Securely Connect AWS Services with HashiCorp Consul Service Mesh

Connect application services to improve security and observability using HashiCorp Consul

In collaboration with

HashiCorp

Table of contents

Welcome to the world of dynamic infrastructure

Modern infrastructure is transitioning from being primarily static to dynamic. Static infrastructure is defined by monolithic applications running in private datacenters with static IPs protected by perimeter security and coarse-grained network segments.

However, static infrastructure may not be able to keep up with modern demands. If you are running microservices or using a runtime with containers, for example, you may need to quickly scale resources up and down. It may take time for you to update the load balancers in a traditional static infrastructure architecture, resulting in unexpected traffic routes

In dynamic infrastructure, services change multiple times per day and are deployed across many machines in both public and private datacenters. Services may run in different networks, runtimes, or compute solutions, such as Amazon Elastic Cloud Compute (Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), AWS Fargate, Amazon Elastic Container Service (Amazon ECS), or AWS Lambda. These services are often ephemeral with dynamic IPs. In addition to routing traffic into and out of the datacenter (north-south), dynamic infrastructure also routes traffic to nodes within the datacenter (east-west), often into different networks.

A service mesh addresses these concerns for both static and dynamic infrastructure in two ways:

- Service discovery, which enables services to automatically find each other.
- Secure connections that enable communication only between specific services according to your security policies.

Read this ebook to learn more about service mesh and how Consul service mesh can help your business run smoother on the AWS Cloud.

What exactly is a service mesh?

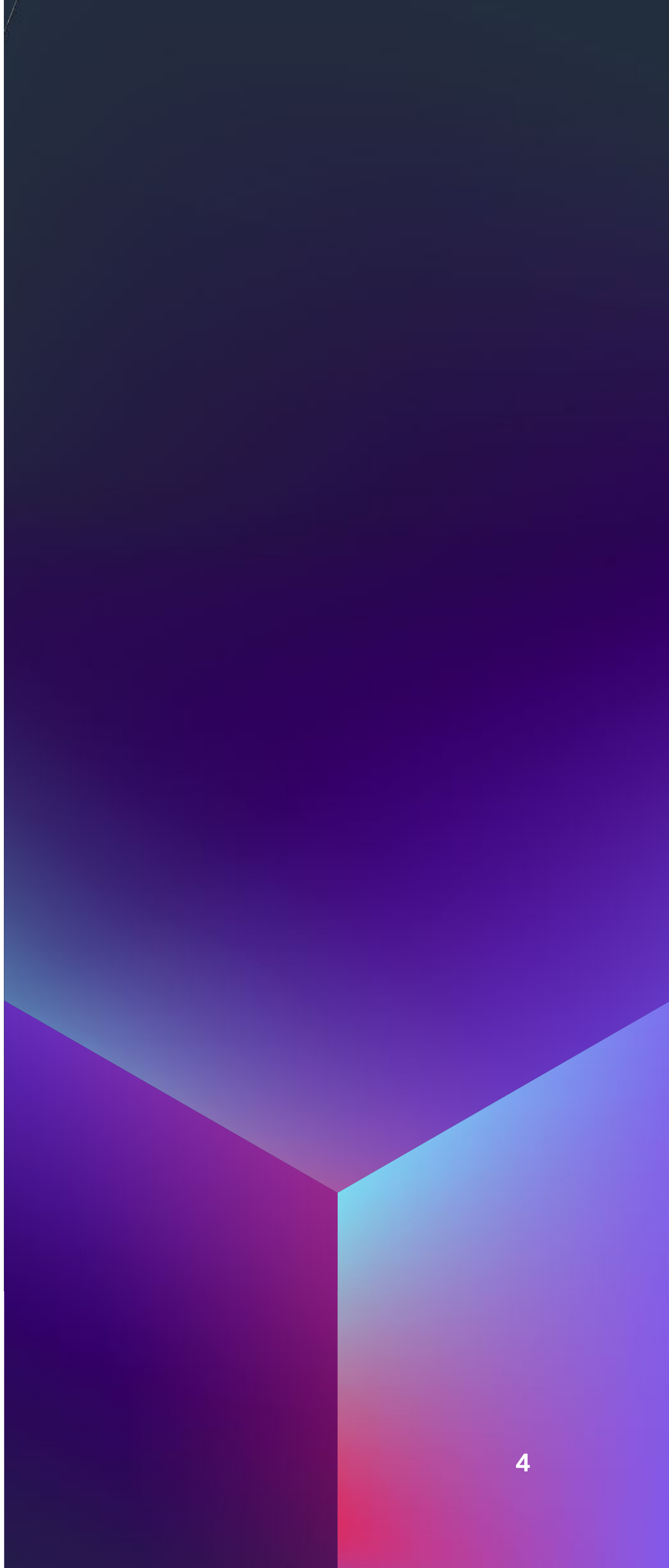
A service mesh is a dedicated network layer that provides secure service-to-service communication within and across infrastructure, including on-premises and cloud environments. Service meshes are often used with a microservice architectural pattern, but can provide value in any complex networking scenario. A service mesh provides many benefits, from security to improved application resiliency.

A service mesh typically consists of a control plane and a data plane. The control plane maintains a central registry that keeps track of all services and their respective IP addresses. As long as the application is registered with the control plane, other members in the service mesh can retrieve information about how to communicate with the application from the control plane. The control plane can also enforce rules about which services can communicate with each other.

The data plane handles communication between services. Many service mesh solutions employ a sidecar proxy to handle data plane communications, and thus limit the level of awareness the services need to have about the network environment.

A service mesh controls how different parts of an application share data with one another. Unlike other systems for managing this type of communication, a service mesh is a platform layer on top of the infrastructure layer that enables managed, observable, and secure communication between individual services. This platform layer enables companies to manage robust enterprise applications made up of many microservices on a chosen infrastructure. When services are registered into the mesh, it provides visibility into how well or poorly different parts of an application interact, making it easier to optimize communication and avoid downtime as an application grows.

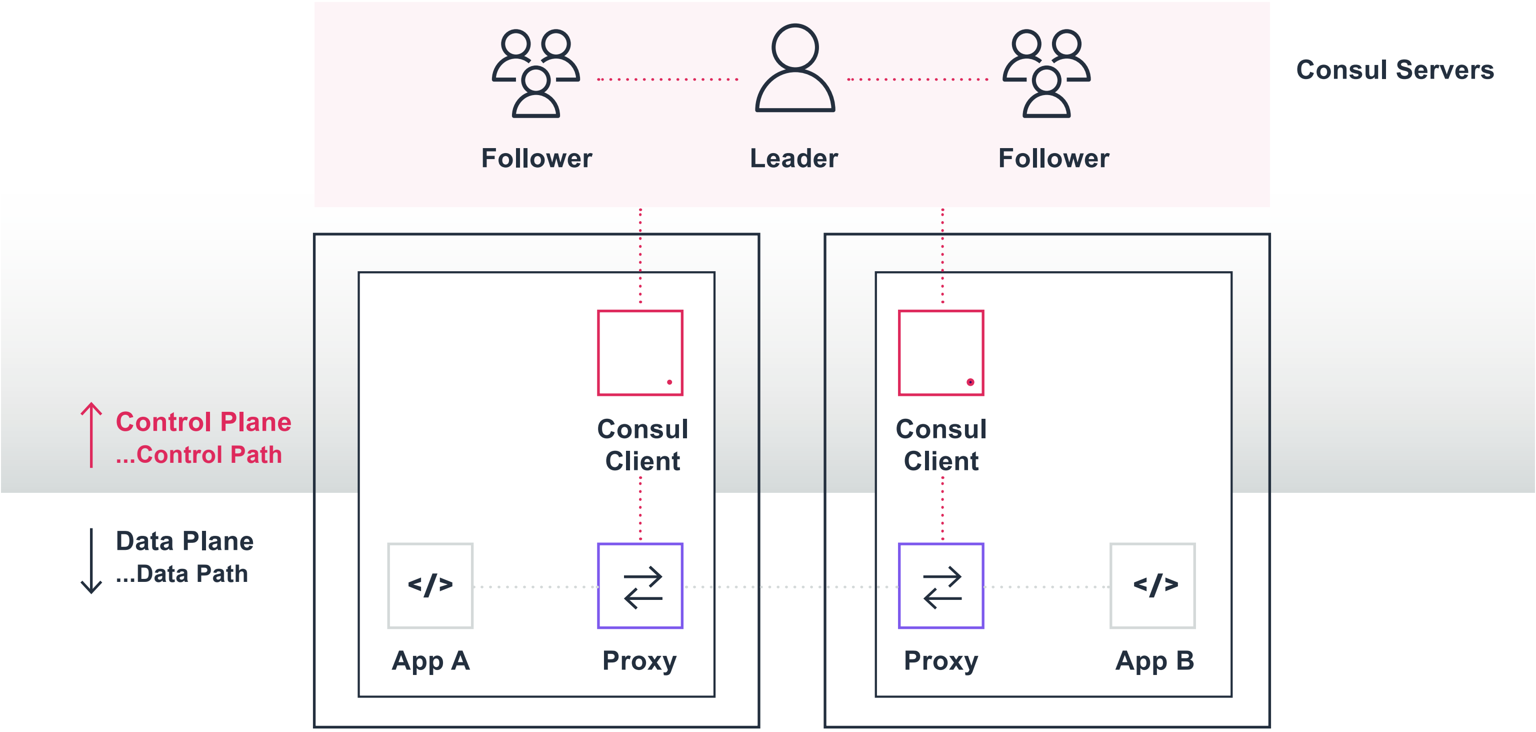
Service meshes use consistent tools to factor out the common concerns of running a service, such as monitoring, networking, and security. That means service developers and operators can focus on creating and managing applications for their users instead of worrying about detailed network implementation and connectivity.



Consul helps you securely connect your services and more

Enter Consul service mesh — a service networking solution that enables teams to manage secure network connectivity between services and across on-premises and multi-cloud environments and runtimes. Consul offers service discovery, service mesh, traffic management, and automated updates to network infrastructure. You can use these services individually or in a single Consul deployment. In addition, your overall security posture is improved because traffic going through Consul service mesh is encrypted with mutual transport layer security (mTLS).

Consul provides a control plane that enables you to register, query, and secure services deployed across your network. The control plane is the part of the network infrastructure that maintains a central registry to track services and their respective IP addresses. It is a distributed system that runs on clusters of nodes, such as physical servers, cloud instances, virtual machines, or containers. Consul interacts with the data plane through proxies.



Consul benefits include:

- Increased application resilience with failure handling, retries, and network observability
- Less downtime
- Accelerated application deployment
- Improved security across service-to-service communications

Consul also automates service discovery by replacing service connections usually handled with load balancers with an identity-based service catalog. The catalog always knows which services are available, which have been removed, and which are healthy.

Consul also routes network traffic to any runtime or infrastructure environment your services need to reach. In addition, you can use Consul API Gateway to route traffic into and out of the network.

Consul service mesh provides additional capabilities:

- Securing communication between services
- Traffic management
- Observability with no application code changes

With Consul, you can enable zero trust security. Consul provides several mechanisms that enhance network security without any changes to your application code, including mTLS encryption on all traffic between services and Consul intentions, which are service-to-service permissions that you can manage through the Consul user interface, API, and command line interface.

You can deploy Consul to several runtimes, which reduces service discovery tool sprawl and creates a single source of truth for tracking and routing services. Using the Consul service mesh along with Consul API gateway centralizes traffic management, reducing manual workflows.

You can use these features individually as needed or enable all of them to build a full service mesh that helps promote zero trust security.

The four pillars of service networking

A service mesh helps head off potential problems in a dynamic, cloud infrastructure. A service mesh controls service-to-service communication over a network and automatically routes requests from one service to the next while optimizing how all these moving parts work together. This method enables separate parts of an application to communicate with each other.

1 Discover services

Detecting different services and network protocols can be challenging. Service instances are constantly being created and destroyed and their availability must constantly be communicated.

Often called the first step in service mesh adoption, service discovery allows developers to use a central registry that tracks services, updates, and health statuses in real time, and catalog the network location and health of all registered services on their network. Discovery is a way for applications and microservices to locate each other on a network, shortening long configuration setup processes. Consul's discovery feature supports different services and network protocols.

2 Secure networking

With the proliferation of microservices, the surface area available for cyber attacks has increased exponentially, putting critical data at greater risk. In addition, network-related issues such as access control, load balancing, and monitoring now must be handled separately for each service within a cluster. It's important to ensure all service-to-service communication is authenticated, authorized, and encrypted.

Consul service mesh addresses service networking issues by:

- Simplifying microservices security with mutual authentication and encryption
- Managing identity, certificates, and authorization
- Providing access control and enforcing the level of least privilege
- Monitoring service health and enabling observability

3 Automate cloud networks

Automated networking facilitates easier cloud management because it helps streamline workflows, which enables faster delivery times.

Benefits of automated cloud networks include:

- Reduced dependence on manual ticketing systems
- Minimized risks for misconfigurations
- Lowered operator burden by automating key tasks

Consul further helps with cloud management by offering unique integrations with infrastructure provisioning tools such as HashiCorp Terraform.

Network infrastructure automation through Consul-Terraform-Sync (CTS) enables dynamic updates to network infrastructure devices triggered by service changes. CTS uses Consul as a data source that contains networking information about services and monitors those services. CTS uses Terraform as the underlying automation tool and leverages the Terraform provider ecosystem to drive relevant changes to the network infrastructure.

4 Control access

To protect against threats, organizations must keep an eye on vulnerabilities in private networks where east-west traffic flows. But controlling ingress traffic requires careful consideration of needed security controls to protect against external threats and unwanted access while still enabling authorized uses.

Increasingly, organizations want a single control plane to manage both service-to-service traffic (east-west) as well as inbound requests from external clients (north-south). The Consul API Gateway detects inbound requests to mesh-based applications, presents those clients with a verifiable certificate from a trusted authority, and facilitates the necessary secure connections to fulfill the requests. By combining the Consul API Gateway with Consul's service mesh, users gain a single control plane that makes it easier to consistently manage both east-west and north-south traffic.

The Consul API Gateway also simplifies traffic management by balancing requests across services and routing traffic to the appropriate service by matching one or more criteria, including:

- Hostname
- Path
- Header presence or value
- HTTP method type

Service networking with Consul and AWS

HashiCorp and AWS support many of the largest companies in the world, including one of the largest multinational telecommunications companies in America.

The architecture supporting this business includes multiple on-premises datacenters and runtimes, including Amazon ECS, AWS Fargate, AWS Lambda, Amazon EC2 VMs, on-premises Kubernetes, and on-premises VMs.

The company needed to address several business goals, including responsive multi-regional failover and seamless routing. It also needed increased observability and faster and less expensive deployments. Consul helped the telecom company reduce the networking complexity of running numerous services on multiple AWS datacenters across regions, runtimes, and on-premises environments.

The company adopted Consul because it flexibly supports both its cloud and on-premises workloads in multiple AWS regions, as well as its own datacenters. Consul helps manage this complexity while scaling with resiliency.

Getting Started with Consul on AWS

These resources can help you learn how to use Consul to securely connect your services on AWS.

Consul documentation:

- What Is Consul?
- Consul Architecture

Tutorials:

- Get Started with Consul on Kubernetes
- Get Started with Consul on VMs
- Consul with Amazon ECS Workloads
- Consul with AWS Lambda Workloads
- Consul Cluster Peering on Kubernetes in AWS

Video and publications:

- Consul Learn Lab: Deploy Resilient Applications with Service Mesh and AWS Lambda
- Consul: Up and Running

New to Consul? Sign up for HCP Consul to deploy a production-ready Consul cluster >

In collaboration with

HashiCorp

aws

PARTNER
Premier Tier
Services