



# Consul Onboarding Program

COBRA Team | HashiCorp Customer Success

October 2022



---

# Agenda

1. Welcome
2. Consul Onboarding Program
3. Consul Overview
4. Key Concepts
5. Consul Architecture
6. Project Success Considerations

# Code of Conduct



**HashiCorp is dedicated to providing a harassment-free Consul Enterprise onboarding experience for everyone, regardless of gender, gender identity, sexual orientation, disability, physical appearance, body size, race, national origin, or religion. We value your attendance and do not wish anyone to feel uncomfortable or threatened at any time.**

The bottom line is that we do not tolerate harassment of conference participants in any form. Harassment includes but is not limited to offensive verbal comments related to gender, gender identity, sexual orientation, disability, physical appearance, body size, race, national origin, religion; sexual or inappropriate images in public spaces; deliberate intimidation; stalking; trolling; sustained disruption of talks or other events; and unwelcome sexual attention. Participants asked to stop any harassing behavior are expected to comply immediately. If you are being harassed, notice that someone else is being harassed, or have any other concerns, please let the HashiCorp event representative know immediately or email [customer.success@hashicorp.com](mailto:customer.success@hashicorp.com).



# Consul Enterprise Onboarding Program



HashiCorp

# Consul Enterprise Onboarding Journey



A 5-week guided community program following a prescriptive path to successfully onboarding and adopting Consul

- Week 1 - Kickoff - Introduction to Consul & Architectural Basics
- [Week 2 - Webinar - Consul Foundations](#)
- Week 3 - Webinar - Consul Deployment & Operations
- [Week 4 - Office Hours](#)
- Week 5 - Webinar - Advanced Concepts
- [Exit Ramp and Operational Readiness Check](#)



# Onboarding Goal

Our objective is to make you successful with our products and see value within 90 days



## Consul Installed

- Consul Enterprise installed in your environment
- Basic configuration completed
- Telemetry and monitoring in place
- Deployment and operational patterns established



## Consul Operational

- 3+ foundational use cases in place
  - Service Catalog
  - Service Health Checking
  - Service Discovery
  - Consul DNS
  - Consul Key Value store
- A roadmap created for onboarding additional use cases (Service Mesh track or NIA track).



## Completed within 90 days

— 01

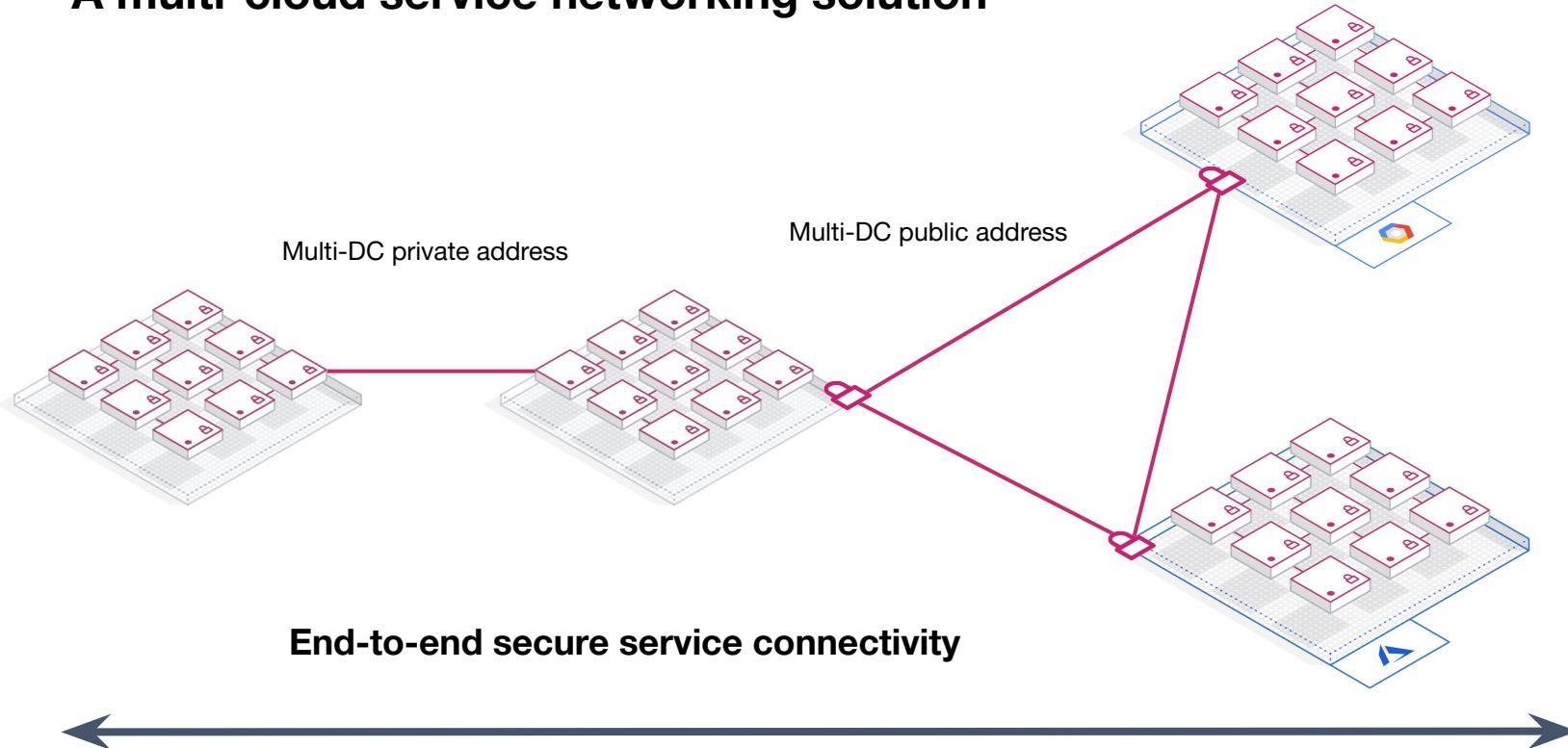
# Consul Overview





# What is Consul?

A multi-cloud service networking solution

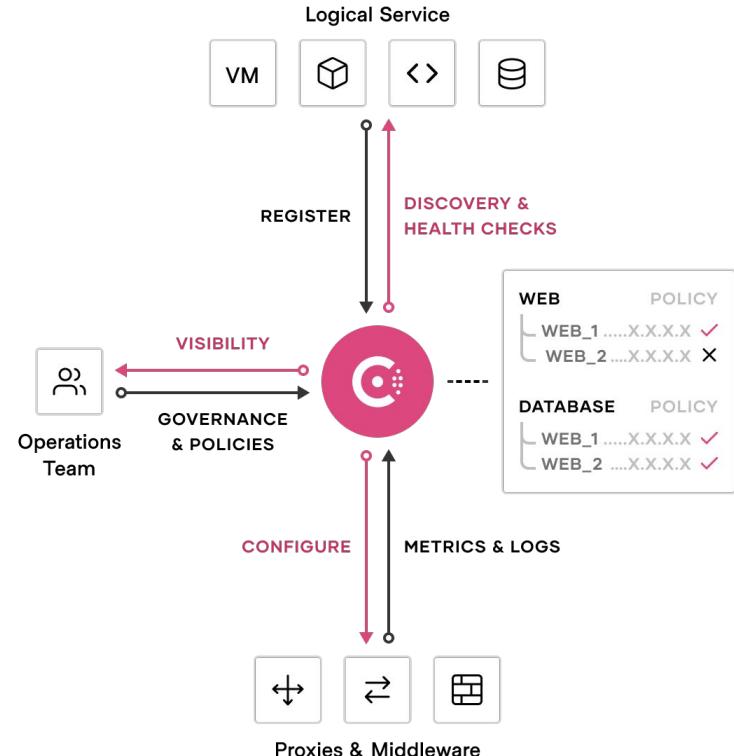




# Service Networking

Discover and securely connect any service on any cloud or runtime

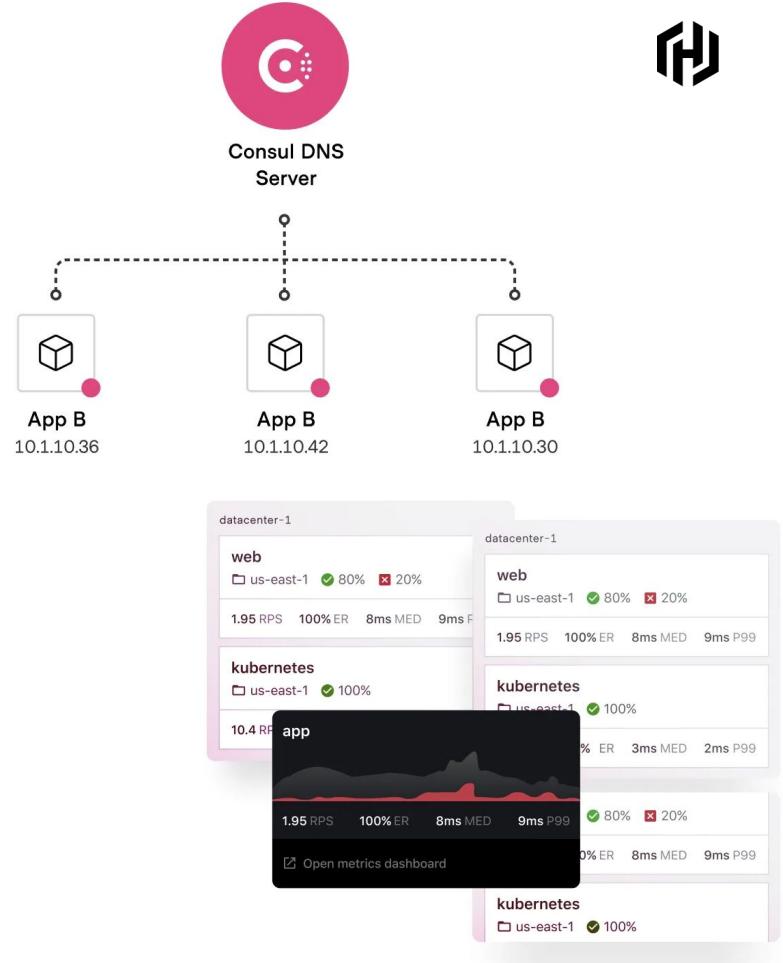
- **Discover**
  - Service discovery and health checks
- **Connect**
  - Service Identity
  - Service mesh to connect and secure services
  - Governance
  - Observability + Resiliency
  - Layer 7 traffic shaping
- **Automate**
  - Network Infrastructure Automation
- **Access**
  - Control access into and out of the service mesh with the API Gateway



# Service Discovery



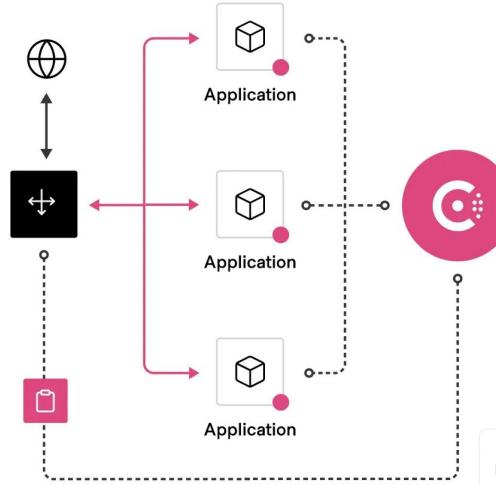
- Centralized catalog to register, track, discover, and monitor services
- Single source of truth for all services
- DNS and API access for service registration
- Health checks for systems and applications



# Load Balance and Manage Traffic



- Works as an L4/L7 load balancer
- Integrates with NGINX, HAProxy, and F5 for automatic service updates
- Single control plane for east/west and north/south traffic
- Deployment patterns include:
  - A/B test
  - Blue/green
  - Soft multi-tenancy (prod/qa/staging sharing compute resources)



All Intentions

### Edit Intention

Source service  
Search for an existing service, write a new URL, or write any service URL.

Destination service  
You cannot edit the destination name after initial creation.

Should this source connect to the destination?

Allow → The source service will be allowed to connect to the destination.  
 Deny → The source service will not be allowed to connect to the destination.  
 Application aware → The source service may or may not be allowed to connect to the destination via unique permissions based on L7 criteria, path, header, or method.

Description (Optional)  
Description (Optional)

Permissions

Permissions are L7 attributes. If any of the following permissions match the request, the intention will apply. Requests that fail to match any of the provided routes will do the opposite of the allowed/deny action above.

Learn more about permissions

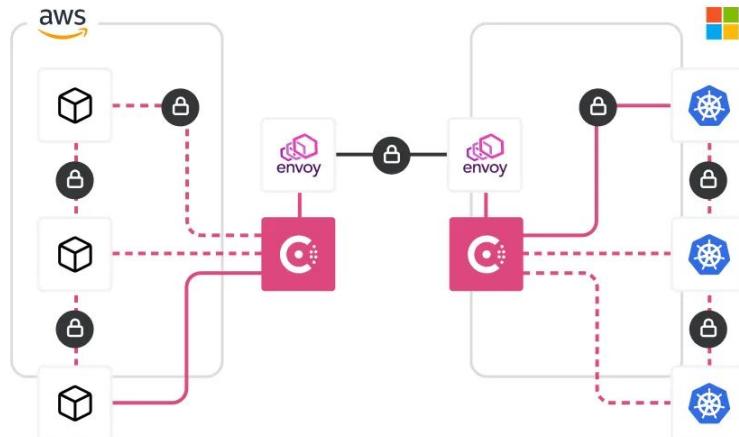
Allow → prefixed by /debug-stuff?query=1 | x-debug not exactly matching "on"  
 Deny → prefixed by /debug-stuff?query=1 | x-debug not exactly matching "on"

Save Cancel

# Zero Trust Networking



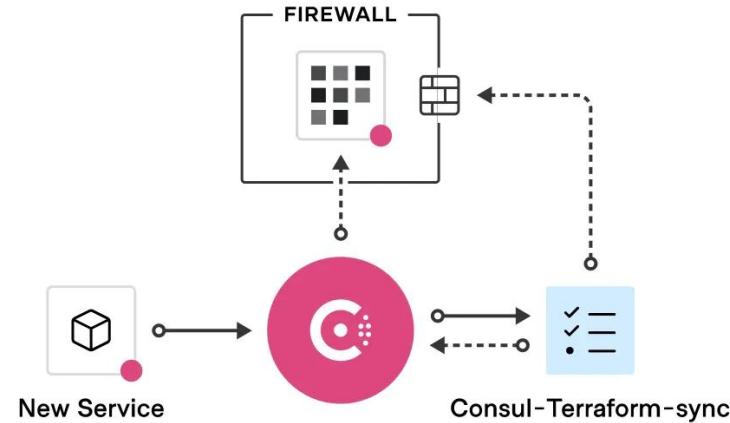
- Service mesh provides identity-based access and mTLS for all service to service communication
- Consul supports multiple Certificate Authorities (CAs)
- Service intentions secure service communications



# Network Infrastructure Automation



- Automate networking tasks and configuration changes
- Triggers include:
  - Service scaling (up and down)
  - Service port changes
  - Health changes
  - Metadata changes



— 02

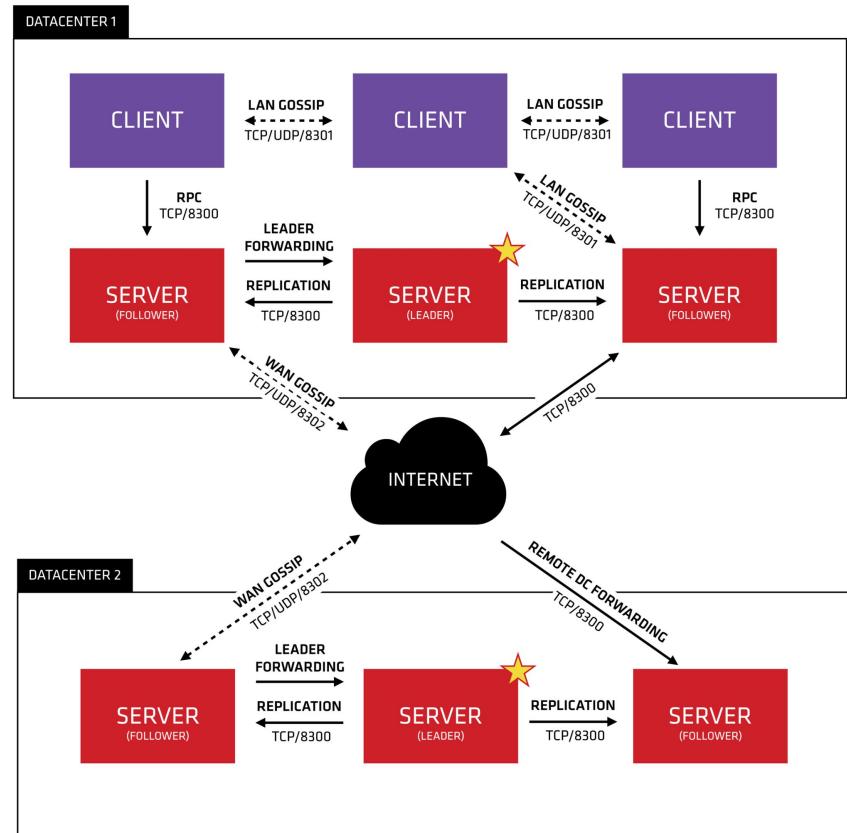
# Consul Key Concepts



# Consul Key Concepts



- Consul Servers & Clients
- Consul Clusters
- LAN Gossip Pool
- Consul Datacenters
- WAN Gossip

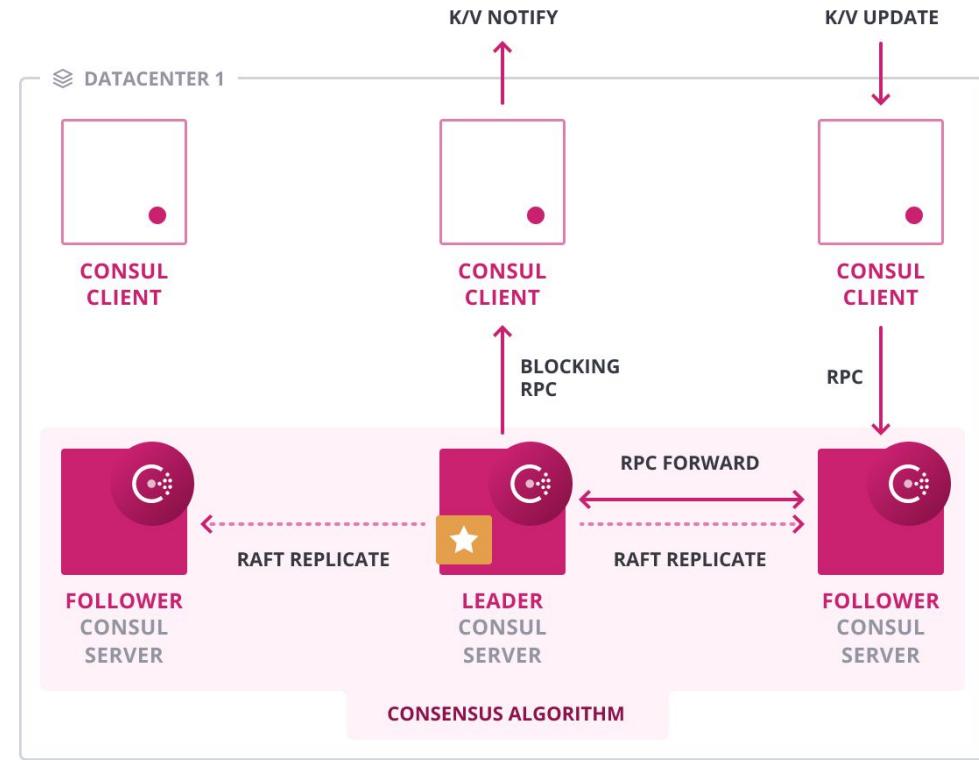




# Consul Servers & Clients

## Consul Servers

- Hold Key/Value store, Sessions, ACLs, Prepared Queries, Intentions
- Enforce ACLs for reading and writing access
- Use Raft protocol to provide consistency
- Enhanced read scalability provides for scaling of reads without impacting write latency
- Collate health check data from clients

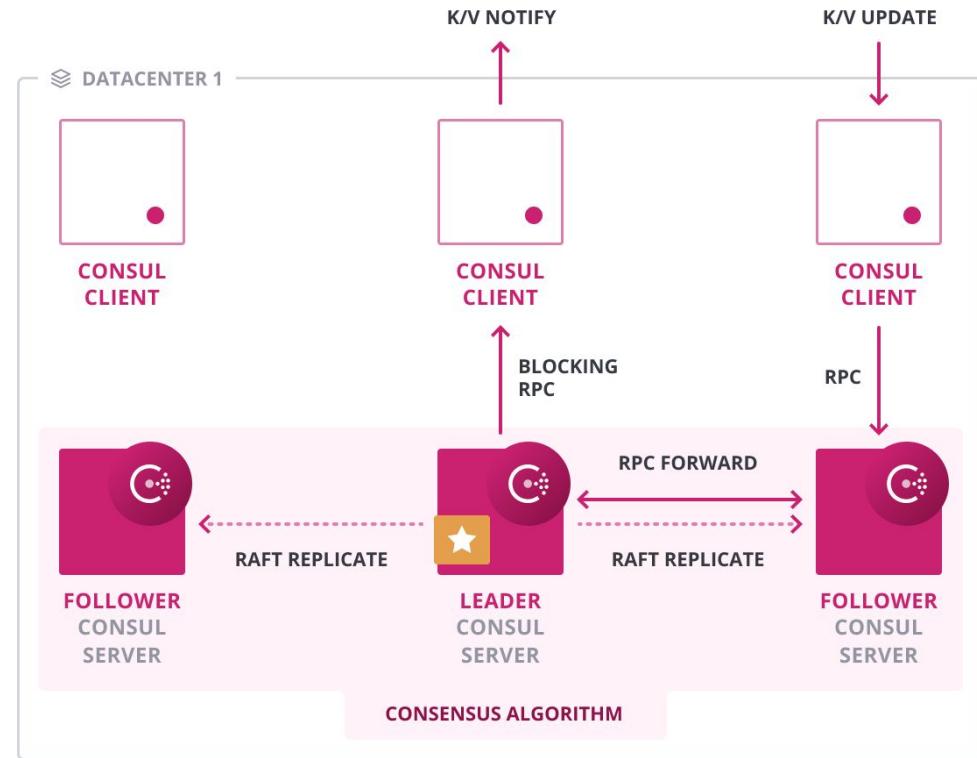




# Consul Servers & Clients

## Consul Clients

- Register services & checks
- Hold service registration and health check data
- Determine pass/fail of checks and sync to Consul servers
- Authoritative source of truth for configured checks it is managing



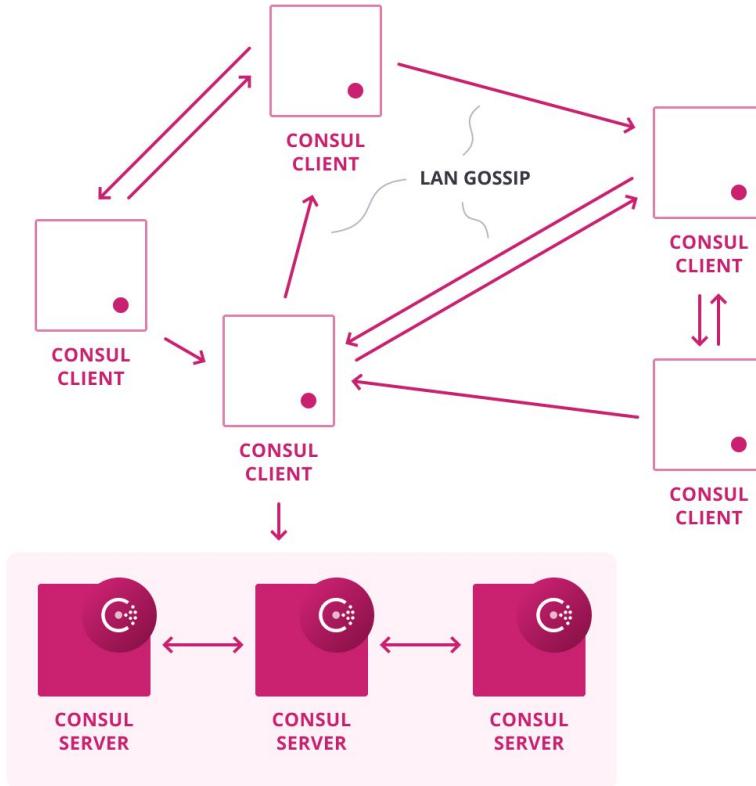


# Consul LAN Gossip

Each datacenter has a **LAN gossip pool** containing all members, both clients and servers

## Responsible for:

- Membership information allows clients to automatically discover servers
- Distributed failure detection avoids concentrating the load on a few servers
- Reliable and fast event broadcasts





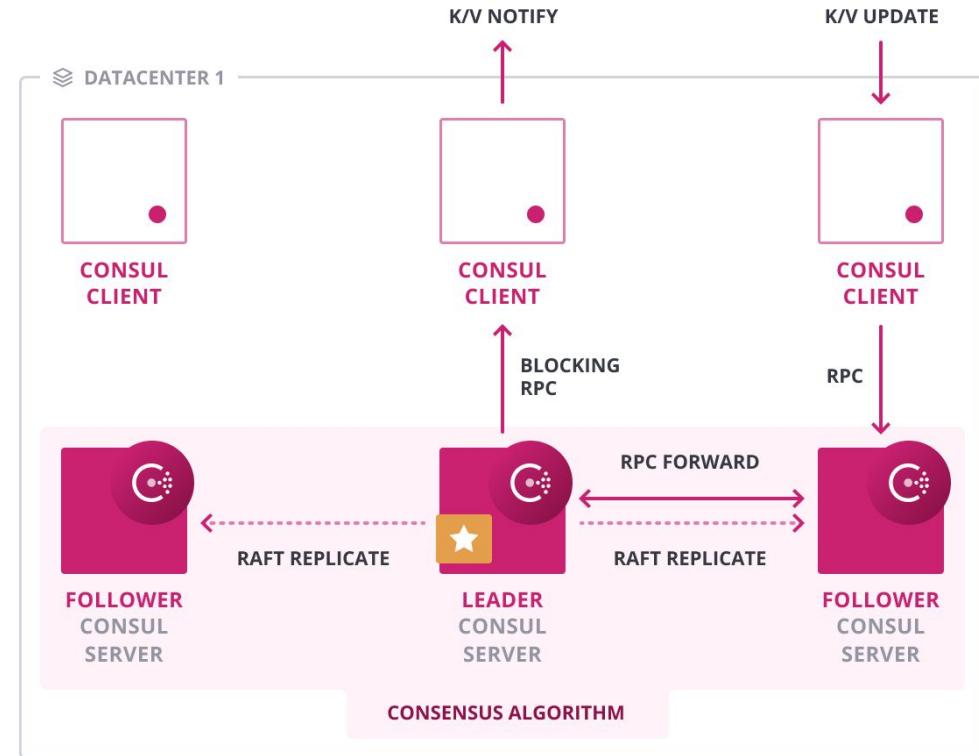
# Consul Datacenters & Clusters

## Consul Datacenter

- Smallest unit of Consul infrastructure that can before basic Consul operations
- Contains at least one Consul server, typically 3+ server nodes and client agents

## Consul Cluster

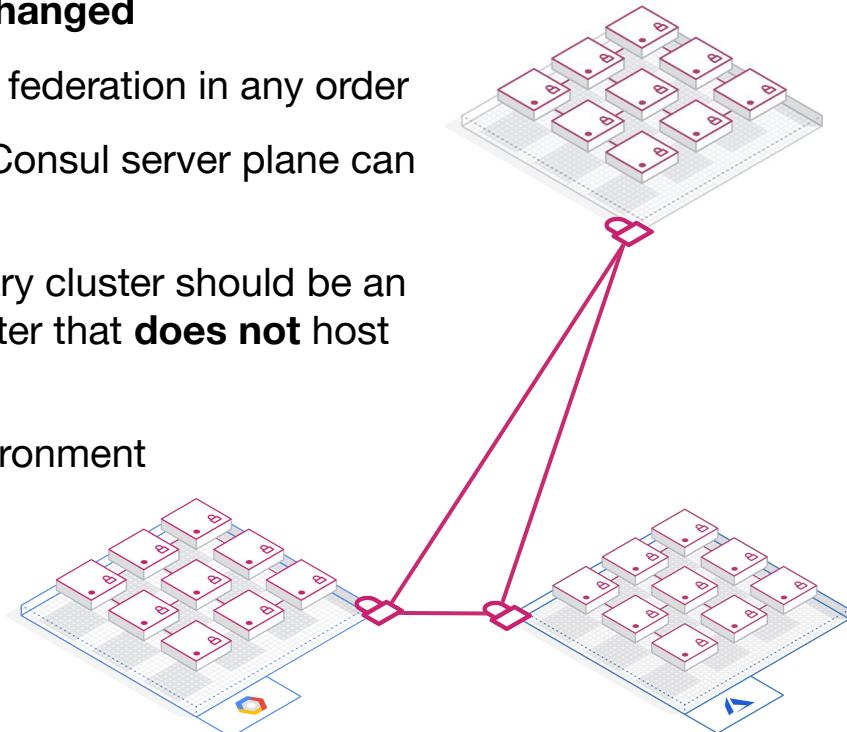
- A collection of agents that are aware of each other, often used interchangeably with datacenter
- In some contexts is only a collection of client agents



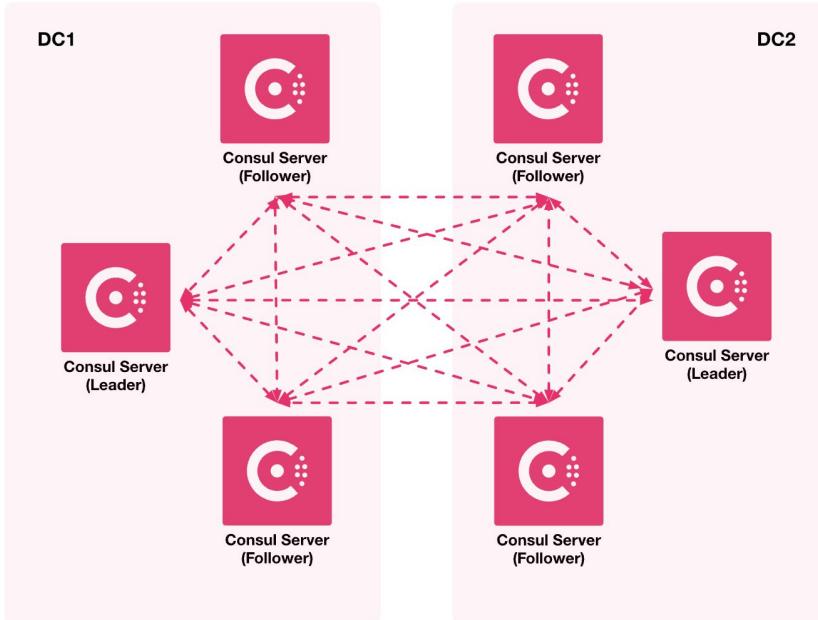
# Consul Datacenter Creation



- The **first Consul datacenter** created in a federated deployment will be the primary Datacenter and **cannot be changed**
- Additional data centers can be added to the federation in any order
- When running Consul in Kubernetes only 1 Consul server plane can be deployed per Kubernetes Cluster
- In medium and large deployments the primary cluster should be an operational and administrative-only datacenter that **does not** host services
- Upgrade pattern for a federated Consul environment



# WAN Gossip



- Designed for loose coupling between Consul datacenters and optimized for typical Internet latency
- Enables Consul servers to exchange information like addresses and health status
- Gracefully handles loss of connectivity in the event of failure in connectivity, etc
- Typically uses UDP/TCP 8302

# Architecture





# Consul Installation

What do we need to  
decide?

1

## Cluster Platform

- Virtual Machines
- Bare Metal
- Containers
- Kubernetes

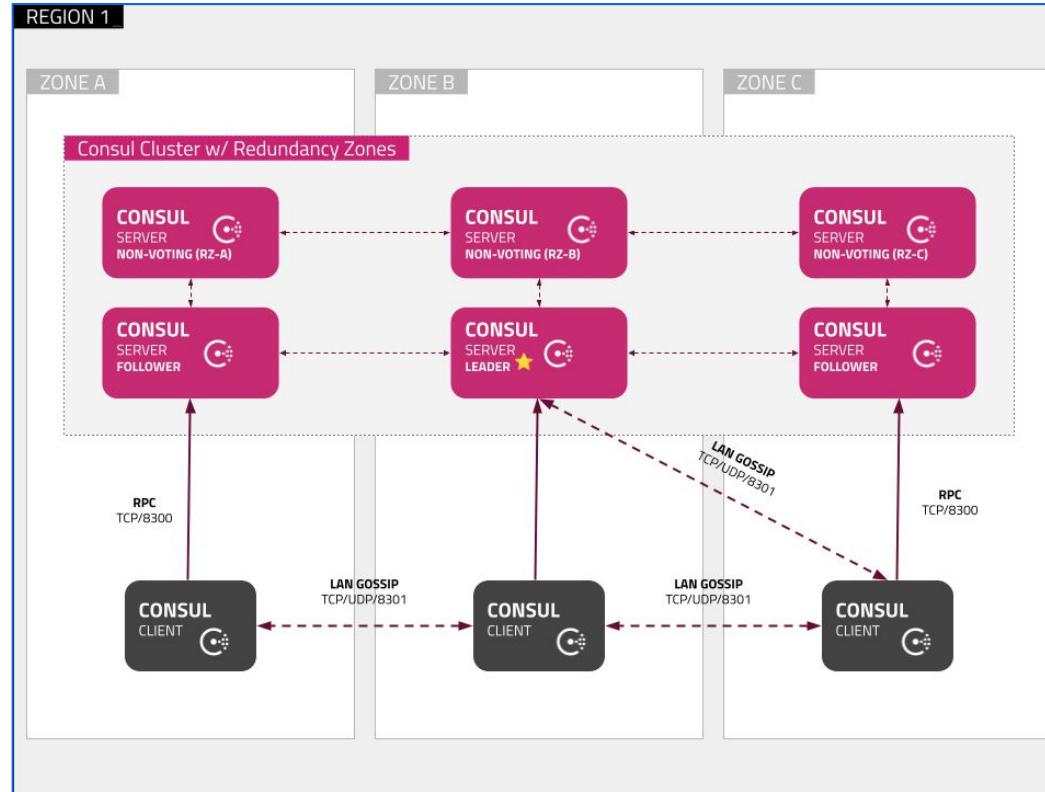
2

## Deployment Pattern

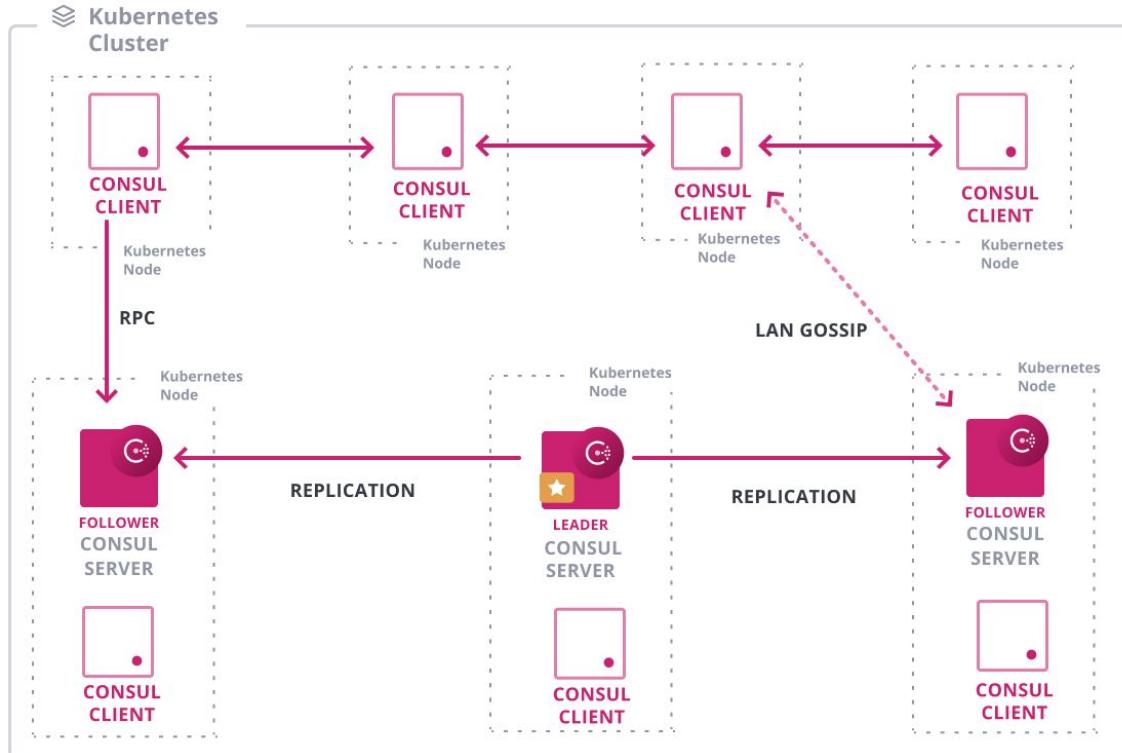
- Static vs. Immutable
- Automation and upgrade pattern
- Sizing
- Agent locations



# VM or Bare Metal Deployment

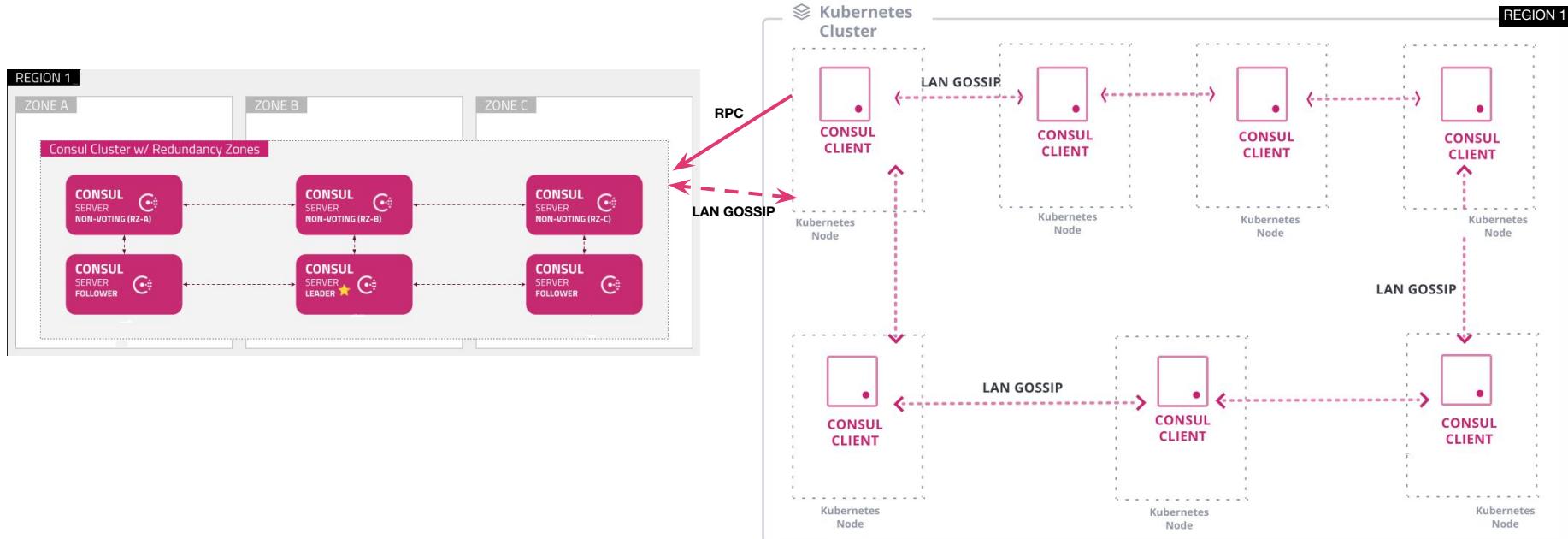


# Kubernetes Deployment Patterns



**Consul Deployed inside Kubernetes**

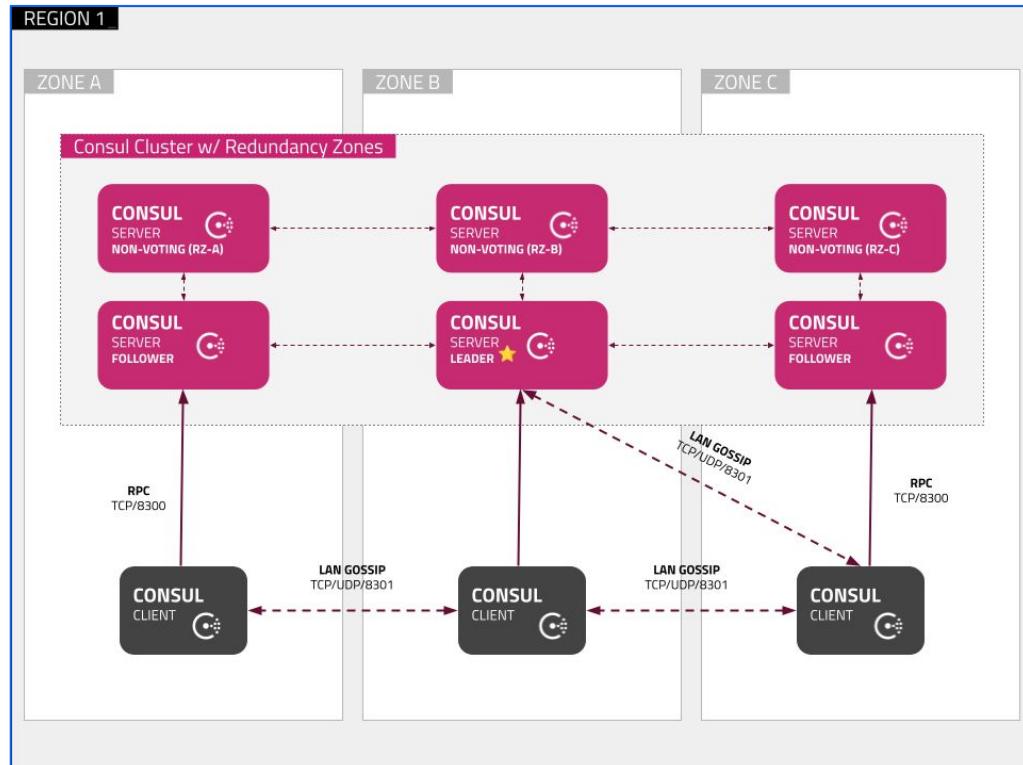
# External Kubernetes Deployment



# Consul Enterprise Reference Architecture



- Provides a highly resilient and scalable deployment for a single Consul cluster
- 6 node cluster with 3 non-voting nodes is capable of withstanding the loss of two nodes or an entire Availability Zone (AZ)
- Uses Consul Enterprise Autopilot and non-voting nodes for redundancy
- [Consul and Kubernetes Deployment Guide](#)





# Sizing

Per instance sizing  
recommendations

	Small (Dev/Test/Staging/QA)	Large (Production)
<b>CPU</b>	2 - 4 Core	8 - 16 Core
<b>Memory</b>	8 - 16 GB RAM	32 - 64 GB RAM
<b>Disk Capacity</b>	100+ GB	200+ GB
<b>Disk IO</b>	3000+ IOPS	7500+ IOPS
<b>Disk Throughput</b>	75+ MB/s	250+ MB/s
<b>AWS</b>	m5.large, m5.xlarge	m5.2xlarge, m5.4xlarge
<b>Azure</b>	standard_d2s_v3, standard_d4s_v3	standard_d8s_v3, standard_d16s_v3
<b>GCP</b>	n2-standard-2, n2-standard-4	n2-standard-8, n2-standard-16

# Network Connectivity



Name	Port / Protocol	Source	Destination	Description
RPC	8300 TCP	All agents (client & server)	Server agents	Used by servers to handle incoming requests from other agents
Serf LAN	8301 TCP & UDP	All agents (client & server)	All agents (client & server)	Used to handle gossip in the LAN. Required by all agents
Serf WAN	8302 TCP & UDP	Server agents	Server agents	Used by server agents to gossip over the WAN to other server Agents. Only used in multi-cluster environments.
HTTP/HTTPS	8500 & 8501 TCP	Localhost of client or server agent	Localhost of client or server agent	Used by clients to talk to the HTTP API. HTTPS is disabled by default.
DNS	8600 TCP & UDP	Localhost of client or server agent	Localhost of client or server agent	Used to resolve DNS queries.
gRPC (Optional)	8502 TCP	Envoy Proxy	Client agent or server agent that manages the proxies service registration	Used to expose the xDS API to Envoy proxies. Disabled by default.
Sidecar Proxy	2100 - 21255 TCP	All agents (client & server)	Client agent or server agent that manages the proxies service registration	Port range used for automatically assigned sidecar service registrations.
Mesh Gateway	8443* or 443* TCP	Varies	Services enabled for connectivity	*This port is configurable, the Helm chart uses 443 as a default for external services, 8443 is commonly used for traffic from Load Balancer to client nodes

# Network Latency & Bandwidth



- LAN gossip occurs between all agents in a Consul datacenter. Client and Server agents participate in the gossip.
- LAN gossip is latency dependant, for a cluster to stay in sync, network latency between availability zones is required to be less than **eight milliseconds (8 ms)**.
- Network bandwidth consumed by Consul is entirely dependant upon environment specific usage patterns. In many cases, even a high request volume will not translate to a large amount of network bandwidth consumption. **All data** written to Consul will be **replicated across all server agents**. It's important to consider bandwidth requirements to other external systems such as monitoring and logging collectors.
- Environment specific DNS Forwarding and DNS Caching considerations need to be included in architecture planning.

# **Key Consul Success Considerations**

prepare for the upcoming weeks





# Use Case Considerations

- What are the major problems/challenges/workflows that Consul is solving for?
  - What is the current solution in place?
  - What changes, improvements, is Consul solving?
- What are organizational goals for Consul?
  - Near term
  - Long term
- What is the rollout plan?
  - Where will the first deployment be?
  - How many data centers are planned?



# Cluster Architecture Considerations

- Where will Consul be deployed?
- What integrations with external services or external tooling need to be implemented during the project (example Kubernetes clusters).
- Where are the target applications for the initial use case hosted? What are the networking and connectivity requirements for these target applications?
- What are the target Disaster Recovery RPO and RTO?
- What CA will be used to provide Consul certificates for mTLS?
- Are there any noteworthy regulatory constraints in the environment that need to be considered?



# Your Success Metrics

- What are **your** short term goals for the rollout of Consul?
  - What are the must-haves?
  - What metrics are being used to gauge the success of this project?
- What are **your** longer term goals for the rollout of Consul?
  - Are there particular features that are planned to be adopted?
  - Are there particular business problems that Consul is going to solve?

# Resources



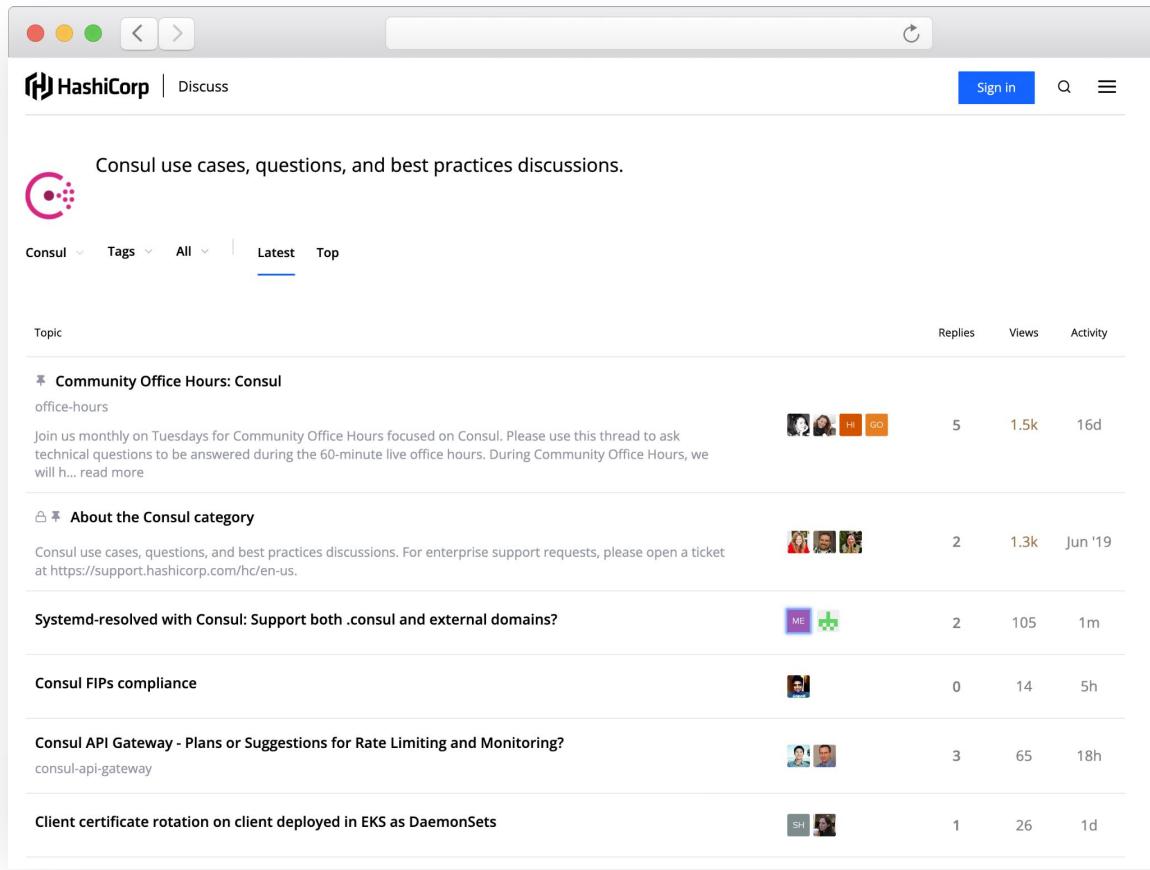
# Learn

<https://learn.hashicorp.com/consul>

## Step-by-step guides to accelerate deployment of Consul

The screenshot shows the HashiCorp Learn platform interface for Consul. The left sidebar contains navigation links for 'GET STARTED' (Consul on HCP, Consul on Kubernetes, Consul on VMs) and 'USE CASES' (Kubernetes Service Mesh, Microservices, NIA, Service Discovery & Health, Service Mesh & Gateways). The main content area features a prominent banner with the text 'Deploy a fully managed service mesh' and a call-to-action 'Sign up for HCP Consul'. Below the banner, there are three main sections: 'Learn Consul fundamentals' (7 TUTORIALS), 'HashiCorp Cloud Platform (HCP) Consul' (5 TUTORIALS), and 'Get Started on VMs' (9 TUTORIALS).

TUTORIALS	TUTORIALS	TUTORIALS
7 TUTORIALS	5 TUTORIALS	9 TUTORIALS
<b>HashiCorp Cloud Platform (HCP) Consul</b> Quickly get hands-on with HashiCorp Cloud Platform (HCP) Consul using the HCP portal quickstart deployment, experiment with the...	<b>Get Started on Kubernetes</b> Setup Consul service mesh to get experience deploying service sidecar proxies and securing service with mTLS.	<b>Get Started on VMs</b> Consul is a networking tool that provides a fully featured service mesh and service discovery. Try Consul locally.



HashiCorp | Discuss

Sign in  

Consul use cases, questions, and best practices discussions.

Topic

Community Office Hours: Consul office-hours

Join us monthly on Tuesdays for Community Office Hours focused on Consul. Please use this thread to ask technical questions to be answered during the 60-minute live office hours. During Community Office Hours, we will h... read more

About the Consul category

Consul use cases, questions, and best practices discussions. For enterprise support requests, please open a ticket at <https://support.hashicorp.com/hc/en-us>.

Systemd-resolved with Consul: Support both .consul and external domains?

Consul FIPS compliance

Consul API Gateway - Plans or Suggestions for Rate Limiting and Monitoring? consul-api-gateway

Client certificate rotation on client deployed in EKS as DaemonSets

Replies Views Activity

Hi GO

ME

Sh



# Discuss

Engage with the HashiCorp Cloud community including HashiCorp Architects and Engineers.

[discuss.hashicorp.com](https://discuss.hashicorp.com)

# Need Additional Help?



## Customer Success

Contact our Customer Success Management team with any questions. We will help coordinate the right resources for you to get your questions answered.

[customer.success@hashicorp.com](mailto:customer.success@hashicorp.com)

## Discuss

Engage with the HashiCorp Cloud community including HashiCorp Architects and Engineers

[discuss.hashicorp.com](https://discuss.hashicorp.com)

## Technical Support

Something not working quite right? Engage with HashiCorp Technical Support by opening a new ticket for your issue at [support.hashicorp.com](https://support.hashicorp.com).

## HashiCorp Academy

Consul Enterprise Academy classes are virtual and delivered by a live instructor with in-depth Consul knowledge and implementation expertise.

Academy courses include a sandbox environment for hand-on experience in the 10 labs throughout the 3-day course.



---

# Resources

- [A Raft Consensus Primer - Secret Lives of Data](#)
- [Consul Reference Architecture](#)
- Terraform starter code (VM installation)
  - [AWS](#)
  - [Azure](#)
  - [GCP](#)
- [Consul and Kubernetes Reference Architecture](#)
- [Consul Helm Chart](#)
- Terraform starter code for managed Kubernetes
  - [AWS EKS](#)
  - [Azure AKS](#)
  - [Google GKE](#)



# Next Steps

# Up Next



**Webinar:** Consul Foundations



**Authorized users for Support**

Please email [customer.success@hashicorp.com](mailto:customer.success@hashicorp.com) with your Support Contacts



**Q & A**

A Q&A will be held after this session

# Q&A



# Thank You

[customer.success@hashicorp.com](mailto:customer.success@hashicorp.com)  
[www.hashicorp.com/customer-success](http://www.hashicorp.com/customer-success)