Consul Extension for ACI : FAQs

What is HashiCorp Consul?

Consul is a highly distributed service mesh solution by HashiCorp for providing a full featured control plane with service discovery, configuration, and segmentation functionality at L4-L7. Consul provides Service Mesh any runtime or infrastructure - Bare Metal, Virtual Machines, and Kubernetes clusters, across any cloud; and Secure, Multi-Cloud Service Networking by leveraging intention based policies and automatic mTLS encryption between service mesh resources.
For more details on Consul, https://www.consul.io/.

What is a service mesh and how does it relate to the network?

Service mesh is a control plane layer to facilitate service-to-service networking, load balancing, monitoring, and security. To more details on how it is relevant to L2-L3 network infrastructure, please refer to https://www.hashicorp.com/resources/what-is-a-service-mesh/

Which personas use HashiCorp Consul?

HashiCorp Consul is a product primarily used by DevOps, CloudOps, SecOps and application development personas. These personas are responsible for developing the application, deploying the application and keeping the application up and running. These personas have a limited knowledge and visibility of the underlying L2-L3 network infrastructure.

Which personas use Cisco ACI?

Cisco ACI is an SDN technology primarily used by network engineers, NetOps and NetSecOps personas. These personas are responsible for deploying and operating the network to support the applications. These personas have a limited knowledge and visibility of the L4-L7 application services.

What problems is Cisco ACI and HashiCorp Consul integration solving?

Currently, applications are manually provisioned independent of the network results leading to longer lead times to get the applications up and running while introducing the possibility of human error. This stems from the lack of real-time visibility and automation between L4-L7 application services and their deployment on L2-L3 infrastructure.
The integration between Cisco ACI and HashiCorp Consul is developed to address these challenges.

This integration unlocks the cloud operating model for the ACI operators by providing them visibility into dynamic L4-L7 services and service health in the context of the L2-L3

infrastructure. Enabling organisations to reduce mean-time-to-resolution (MTTR) and supporting Network Middleware Automation.

This integration maintains organization operational model and ownership.

What is Network Middleware Automation?

Network operators currently follow a time consuming manual ticket-based approach to deploy and manage the network. Network Middleware Automation through Consul reduces the time to deploy applications and eliminate manual processes by automating complex networking tasks. Enabling operators to easily deploy, manage and optimize network infrastructure. In the case of Cisco ACI, this translates to creation of ACI policy (contracts, filters and EPGs) based on the L4-L7 service definitions and service mesh intentions.

What privileges do I need to enable this integration on APIC?

Your Cisco ACI user account should have “admin read-only” privileges associated to install and view the complete functionality of the application.
A non-admin instance of Consul Extension for ACI available with limited functionality, in case you want to install and enable this app for non-admin users. Please reach out to your Cisco or HashiCorp rep for this version or make a “non-admin version request” on https://github.com/ciscoecosystem/consul-aci/issues.

Will the application POST/ UPDATE any configuration on APIC or Consul?

Current version of the application does not POST/UPDATE any configuration on APIC or Consul. This application will support the capability to post/update configuration on APIC for Network Middleware Automation in the future.

Will any configuration on APIC or Consul be affected if this application is deleted?

There is NO impact on ACI and Consul configurations if the application is deleted.

What kind of deployment is supported by this application?

This application supports both green field and brown field deployments. It also supports network centric and application centric configuration of Cisco ACI.

Does this integration change the operational ownership structure of teams within my organization?

NO. This integration maintains organization operational model and ownership.

Does this integration work with Kubernetes?

Yes. You will need to enable ACI CNI and Consul Connect on Kubernetes cluster for visibility into Kubernetes workloads.

Does this integration work with cloud APIC or Multi-Site Orchestrator (MSO)?

Currently, the integration is only supported on on-premise APIC. Support for cloud APIC and Multi-Site Orchestrator (MSO) will be delivered in the future.

Which versions of APIC and Consul does this integration work with?

This integration works with on-premise APIC version 3.2(1l) and above. This integration requires Consul Enterprise or Consul open-source versions 1.6.3 and above.

Is there a demo environment for me to explore this integration?

You can reach out to your Cisco or HashiCorp account teams or email us at ask-aci-consul@external.cisco.com to schedule a demo.

How do I request a new feature, report a bug or express my interest to operationalize this integration?

You can request a new feature, report a bug or express interest in operationalizing this integration by opening an issue at https://github.com/ciscoecosystem/consul-aci/issues.

Do I need to pay for this integration?

NO. This integration is available as a free application to download on https://dcappcenter.cisco.com/ . There is no license needed to enable this application.

What is Consul terminology and how does it relate to ACI?

Consul Terminology	**What it mean and how it relates to ACI**
Agent	The Consul agent is the core process of Consul. The agent maintains membership information, registers services, runs checks, responds to queries, and more. The agent must run on every node that is part of a Consul cluster. Any agent may run in one of two modes: client or server. A server node takes on the additional responsibility of being part of the consensus quorum. No approximation to APIC terminology
Connect	Consul Connect provides service-to-service connection authorization and encryption using mutual Transport Layer Security (TLS). Applications can use sidecar proxies in a service mesh configuration to establish TLS connections for inbound and outbound

	connections without being aware of Connect at all. Applications may also natively integrate with Connect for optimal performance and security. Connect can help you secure your services and provide data about service-to-service communications. L4-L7 approximation of ACI policy
Datacenter	Consul datacenter is a networking environment that is private, low latency, and high bandwidth. This excludes communication that would traverse the public internet, but for our purposes multiple availability zones Approximation of a Pod or a site in ACI
Namespace (Enterprise feature)	Namespaces allow multiple teams within the same organization to share the same Consul datacenter(s) by separating services, Consul KV data, and other Consul data per team. This provides operators with the ability to more easily provide Consul as a service. Namespaces also enable operators to delegate ACL management. Approximation of a Tenant in ACI
Network Segments (Enterprise feature)	Consul Network Segments enables operators to create separate LAN gossip segments in one Consul cluster. Agents in a segment are only able to join and communicate with other agents in it's network segment. This functionality is useful for clusters that have multiple tenants that should not be able to communicate with each other. Approximation of a VRF in ACI.
Node	Node is a representation of a virtual or physical machine which runs your workload. Approximation of an Endpoint in ACI.

Service	Service is a well defined component of functional behaviour that provides a logical grouping of application functions. A service is defined in a configuration file or added at runtime over the HTTP interface. Approximation of an End Point Group (EPG) in ACI
Access Control (ACLs)	Consul uses Access Control Lists (ACLs) to secure the UI, API, CLI, service communications, and agent communications. At the core, ACLs operate by grouping rules into policies, then associating one or more policies with a token. Consul ACL can be used to control access to data and APIs. Approximation of Role-based Access Control (RBAC) in ACI
Intentions	Intentions define access control for services via Connect and are used to control which services may establish connections. Intentions are enforced by the proxy or natively integrated application on inbound connections. After verifying the TLS client certificate, the authorize API endpoint is called which verifies the connection is allowed by testing the intentions. If authorize returns false the connection must be terminated. L4-L7 approximation of ACI Filters, Filter Entries and Contracts