best practices across all cloud provisioning. Automated enforcement of policies ensures changes are in compliance without creating a manual review bottleneck.

HashiCorp and Alibaba Cloud

Since 2017, HashiCorp and Alibaba Cloud have partnered closely in the development of Terraform. Together, we are focused on empowering organizations with the scalability and flexibility of infrastructure as code (IaC).

HashiCorp Terraform codifies infrastructure in configuration files that describe the topology of cloud resources. These resources include virtual machines, storage accounts, and networking interfaces. The Terraform CLI provides a simple mechanism to deploy and version the configuration files to Alibaba Cloud. This is truly a hybrid and multi-cloud implementation that connects a customer's private cloud infrastructure as well as their public-cloud deployment with Alibaba.

Alibaba Cloud has a dedicated team responsible for maintaining the code in the [Alibaba Cloud Provider](#). The Alibaba Cloud product R&D team publishes weekly updates to the provider to help customers be more productive with Terraform on Alibaba Cloud. What's more, Alibaba Cloud has published the [Terraform Module Web GUI](#) to help developers to use the Terraform Module more simply and conveniently.

Multi-Cloud Security with Vault

Dynamic cloud infrastructure means a shift from host-based identity to application-based identity, with low- or zero trust networks spanning multiple clouds without a clear network perimeter.

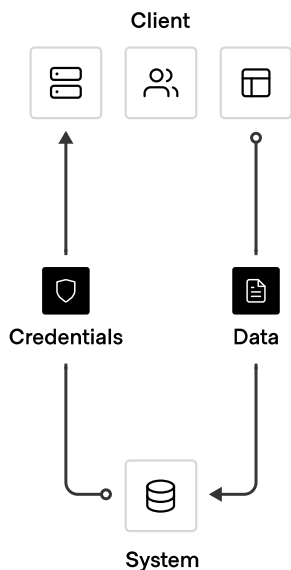
The traditional security world assumed high trust internal networks, which resulted in a hard shell and soft interior. The modern zero trust approach works to harden the inside as well. This requires that applications be explicitly authenticated, authorized to fetch secrets and perform sensitive operations, and tightly audited.

[HashiCorp Vault](#) enables teams to securely store and tightly control access to tokens, passwords, certificates, and encryption keys for protecting machines and applications. This provides a comprehensive secrets management solution. Beyond that, Vault helps protect data at rest and data in transit. Vault exposes a high-level cryptography API for developers to secure sensitive data without exposing encryption keys. Vault also can act like a certificate authority, to provide dynamic short lived certificates to secure communications with SSL/TLS. Lastly, Vault enables the brokering of identity between different platforms, such as Active Directory in on-premises deployments and [Alibaba Cloud RAM](#) and [Cloud SSO](#) to allow applications to work across platform boundaries.

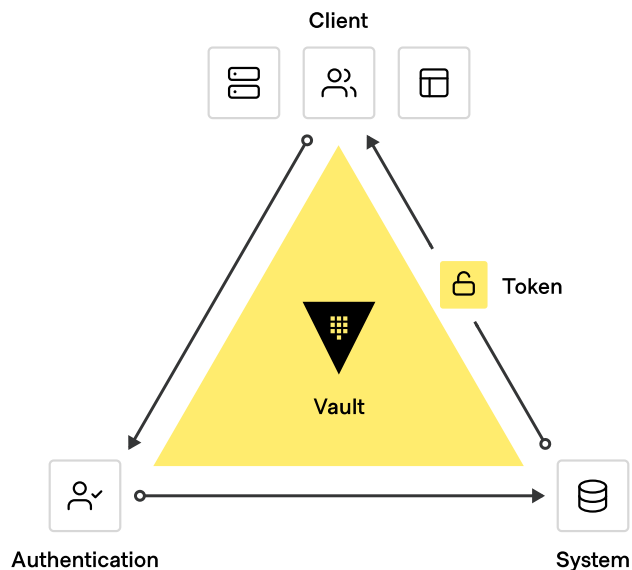
Vault is widely used across many industries — including stock exchanges, large financial organizations, and hotel chains — to provide security in the cloud operating model.

To achieve shared services for security, IT teams should enable centralized secrets management services, and then use those services to deliver more sophisticated Encryption-as-a-Service use cases such as certificate and key rotations and encryption of data in transit and at rest.

Before Vault



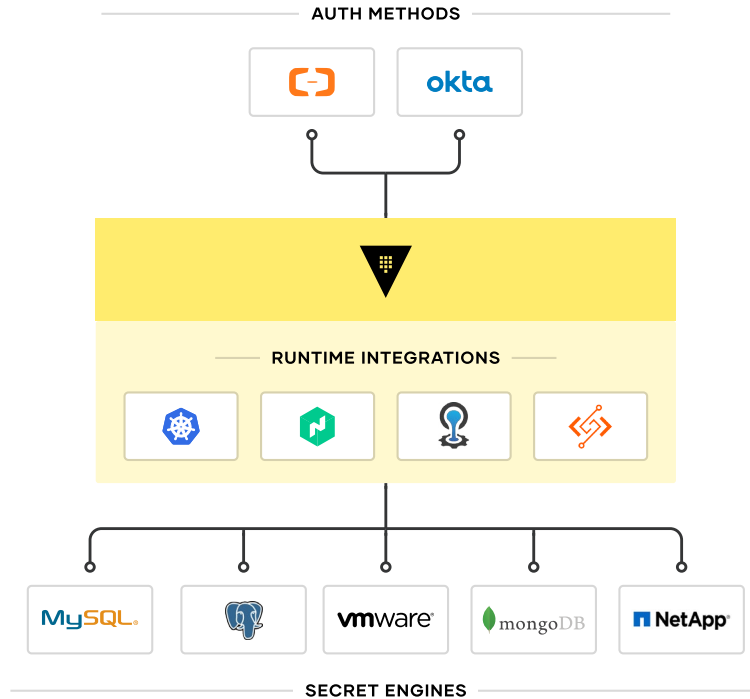
After Vault



Secrets Management

The first step in cloud security is typically secrets management: the central storage, access control, and distribution of dynamic secrets. Instead of depending on static IP addresses, integrating with identity-based access systems such as [Alibaba Cloud IDaaS](#) to authenticate and access services and resources is crucial.

Vault uses policies to codify how applications authenticate, which credentials they are authorized to use, and how auditing should be performed. It can integrate with an array of trusted identity providers such as cloud identity and access management (IAM) platforms, Kubernetes, Active Directory, and other Security Assertion Markup Language (SAML) based systems for authentication. Vault then centrally manages and enforces access to secrets and systems based on trusted sources of application and user identity.



Enterprise IT teams should build shared services that enable the request of secrets for any system through a consistent, audited, and secured workflow.

Encryption-as-a-Service

Additionally, enterprises need to encrypt application data at rest and in transit. Vault can provide Encryption-as-a-Service to provide a consistent API for key management and cryptography. This allows developers to perform a single integration and then protect data across multiple environments.

Using Vault as a basis for Encryption-as-a-Service solves difficult problems faced by security teams, such as certificate and key rotation. Vault enables centralized key management to simplify encrypting data in transit and at rest across clouds and data centers. This helps reduce costs around expensive hardware security modules (HSM) and increases productivity with consistent security workflows and cryptographic standards across the organization.

While many organizations mandate developers to encrypt data, they often don't often explain the "how," which forces developers to build custom solutions without an adequate understanding of cryptography. Vault offers developers a simple, easy to use API, while giving central security teams the policy controls and lifecycle management APIs they need.

Advanced Data Protection

Organizations moving to the cloud or spanning hybrid environments must typically still maintain and support on-premises services and applications that need to perform cryptographic operations, such as data encryption for storage at rest. Development teams do not necessarily want to implement the logic around managing these cryptographic keys, and thus seek to delegate the task of key management to external providers. Advanced data protection allows organizations to securely connect, control, and integrate advanced encryption keys, operations, and management between infrastructure and Vault Enterprise, including automatically protecting data in MySQL, MongoDB, PostgreSQL, and other databases using transparent data encryption (TDE).

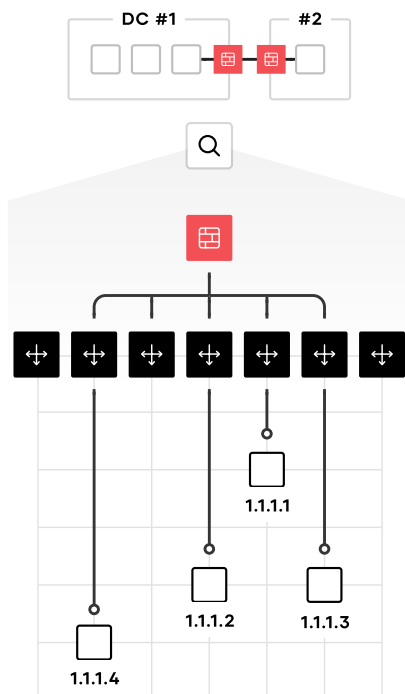
Organizations with high security requirements for data compliance (PCI DSS, HIPAA, etc.) often adopt more sophisticated technologies that can cryptographically protect anonymity for personally identifiable information (PII). Advanced data protection provides functionality for data tokenization, such as data masking, to protect sensitive data such as credit cards, sensitive personal information, bank numbers, and so on.

Multi-Cloud Service Networking with Consul

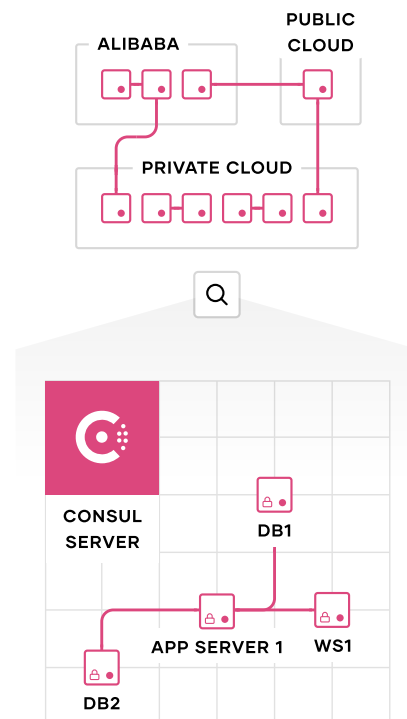
Networking in the cloud is often one of the most difficult aspects of adopting the cloud operating model. The combination of dynamic IP addresses, a significant growth in east-west traffic in microservices architectures, and the lack of a clear network perimeter is a formidable challenge. [HashiCorp Consul](#) provides a multi-cloud service networking layer to connect and secure services. Consul is widely deployed at scale, with many customers running significantly more than 100,000 nodes in their environments.

Networking services should be provided centrally, where a single IT team provides service registry and service discovery capabilities to development teams. A common registry provides a “map” of what services are running, where they are, and their current health status. The registry can be queried programmatically to enable service discovery or drive network automation of API gateways, load balancers, firewalls, and other critical middleware components. These middleware components can be moved out of the network using a service mesh approach, where proxies run on the edge to provide equivalent functionality. Service mesh approaches can simplify the network topology, especially for multi-cloud and multi-datacenter topologies.

Before Consul



After Consul



Service Discovery

The starting point for networking in the cloud operating model is typically a common service registry, which provides a real-time directory of what services are running, where they are, and their current health status. Traditional approaches to networking rely on load balancers and virtual IPs to provide naming abstractions to represent a service with a static IP. Tracking the network location of services is often done with spreadsheets, load-balancer dashboards, or configuration files, all of which are disjointed manual processes prone to error.

Consul programmatically registers each service and provides DNS and API interfaces to enable any service to be discovered by other services. The integrated health check monitors each service instance's health status so the IT team can triage the availability of each instance. What's more, Consul can help prevent routing traffic to unhealthy service instances.

Consul can integrate with other services that manage existing north-south traffic, such as traditional load balancers, and distributed application platforms such as Kubernetes, to provide a consistent registry and discovery service across multi-datacenter, multi-cloud, and multi-platform environments.

Network Middleware Automation

The next step is to reduce operational complexity with existing networking middleware through network automation. Instead of a manual, ticket-based process to reconfigure load balancers and firewalls every time there is a change in service network locations or configurations, Consul can automate these network operations. This is achieved by enabling network middleware devices to subscribe to service changes from the service registry, enabling highly dynamic infrastructure that can scale significantly higher than static-based approaches.

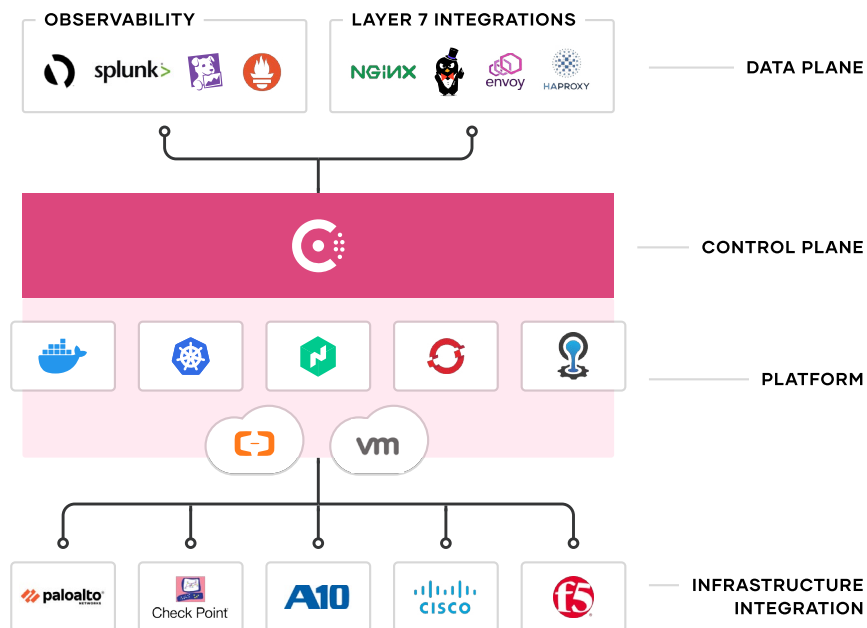
This decouples the workflow between teams, as operators can independently deploy applications and publish to Consul, while NetOps teams can subscribe to Consul to handle the downstream automation.

Zero Trust Networking with Service Mesh

As organizations scale with microservices-based and cloud-native applications, the underlying infrastructure becomes larger and more dynamic, leading to an explosion of east-west traffic. This can bring a proliferation of expensive network middleware that carry single points of failure and significant operational overhead.

Consul provides a distributed service mesh that pushes routing, authorization, and other networking functionalities to the endpoints in the network, rather than imposing them through middleware. This makes the network topology simpler and easier to manage, removes the need for expensive middleware within east-west traffic paths, and makes service-to-service communication much more reliable and scalable.

Consul is an API-driven control plane that integrates with sidecar proxies alongside each service instance (proxies such as Envoy, HAProxy, and NGINX). These proxies provide the distributed data plane. Together, these two planes enable a zero trust network model that secures service-to-service communication with automatic TLS encryption and identity-based authorization. Network operation and security teams can define the security policies with logical services rather than IP addresses.



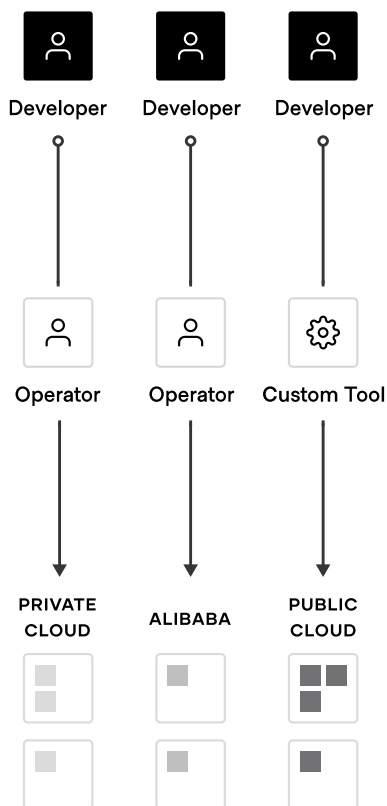
Consul enables fine-grained service segmentation to secure service-to-service communication with automatic TLS encryption and identity-based authorization. Consul can be integrated with Vault for centralized PKI and certificate management. Service configuration is achieved through an API-driven key-value store that can be used to easily configure services at runtime in any environment.

Multi-Cloud Application Delivery with Nomad

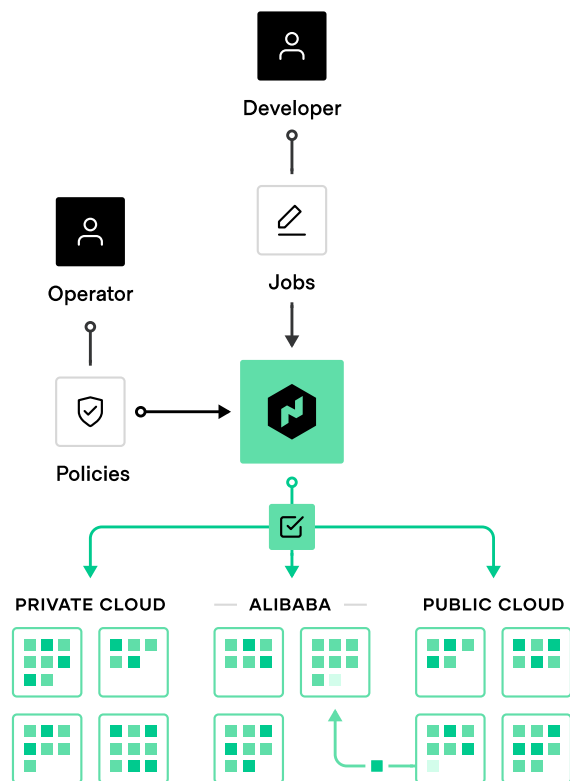
Finally, at the application layer, new apps are increasingly distributed while legacy apps still need to be managed more flexibly. [HashiCorp Nomad](#) is a flexible orchestrator. The product can deploy and manage both legacy and modern applications for all types of workloads: from long-running services to short-lived batch jobs to system agents.

To get the benefits of shared services for application delivery, IT teams should use Nomad in concert with Terraform, Vault, and Consul. This combination enables the consistent delivery of applications on cloud infrastructure, while meeting necessary compliance, security, and networking requirements.

Before Nomad



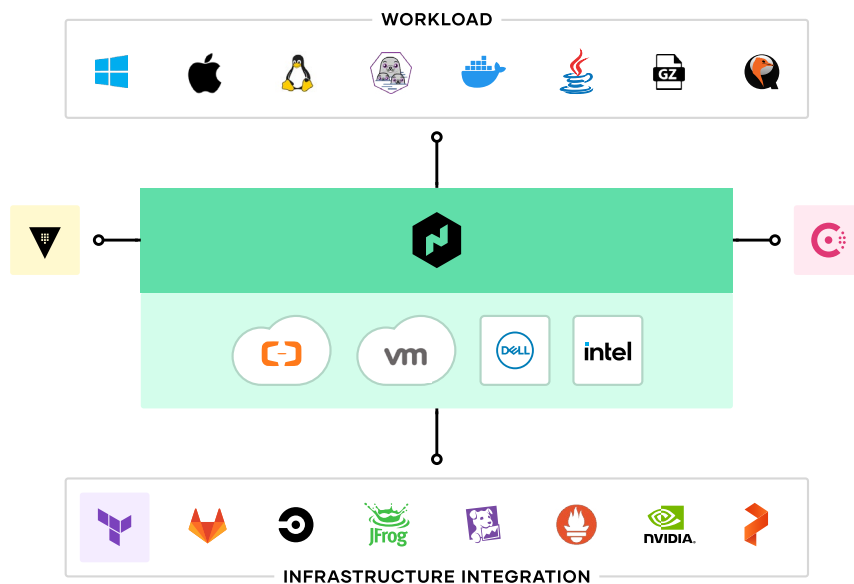
After Nomad



Mixed Workload Orchestration

Today, many new workloads are developed with container packaging to be deployed to Kubernetes or other container management platforms. But many legacy workloads will not be moved onto those platforms, nor will future serverless applications. Nomad provides a consistent process for deployment of all workloads from virtual machines through standalone binaries and containers. It provides core orchestration benefits across all those workloads such as release automation, multiple upgrade strategies, bin packing, and resilience.

For modern applications — typically built in containers — Nomad provides the same consistent workflow at scale in any environment. Nomad is focused on simplicity and effectiveness at orchestration and scheduling, and avoids the complexity of platforms such as Kubernetes that require specialist skills to operate and solve only for container workloads.



Nomad integrates into existing CI/CD workflows to provide fast, automatic application deployments for legacy and modern workloads.

High Performance Compute

Nomad is designed to schedule applications with low latency across very large clusters. This is critical for customers with large batch jobs, as is common with high performance computing (HPC) workloads. In the [2 Million Container Challenge](#), Nomad was able to schedule one million instances of Redis across 5,000 machines in three datacenters, in less than 5 minutes. Several large Nomad deployments run at even larger scales.

Nomad makes it easy for high-performance applications to use an API to consume capacity dynamically, enabling efficient sharing of resources for data analytics applications like Spark. The low latency scheduling ensures results are available quickly and minimizes wasted idle resources.

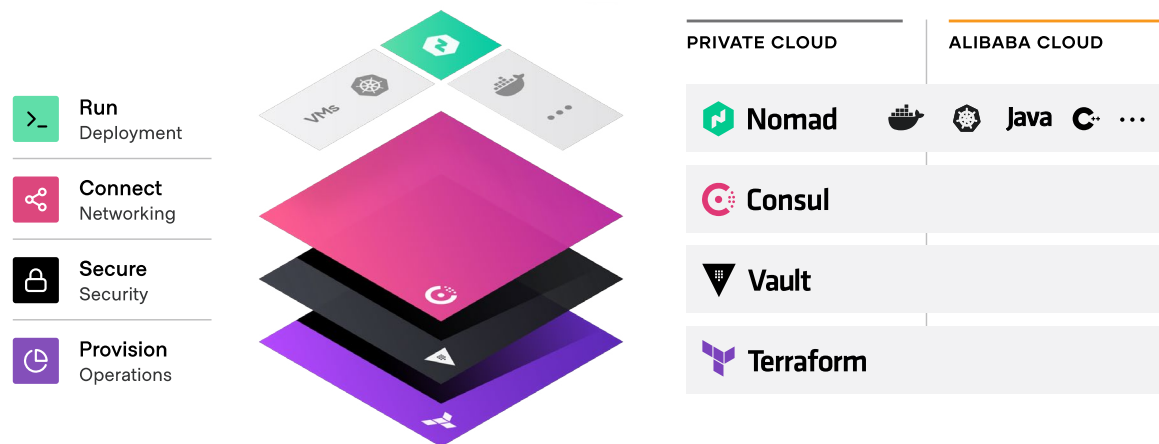
Multi-Datacenter Workload Orchestration

Nomad is multi-region and hybrid-cloud by design, with a consistent workflow to deploying any workload. As teams roll out global applications in multiple data centers, or across cloud boundaries, Nomad provides orchestration and scheduling for those applications. The product is supported by the infrastructure, security, and networking resources and policies to ensure the application is successfully deployed.

Industrialized Application Delivery Process

Ultimately, these shared services across infrastructure, security, networking, and application runtime present an industrialized process for application delivery, while taking advantage of the dynamic nature of each layer of the cloud.

Embracing the cloud operating model enables self-service IT that is fully compliant and governed for teams to deliver applications at increasing speed.



Alibaba Cloud Well-Architected Framework Pillars

The cloud operating model is complemented by [Alibaba Cloud's Well-Architected Framework](#). The three pillars of this framework offer guidance from Alibaba Cloud experts on infrastructure with high reliability, security, and performance.

- **Reliability.** The reliability pillar focuses on Alibaba Cloud's ability to ensure business continuity. This pillar addresses the reliability design for core Alibaba Cloud products and solutions from service scalability, costs, and security perspectives.
- **Security.** The security pillar focuses on information security. This area addresses shared security responsibilities, security compliance and privacy, Alibaba Cloud infrastructure, and security architecture.
- **Performance.** The performance-efficiency pillar focuses on the efficient use of computing resources to meet various requirements, even as they evolve and change over time.

HashiCorp & Alibaba Cloud: Better Together

HashiCorp and Alibaba Cloud have a long-term history of product and technology collaboration. Both companies actively participate in the open source community, and have a track record of high-frequency releases. This fast pace of innovation enables practitioners and the community to be more productive with Alibaba Cloud and other important enterprise technologies.

About Alibaba Cloud

Alibaba Cloud, founded in 2009, is a global leader in cloud computing and artificial intelligence, providing services to thousands of enterprises, developers, and government organizations in more than 200 countries and regions. Committed to the success of its customers, Alibaba Cloud provides reliable and secure cloud computing and data processing capabilities as a part of its online solutions. In January 2017, Alibaba Cloud became the official cloud services partner of the Olympics.

About HashiCorp

HashiCorp is a leader in multi-cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows and a standardized approach to automating the critical process involved in delivering applications in the cloud: infrastructure provisioning, security, networking, and application deployment. HashiCorp's open source tools Vagrant™, Packer™, Terraform®, Vault™, Consul®, Nomad™, Boundary, and Waypoint™ were downloaded approximately 100 million times during the fiscal year ended January 31, 2021. Enterprise and managed service versions of these products enhance the open source tools with features that promote collaboration, operations, governance, and multi-datacenter functionality. The company is headquartered in San Francisco, though 90% of HashiCorp employees work remotely, strategically distributed around the globe.

Appendix: Seven Steps to the Alibaba Cloud

The transition to cloud and hybrid-cloud environments is a generational transition for IT. For many enterprises, this transition means shifting from a static to dynamic environment and focusing on developing a cloud migration plan.

Alibaba Cloud recommends seven critical steps to drive the right outcomes for your organization:



1. Assess migration. Assess the business value, migration workload, and migration method and cost.

- **Evaluate cloud capacity:** Analyze your current business situation to forecast cloud infrastructure demands and migration workloads to help determine the right migration time and method.
- **Evaluate migration needs:** Evaluate the downtime tolerance, current or potential fault risks, and the compatibility of the current system with the target cloud platform.
- **Estimate cloud infrastructure cost.** Calculate the TCO of infrastructure cost on Alibaba Cloud with the [Alibaba Cloud TCO calculator](#).

2. Customize architecture. Customize your cloud infrastructure to maximize compatibility and stability after migration.

- **Design architecture and structure:** Customize cloud infrastructure and architecture to meet high availability, scalability, and performance requirements.

3. Migrate to Alibaba Cloud. Migrate application servers, containers, databases, and data to Alibaba Cloud with tailored products and services.

- **Migrate application servers:** Migrate source servers including servers in datacenters, VMs, and servers on other cloud platforms to Alibaba Cloud.
- **Migrate containers:** You can choose to migrate applications with your self-built CI/CD platform or [Alibaba Cloud Velero](#). You can also use [Alibaba Cloud's Image Syncer](#) synchronization tool to migrate Docker image files.
- **Migrate databases:** Migrate to fully managed cloud databases with scalability, reliability, end-to-end security, and cost efficiency.

4. **Set up disaster recovery.** Configure backup and disaster-recovery policies on Alibaba Cloud to improve stability.
 - **Set up ECS-level backup:** Use [Alibaba Cloud Snapshot](#) to create snapshots for all disk categories, or use backup recovery services to configure cross-zone disaster recovery.
 - **Set up database-level backup:** Configure real-time data backups to meet common disaster recovery objectives.
5. **Optimize migrated applications.** Continuously optimize deployed applications after migration to manage costs and improve efficiency.
 - **Optimize cloud usage:** Streamline your cloud usage and optimize your deployed applications to improve scalability and cost control.
6. **Enhance cloud security.** Implement a workable IT governance framework to control and track costs, analyze failure, and guarantee cloud security.
 - **Secure identities:** Create roles and accounts with limited permissions with resource access management (RAM), and track user operations in the console.
 - **Secure infrastructures:** Establish robust, end-to-end protection to address application and platform security in the cloud for new and migrated applications, and easily audit and govern your ongoing security posture.
 - **Secure data:** Build a robust cloud security framework to safeguard your data assets throughout the data-security lifecycle.
7. **Manage resources in the cloud.** Track the health of your cloud systems and set access controls for employees and vendors.
 - **Monitor cloud resources:** Monitor usage of cloud resources and the status and health of your business to ensure the availability of your application.
 - **Manage vendors.** Manage permissions for users in a centralized manner, monitor all operations, and reproduce operational scenarios in real time to facilitate identity authentication, access control, and audits.

