ALIBABA CLOUD

Alibaba Cloud

Alibaba Cloud Service Mesh
User Guide

Document Version: 20220615

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Instance management

1.1. Create an ASM instance

To use Alibaba Cloud Service Mesh (ASM), you must create an ASM instance. This topic describes how to create an ASM instance in the ASM console.

Prerequisites

- The following services are activated:
  - ASM
  - Auto Scaling (ESS)
  - Resource Access Management (RAM)
  - (Optional) Tracing Analysis
- The permissions of the following roles are obtained: AliyunServiceMeshDefaultRole, AliyunCSClusterRole, and AliyunCSManagedKubernetesRole.

Context

Note When you create and use an ASM instance, ASM may perform the following operations based on your settings:

- Creates a security group that allows access to a virtual private cloud (VPC) by using all Internet Control Message Protocol (ICMP) ports.
- Adds route entries to a VPC.
- Creates an elastic IP address (EIP).
- Creates a RAM role and policies, and attaches the policies to the RAM role to grant full permissions on Server Load Balancer (SLB), CloudMonitor, VPC, and Log Service. The RAM role allows ASM to dynamically create SLB instances and add route entries to a VPC based on your settings.
- Creates an internal-facing SLB instance to expose port 6443.
- Creates an internal-facing SLB instance to expose port 15011.
- Collects the logs of managed components to ensure stability when you use the ASM instance.

Procedure

1.
2.
3. On the **Mesh Management** page, click **Create ASM Instance**.
4. On the **Create Service Mesh** page, set the parameters as required.
   i. The following table describes the basic settings for an ASM instance.

Parameter	Description
Service mesh name	The name of the ASM instance.
Spec	The edition of the ASM instance. Valid values: **Standard Edition**, **Enterprise Edition**, and **Ultimate Edition**. For more information about the features of each edition, see the "Instance types" section of the Instance editions topic.
Region	The region in which the ASM instance resides.
Payment type	The billing method of the ASM instance. Valid values: **Pay as you go** and **Subscription**. If you set this parameter to **Subscription**, you must set the following parameters: **Note** If you set the **Payment type** parameter to **Subscription**, only the internal-facing SLB instances of the Istio control plane and API server are billed in subscription mode. The EIPs of the ASM instance and API server are still billed in pay-as-you-go mode. ■ **Purchase time**: the subscription period. Valid values: 1 month, 2 months, 3 months, 6 months, 1 year, 2 years, and 3 years. ■ **Automatic renewal**: specifies whether to enable auto-renewal.
Istio Version	The Istio version.
VPC	The VPC of the ASM instance. You can click **Create VPC** to create a VPC. For more information, see 创建和管理专有网络.
vSwitch	The vSwitch of the ASM instance. You can click **Create vSwitch** to create a vSwitch. For more information, see Work with vSwitches.
Istio control plane access	The SLB instance that is used to control access to the Istio control plane.
API Server access	The SLB instance that is used to control access to the API server. You can specify whether to enable access to the API server by using an EIP. ■ If you select Use EIP to expose API Server, an EIP is created and associated with the internal-facing SLB instance. Then, you can use the kubeconfig file to connect to and manage the ASM instance over the Internet. ■ If you clear Use EIP to expose API Server, no EIP is created. You can use the kubeconfig file to connect to and manage the ASM instance only in the VPC.

Parameter	Description
Observability	Specifies whether to enable Tracing Analysis for the ASM instance. ASM integrates with Tracing Analysis. Tracing Analysis provides a wide range of tools to help you efficiently identify the performance bottlenecks of distributed applications. For example, you can use these tools to map traces, display trace topologies, analyze application dependencies, and count the number of requests. This helps you improve the efficiency of developing and troubleshooting distributed applications. For more information about Tracing Analysis, see Use Tracing Analysis to trace applications inside and outside an ASM instance. **Note** Before you enable Tracing Analysis, make sure that you have activated Tracing Analysis in the Tracing Analysis console.
	Specifies whether to enable Prometheus Service (Prometheus) for the ASM instance. For more information about Prometheus, see Monitor service meshes based on ARMS Prometheus and Deploy a self-managed Prometheus instance to monitor ASM instances.
	Specifies whether to enable Kiali for ASM. Kiali for ASM is a tool that is used to observe ASM instances. This tool provides a GUI that allows you to view services and configurations. Kiali for ASM is a built-in tool in ASM instances whose Istio version is 1.7.5.25 or later. For more information, see Enable Kiali for ASM to observe an ASM instance in the ASM console.
	Specifies whether to enable collection of access logs. If access logs are collected, you can use Log Service to view the access logs of ingress gateway services. For more information about access logs, see Use Log Service to collect logs of ingress gateways on the data plane and Use Log Service to collect access logs of the data plane.
	Specifies whether to enable collection of control plane logs. ASM can collect logs of the control plane and generate alerts based on the logs. For example, ASM can collect logs related to configuration push from the control plane to the sidecar proxies on the data plane. For more information, see Enable collection of control plane logs and control plane alerting.

Parameter	Description
Mesh Audit	Specifies whether to enable the mesh audit feature. You can enable the mesh audit feature to record and trace the operations of users. This is an important O&M feature that ensures cluster security. For more information about the mesh audit feature, see Use the KubeAPI operation audit feature in ASM.
Resource configuration	Specifies whether to enable version control for custom Istio resources. When you update fields in the `spec` block of an Istio resource, ASM records the resource version before the update. ASM stores up to five latest versions. For more information about how to roll back an Istio resource to an earlier version, see Roll back an Istio resource to an earlier version.
	Specifies whether to allow access to Istio resources by using the Kubernetes API of clusters on the data plane. ASM allows you to create, delete, modify, and query Istio resources by using the Kubernetes API of clusters on the data plane. For more information, see Use the Kubernetes API of clusters on the data plane to access Istio resources.
Cluster Domain	The cluster domain for the ASM instance. Default value: cluster.local. You can add only Kubernetes clusters that share the same cluster domain with the ASM instance to the ASM instance. **Note** You can set this parameter only if the Istio version of the ASM instance is 1.6.4.5 or later. Otherwise, this parameter is unavailable.

5. Activate ASM in pay-as-you-go mode.

   If you create an ASM instance of a commercial edition for the first time, the value in the **State** column on the right of **Dependency Check** is **Not pass.** In this case, you must activate ASM in pay-as-you-go mode.

   Click **Activate now** in the **Illustrate** column on the right of **Dependency Check**. On the page that appears, select **ASM (Pay-as-you-go) Terms of Service** and click **Activate Now**. Return to the **Create Service Mesh** page and click **Check again** for **ASM service activation check**. **Pass** is displayed in the **State** column.

6. Select **I have understood and accepted the Service Agreement and have read and agreed Alibaba Cloud Service Mesh ASM Service Level Agreement**.

7. Click **Create Service Mesh**.

   Note It takes about 2 to 3 minutes to create an ASM instance.

Result

After the ASM instance is created, you can view information about the instance by performing the following operations:

- On the **Mesh Management** page, view the basic information about the ASM instance.

  To view the latest information about the ASM instance, click the icon on the right.

- On the **Mesh Management** page, find the ASM instance and click **Log** in the **Actions** column. In the ASM Instance Logs panel, you can view the logs of the ASM instance.
- On the **Mesh Management** page, find the ASM instance and click **Specification change** in the **Actions** column to update the instance type. For more information, see 升级ASM实例.
- On the **Mesh Management** page, find the ASM instance and click **Manage** in the **Actions** column. On the Basic Information page, you can view the basic information of the instance, such as the instance ID and the security group.

  By default, the system creates five namespaces for a new ASM instance. Only the istio-system and default namespaces can be viewed in the ASM console. You can use the kubectl client to query and manage all namespaces, including istio-system, kube-node-lease, kube-public, kube-system, and default.

1.2. View an ASM instance

After you create an Alibaba Cloud Service Mesh (ASM) instance, you can view the detailed information and logs of the ASM instance. This topic describes how to view the instance information, logs, and deployed applications of an ASM instance.

View instance information

1.
2. In the left-side navigation pane, choose **Service Mesh > Mesh Management**.
   On the **Mesh Management** page, you can view the basic information about existing ASM instances.
3. On the **Mesh Management** page, find the ASM instance that you want to view. Then, click the name of the ASM instance or click **Manage** in the **Actions** column of the ASM instance.
   On the **Basic Information** page, you can view the basic information about the ASM instance. For example, you can view the instance ID and the region in which the ASM instance resides.

View instance logs

1.
2.
3. On the **Mesh Management** page, find the ASM instance that you want to view and click **Log** in the **Actions** column.
   In the **ASM Instance Logs** panel, you can view the logs of the ASM instance.

View deployed applications

1.
2.
3.

4. On the details page of the ASM instance, choose **ASM Instance > Instances Status** in the left-side navigation pane.

   On the page that appears, you can view the information about applications that are deployed in the ASM instance.

   Click the icon in the upper-right corner to display the deployed applications in a chart. To display the applications in a list again, click the icon. To view the latest information about application deployment, click the icon.

1.3. Modify an ASM instance

After you create an Alibaba Cloud Service Mesh (ASM) instance, you can modify the ASM instance as required. This topic describes how to modify an ASM instance.

1.
2.
3.
4. On the **Basic Information** page, click **Settings** in the upper-right corner. In the **Settings Update** panel, modify the parameters as needed and click OK.

Parameter	Description
	Specify whether to enable **Tracing Analysis** for the ASM instance. If you enable this feature, you must set the **Sampling Percentage** and **Sampling Method** parameters. ASM integrates with Tracing Analysis. Tracing Analysis provides a wide range of tools to help you efficiently identify the performance bottlenecks of distributed applications. You can use these tools to map traces, display trace topologies, analyze application dependencies, and count the number of requests. This improves your efficiency in developing and troubleshooting distributed applications. For more information, see Use Tracing Analysis to trace applications inside and outside an ASM instance. **Note** Before you enable Tracing Analysis for the ASM instance, make sure that you have activated the Tracing Analysis service in the Tracing Analysis console.
	Specify whether to enable **Prometheus** for the ASM instance. If you enable this feature, you must select **Enable Alibaba Cloud Prometheus** or **Enable Self-managed Prometheus**. ASM integrates with Prometheus Service of Application Real-Time Monitoring Service (ARMS) and self-managed Prometheus systems. This helps you monitor ASM instances. For more information, see Monitor service meshes based on ARMS Prometheus and Deploy a self-managed Prometheus instance to monitor ASM instances.

Parameter	Description
Observability	Specify whether to enable **Kiali** for the ASM instance. If you enable this feature, you must enter the endpoint of the Prometheus instance used by Kiali. Kiali for ASM is a tool that is used to observe ASM instances. This tool provides a GUI that allows you to view related services and configurations. For more information, see Enable Kiali for ASM to observe an ASM instance in the ASM console. **Note** To enable Kiali, you must enable Prometheus.
	Specify whether to enable **access log collection**. The Envoy proxy that is deployed on the data plane generates logs for all access records. The data plane contains the Kubernetes clusters of an ASM instance. You can enable the access log collection feature. After that, you can view the access logs on the data plane. For more information, see Customize access logs on the data plane.
	Specify whether to enable **access log query**. If you enable this feature, you must set the Log Service Project parameter to use the default or existing project in Log Service. Container Service for Kubernetes (ACK) integrates with Log Service. You can collect the access logs of clusters on the data plane of an ASM instance. To use the log collection feature for an ASM instance, you must enable access log query for the ASM instance. For more information, see Use Log Service to collect logs of ingress gateways on the data plane and Use Log Service to collect access logs of the data plane.
Traffic Management	Specify whether to use **HTTP/1**. By default, HTTP/2 is used. To use HTTP/1, select **Enable HTTP 1.0**.
Policy Control	Specify whether to enable the **Open Policy Agent (OPA) plug-in**. ASM integrates with OPA to help you implement fine-grained access control on your applications. If you enable the OPA plug-in, OPA containers and Istio Envoy proxy containers are injected into the pods of applications. Then, you can use OPA to define access control policies. This out-of-box feature improves your efficiency in developing distributed applications. For more information, see Use OPA to implement fine-grained access control in ASM.

Parameter	Description
Data Plane Extension	Specify whether to use the **WebAssembly (Wasm)-based ASM instance extension**. ASM supports Wasm. You can deploy Wasm filters in the Envoy proxy that is used to manage clusters on the data plane. This helps you extend the data plane with new features. For more information, see Write WASM filters for Envoy and deploy them in ASM.
Service Mesh Resource Configuration	Specify whether to enable the **rollback feature for Istio resources**. ASM provides the rollback feature for Istio resources. This feature records up to five historical versions of Istio resources that are updated in the recent period. For more information, see Roll back an Istio resource to an earlier version.
	Specify whether to **allow the Kubernetes API of clusters on the data plane to access Istio resources**. ASM allows you to create, delete, modify, and query Istio resources by using the Kubernetes API of clusters on the data plane. For more information, see Use the Kubernetes API of clusters on the data plane to access Istio resources.
Performance Optimization	Specify whether to enable **MultiBuffer-based TLS encryption and decryption performance optimization**. ASM combines with Intel Multi-Buffer to accelerate TLS processing in Envoy to alleviate the bottleneck. For more information, see Enable Multi-Buffer for TLS acceleration. **Note** This feature is supported only by ASM Enterprise Edition and Ultimate Edition instances.

1.4. Delete an ASM instance

You can delete an Alibaba Cloud Service Mesh (ASM) instance that you no longer need.

Prerequisites

Clusters in the ASM instance that you want to delete are removed from the instance. For more information, see Remove a cluster from an ASM instance.

Procedure

1.
2.
3. On the **Mesh Management** page, click the icon in the Actions column of the ASM instance that you want to delete. Then, click **Delete**.

4. In the **Delete ASM Instance** dialog box, select the resources that you want to retain and click **OK**.

Result

The status of the ASM instance to be deleted becomes **Deleting**. Click **Refresh**. Then, the deleted instance disappears from the **Mesh Management** page.

1.5. Use kubectl to connect to an ASM instance

If you want to use API operations to manage an Alibaba Cloud Service Mesh (ASM) instance, you can use the kubectl client to connect to the ASM instance.

Context

kubectl is a command-line tool of Kubernetes. You can use kubectl to manage Kubernetes clusters, containerized applications deployed in Kubernetes clusters, and ASM instances.

Based on the role-based access control (RBAC) mode of Kubernetes, ASM provides predefined RBAC roles with different permissions on an ASM instance. You can assign roles with the following permissions to users as required:

- The permissions to manage namespaces on the control plane, including the permissions to perform the create, delete, get, list, patch, update, and watch operations.
- The permissions to manage Istio resources, including the permissions to perform the create, delete, get, list, patch, update, and watch operations.
- The permissions to manage `istiogateways.istio.alibabacloud.com` resources for deploying ingress gateways, including the permissions to perform the create, delete, get, list, patch, update, and watch operations.
- The read-only permissions on `istio.alibabacloud.com` resources, including the permissions to perform the get and list operations.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: istio-admin
rules:
- apiGroups: [""]
  resources: ["namespaces"]
  verbs:
  - create
  - delete
  - get
  - list
  - patch
  - update
  - watch
- apiGroups:
  - config.istio.io
  - networking.istio.io
  - authentication.istio.io
  - rbac.istio.io
  - security.istio.io
  resources: ["*"]
  verbs:
  - create
  - delete
  - get
  - list
  - patch
  - update
  - watch
- apiGroups:
  - istio.alibabacloud.com
  resources: ["istiogateways"]
  verbs:
  - create
  - delete
  - get
  - list
  - patch
  - update
  - watch
- apiGroups:
  - istio.alibabacloud.com
  resources: ["*"]
  verbs:
  - get
  - list
```

Procedure

1. Select and download a version of kubectl from GitHub. Then, install and configure the kubectl client. For more information, see Install and Set Up kubectl.

2. View the connection configuration of the ASM instance.
   i. Log on to the .
   ii.
   iii.
   iv. Click **Connection** in the upper-right corner.
   In the **Connection** panel, you can view the Internet connection configuration on the **Internet Access** tab, and the internal connection configuration on the **Internal Access** tab.

   > **Notice** You can access an ASM instance from the Internet only if an elastic IP address (EIP) is associated with the API server of the ASM instance to expose the API Server to the Internet. Otherwise, the Internet Access tab is not displayed in the **Connection** panel.

3. Add the credential for connecting to the ASM instance.
   - If the ASM instance supports Internet access, click the **Internet Access** tab and copy the content in the code editor to the config file in the $HOME/.kube directory. This is the default file from which kubectl obtains credentials. If the *config* file does not exist in the specified directory, create one by yourself.
   - If the ASM instance supports internal access, click the **Internal Access** tab and copy the content in the code editor to the config file in the $HOME/.kube directory. This is the default file from which kubectl obtains credentials. If the *config* file does not exist in the specified directory, create one by yourself.
4. Run the following command to check whether you can connect to the ASM instance from the kubectl client. If the namespace information is returned, the connection succeeds.

   ```
   kubectl get ns
   ```

2.Data plane

2.1. Add a cluster to an ASM instance

Applications that are deployed in an Alibaba Cloud Service Mesh (ASM) instance run in clusters. To use an ASM instance to manage applications, you must add a Container Service for Kubernetes (ACK) cluster to the ASM instance.

Prerequisites

- An ASM instance is created. For more information, see Create an ASM instance.
- An ACK cluster is created. For more information, see Create an ACK dedicated cluster and Create an ACK managed cluster.
- The API server of the Container Service for Kubernetes cluster can be accessed from the Internet.

Procedure

1.
2.
3.
4.
5. In the **Add Cluster** panel, select the cluster to be added to the ASM instance and click **OK**.

   > Note
   > - If your application runs in a single cluster or multiple clusters in a VPC, we recommend that you select **Clusters in the Same VPC as the ASM Instance** to filter clusters.
   > - Make sure that the proxy container of the cluster to be added to the ASM instance can access Istio Pilot of the ASM instance. If Istio Pilot of the ASM instance does not allow Internet access, make sure that it can be accessed by the proxy container in the VPC.

6. In the **Note** message, click **OK**.

Result

After you add a cluster to the ASM instance, the status of the ASM instance changes to **Updating**. Wait a few seconds and click the **Refresh** icon in the upper-right corner. If the cluster is added to the ASM instance, the status of the ASM instance becomes **Running**. You can add multiple clusters to the ASM instance at a time. The waiting duration may vary with the number of clusters that you add. On the **Kubernetes Clusters** page, you can view the information about the added cluster.

2.2. Add an ECS instance to an ASM instance

Alibaba Cloud Service Mesh (ASM) allows you to add Elastic Compute Service (ECS) instances to an ASM instance. This way, you can connect the workloads on the ECS instances to the ASM instance. This topic describes how to add an ECS instance to an ASM instance.

Prerequisites

-
- An ECS instance is created. For more information, see Create an instance by using the wizard.

> **Note** To add an ECS instance to an ASM instance, make sure that the ECS instance resides in the same virtual private cloud (VPC) as the ASM instance.

Procedure

1.
2.
3.
4.
5. In the **Add VM** panel, select an ECS instance and click **OK**.
   On the **VMs** page, you can view the information about the added ECS instance.

Related information

- Install Istio Proxy on a virtual machine
- Use ASM to manage a Bookinfo application on virtual machines
- Use ASM to manage non-containerized applications

2.3. Remove a cluster from an ASM instance

If you no longer need a cluster in an Alibaba Cloud Service Mesh (ASM) instance, you can remove the cluster from the ASM instance.

Procedure

1.
2.
3.
4.
5. On the **Kubernetes Clusters** page, select the cluster that you want to remove and click **Remove**.
6. In the Submit message, click **OK**.
   The cluster disappears from the **Kubernetes Clusters** page.

3.Control plane

3.1. Manage namespaces

Namespaces are used to divide Kubernetes cluster resources into virtual and isolated spaces. This topic describes how to create, define, and delete a namespace for an Alibaba Cloud Service Mesh (ASM) instance.

Context

The namespaces that you create in an ASM instance, whether in the ASM console or by using the kubectl client, belong only to the ASM instance. They are independent of the Kubernetes clusters in the data plane that are managed by the ASM instance. Therefore, the namespaces in the control plane of the ASM instance may be different from the namespaces of the Kubernetes clusters in the data plane. When you create or delete namespaces for the ASM instance, the namespaces of the Kubernetes clusters in the data plane are not affected.

Create a namespace

1.
2.
3.
4.
5. In the **Create Namespace** panel, set the parameters and click **OK**.

Parameter	Description
Name	The name of the namespace. The name must be 1 to 63 characters in length and can contain only digits, letters, and hyphens (-). It must start and end with a letter or digit.
Tag	You can add multiple tags to a namespace. Tags are used to identify namespaces. For example, you can tag a namespace as one that is used in the test environment. To add a tag, click Add in the Tag section and enter the key and value of the tag in the row that appears.

Enable automatic sidecar injection

After you enable automatic sidecar injection for a namespace, an Envoy proxy is automatically injected as a sidecar into each pod that is created in the namespace. These Envoy proxies comprise the data plane of the ASM instance.

1.
2.
3.
4.

5. On the **Namespaces** page, find the namespace for which you want to enable automatic sidecar injection and click **Enable Automatic Sidecar Injection** in the **Automatic Sidecar Injection** column.
6. In the **Submit** message, click **OK**.

Define a namespace

1.
2.
3.
4.
5. On the **Namespaces** page, find the namespace that you want to define and click **YAML** in the **Actions** column.
6. In the **Edit** panel, define the namespace and click **OK**.

Delete a namespace

1.
2.
3.
4.
5. On the **Namespaces** page, find the namespace that you want to delete and click **Delete** in the **Actions** column.
6. In the Submit message, click **OK**.
   The namespace disappears from the **Namespaces** page.

3.2. Manage virtual services

Virtual services are critical resources for traffic routing. You can use virtual services to manage requests that are sent to services in an Alibaba Cloud Service Mesh (ASM) instance. This topic describes how to create, modify, and delete a virtual service.

Create a virtual service

1.
2.
3.
4.
5. Set the parameters for creating a virtual service by using one of the following methods:
   - On the **Create** page, select a namespace from the **Namespace** drop-down list, select a template that is used to create a virtual service from the **Template** drop-down list, modify the configurations of the template in the **YAML** code editor, and then click **Create**.
   - On the **Create** page, select a namespace from the **Namespace** drop-down list, select no template from the **Template** drop-down list, customize the configurations of a virtual service in the **YAML** code editor, and then click **Create**.

What to do next

Modify a virtual service

On the details page of the ASM instance, choose **Traffic Management > VirtualService** in the left-side navigation pane. On the **VirtualService** page, find the virtual service that you want to modify and click **YAML** in the **Actions** column. In the **Edit** panel, modify the configurations of the virtual service and click **OK**.

Delete a virtual service

On the details page of the ASM instance, choose **Traffic Management > VirtualService** in the left-side navigation pane. On the **VirtualService** page, find the virtual service that you want to delete and click **Delete** in the **Actions** column. In the **Submit** message, click **OK**.

3.3. Manage destination rules

Destination rules are critical resources of Alibaba Cloud Service Mesh (ASM) instances. Destination rules define policies for the traffic that is intended for a service after routing has occurred, such as the policies for service subsets and Envoy proxies. This topic describes how to create, modify, and delete a destination rule.

Create a destination rule

1.
2.
3.
4.
5. In the **Create** panel, set the parameters and click **OK**.
   i. Select a namespace from the **Namespaces** drop-down list.
   ii. In the code editor, enter code to configure a destination rule.

   On the **DestinationRule** page, you can view the created destination rule.

Modify a destination rule

1.
2.
3.
4.
5. On the **DestinationRule** page, find the destination rule that you want to modify and click **YAML** in the **Actions** column.
6. In the **Edit** panel, modify the destination rule and click **OK**.

Delete a destination rule

1.
2.
3.
4.
5. On the **DestinationRule** page, find the destination rule that you want to delete and click **Delete**

in the **Actions** column.

6. In the Submit message, click **OK**.
   The destination rule disappears from the **DestinationRule** page.

3.4. Manage Istio gateways

An Istio gateway defines a load balancer that runs at the edge of an Alibaba Cloud Service Mesh (ASM) instance to receive inbound or outbound HTTP/TCP traffic. This topic describes how to create, modify, and delete an Istio gateway.

Create an Istio gateway

1.
2.
3.
4.
5. Set the parameters for creating an Istio gateway by using one of the following methods:
   - On the **Create** page, select a namespace from the **Namespace** drop-down list, select a template that is used to create an Istio gateway from the **Template** drop-down list, modify the configurations of the template in the **YAML** code editor, and then click **Create**.
   - On the **Create** page, select a namespace from the **Namespace** drop-down list, select no template from the **Template** drop-down list, customize the configurations of an Istio gateway in the **YAML** code editor, and then click **Create**.

What to do next

Modify an Istio gateway

On the details page of the ASM instance, choose **Traffic Management > Gateway** in the left-side navigation pane. On the **Gateway** page, find the Istio gateway that you want to modify and click **YAML** in the **Actions** column. In the **Edit** panel, modify the configurations of the Istio gateway and click **OK**.

Delete an Istio gateway

On the details page of the ASM instance, choose **Traffic Management > Gateway** in the left-side navigation pane. On the **Gateway** page, find the Istio gateway that you want to delete and click **Delete** in the **Actions** column. In the **Submit** message, click **OK**.

3.5. Manage service entries

You can add an entry of a service to the internal service registry of an Alibaba Cloud Service Mesh (ASM) instance. A service entry describes the domain name, port, protocol, and endpoint of a service. This topic describes how to create, modify, and delete a service entry.

Create a service entry

1.
2.
3.

4.
5. In the **Create** panel, set the parameters and click **OK**.
   i. Select a namespace from the **Namespaces** drop-down list.
   ii. In the code editor, enter code to configure a service entry.

   On the **ServiceEntry** page, you can view the created service entry.

Modify a service entry

1.
2.
3.
4.
5. On the **ServiceEntry** page, find the service entry that you want to modify and click **YAML** in the **Actions** column.
6. In the **Edit** panel, modify the service entry and click **OK**.

Delete a service entry

1.
2.
3.
4.
5. On the **ServiceEntry** page, find the service entry that you want to delete and click **Delete** in the **Actions** column.
6. In the Submit message, click **OK**.
   The service entry disappears from the **ServiceEntry** page.

3.6. Manage Envoy filters

Envoy filters are used to configure filter conditions, listeners, and other settings for Envoy proxies. This further enhances capabilities of the Alibaba Cloud Service Mesh (ASM) control plane. This topic describes how to create, modify, and delete an Envoy filter.

Usage notes

The method for creating an Envoy filter varies with the version of your ASM instance.

- If the version of your ASM instance is V1.12.4.0-g7d140f10-aliyun or later, you can create an Envoy filter by using an Envoy filter template.
- If the version of your ASM instance is earlier than V1.12.4.0-g7d140f10-aliyun, you need to to create an Envoy filter. You can also update your ASM instance to V1.12.4.0-g7d140f10-aliyun or later. Then, you can create an Envoy filter by using an Envoy filter template. For more information about how to update an ASM instance, see 升级ASM实例.

Relationships between Envoy filter templates and Envoy filters

User-created Envoy filters may be incompatible with ASM instances after the instances are updated or maintained. In an ASM instance of V1.12.4.0-g7d140f10-aliyun or later, you can create Envoy filters by using Envoy filter templates. After you update the ASM instance, the system automatically recreates or modifies the Envoy filters that were created by using Envoy filter templates to ensure that the Envoy filters are compatible with the ASM instance. This prevents version compatibility issues of Envoy filters and makes Envoy filters easier to use.

After you create an Envoy filter template, you must bind the Envoy filter template to a workload or namespace. Then, ASM automatically creates an Envoy filter by using the template. An Envoy filter template can be bound to multiple workloads and namespaces. This way, you can create multiple Envoy filters by using the template.

Create an Envoy filter template

ASM allows you to create an Envoy filter template by using a preset template or by customizing the Envoy filter template.

Create an Envoy filter template by using a preset template

1.
2.
3.
4.
5. On the **Market Place** page, find the preset template that you want to use to create an Envoy filter template and click **Apply this template**.
6. In the **Fill template parameters** step, set the parameters of the Envoy filter template and click **Next**.
7. In the **Create** step, enter a name for the Envoy filter template and click **OK**.

   On the details page of the ASM instance, choose **Plugin Center > EnvoyFilter Template** in the left-side navigation pane. On the **EnvoyFilter Template** page, you can view the Envoy filter template that you created.

Create an Envoy filter template by customizing the template

1.
2.
3.
4.
5. On the **Market Place** page, find the **Customize EnvoyFilter template** card and click **Apply this template**.
6. In the **Basic Information** section, enter a name for the Envoy filter template.
7. In the **Multi-version adapted EnvoyFilter templates** section, click **Add an EnvoyFilter template for specific adapted istio version**, select an Istio version, customize the configurations of the Envoy filter template, and then click **OK**.

   On the details page of the ASM instance, choose **Plugin Center > EnvoyFilter Template** in the left-side navigation pane. On the **EnvoyFilter Template** page, you can view the Envoy filter template that you created.

Bind an Envoy filter template to a workload or namespace

After you create an Envoy filter template, you must bind the Envoy filter template to workloads or namespaces. Then, the Envoy filter template takes effects on the specified workloads or namespaces. After you bind the Envoy filter template to workloads or namespaces, ASM automatically creates Envoy filters by using the template.

Bind an Envoy filter template to a workload

1.
2.
3.
4.
5. On the **EnvoyFilter Template** page, find the Envoy filter template that you want to configure and click **Edit template** in the **Actions** column.
6. On the **Edit EnvoyFilter Template** page, click the **Bind template to workloads** tab and click **Bind EnvoyFilter to Workloads**.
7. In the **Bind EnvoyFilter to Workloads** dialog box, set the **Namespace** and **Workload Type** parameters, click **Bind** next to a workload in the **Not bound** section, and then click **OK**.

   On the details page of the ASM instance, choose **Plugin Center > EnvoyFilter** in the left-side navigation pane. On the **EnvoyFilter** page, you can view the Envoy filter that is automatically created.

Bind an Envoy filter template to a namespace

1.
2.
3.
4.
5. On the **EnvoyFilter Template** page, find the Envoy filter template that you want to configure and click **Edit template** in the **Actions** column.
6. On the **Edit EnvoyFilter Template** page, click the **Bind template to workloads** tab and click **Bind EnvoyFilter to Namespace**.
7. In the **Bind EnvoyFilter to Namespace** dialog box, click the namespace that you want to configure in the **Not bound** section and click **OK**.

   > **Note** If you bind an Envoy filter template to the istio-system namespace, the Envoy filter template globally takes effect. The Envoy filter template is automatically unbound from other workloads or namespaces to which the template is bound. Therefore, you need to confirm that you want to bind Envoy filter template to the istio-system namespace.

   On the details page of the ASM instance, choose **Plugin Center > EnvoyFilter** in the left-side navigation pane. On the **EnvoyFilter** page, you can view the Envoy filter that is automatically created.

What to do next

Modify an Envoy filter

> **Note** You can modify only Envoy filters that are created by using custom templates. You cannot modify Envoy filters that are created by using preset templates.

On the **EnvoyFilter Template** page, find the Envoy filter template that you want to modify and click **Edit template** in the **Actions** column. Modify the template parameters and click **Modify template contents**. After you modify the Envoy filter template, the Envoy filters that were created by using the template are automatically updated.

Delete an Envoy filter

- Delete an Envoy filter by deleting an Envoy filter template

  On the **EnvoyFilter Template** page, find the Envoy filter template that you want to delete and click **Delete** in the **Actions** column. In the message that appears, click **OK**. After you delete the Envoy filter template, the Envoy filters that were created from the template are automatically deleted.

- Delete an Envoy filter by unbinding an Envoy filter template from a workload

  On the **EnvoyFilter Template** page, find the Envoy filter template that you want to configure and click **Edit template** in the **Actions** column. On the **Bind template to workloads** tab, click **Bind EnvoyFilter to Workloads**. In the **Bind EnvoyFilter to Workloads** dialog box, click **Unbind** next to the workload from which you want to unbind the template and click **OK**. After you unbind the Envoy filter template from the workload, the Envoy filter that was created by using the template for the workload is automatically deleted.

- Delete an Envoy filter by unbinding an Envoy filter template from a namespace

  On the **EnvoyFilter Template** page, find the Envoy filter template that you want to configure and click **Edit template** in the **Actions** column. On the **Bind template to workloads** tab, click **Bind EnvoyFilter to Namespace**. In the **Bind EnvoyFilter to Namespace** dialog box, click the namespace from which you want to unbind the template in the **Bound** section and click **OK**. After you unbind the Envoy filter template from the namespace, the Envoy filter that was created by using the template for the namespace is automatically deleted.