Consul control plane architecture

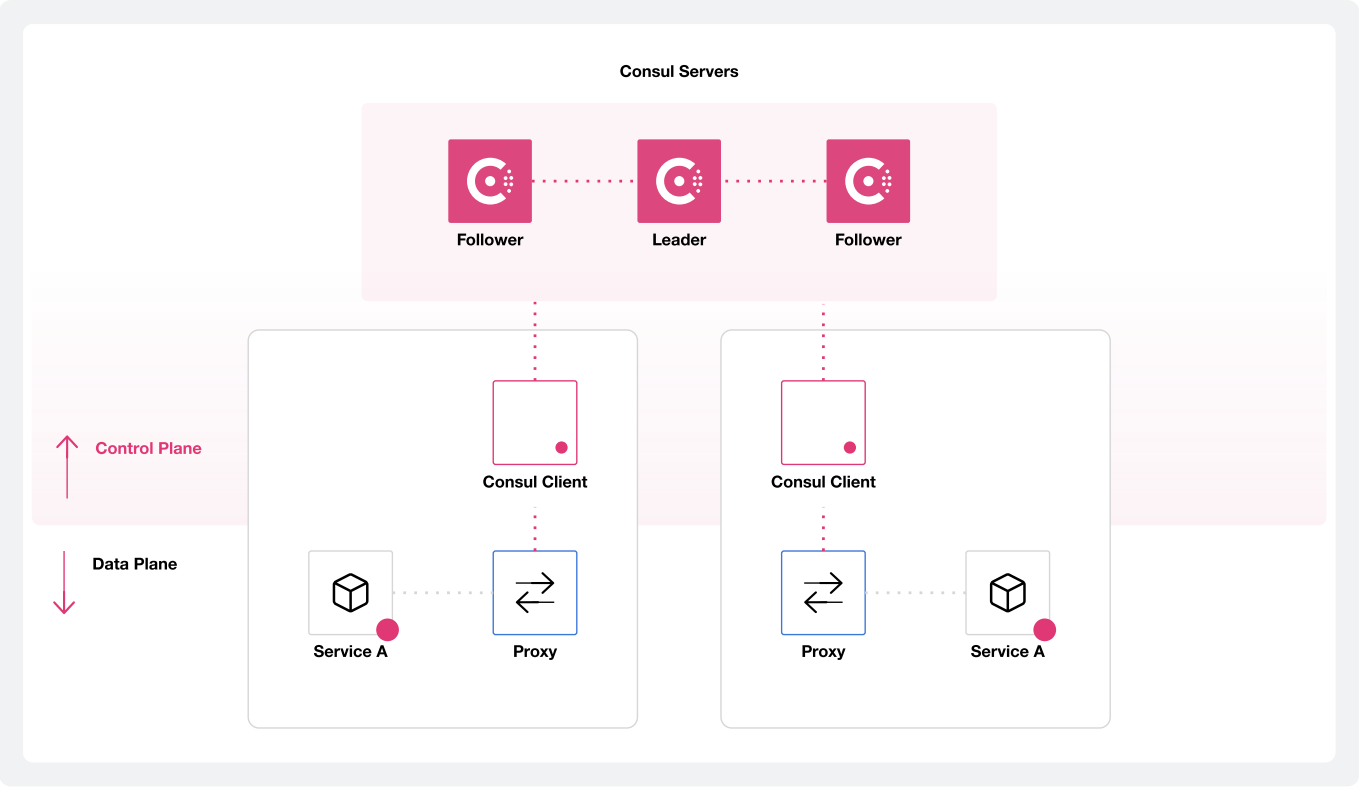
This topic provides an overview of the Consul architecture. We recommend reviewing the Consul glossary as a companion to this topic to help you become familiar with HashiCorp terms.

> Refer to the Reference Architecture tutorial for hands-on guidance about deploying Consul in production.

Introduction

Consul provides a control plane that enables you to register, access, 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.

When using Consul's service mesh capabilities, Consul dynamically configures sidecar and gateway proxies in the request path, which enables you to authorize service-to-service connections, route requests to healthy service instances, and enforce mTLS encryption without modifying your service's code. This ensures that communication remains performant and reliable. Refer to Service Mesh Proxy Overview for an overview of sidecar proxies.



Datacenters

The Consul control plane contains one or more *datacenters*. A datacenter is the smallest unit of Consul infrastructure that can perform basic Consul operations. A datacenter contains at least one Consul server agent, but a real-world deployment contains three or five server agents and several Consul client agents. You can create multiple datacenters and allow nodes in different datacenters to interact with each other. Refer to Bootstrap a Datacenter for information about how to create a datacenter.

Clusters

A collection of Consul agents that are aware of each other is called a *cluster*. The terms *datacenter* and *cluster* are often used interchangeably. In some cases, however, *cluster* refers only to Consul server agents, such as in HCP Consul Dedicated. In other contexts, such as the *admin partitions* feature included with Consul Enterprise, a cluster may refer to collection of client agents.

Agents

You can run the Consul binary to start Consul *agents*, which are daemons that implement Consul control plane functionality. You can start agents as servers or clients. Refer to Consul agent for additional information.

Server agents

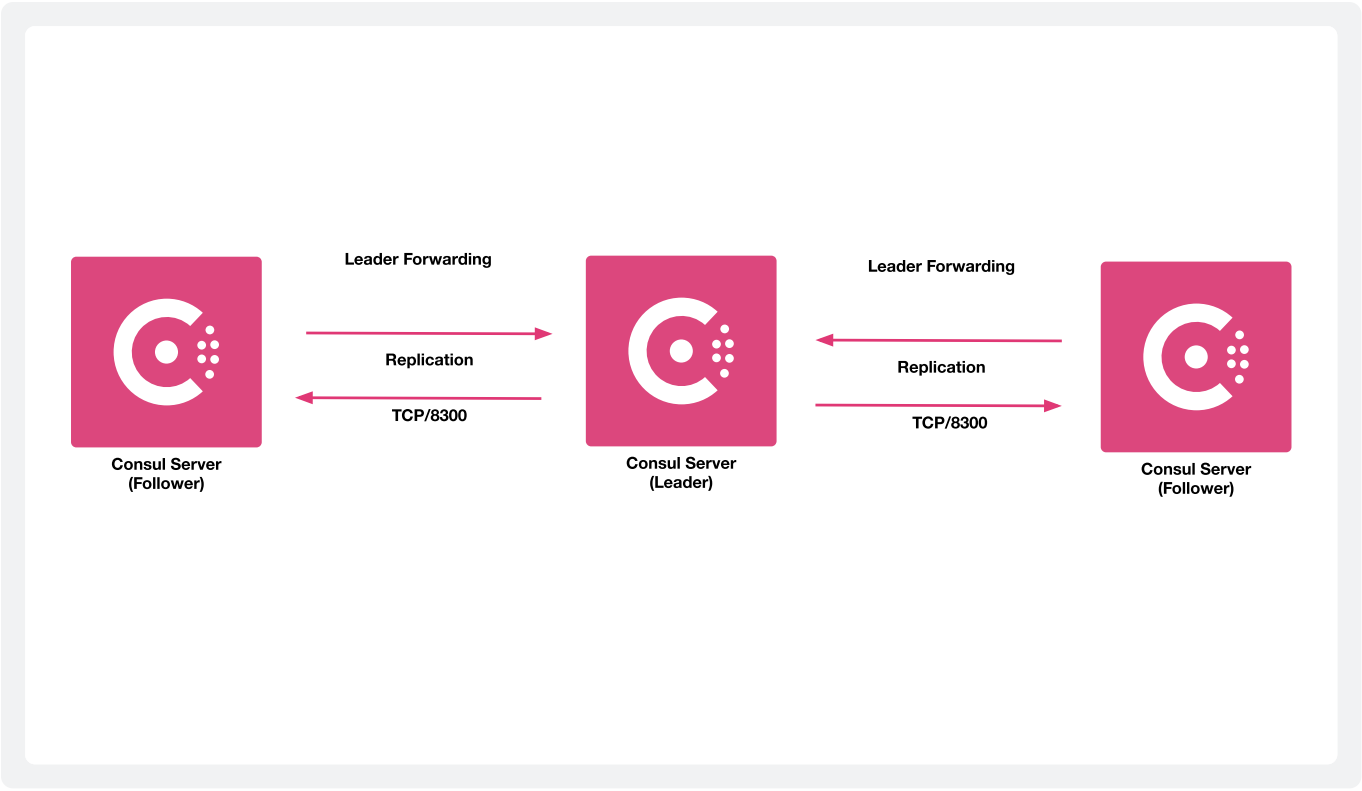
Consul server agents store all state information, including service and node IP addresses, health checks, and configuration. We recommend deploying three or five servers in a cluster. The more servers you deploy, the greater the resilience and availability in the event of a failure. More servers, however, slow down cluster consensus, which is a critical server function that enables Consul to efficiently and effectively process information.

Consensus protocol

Consul clusters elect a single server to be the *leader* through a process called *consensus*. The leader processes all queries and transactions, which prevents conflicting updates in clusters containing multiple servers.

Servers that are not currently acting as the cluster leader are called *followers*. Followers forward requests from client agents to the cluster leader. The leader replicates the requests to all other servers in the cluster. Replication ensures that if the leader is unavailable, other servers in the cluster can elect another leader without losing any data.

Consul servers establish consensus using the Raft algorithm on port `8300`. Refer to Consensus Protocol for more information.



Client agents

Consul clients report node and service health status to the Consul cluster. In a typical deployment, you must run client agents on every compute node in your datacenter. Clients use remote procedure calls (RPC) to interact with servers. By default, clients send RPC requests to the servers on port `8300`.

There are no limits to the number of client agents or services you can use with Consul, but production deployments should distribute services across multiple Consul datacenters. Using a multi-datacenter deployment enhances infrastructure resilience and limits control plane issues. We recommend deploying a maximum of 5,000 client agents per datacenter. Some large organizations have deployed tens of thousands of client agents and hundreds of thousands of service instances across a multi-datacenter deployment. Refer to Cross-datacenter requests for additional information.

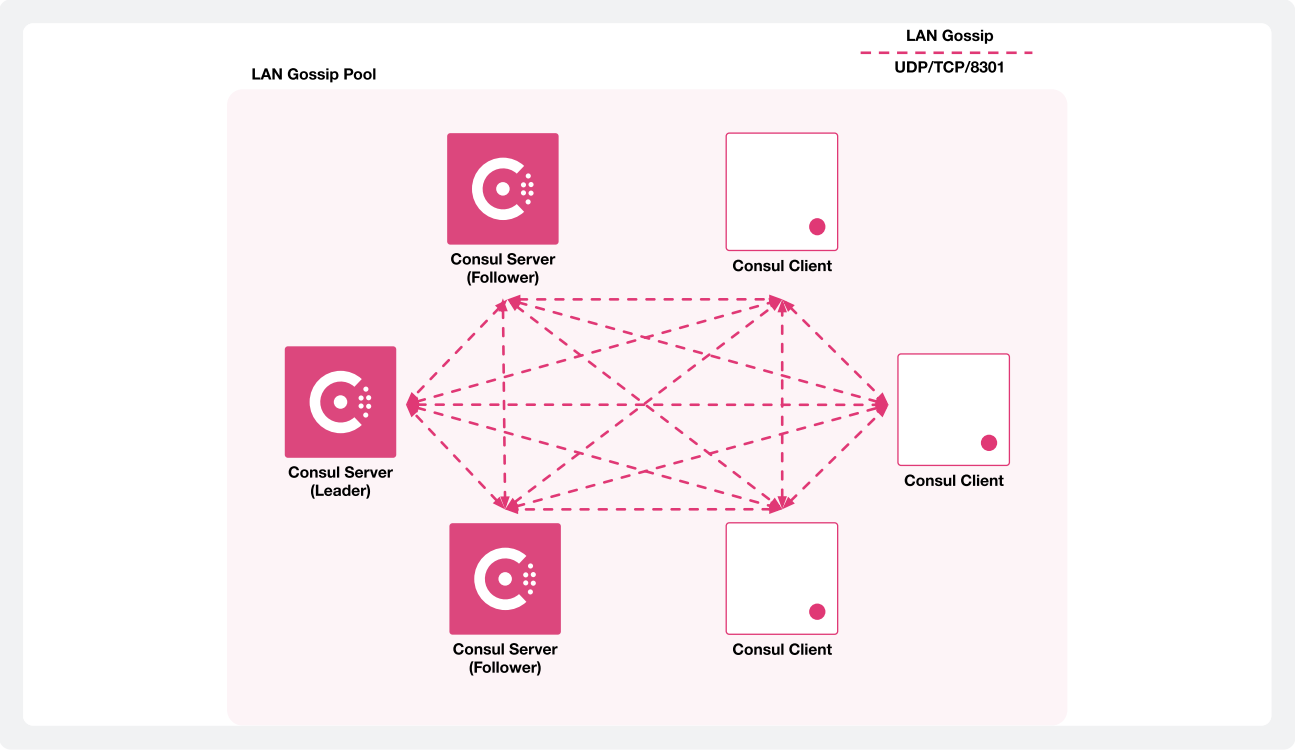
You can also run Consul with an alternate service mesh configuration that deploys Envoy proxies but not client agents. Refer to Simplified Service Mesh with Consul Dataplanes for more information.

LAN gossip pool

Client and server agents participate in a LAN gossip pool so that they can distribute and perform node health checks. Agents in the pool propagate the health check information across the cluster. Agent gossip communication occurs on port `8301` using UDP. Agent gossip falls back to TCP if UDP is not available. Refer to gossip protocol for additional information.

The following simplified diagram shows the interactions between servers and clients.

LAN gossip pool | RPC



Cross-datacenter requests

Each Consul datacenter maintains its own catalog of services and their health. By default, the information is not replicated across datacenters. WAN federation and cluster peering are two multi-datacenter deployment models that enable service connectivity across datacenters.

WAN federation

WAN federation is an approach for connecting multiple Consul datacenters. It requires you to designate a *primary datacenter* that contains authoritative information about all datacenters, including service mesh configurations and access control list (ACL) resources.

In this model, when a client agent requests a resource in a remote secondary datacenter, a local Consul server forwards the RPC request to a remote Consul server that has access to the resource. A remote server sends the results to the local server. If the remote datacenter is unavailable, its resources are also unavailable. By default, WAN-federated servers send cross-datacenter requests over TCP on port `8300`.

You can configure control plane and data plane traffic to go through mesh gateways, which simplifies networking requirements.

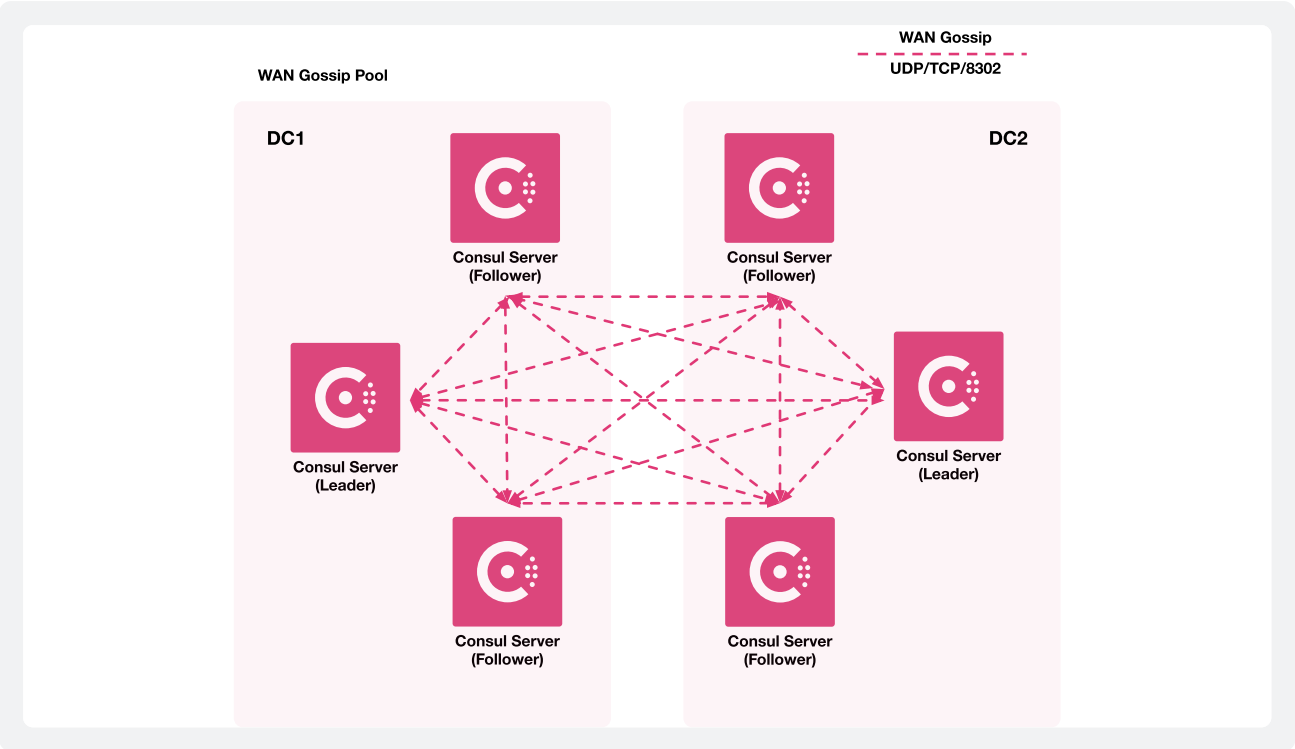
> **Hands-on**: To enable services to communicate across datacenters when the ACL system is enabled, refer to the ACL Replication for Multiple Datacenters tutorial.

WAN gossip pool

Servers may also participate in a WAN gossip pool, which is optimized for greater latency imposed by the Internet. The pool enables servers to exchange information, such as their addresses and health, and gracefully handle loss of connectivity in the event of a failure.

In the following diagram, the servers in each data center participate in a WAN gossip pool by sending data over TCP/UDP on port `8302`. Refer to Gossip Protocol for additional information.

WAN gossip pool | Remote datacenter forwarding



Cluster peering

You can create peering connections between two or more independent clusters so that services deployed to different datacenters or admin partitions can communicate. An admin partition is a feature in Consul Enterprise that enables you to define isolated network regions that use the same Consul servers. In the cluster peering model, you create a token in one of the datacenters or partitions and configure another datacenter or partition to present the token to establish the connection.

Refer to cluster peering overview for additional information.

Edit this page on GitHub