HashiCorp Consul

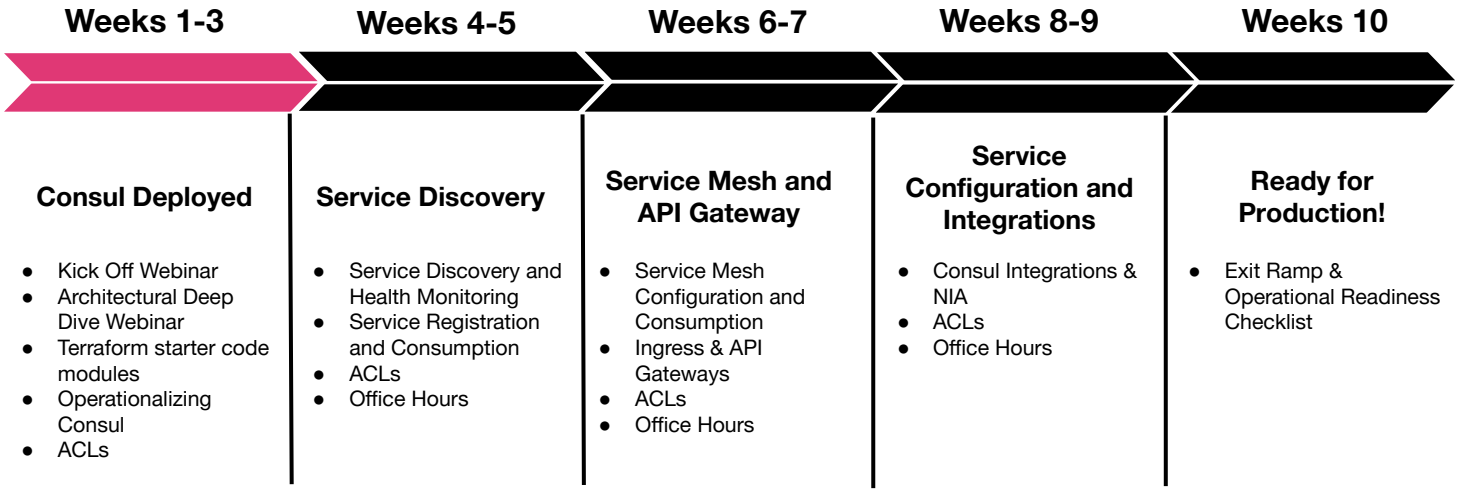
Consul Enterprise Getting Started & Technical Overview

July 2022

Agenda

1. Overview
2. Key Concepts
3. Architecture
4. Deployment Patterns
5. Operations & Runbooks
6. Next Steps

Consul Enterprise Path to Production

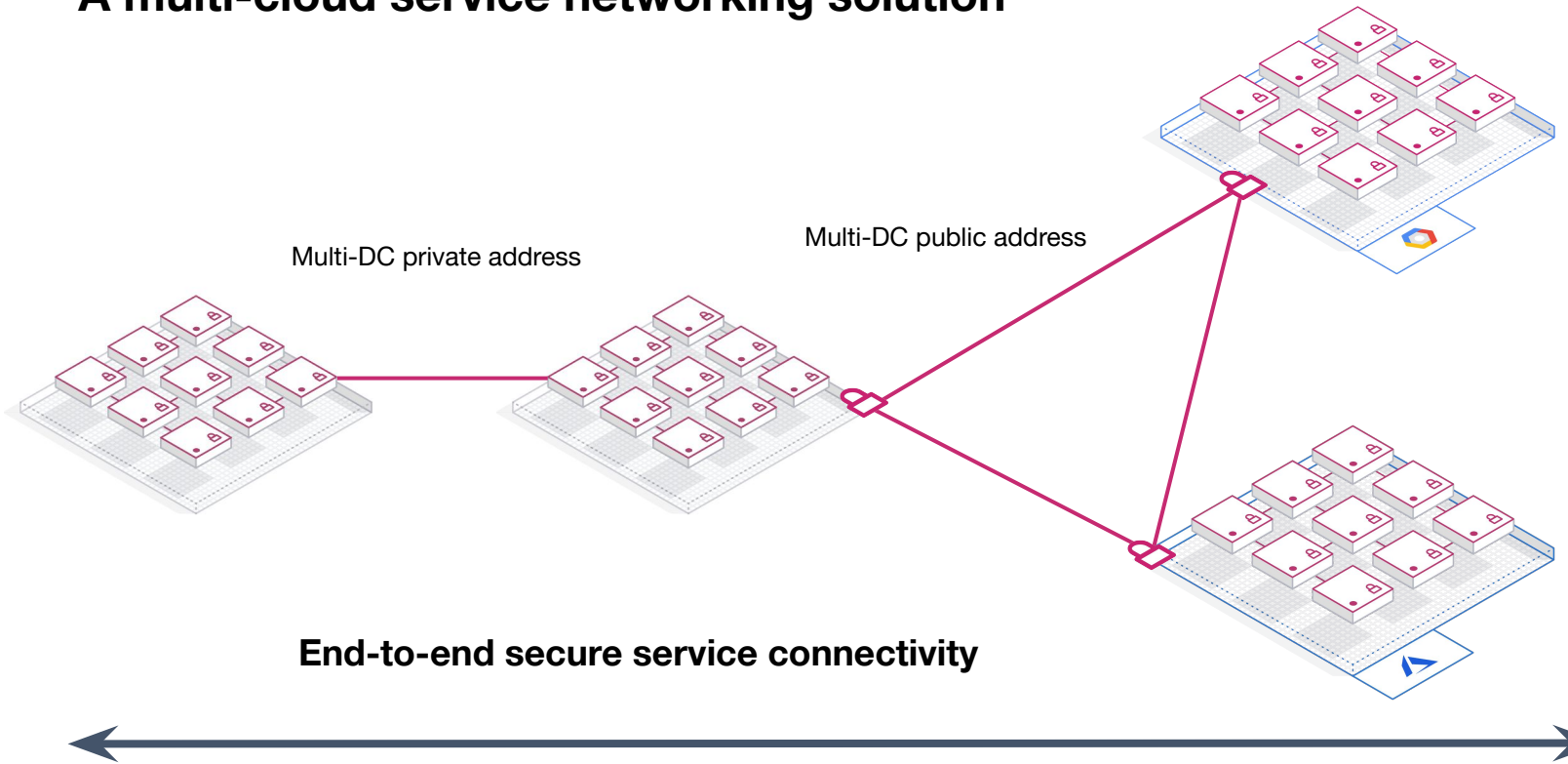


01

Consul Overview

What is Consul?

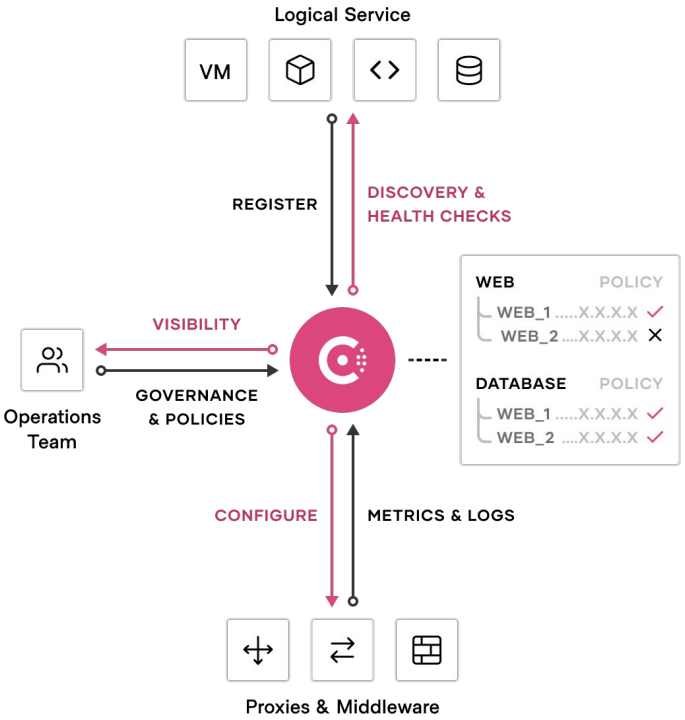
A multi-cloud service networking solution



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.

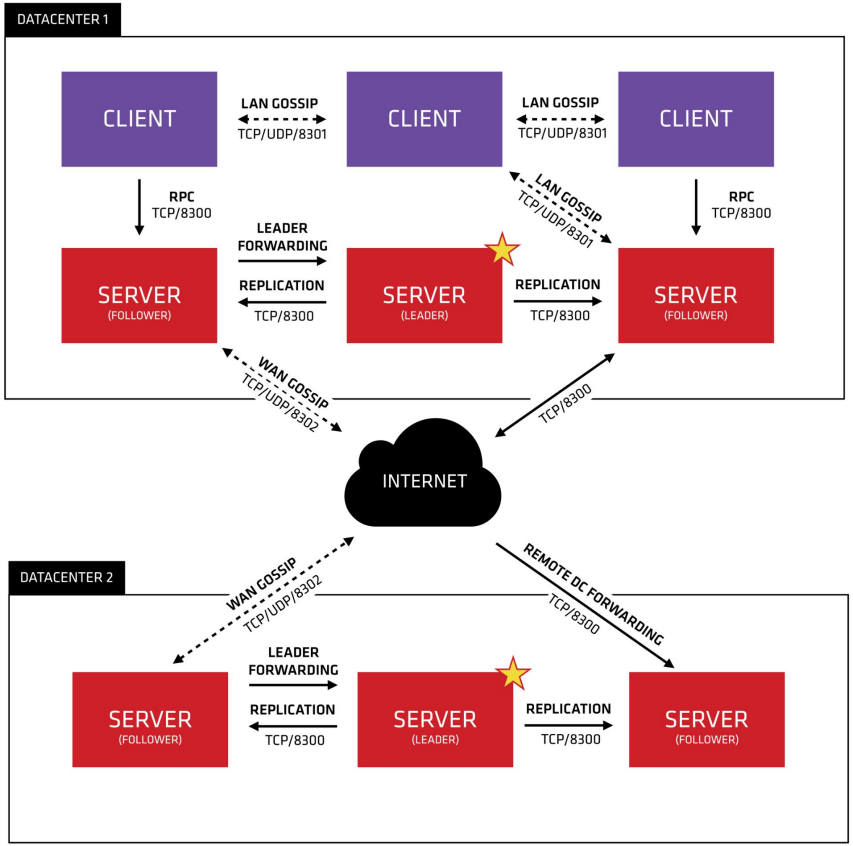


02

Consul Key Concepts

Consul Key Concepts

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



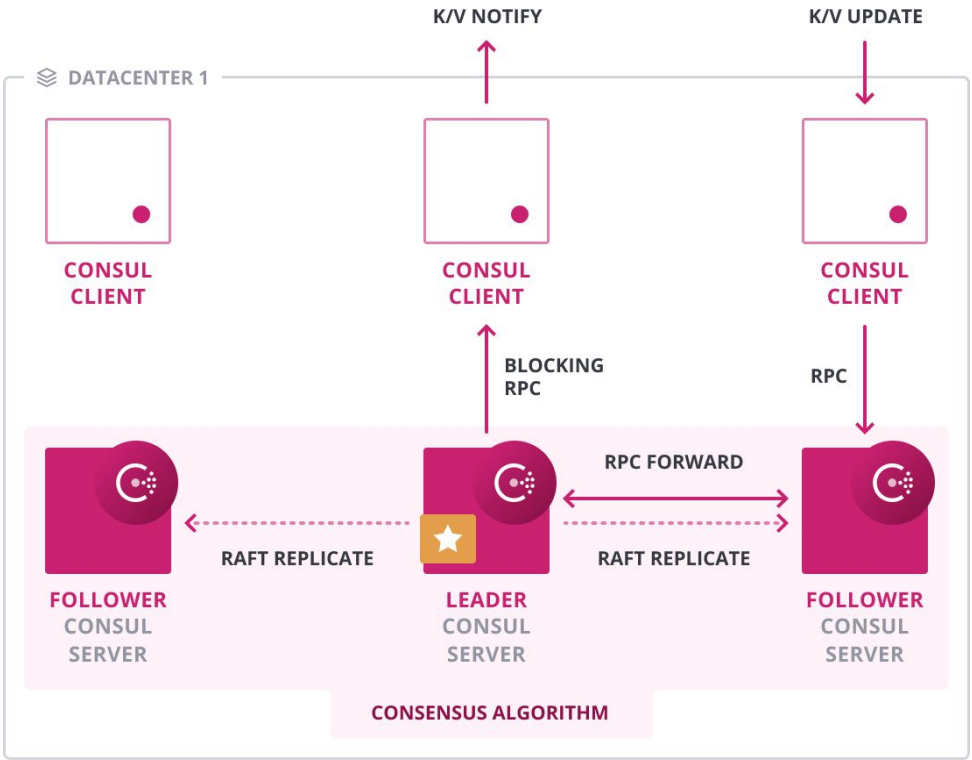
Consul Clusters & Clients

Consul Clients hold service registration and health check data:

- Sync back to Consul servers but clients are authoritative

Consul Servers hold everything else (key/value, sessions, ACL, prepared query, intentions etc)

- Clients make RPC calls to the Consul servers for this data; servers enforce ACLs for reading and writing access
- Servers use Raft protocol to provide consistency
- Enhanced read scalability helps to scale reads without impacting write latency.

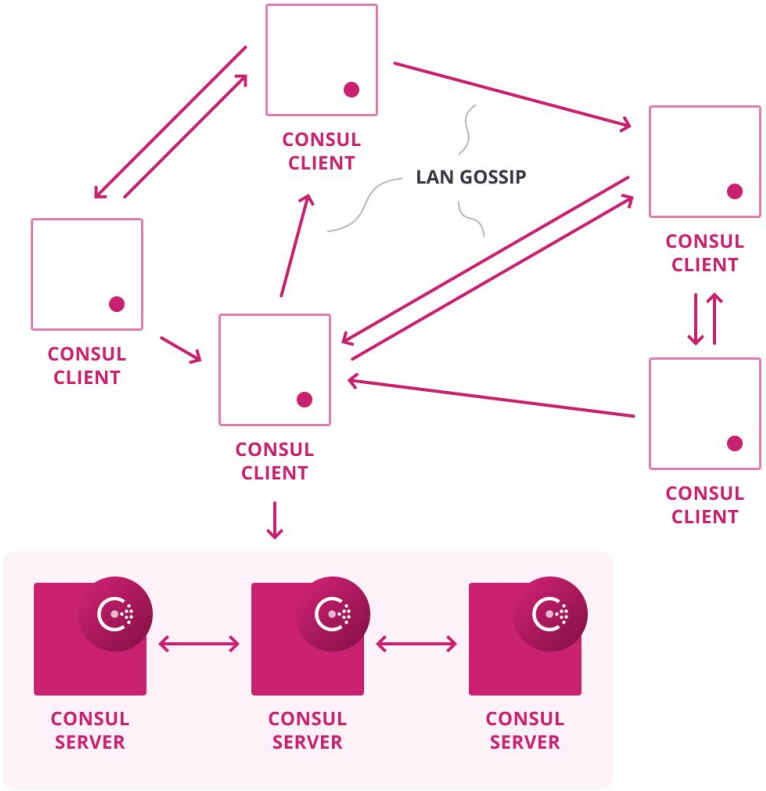


Consul LAN Gossip

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

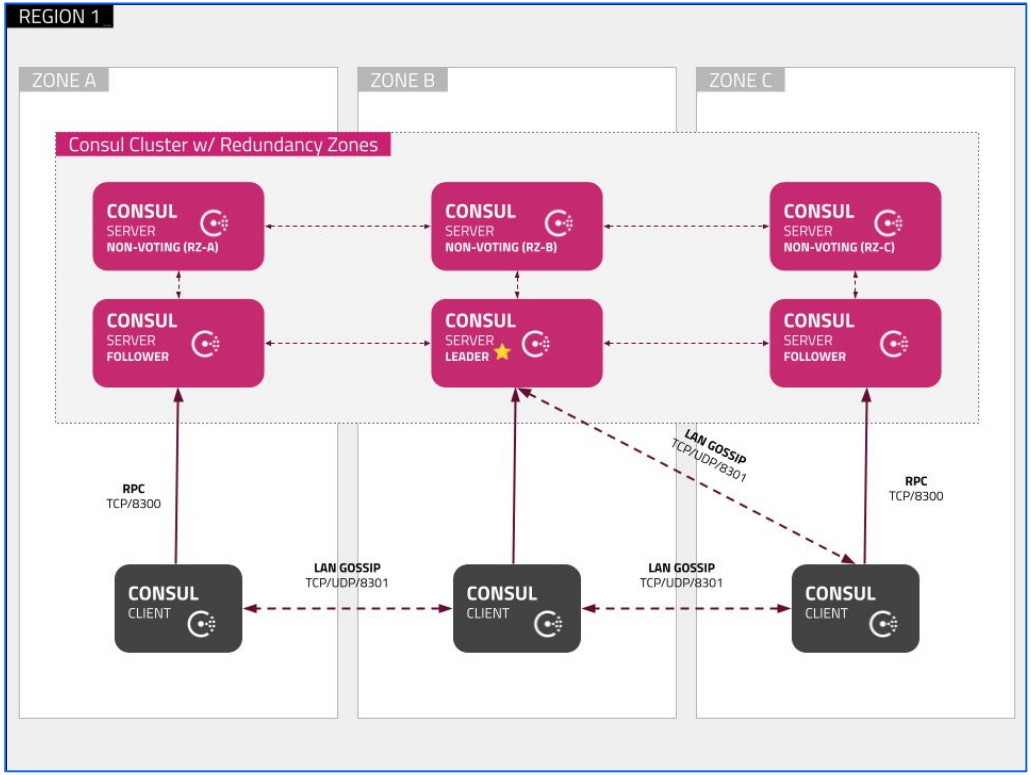


03

Consul Architecture

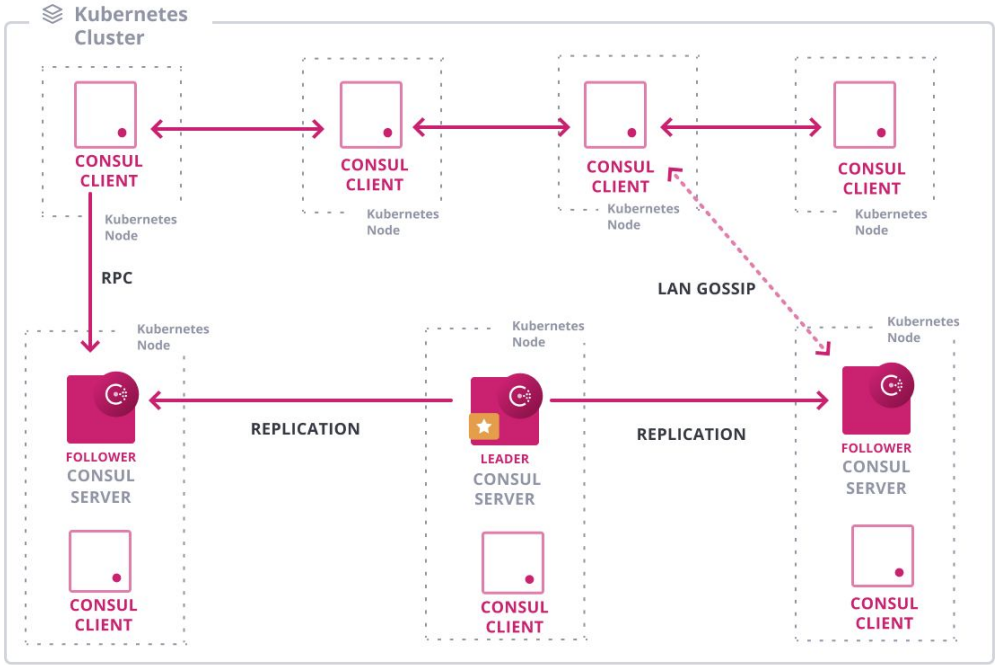
Consul Enterprise Reference Architecture

- This architecture provides a highly resilient and scalable deployment for a single Consul cluster
- This 6 node cluster with 3 non-voting nodes is capable of withstanding the loss of two nodes or an entire Availability Zone (AZ)
- This design uses Consul Enterprise Autopilot and non-voting nodes for redundancy
- Consul Enterprise replication features provide resilience across multiple clusters and/or regions.



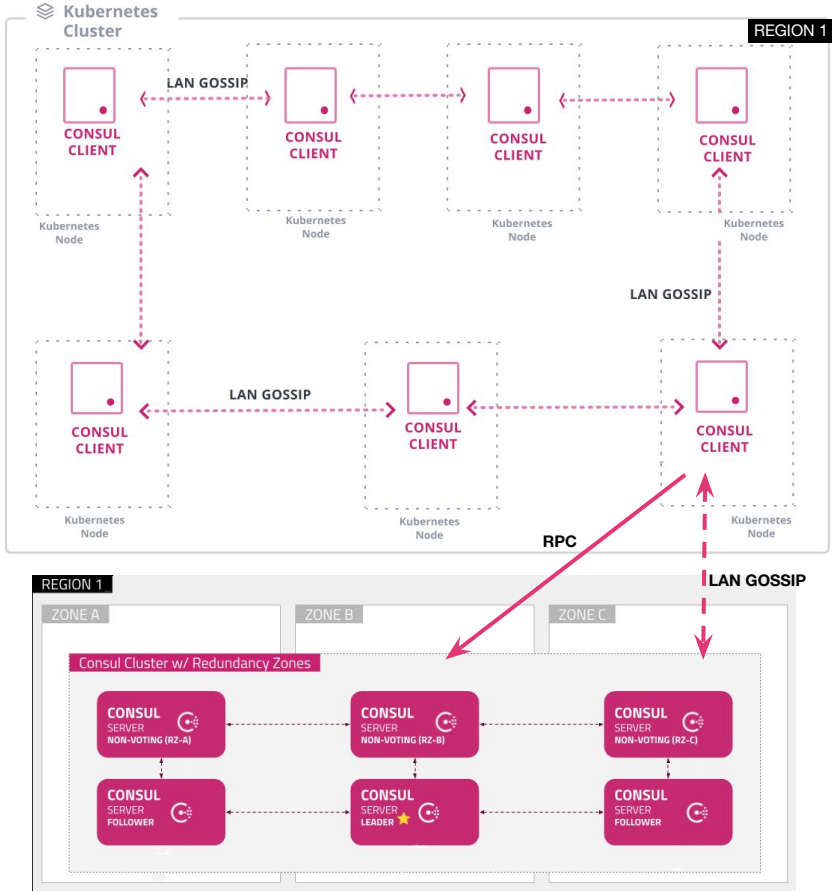
Consul in Kubernetes Reference Architecture

- Helm deployment is recommended
- Install Consul into a dedicated Kubernetes namespace
- Consul on Kubernetes requires persistent volumes (PV)
- RBAC needs enabled on cluster prior to Consul deployment
- Consul and Kubernetes Deployment Guide
  - Azure AKS Terraform Module
  - Google GKE Terraform Module
  - AWS EKS Terraform Module
  - Redhat OpenShift Deployment Guide



External Kubernetes Deployment

- Consul datacenter external to Kubernetes cluster manages services within a cluster
- Kubernetes-defined services sync to Consul
- Catalog sync allows services to sync between Consul and Kubernetes, sync can be unidirectional or bidirectional
- Services synced from Kubernetes are discoverable
- Consul Client deployed via Helm
- Consul datacenter must exist in same region as the Kubernetes cluster



Sizing

Per instance sizing recommendations

	Small (Dev/Test/Staging/ QA)	Large (Production)
CPU	2 - 4 Core	8 - 16 Core
Memory	8 - 16 GB RAM	32 - 64 GB RAM
Disk Capacity	100+ GB	200+ GB
Disk IO	3000+ IOPS	75000+ IOPS
Disk Throughput	75+ MB/s	250+ MB/s

Instance Sizing

Kubernetes

CODE EDITOR

```
server:
  resources:
    requests:
      memory: "16Gi"
      cpu: "4"
    limits:
      memory: "16Gi"
      cpu: "4"
  storage: 50Gi
```

Cloud Instance Sizing

Provider	Size	Instance/VM Types	Disk Volume Specs
AWS	Small	m5.large, m5.xlarge	100+ GB gp3, 3,000 IOPS 125 MB/s
	Large	m5.2xlarge, m5.4xlarge	200+ GB gp3, 10,000 IOPS 250 MB/s
Azure	Small	standard_d2s_v3, standard_d4s_v3	1024 GB Premium SSD, 5,000 IOPS 200 MB/s
	Large	standard_d8s_v3, standard_d16s_v3	2048 GB Premium SSD, 7,500 IOPS 200 MB/s
GCP	Small	n2-standard-2, n2-standard-4	512 GB pd-balanced, 15,000 IOPS 240 MB/s
	Large	n2-standard-8, n2-standard-16	1000 GB pd-ssd, 30,000 IOPS 480 MB/s

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 is 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.

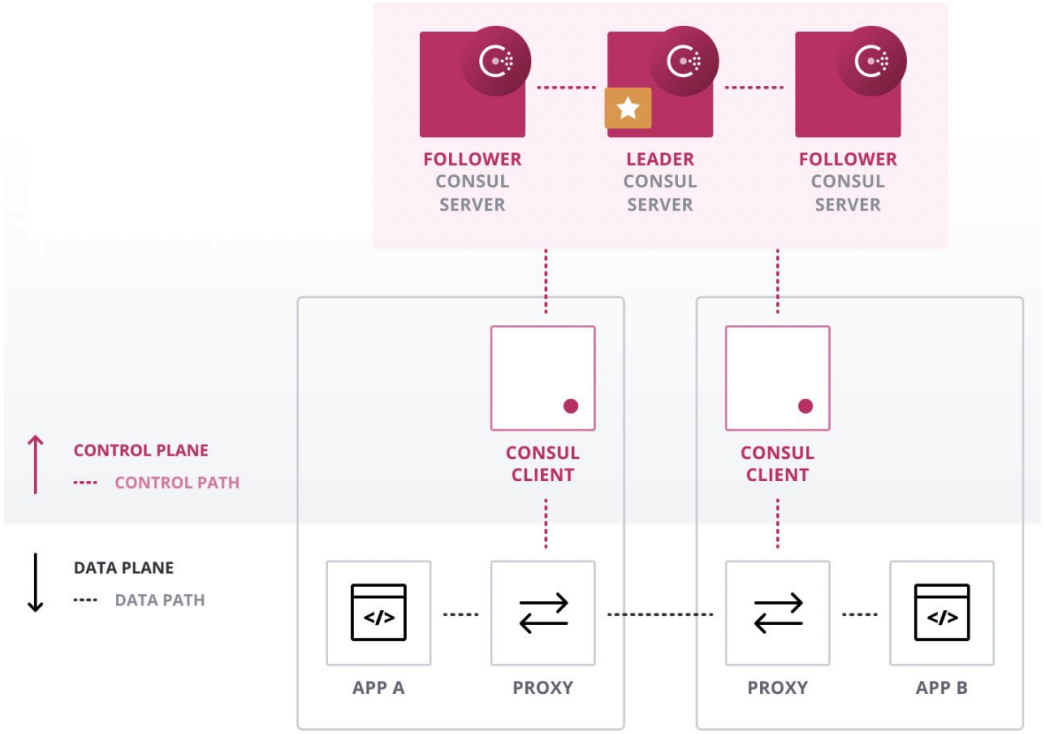
Consul Architecture

Consul has a client-server architecture and is the **control plane** for the service mesh.

- Multiple Consul servers for high availability
  - Holds single source of truth including K/V, sessions, ACLs, prepared query, service catalog and access policies
- Consul client runs on each node
  - Manages registered services and health checks for that node
  - Manages certificates and access policies and configures the proxy
  - Forwards client requests to a Consul server, manages server connections

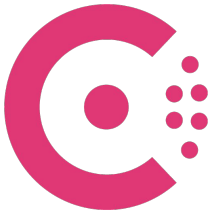
Data plane

- Applications via the local proxies (built-in or third party), which communicate directly with the destination services.



Consul Agent

- Consul agent gets deployed on **every** Consul **server node**
- Consul agent gets deployed on **every client** that participates in service discovery, service mesh, and/or active health checks
- Gets deployed on **every** Kubernetes **worker node**
- Only non-default values must be set in agent configuration file
- Configuration can be read from multiple files



Consul Agent

Configuration Example

TERMINAL

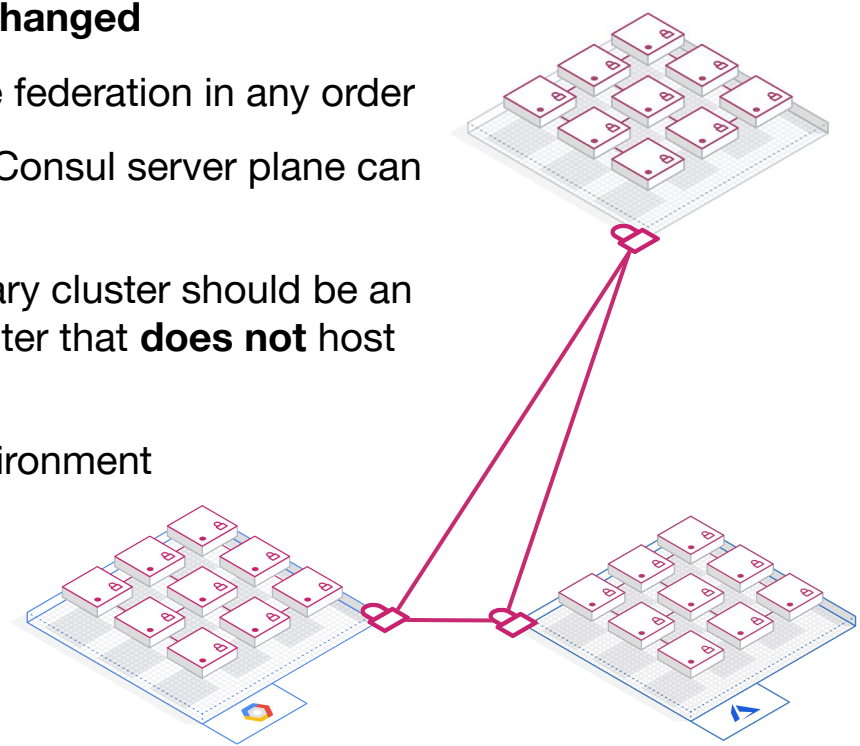
```
$ sudo mkdir /etc/consul.d
$ sudo touch /etc/consul.d/consul.hcl
$ sudo chown - - recursive consul:consul /etc/consul.d
$ sudo chmod 640 /etc/consul.d/consul.hcl


$ cat /etc/consul.d/consul.hcl

datacenter = "dc1"
data_dir = "/opt/consul"
encrypt = "qDOPBEr+/oUVeOFQOnVypxwDaHzLrD+lvjo5vCEBbZ0="
verify_incoming = true
verify_outgoing = true
verify_server_hostname = true
```

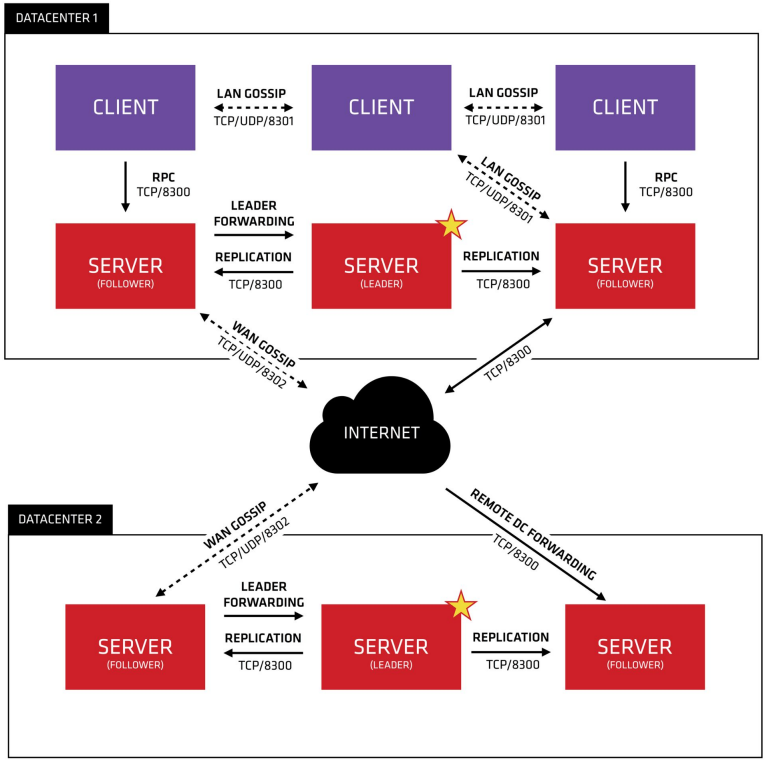
Consul Datacenter Creation

- 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



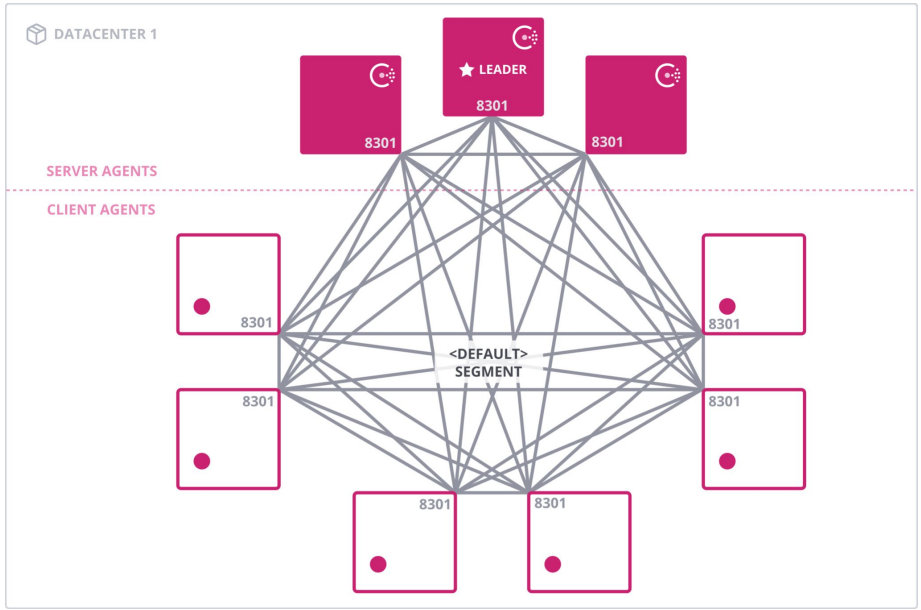
Advanced Architectural Concepts

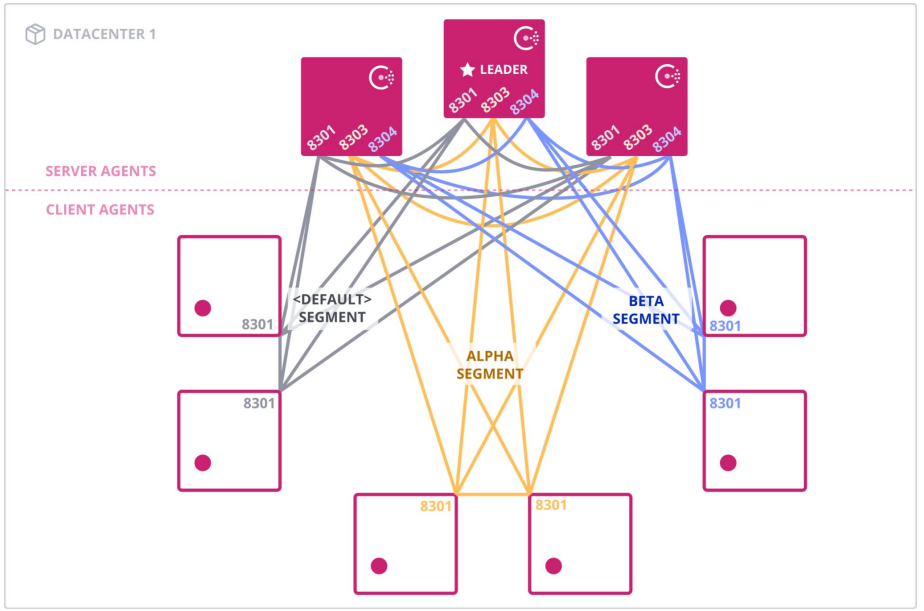
- Network Segments
- WAN Gossip & Data Replication
- WAN Federation



Network Segmentation

Default

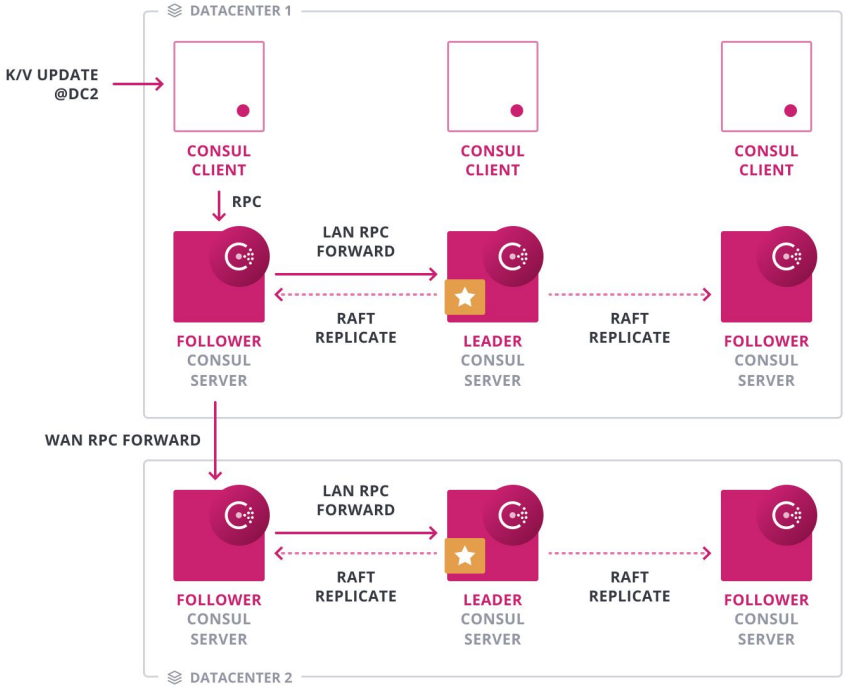




Segmented

WAN Data Replication

- Remote requests are forwarded to remote data centers.
  - This includes key/value data; each datacenter has its own store.
  - There is no built-in replication between datacenters, though tools like consul-replicate are available if you need it.
- ACLs always reside in a single “ACL” datacenter. Other data centers can be configured to cache to ride out partitions.
- Consul Enterprise enables replication of intentions and cross-data center certificate management.

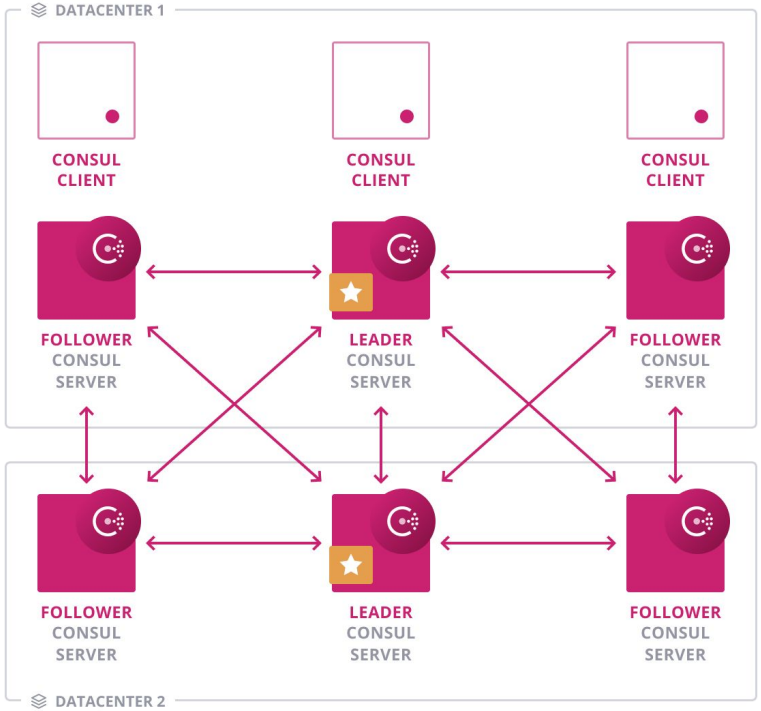


WAN Federation

Consul server from multiple data centers form a globally unique WAN cluster.

Responsible for:

- Membership information allows servers to perform cross datacenter requests
- Integrated failure detection allows to gracefully handle an entire datacenter losing connectivity or a single server in a remote data center
- Consul Enterprise enables advanced communication patterns to support complex network topologies



04

Deployment Patterns

Recommended Patterns

Immutable Builds

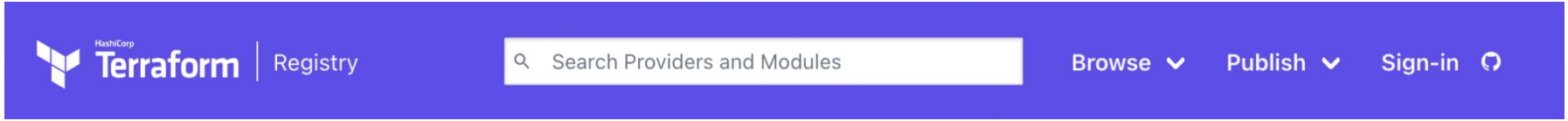
Tooling like Packer can be used to build immutable images of Consul and perform blue/green deployment using your existing CI/CD orchestration. This can streamline your lifecycle processes.

Configuration Management

For organizations who have not adopted the above pattern, Consul can be integrated into your configuration management patterns to install, upgrade, and configure Consul.

Terraform Modules

Quickly deploy Consul cluster(s) based on reference architecture



Terraform modules provide an immutable foundation for deployment of Consul in Cloud Providers & Cloud Managed Kubernetes

- Consul Enterprise GCP Module (VM)
- Consul Enterprise Azure Module (VM)
- Consul Enterprise AWS Module (VM)
- Azure AKS Terraform Module (K8S)
- Google GKE Terraform Module (K8S)
- AWS EKS Terraform Module (K8S)

Upgrades

- Major releases of Consul Enterprise are released quarterly, minor releases occur monthly and as needed.
- The process to update Consul Enterprise should be automated as much as possible to ensure Consul remains patched with the latest bug and security fixes.
- We ensure upgrade compatibility with **N-2 major releases**. Major upgrades should a minimum of 2X per year to stay within version support window.
- Prior to any upgrade review the changelog and version specific upgrade guide, test against version in QA environment, and ensure up to date snapshots in case a restore is required.

Migration from Consul OSS to Enterprise

- Once an instance has been upgraded to Consul Enterprise it cannot be downgraded to OSS
- Consul Enterprise 1.10.0+ requires license files be loaded from configuration or environment variables
- In-place migration via standard upgrade procedure
  - Backup instance via Consul snapshot
  - Identify Leader Node and leave for last
  - Replace binary on follower node
  - Add licensing configuration and cycle node
  - Repeat on all follower nodes
  - Replace binary and add licensing to leader node

05

Operations

Consul Production Readiness

Review the Consul Production Readiness Checklist prior to deploying the first datacenter into production.

Key elements to review:

- Backup & Restore Procedures
- Outage Recovery Procedures & Runbooks
- Foundational Security Policies Enabled
- Server Performance Parameters
- Telemetry & Monitoring

Backup & Restore

The Consul Snapshot Agent, an enterprise feature, runs as a service and takes periodic snapshots of Consul

- Snapshots are atomic, point-in-time, and datacenter specific
- Snapshots include:
  - Key/Value Store Entries
  - Service Catalog Registrations
  - Prepared Queries
  - Session
  - Access Control Lists (ACLs)
  - Namespaces
- Determine snapshot storage location (S3, Azure Blob storage, etc)
- Configure interval and retention based on your RPO/RTO requirements.
- Test the restore process on a regular basis and update your runbook after major upgrades

Outage Recovery Procedures & Runbooks

- Snapshots are used to restore a cluster from an outage or unrecoverable quorum loss
- Snapshots are datacenter specific, ensure naming conventions are clearly defined
- At recovery Consul agents might also need to be re-installed / reconfigured
- Automation for DR tasks and procedures can improve RTO
- Token persistence and ACL token specification in agent configuration settings will impact agents after a restoration

Token persistence enabled	ACL token provided in Consul client config	Consul client requires a re-configuration
Yes	No	No
No	Yes	No
Yes	Yes	No
No	No	Yes

Disaster Recovery for Consul on Kubernetes

- Consul on Kubernetes requires backing up 4 essential secrets:
  - The last active Consul ACL bootstrap token
  - The last active Consul CA cert
  - The last active Consul CA key
  - The last active gossip encryption key

- Without these 4 secrets you **cannot recover** from a disaster
- These secrets need to be secure and stored **outside** the Kubernetes secrets engine
- Update and take a new Consul snapshot whenever secrets are rotated
- Automate the rotation and backup procedure(s)

Foundational Security Policies

Implementing three baseline security configurations is a critical step prior to go-live with your first production Consul datacenter.

- Enable TLS encryption for RPC traffic and consensus (gossip) communication incoming and outgoing
- Configure a Certificate Authority and ensure agent certificate have been distributed to all agents
- Enable ACLs and verify that tokens have been created for all agents and services

Enable Gossip Traffic Encryption

The Consul agent **needs** an encryption key when starting

- Key can be set with the encrypt parameter in agent config
- Key can also be placed in a separate config file with only the encrypt field, Consul agent can merge multiple config files
- Keys must be 32-bytes, Base64 encoded
- Consul **`keyring`** is used for rotation and lifecycle management of encryption keys

Enable Gossip Encryption

New Consul datacenter

TERMINAL

```
$ consul keygen
o9fgtzMpKFBA5TcHaCzJWMxxU4dTreuxBGhRE/iocA57

$ cat /etc/consul.d/consul.hcl
data_dir = "/opt/consul"
log_level = "INFO"
node_name = "app-svr01"
encrypt = "o9fgtzMpKFBA5TcHaCzJWMxxU4dTreuxBGhRE/iocA57"


$ consul agent -config-dir=/etc/consul.d/
 ==> Starting Consul agent...
            Version: '1.8.1+ent'
            Node ID: 'b5b5a237-458d-c9eb-b301-db1445e50b80'
          Node name: 'bulldog'
         Datacenter: 'dc1' (Segment: '<all>')
             Server: true (Bootstrap: false)
        Client Addr: [127.0.0.1] (HTTP: 8500, HTTPS: -1, gRPC: 8502,
DNS: 8600)
       Cluster Addr: 127.0.0.1 (LAN: 8301, WAN: 8302)
            Encrypt: Gossip: true, TLS-Outgoing: false, TLS-Incoming:
false, Auto-Encrypt-TLS: false
```

ACL Token Setup

- ACL bootstrapping is a 2 step process
  - Enable ACLs
  - Create the bootstrap token
- Add ACL parameters to agent configuration file and restart Consul

```
agent.hcl

acl = {
  enabled = true
  default_policy = "deny"
  enable_token_persistence = true
}
```

- ACL parameters must match on every server and client in a datacenter
- Create the initial bootstrap token

```
consul acl bootstrap
```

- Apply tokens to agents and configure policy
- Secure Consul with ACLs Learn Guide

Server Performance Parameters

- By default “raft_multiplier” value is set to a non-production value (“5”)
- Most production instances should have “raft_multiplier” set to “1”
- Consul is typically write limited by disk I/O and read limited by CPU
- Server Performance Documentation

Telemetry & Monitoring

Consul should be monitored closely to ensure the service remains healthy and available in production.

- **Telemetry** - Export telemetry data to a solution that can analyze and identify trends overtime.
- **Enable Audit Logs** - Capture a record of all events so audit teams can inspect event data including credentials used, and timestamps of transactions.
- **Monitor Consul health and Server health** - The Consul health metrics reveal information about the Consul datacenter while the server metrics provide information about the health of your datacenter

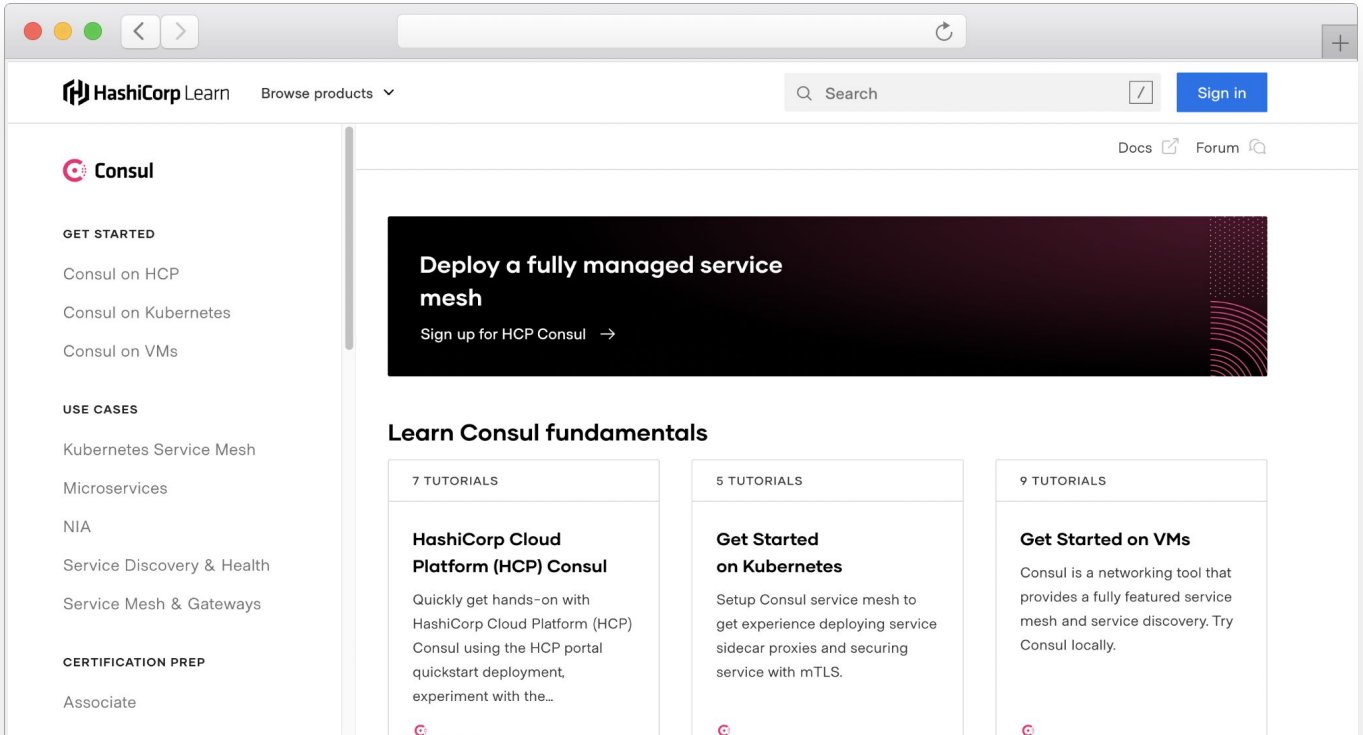
06

Next Steps

Learn

https://learn.hashicorp.com/consul

Step-by-step guides to accelerate deployment of Consul



Resources

- Consul Reference Architecture
- Terraform starter code (VM installation) for AWS, Azure, and GCP
- Consul and Kubernetes Reference Architecture
- Consul Helm Chart
- Terraform starter code for managed Kubernetes:
  - AWS EKS
  - Azure AKS
  - Google GKE
- Consul Upgrade Guide
- Consul Production Readiness Checklist
- Consul Metrics List

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

Technical Support

Something not working quite right? Engage with HashiCorp Technical Support by opening a ticket for your issue at support.hashicorp.com.

Discuss

Engage with the HashiCorp Cloud community including HashiCorp Architects and Engineers

discuss.hashicorp.com

Upcoming Onboarding Webinars

Next Week's Webinar:

Operationalizing Consul

Topics include: Consul autopilot and upgrade patterns, DR operations, federation, namespaces, admin partitions, and telemetry and monitoring

Office Hour

An interactive open forum to discuss specific questions about your environment and Use Cases.

Please bring your questions!

Webinar:

Service Discovery and Health Monitoring

Topics include: implementing Consul service catalogue, health checks, and prepared queries for geo-failover

Thank You

customer.success@hashicorp.com
www.hashicorp.com/customer-success