# Istio add-on for AKS cluster

Last updated by | Naga Venkata Saikumar | Jan 16, 2025 at 2:12 PM GMT+1

Contents



## Overview

Istio seamlessly integrates with existing distributed applications, monitor and secures them in a Kubernetes cluster

Its robust features offer a consistent and more effective approach to securing, connecting, and monitoring services. With Istio, you can achieve load balancing, service-to-service authentication, and monitoring without extensive service code modifications.

The powerful control plane brings essential features such as:

- Secure communication between services in a cluster through TLS encryption, robust identity-based authentication, and authorization.
- Automatic load balancing for HTTP, gRPC, WebSocket, and TCP traffic.
- Precise control over traffic behavior, including rich routing rules, retries, failovers, and fault injection.
- A customizable policy layer and configuration API that supports access controls, rate limits, and quotas.
- Automatic generation of metrics, logs, and traces for all traffic within a cluster, encompassing both cluster ingress and egress.
- Automatic adjustment of AKS components, such as coredns, when Istio is activated.
- Managed lifecycle, including upgrades, for Istio components initiated by the user. Validated external and internal ingress setup.
- Compatibility with Azure Monitor managed service for Prometheus and Azure Managed Grafana

## Pre-requisites

You must have Azcli version installed > `2.44` in order to use Istio addon.

and if you want to use bicep you should have api version > `2023-11-01`

**Note: You must speficy network policy that allows inbound and outboud connections to api server by creating custom network policy for asm-istio-system, as we have a default deny-all policy in place which blocks the traffic in the cluster by default. otherwise you will see container health check issues with API server**

## Steps to enable Istio service mesh add-on

In order to use Istio add-on for your cluster follow below steps to enable.

### For **New** clusters

Using `azcli` :

```
az group create --name ${RESOURCE_GROUP} --location ${LOCATION}
az aks create --resource-group ${RESOURCE_GROUP} --name ${CLUSTER} --enable-asm
```

Using `bicep` :

**Note: You must specify the revision version ex: I have used asm-1-19 which is the latest as of now. you can refer the release page mentioned in the references for latest versions**

```
serviceMeshProfile: {
  istio: {
    components: {
      // egressGateways: [
      //   {
      //     enabled: true
      //   }
      // ]
      ingressGateways: [
        {
          enabled: true
          mode: 'Internal'
        }
      ]

    }
    revisions: [
      'asm-1-19'
    ]
  }
  mode: 'Istio'
}
```

### For **Existing** clusters

Using `azcli` :

```
az aks mesh enable --resource-group ${RESOURCE_GROUP} --name ${CLUSTER}
```

Using `bicep` :

**Note: You must specify the revision version ex: I have used asm-1-19 which is the latest as of now. you can refer the release page mentioned in the references for latest versions**

```
serviceMeshProfile: {
  istio: {
    components: {
      // egressGateways: [
      //   {
      //     enabled: true
      //   }
      // ]
      ingressGateways: [
        {
          enabled: true
          mode: 'Internal'
        }
      ]

    }
    revisions: [
      'asm-1-19'
    ]
  }
  mode: 'Istio'
}
```

## Limitations

The Istio-based service mesh extension for AKS comes with the following limitations: Incompatibility with AKS clusters utilizing the Open Service Mesh addon.

- Inability to function on AKS clusters with pre-existing Istio installations outside the add-on setup.
- Lack of support for including pods associated with virtual nodes within the mesh. Windows Server containers are not supported by Istio.
- Current restriction on customizing the mesh using the following custom resources: EnvoyFilter, ProxyConfig, WorkloadEntry, WorkloadGroup, Telemetry, IstioOperator, WasmPlugin.
- The Gateway API for Istio ingress gateway and mesh traffic management (GAMMA) is not currently supported with the Istio add-on

## References

https://learn.microsoft.com/en-us/azure/aks/istio-deploy-addon#install-istio-add-on-for-existing-cluster

https://learn.microsoft.com/en-us/azure/templates/microsoft.containerservice/managedclusters?pivots=deployment-language-bicep

https://learn.microsoft.com/en-us/azure/aks/istio-upgrade#minor-version-upgrade