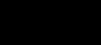
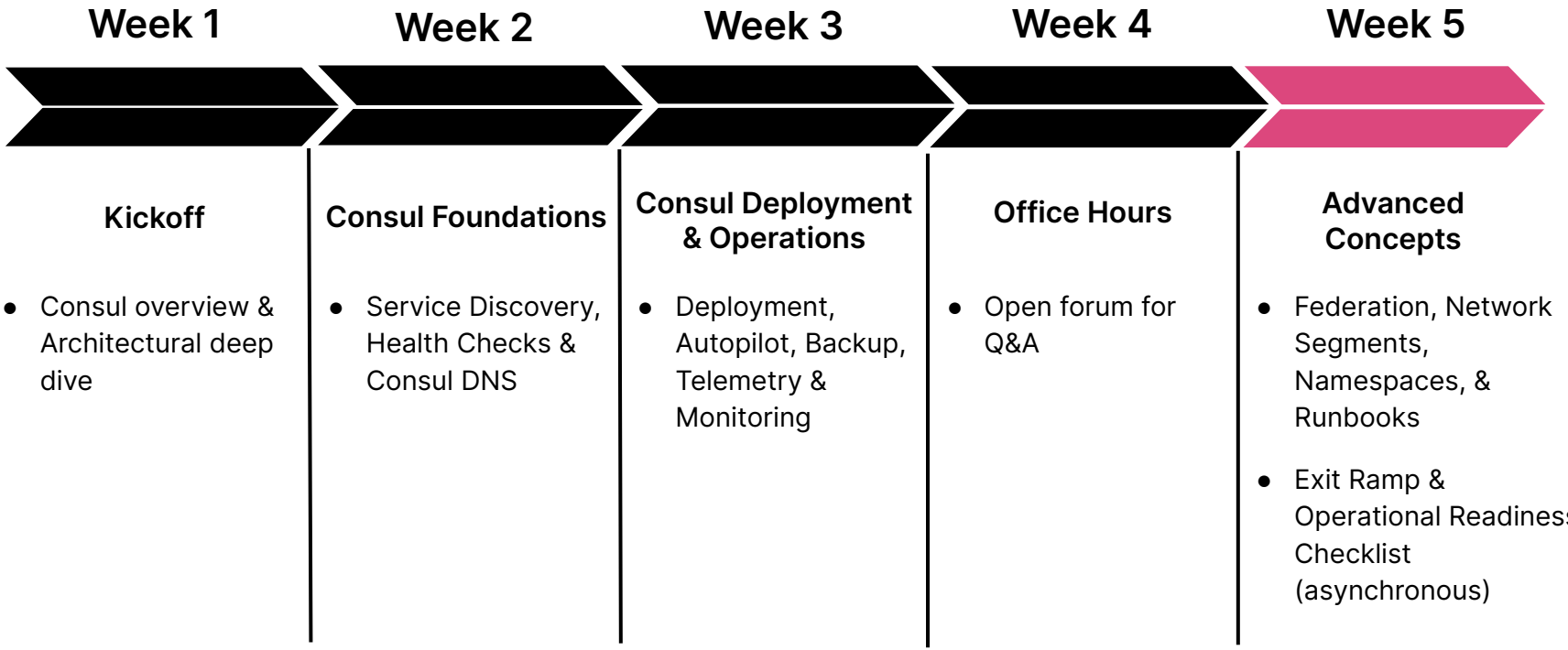
Advanced Concepts



Agenda

Consul Enterprise Path to Production

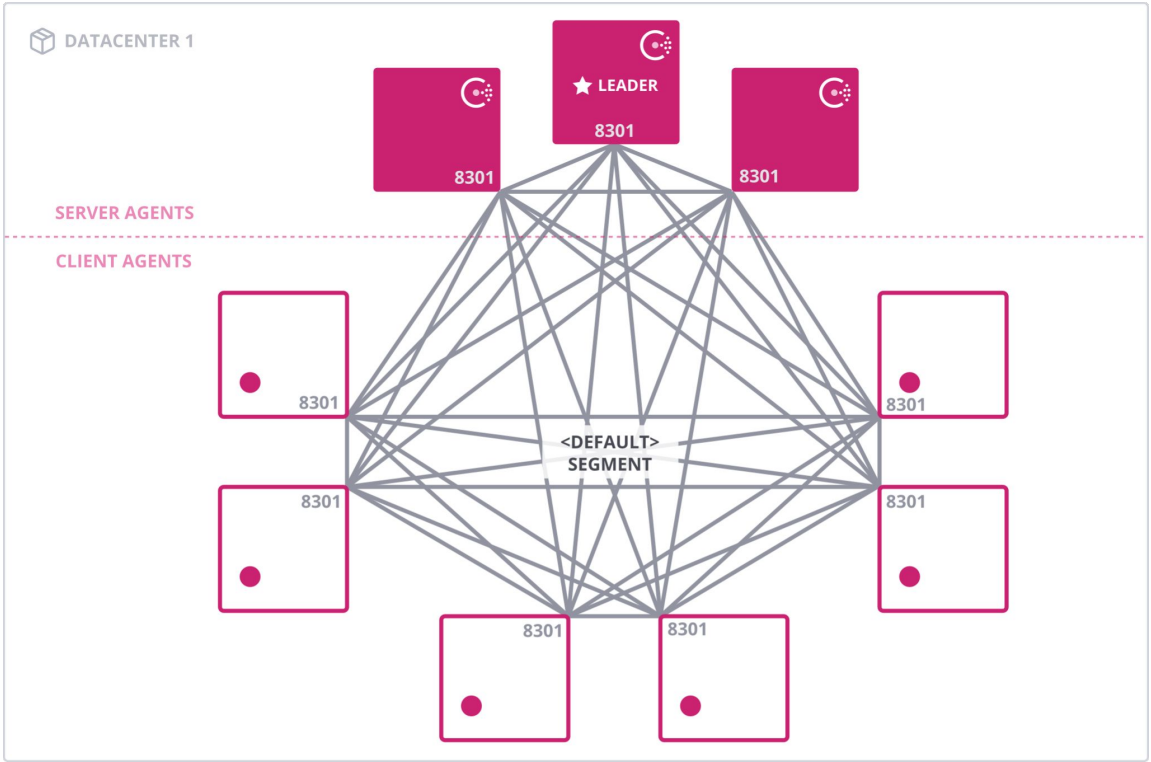


01

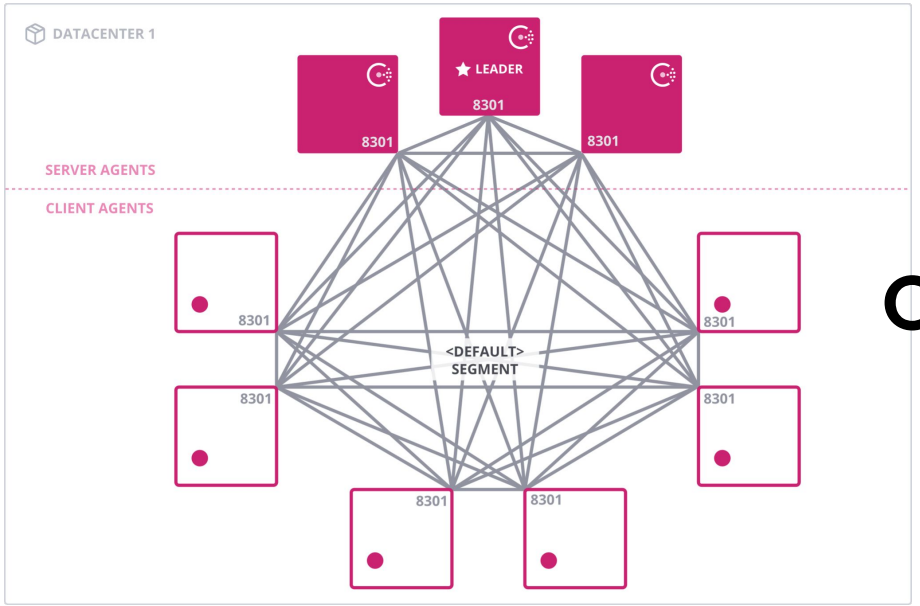
Network Segments

LAN Gossip

- Consul assumes all agents in a datacenter can communicate gossip
- All agents are part of the default gossip pool and network segment
- Full mesh connectivity within the datacenter is required

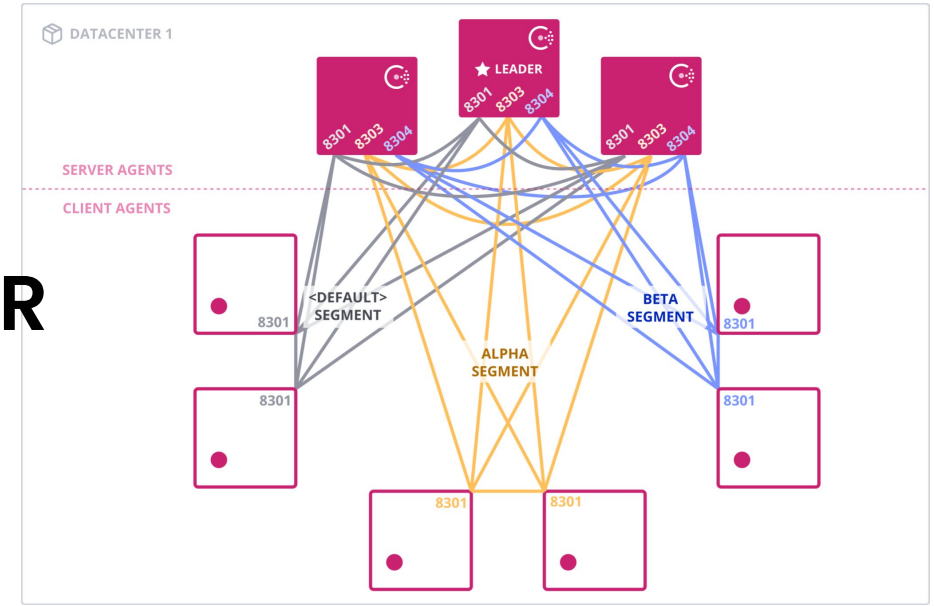


Default LAN Gossip



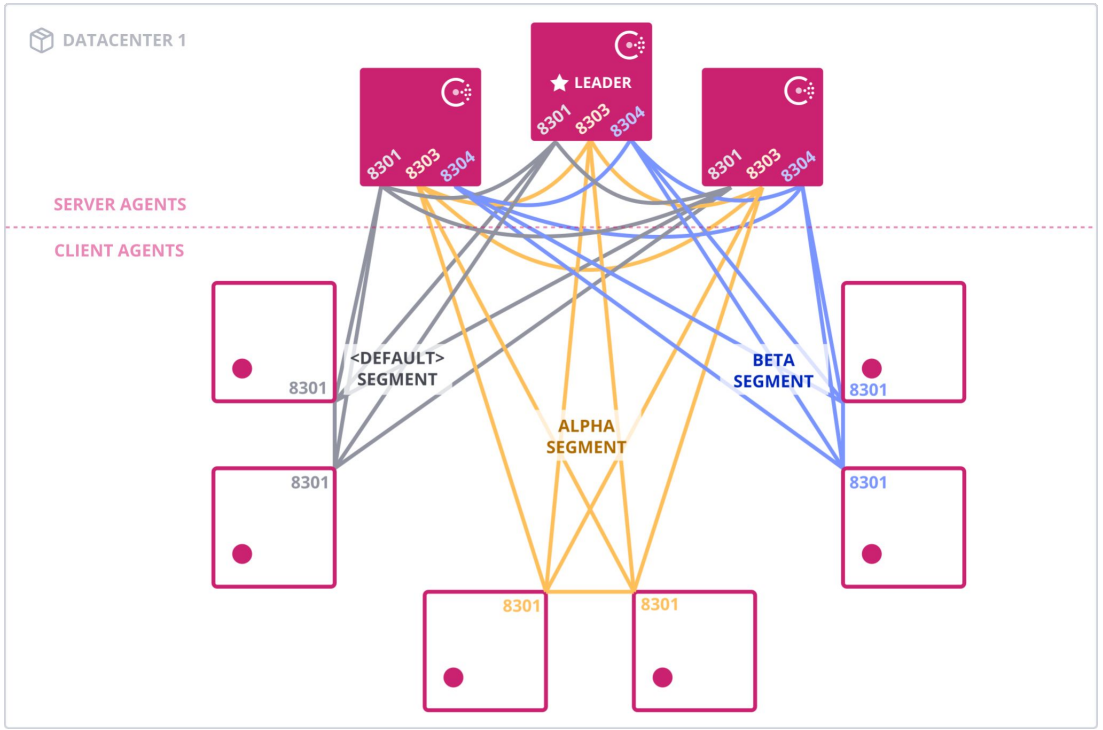
OR

Network Segmentation



Network Segmentation

- Requirements don’t allow full mesh connectivity in a datacenter
- Isolated LAN gossip pools that require connectivity only between agents in the same segment
- Provides the capability to slice LAN gossip along communication boundaries



02

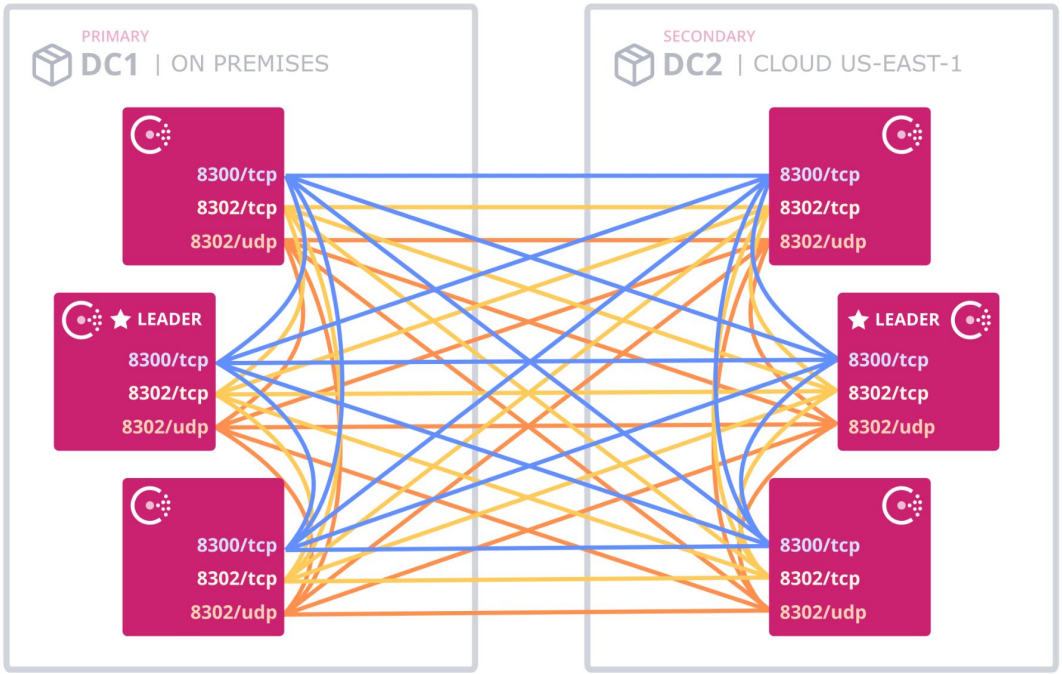
Federation

Consul Federation

- Joins Consul datacenters into a WAN cluster
- Consul servers in federated clusters can communicate with each other
- Federation allows:
  - L7 routing rules can enable multi-cluster failover and traffic splitting
  - Access any datacenter via a drop-down in the UI or a CLI flag
  - Consistent ACL policies across all federated clusters
- Two mechanisms exist:
  - Traditional WAN Federation (shared gossip)
  - WAN Federation via Mesh Gateways (Consul 1.8.0+) - preferred

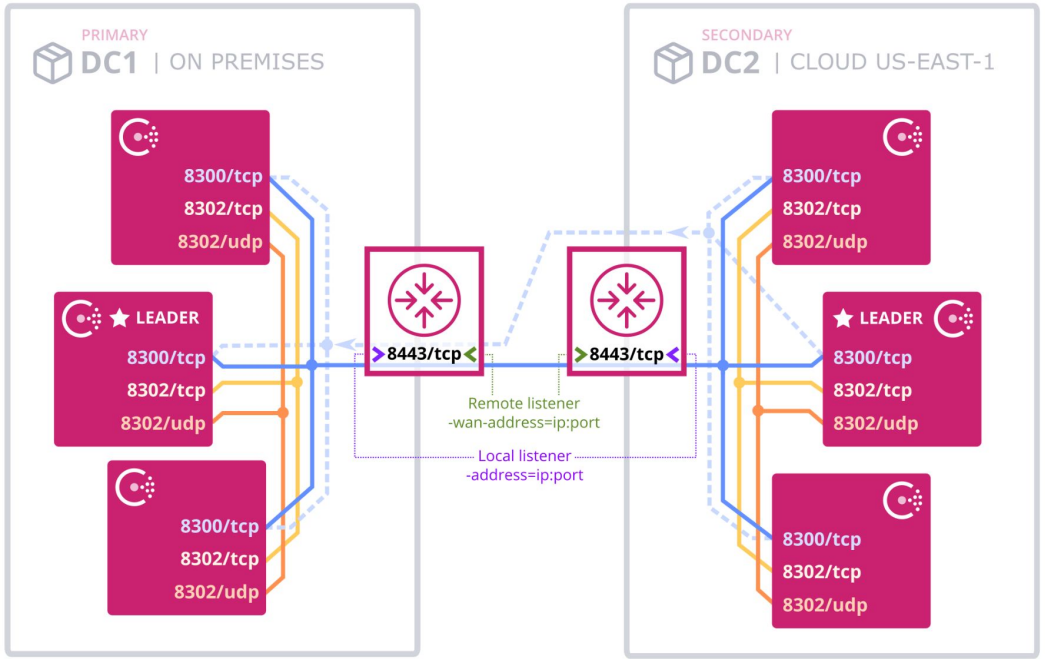
Traditional WAN Federation

- All Consul servers must be exposed on the WAN
- Does not support overlapping IP addresses across federation
- Implementing with Kubernetes requires proxying UDP and TCP
- Cross datacenter service discovery:
  - Multi-dc failover
  - Blue/green deployments
  - Canary testing



WAN Federation over Mesh Gateways

- All Consul traffic passes through Mesh Gateway - including WAN Gossip
- Mesh gateways are exposed with routable addresses, instead of Consul servers
- Secure service communication between clouds without VPN or cloud specific services
- Mesh gateway must be configured for all clusters in the federation



Replication

- In general, data is not replicated between federated Consul datacenters
- Replicated data includes:
  - ACL policies
  - ACL global tokens
  - Service Mesh Configuration Entries
- Consul minimizes the data that is replicated by design

Cluster Peering

- Cluster Peering became GA in Consul 1.14.0
- An alternative model for connecting Consul datacenters which allows for looser coupling than WAN federation
- Establishes peering between two admin partitions, and treats each datacenter as a separate cluster
- List of constraints
- Steps to configure Cluster Peering:
  - Create a peering token in one cluster
  - Use the token to establish peering
  - Export services between clusters
  - Create intentions to authorize services for peers

Cluster Peering

	WAN Federation	Cluster Peering
Connects clusters across datacenters	**Yes**	**Yes**
Shares support queries and service endpoints	**Yes**	**Yes**
Connects clusters owned by different operators	No	**Yes**
Functions without declaring primary datacenter	No	**Yes**
Replicates exported services for service discovery	No	**Yes**
Gossip protocol: Requires LAN gossip only	No	**Yes**
Forwards service requests for service discovery	**Yes**	No
Shares key/value stores	**Yes**	No
Can replicate ACL tokens, policies, and roles	**Yes**	No

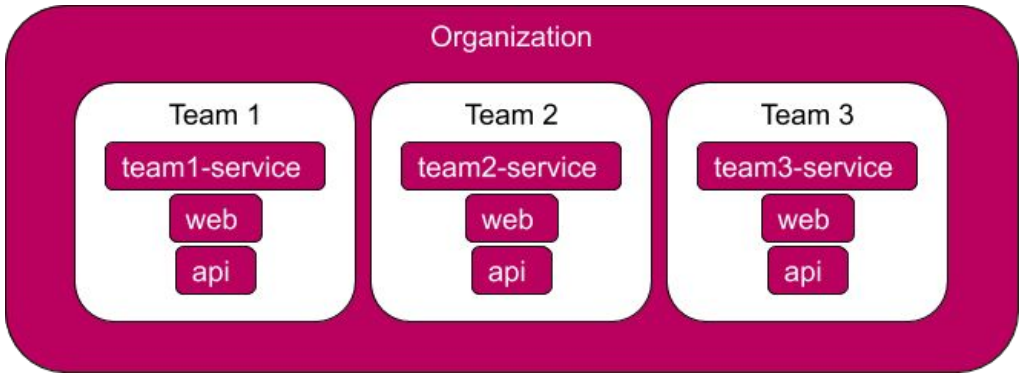
03

Namespaces & Admin Partitions

Consul Namespaces

Provide separation & segmentation of Consul within an organization

- Allow teams to share Consul datacenters with minimal impact potential
- Creates parallel instances of the service catalog and Key/Value Store
- Allows for self service via delegation of admin privileges
- Allow service deployment without coordination between teams of names of services or K/V paths
- Rules like “You can set the intention for *any service in your namespace*” or “You can only query services which exist *in your namespace*” are possible



Namespace Configuration

- Namespaces must be managed via API or the Consul CLI
- API management uses JSON while the CLI will parse either JSON or HCL

```
{
  "Name": "team-1",
  "Description": "Namespace for Team 1",
  "ACLs": {
    "PolicyDefaults": [
      {
        "ID": "77117cf6-d976-79b0-d63b-5a36ac69c8f1"
      },
      {
        "Name": "node-read"
      }
    ],
    "RoleDefaults": [
      {
        "ID": "69748856-ae69-d620-3ec4-07844b3c6be7"
      },
      {
        "Name": "ns-team-2-read"
      }
    ]
  },
  "Meta": {
    "foo": "bar"
  }
}
```

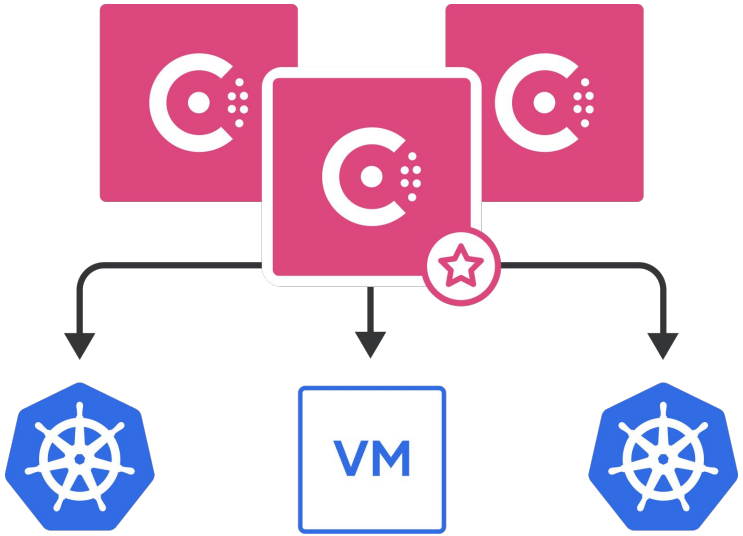
Admin Partitions

- Designed to provide multi-tenancy on a single Consul Datacenter
- Admin partitions exist a level above namespaces in the identity hierarchy, each admin partition contains a default namespace
- Contain one or more namespaces and allow multiple independent tenants to share a Consul server cluster
- Enable operators to define administrative and communication boundaries between services managed by separate teams or belonging to separate stakeholders
- Can be used to segment production and non-production services within a Consul deployment
- Known limitations
    - Only the default admin partition is supported when federating multiple Consul datacenters in a WAN
    - Admin partitions have no theoretical limit, HashiCorp is conducting large-scale testing to identify a recommended max

Before Admin Partitions

Single Consul DC - Multiple Client Cluster

- ➕ Reduces management/cost **BUT**:
- ➖ No overlapping IPs (ex: Kube Pods)
- ➖ Some resources are global (default-proxy)
- ➖ Teams no longer autonomous
- Namespaces help but still limited



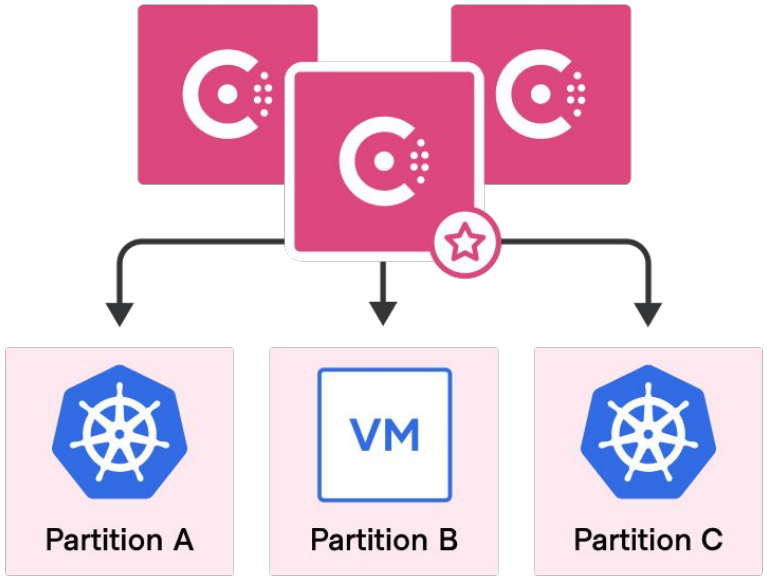
With Admin Partitions

Central operations team manages single Consul DC

- Reduced Management
- Reduce Cost
- Governance/Compliance

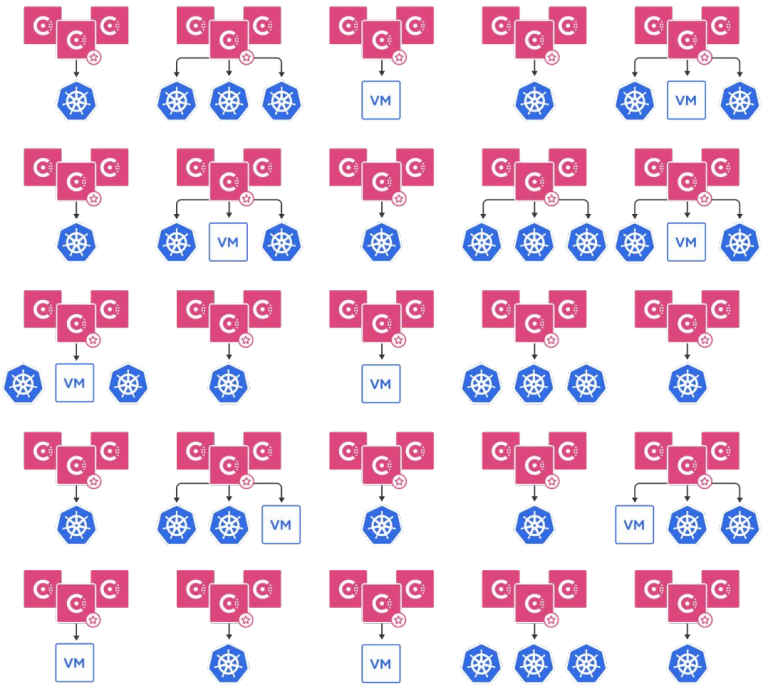
Allows autonomy between teams

- Allows overlapping IPs (ex: Kube Pods)
- More resources scoped inside Partitions (node, proxy-defaults, mesh config entries, namespaces)

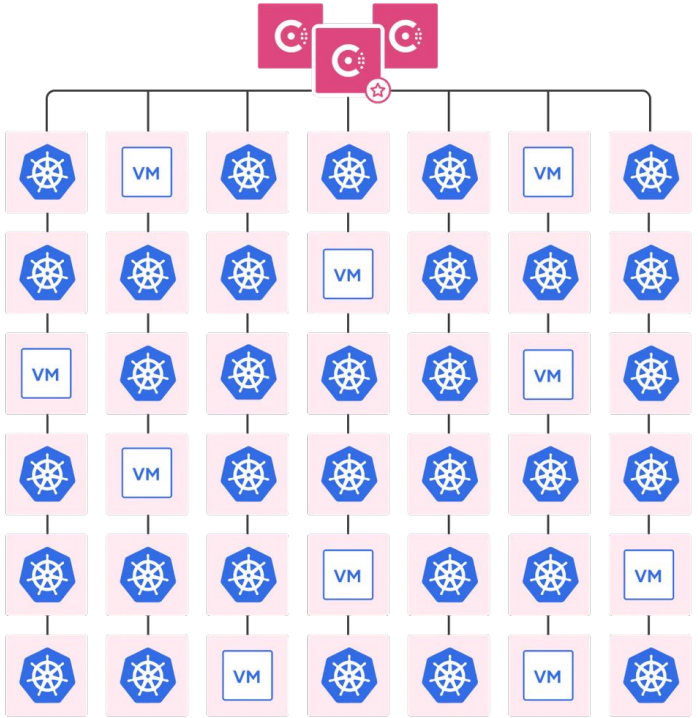


At Scale

Before Admin Partitions



After Admin Partitions



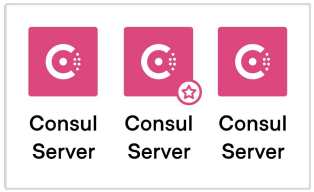
Admin Partition vs. Namespaces

	Namespaces	Admin Partitions
Allow overlapping network between services (example Kubernetes pod IPs)	No	Yes
Support multiple proxy-default config entries per Consul datacenter	No	Yes, 1 per partition
Support multiple mesh config entries per Consul datacenter	No	Yes, 1 per partition
Datacenter scoped config entries between federated Consul datacenters	No	Yes*
Datacenter scoped ACLs between federated Consul datacenters	No	Yes*

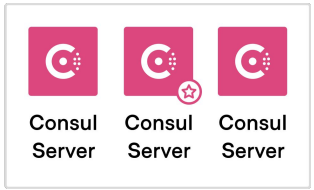
Admin Partition vs. Namespaces

- Very similar from multi-tenancy point of view but AP unlocks more use cases.
- Namespaces provides logical isolations for tenants but some resources are still global like nodes, proxy-defaults, and mesh config entries.
- When in a Federated config with 2 DCs, namespaces will span both DCs. So any config entries created that are not global (ie Service Intentions) will apply to both DCs.
- AP can remain within a single DC even with a federated config.
- AP will include namespaces, nodes, and all config-entries in its scope.
- AP allows for overlapping IP CIDR ranges for applications (ie Kube Pod IPs) between APs. Teams can operate autonomously without having to coordinate IP range with other teams within the same Consul DC.

How to Deploy Consul with Admin Partitions

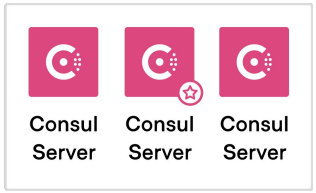


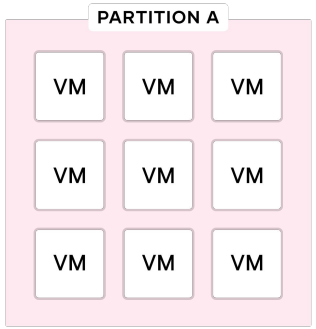
1 Deploy Consul servers (VM or Kubernetes):

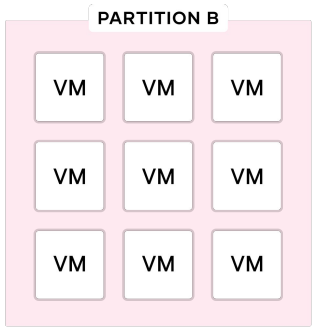


2 Create partitions

```
$consul admin-partition create -name partition-A
$consul admin-partition create -name partition-B
```







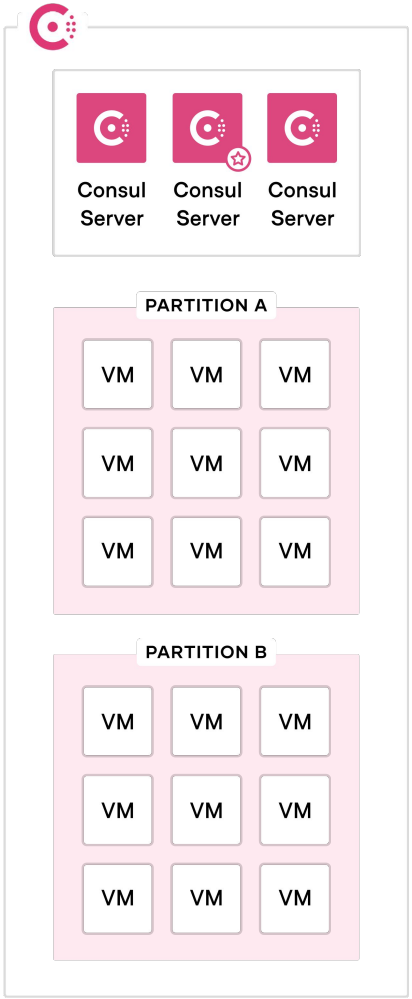
3 Add **partition** parameter to .hcl config file to all client VMs with desired partition name

```
{
  "node_name": "consul-client-X",
  "datacenter": "dc1",
  "partition": "partition-A",
  "data_dir": "/consul/data",
  ...
}
```

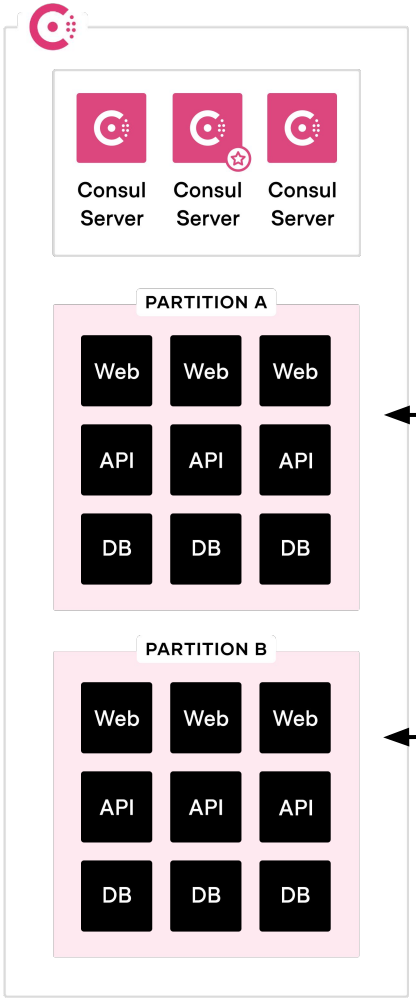
consul-A.hcl file

```
{
  "node_name": "consul-client-X",
  "datacenter": "dc1",
  "partition": "partition-B",
  "data_dir": "/consul/data",
  ...
}
```

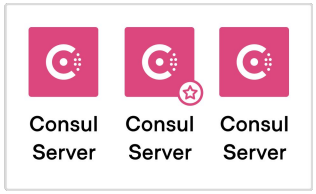
consul-B.hcl file

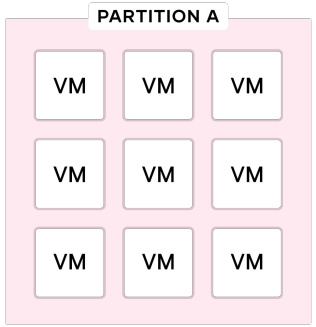


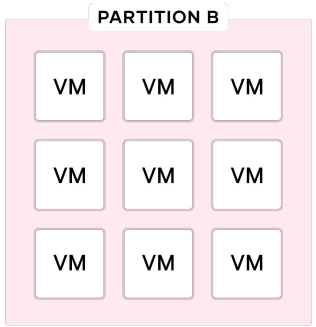
4 Join (or reload) Consul client to Consul datacenter

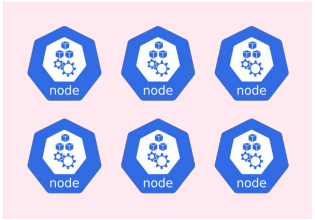


5 Register services from VM in desired partition










```
global:
  enabled: false
  enableConsulNamespaces: true
  image: hashicorp/consul-enterprise:1.11.0-ent-alpha
  adminPartitions:
    enabled: true
    name: "partition-C"
server:
  enterpriseLicense:
    secretName: license
    secretKey: key
externalServers:
  enabled: true
  hosts: ["<partition-service-IP-or-servercluster-IP>"]
  tlsServerName: server.dc1.consul
client:
  enabled: true
  exposeGossipPorts: true
  join: ["<partition-service-IP-or-servercluster-IP>"]
```

helm-C.hcl file

04

Geo Failover & Prepared Queries

Geo Failover

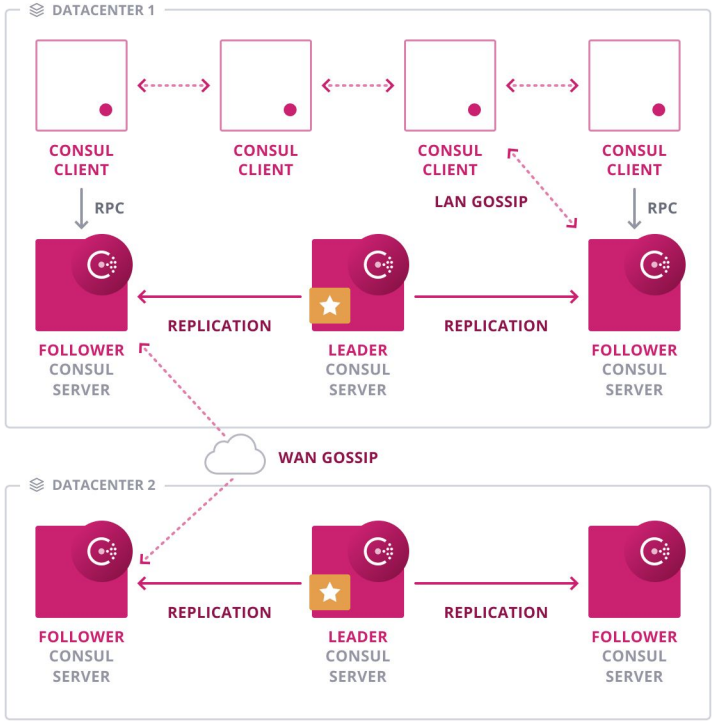
Scaling to multiple data centers is challenging

- Multi-data center deployments provide redundancy, data locality, scalability, and resiliency
- Failover logic doesn’t exist in all applications or is difficult to add or implement
- Failures require manual updates to load balancers or DNS so that traffic routes to healthy instances and/or data centers

Automated Geo Failover

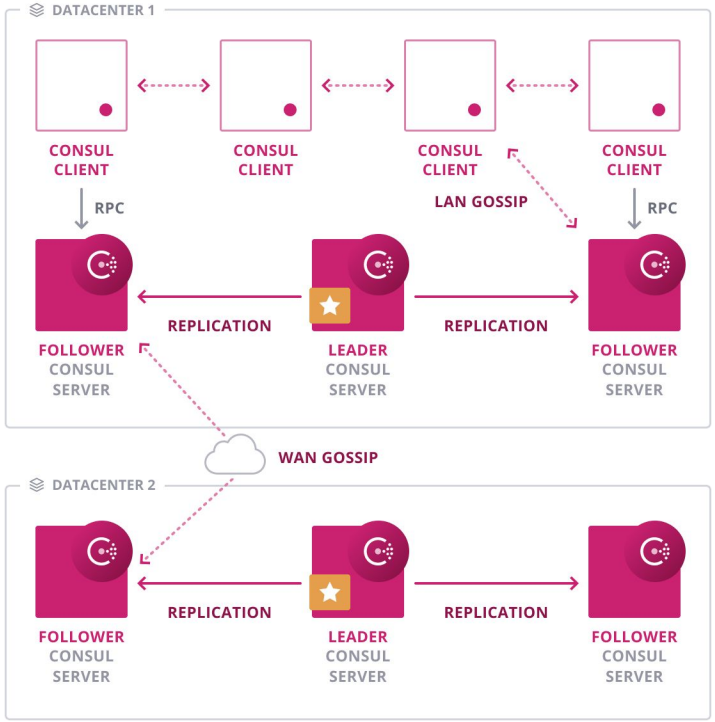
Consul Federation loosely couples & provides connectivity across multiple data centers

- Data centers are independent and failures do not impact others
- Service lookups can occur locally and/or at remote federated data centers



Prepared Queries

- Allow for creation & transparent management of complex failover policies
- Are registered in a datacenter-level namespace
- Define which services to look up, and rules for what to do if none are available in the local datacenter
- Can be executed via HTTP or DNS



Prepared Queries

Database Template Example

- Applications lookup **"geo-db-global.query.consul"**
- Resolving **"geo-db-global.query.consul"** will return a database service instance with the tag "master" from the local datacenter
- If none are available, it will try the next 3 datacenters in order of increasing RTT

```
$ curl -X POST -d \
'{
  "Name": "geo-db-global",
  "Service": {
    "Service": "mysql",
    "Failover": {
      "NearestN": 3
   },
   "Tags": ["global"]
  }
}'  localhost:8500/v1/query
```

Prepared Queries

Catch All Template Example

- Applications lookup **`"*.query.consul"`**
- With a single query template, all services can fail over to the nearest healthy instance in a different datacenter

```
$ curl -X POST -d \
'{
  "Name": "",
  "Template": {
    "Type": "name_prefix_match"
  },
  "Service" : {
    "Service": "${name.full}",
    "Failover": {
      "NearestN": 3
    }
  }
}' localhost:8500/v1/query/query
```

05

Operations & Runbooks

Consul Production Readiness

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

Key elements to review:

- Runbooks
- Backup & Restore Procedures
- Outage Recovery Procedures
- Foundational Security Policies
- Telemetry & Monitoring

Runbooks

Runbooks should be created for the operations involved in managing Consul Datacenters, common runbooks include:

1. Backup/Restore (from snapshots)
2. DR Operations & Testing
3. Upgrade Procedures

Steps for developing runbooks:

1. Identify scenarios
2. Identify RACI
3. Document tasks
4. Test in non-production
5. Implement Runbook in production
6. Lifecycle management

Backup & Restore

- Configure snapshots via the Agent for each Consul Datacenter
- Snapshots are datacenter specific, well defined and easily understood naming convention is important
- Remember snapshots are atomic, point-in-time, & datacenter specific
- Configure interval and retention based on your RPO/RTO requirements
- Test snapshot restore process on a regular basis

Outage Recovery

- Use snapshots to restore a cluster from an outage or unrecoverable quorum loss
- 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

Foundational Security Policies

Prior to production go-live

- 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

Telemetry & Monitoring

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

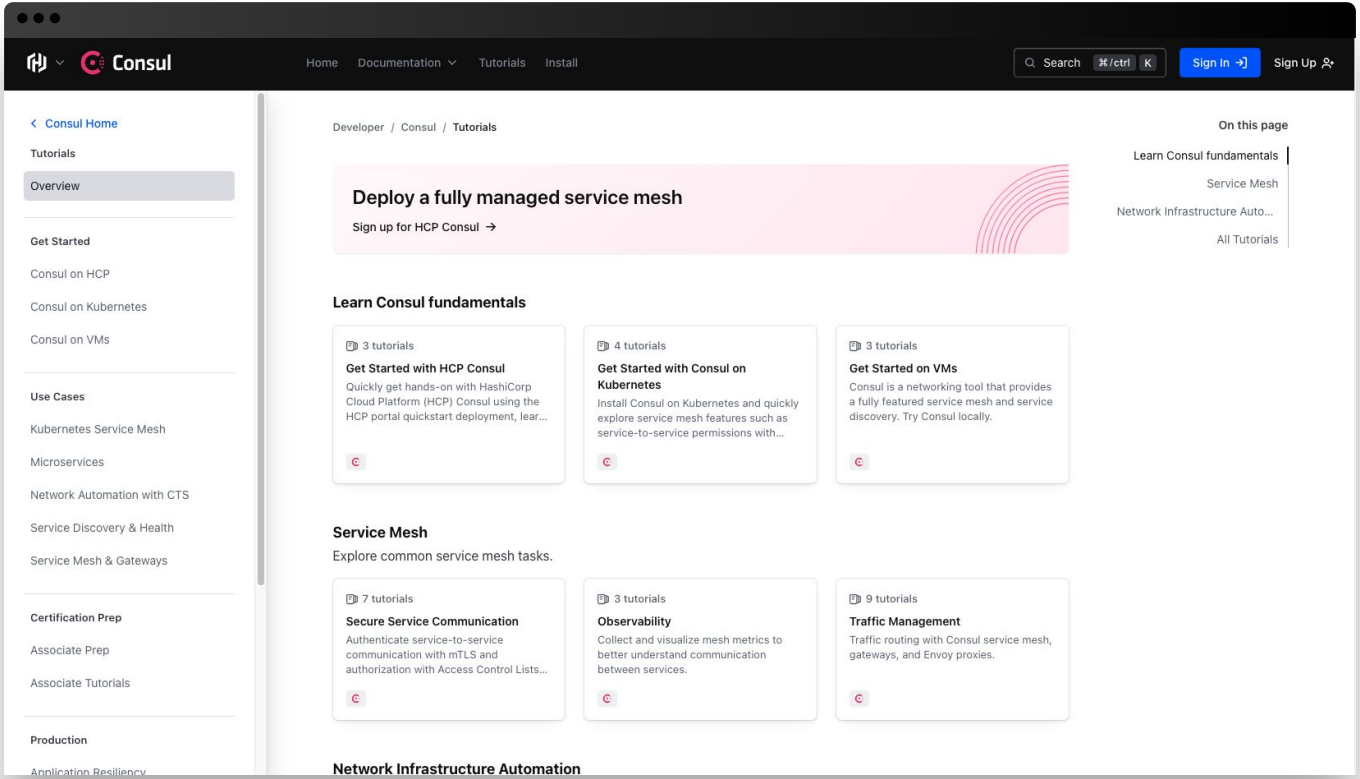
- **Telemetry** - Export telemetry data to a solution that can analyze and identify trends overtime.
- **Enable Audit Logs** - Capture a record of all events so audit teams can inspect event data including credentials used, and timestamps of transactions.
- **Monitor Consul health and Server health**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

Next Steps

Tutorials

https://developer.hashicorp.com/consul/tutorials

Step-by-step guides to accelerate deployment of Terraform Cloud



Additional Resources

- Network Segments
- WAN Federation Through Mesh Gateways
- Federation Between VMs and Kubernetes
- Federation between Kubernetes Clusters
- Create and Manage Cluster Peering Connections
- Namespace Setup Tutorial
- Admin Partitions Tutorial
- Automate Geo-Failover with Prepared Queries
- Datacenter Security Operations
- Disaster Recovery for the Primary Datacenter

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 Webinars

Program Closing

We conclude the webinar series with a short recorded session

The session and accompanying materials include an Operational Readiness Checklist for Consul and links to all of the program materials and recordings

Additional Topics

Additional sessions covering Service Mesh and Network Infrastructure Automation will be available in both live and pre-recorded format

Action Items

- If not done, please share to customer.success@hashicorp.com
  - Authorized technical contacts for support
  - Stakeholders contact information (name and email addresses)
- Share your project status with us
- Review the program closing materials

Q&A

Thank you

customer.success@hashicorp.com

www.hashicorp.com/customer-success