# [Spec] Starter & Essential Private link connection (BETA)

| Time | Comment | Author |
|---|---|---|
| 2025-11-25 | First version | shiyuhang |

## 1. Background

Dataflow services such as **changefeed** and **Data Migration (DM)** in TiDB Cloud require connections to customers' RDS instances or Kafka clusters. While public network connections are technically feasible, **Private Link** provides a far more efficient and secure networking alternative.

The **Private Link Connection** enables private, direct connectivity between TiDB Cloud and customers' target resources (e.g., RDS, Kafka) via Private Link. This feature is specifically designed for integration with TiDB Cloud's changefeed, DM and other services that connect from TiDB Cloud to customers' resources, ensuring data transmission remains within private networks.

- From TiDB Cloud -> customers' resource powered by private link
- Cluster level
- Not related to specified business

> REF: [Spec] TiCDC Private Endpoint Improvements

## 2. Detail Design

### 2.1 Terminology

| Term | Definition |
|---|---|
| Private Link Connection | A connection **from** TiDB Cloud **to** customers' **resources** using **private** link (**usually used in dataflow**). With **private** link connection, TiDB Cloud |

| | |
|---|---|
| https://www.mongodb.com/docs/api/doc/atlas-admin-api-v2/operation/operation-listgroupstreamprivatelinkconnections | **Services** such as DM and changfeed can connect to customers' **resources** such as **MySQL**, Kafka in a **safer** way. |
| AWS Endpoint Service | One type of Private Link Connection. It allows TiDB Cloud connect to an AWS endpoint service.<br>Users can associate any resources behind this AWS endpoint service，such as a NLB target to RDS. |
| AliCloud Endpoint Service | One type of Private Link Connection. It allows TiDB Cloud connect to an AWS endpoint service.<br>Users can associate any resources behind this AliCloud endpoint service，such as a NLB target to RDS. |
| Attach Domain | An action of Private Link Connection. It allows customers cname a domain to the Private Link Connection.<br>For example, if one has already created a Private Link Connection that connects to the AWS endpoint service and attached domain A to it, TiDB Cloud will be redirected to this endpoint service when visiting domain A. It is useful when you try to build a Private Link Connection for Kafka resource. |

## 2.2 Private Link Connection

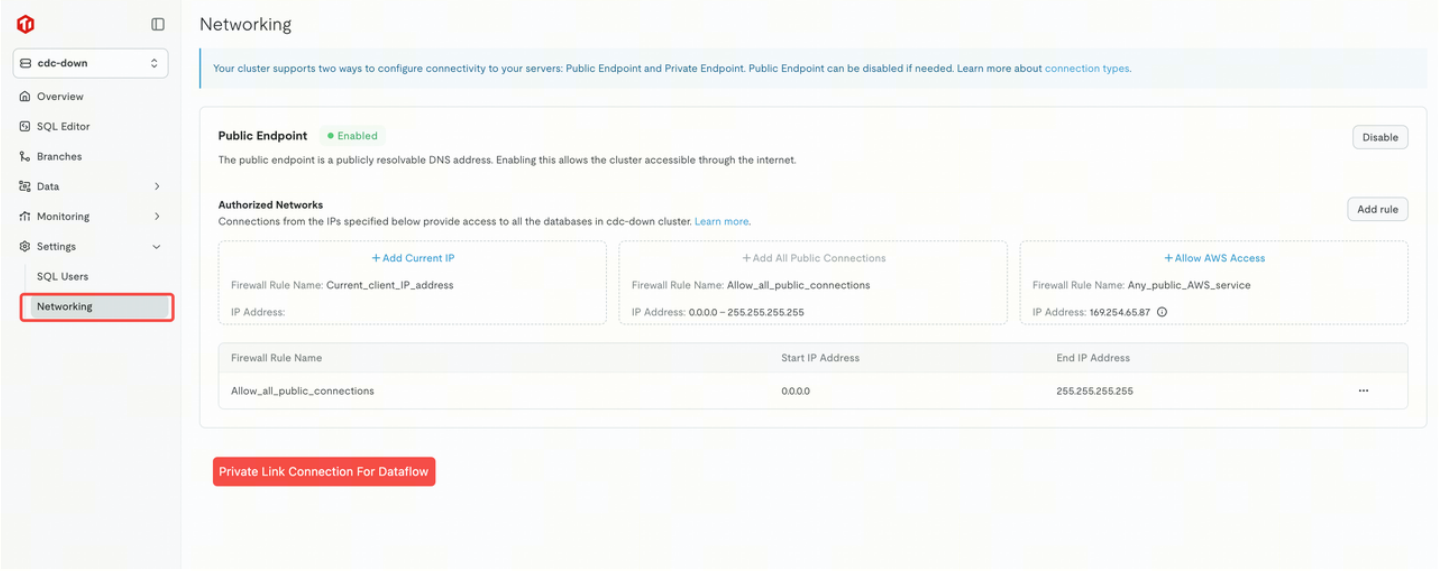
### 2.2.1 Feature Name

Private Link Connection For Dataflow

### 2.2.2 Access Entry

Available in the **Networking** section of the TiDB Cloud console for **Starter** and **Essential** clusters.

- **Need to add an explanation and link to doc**



Networking

Your cluster supports two ways to configure connectivity to your servers: Public Endpoint and Private Endpoint. Public Endpoint can be disabled if needed. Learn more about connection types.

Public Endpoint ● Enabled

The public endpoint is a publicly resolvable DNS address. Enabling this allows the cluster accessible through the internet.

Authorized Networks

Connections from the IPs specified below provide access to all the databases in cdc-down cluster. Learn more.

Firewall Rule Name: Current_client_IP_address
IP Address:

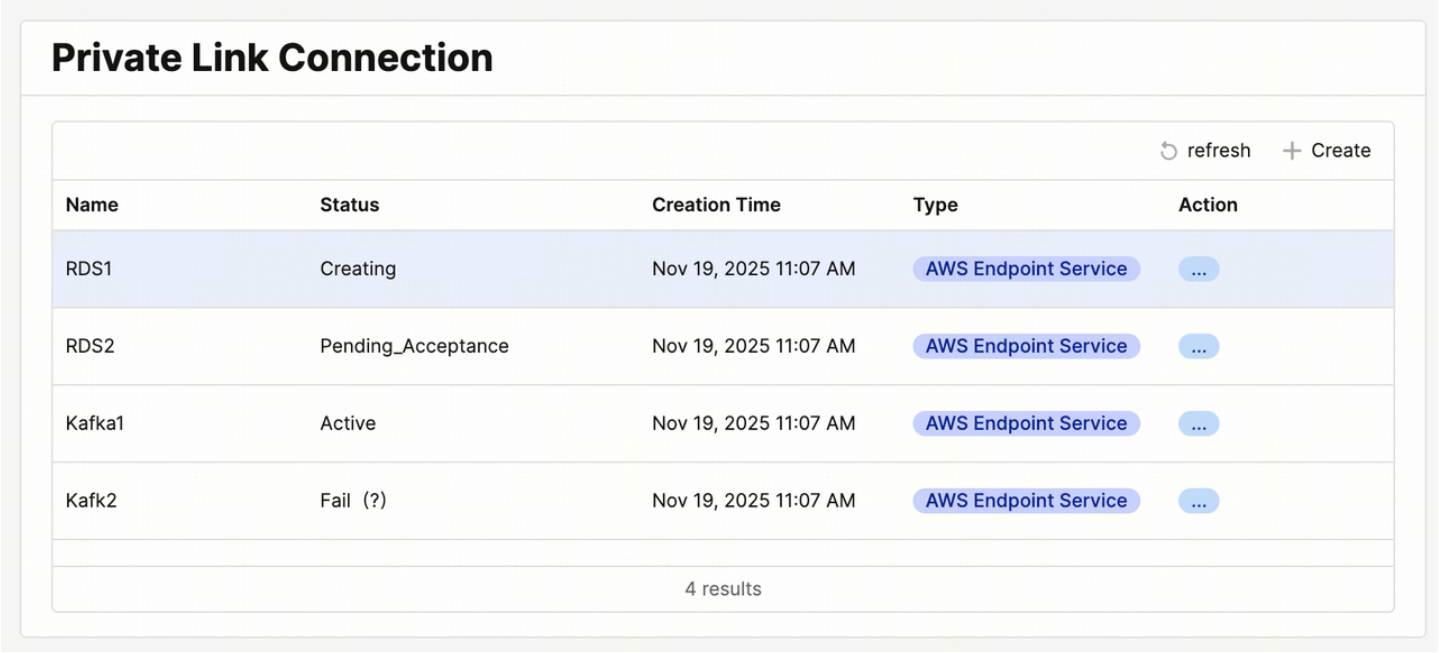
Firewall Rule Name: Allow_all_public_connections
IP Address: 0.0.0.0 – 255.255.255.255

Firewall Rule Name: Any_public_AWS_service
IP Address: 169.254.65.87

| Firewall Rule Name | Start IP Address | End IP Address | |
|---|---|---|---|
| Allow_all_public_connections | 0.0.0.0 | 255.255.255.255 | ··· |

## 2.2.3 List private link connections

- Action:
  - **View**: Access the detailed configuration of a Private Link Connection.
  - **Attach Domains:** Associate domains with the connection.
  - **Detach Domains**: Remove domains from the connection (grayed out if no domains are attached)
  - **Delete**: Remove the Private Link Connection.
- Status
  - Fail: Displays a clear error message

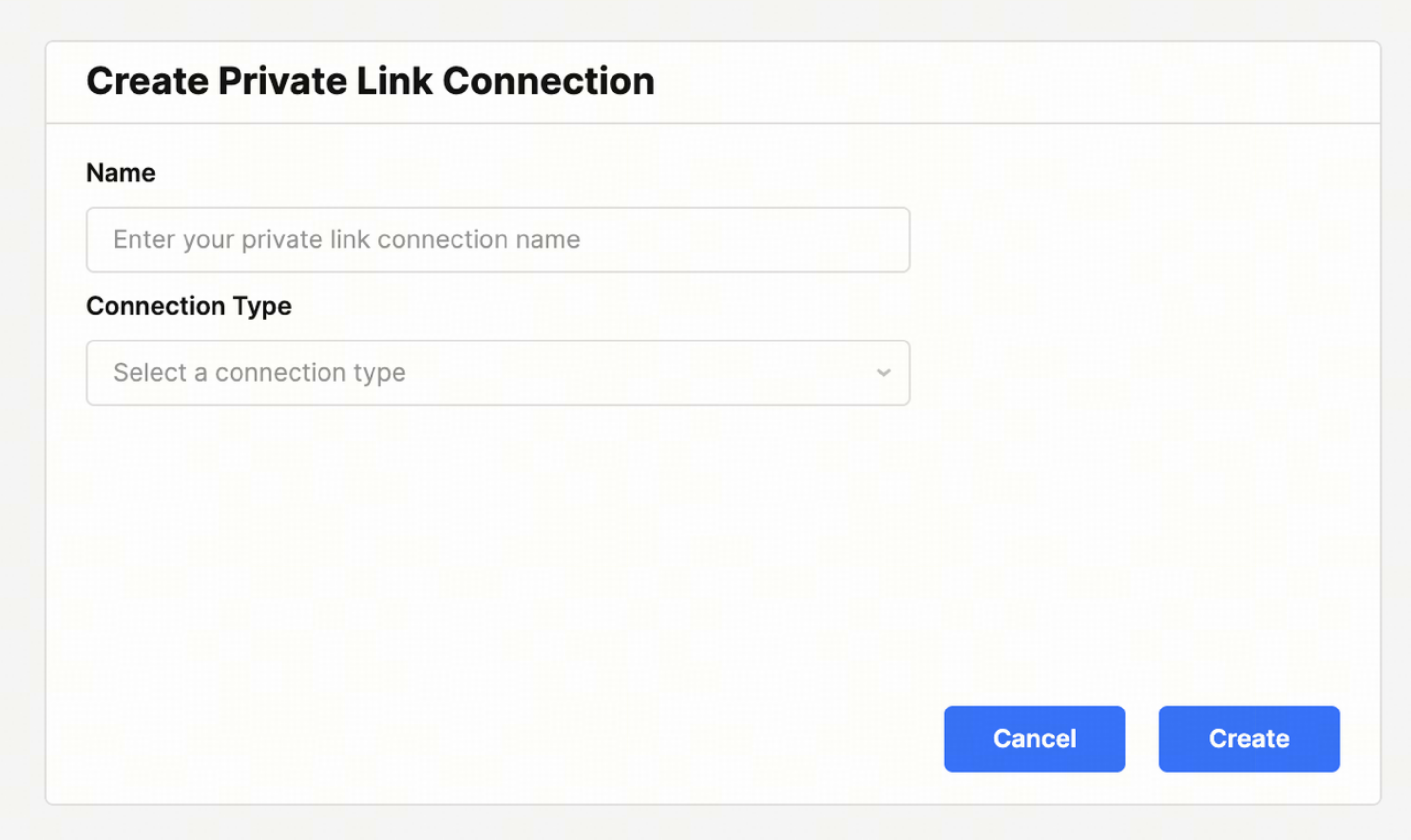


Private Link Connection

| Name | Status | Creation Time | Type | Action |
|---|---|---|---|---|
| RDS1 | Creating | Nov 19, 2025 11:07 AM | AWS Endpoint Service | ... |
| RDS2 | Pending_Acceptance | Nov 19, 2025 11:07 AM | AWS Endpoint Service | ... |
| Kafka1 | Active | Nov 19, 2025 11:07 AM | AWS Endpoint Service | ... |
| Kafk2 | Fail (?) | Nov 19, 2025 11:07 AM | AWS Endpoint Service | ... |

4 results

## 2.2.4 Create a private link connection



Create Private Link Connection

Name

Enter your private link connection name

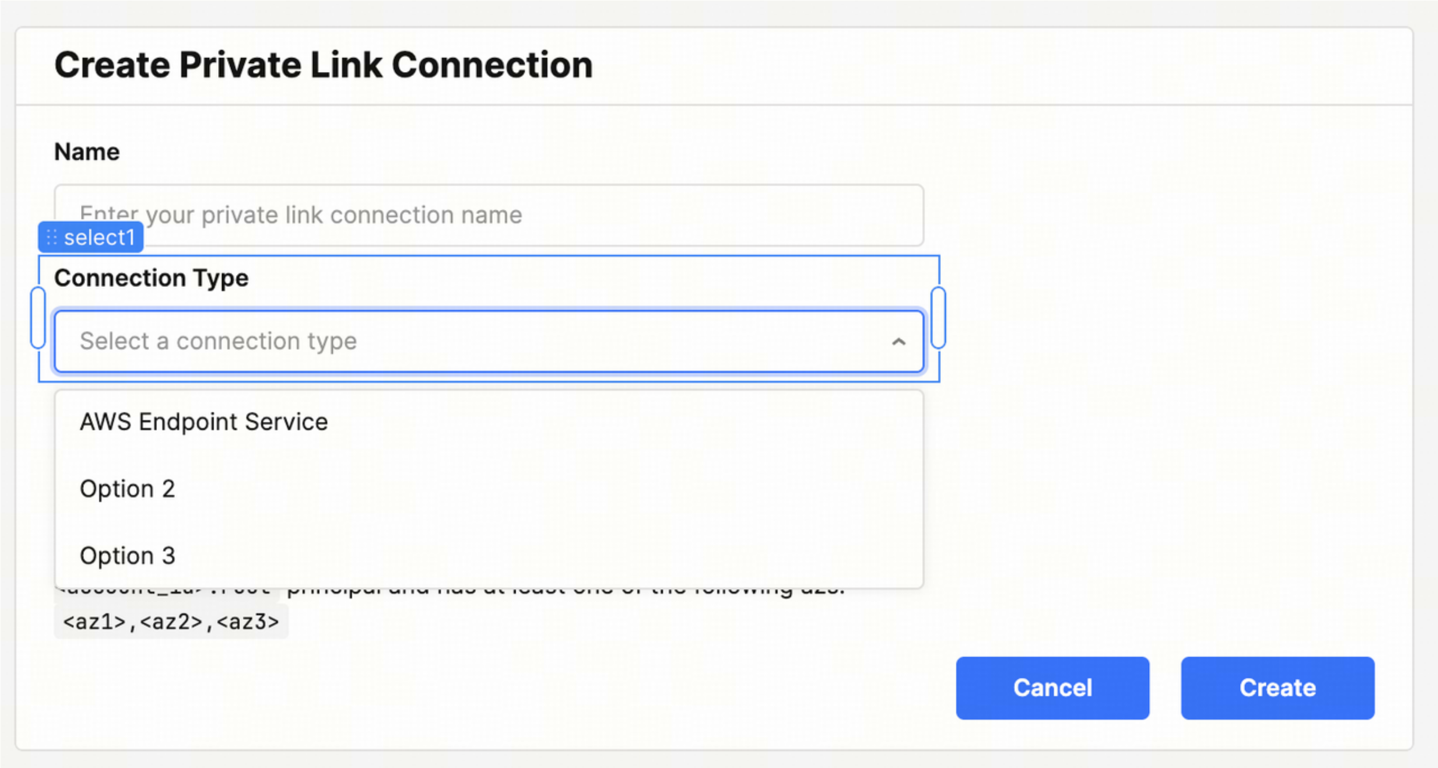
Connection Type

Select a connection type

- Connection Type depends on the cloud provider

| Cloud Provider | Connection Type |
|---|---|
| AWS | Currently only **AWS Endpoint Service** (more types like MSK and Resource Configuration will be added in future releases) |
| Alibaba Cloud | Currently only **AliCloud Endpoint Service** |

## AWS



Create Private Link Connection

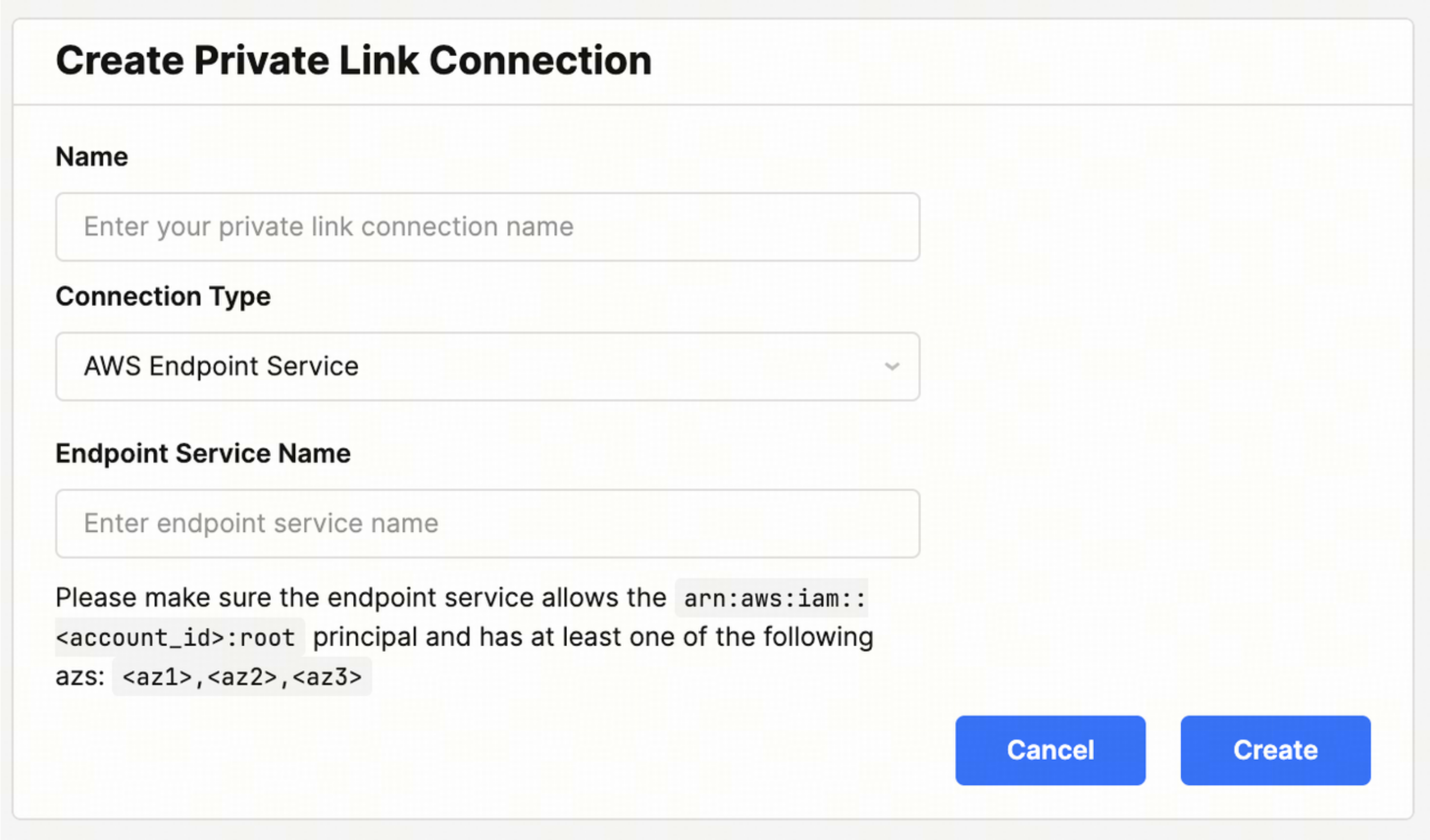
Name

Enter your private link connection name

Connection Type

Select a connection type

`<az1>,<az2>,<az3>`



Create Private Link Connection

Name

Enter your private link connection name

Connection Type

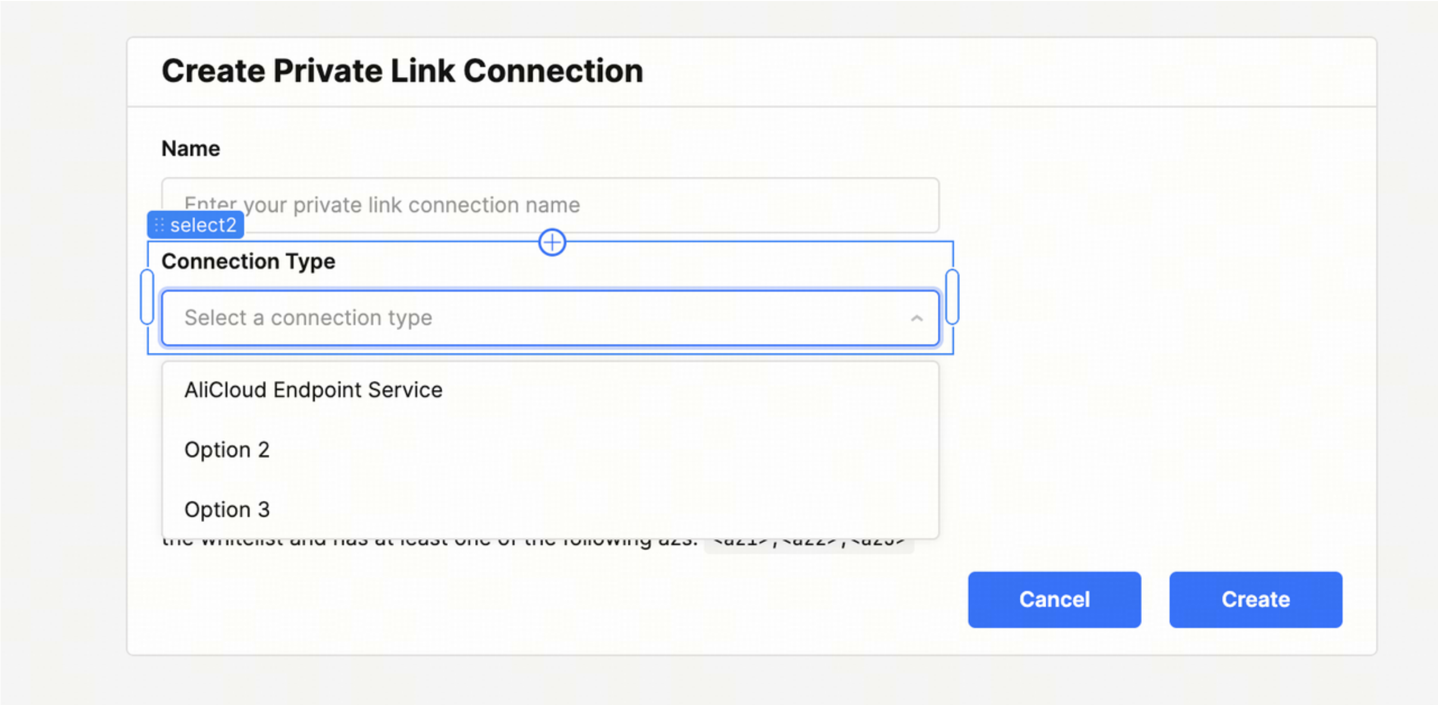
AWS Endpoint Service

Endpoint Service Name

Enter endpoint service name

Please make sure the endpoint service allows the `arn:aws:iam::<account_id>:root` principal and has at least one of the following azs: `<az1>,<az2>,<az3>`

## AliCloud



**Create Private Link Connection**

Name

Enter your private link connection name

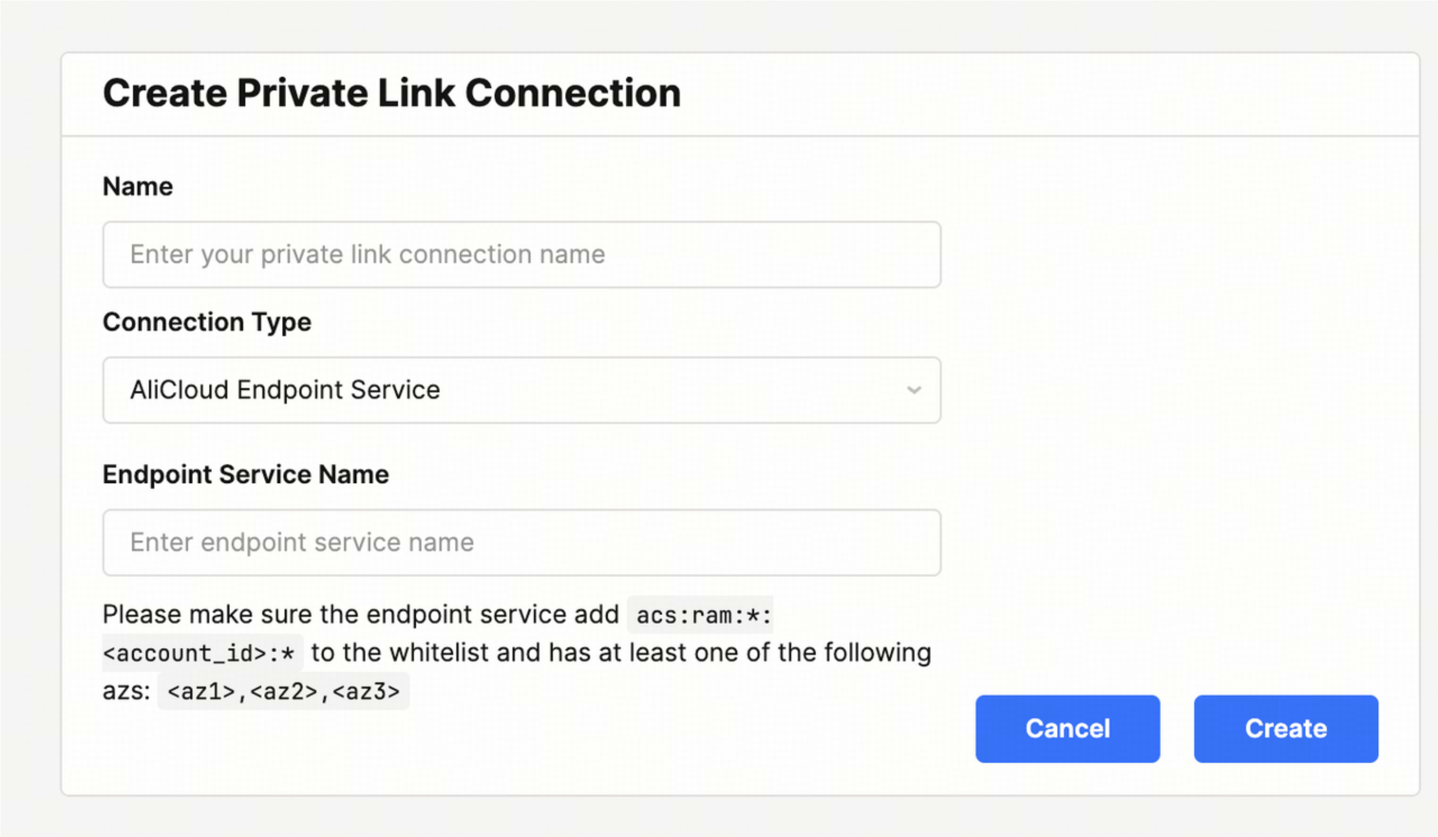
select2

Connection Type

Select a connection type

- AliCloud Endpoint Service
- Option 2
- Option 3

the whitelist and has at least one of the following azs: `<az1>,<az2>,<az3>`



**Create Private Link Connection**

Name

Enter your private link connection name

Connection Type

AliCloud Endpoint Service

Endpoint Service Name

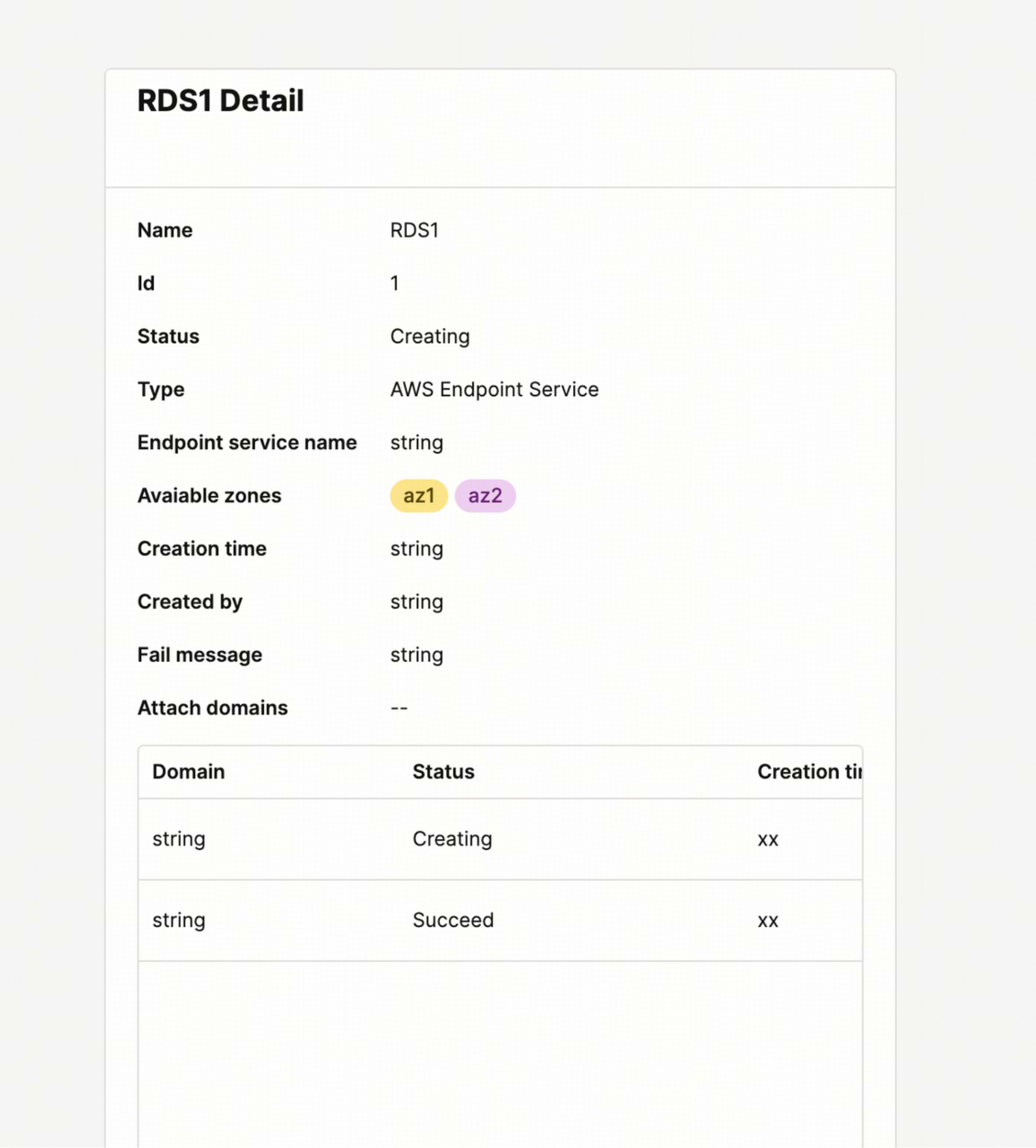
Enter endpoint service name

Please make sure the endpoint service add `acs:ram:*:<account_id>:*` to the whitelist and has at least one of the following azs: `<az1>,<az2>,<az3>`

## 2.2.5 View a private link connection

1. **ConnectionType-Specific Information**:
   - For **AWS Endpoint Service**: Displays "Endpoint Service Name" and "Available Zones".
   - For **AliCloud Endpoint Service**: Displays "Endpoint Service Name" and "Available Zones".
   - For future resource types: Custom fields will be added based on the resource type.
2. **Domain Attachment**: Display the domain list:
   - Domain

- Status: Choose one of them
  - succeed, failed (Creating, Deleting)
  - attached, failed (Attaching, detaching)
- Creation time (optional)



**RDS1 Detail**

| | |
|---|---|
| **Name** | RDS1 |
| **Id** | 1 |
| **Status** | Creating |
| **Type** | AWS Endpoint Service |
| **Endpoint service name** | string |
| **Avaiable zones** | az1 az2 |
| **Creation time** | string |
| **Created by** | string |
| **Fail message** | string |
| **Attach domains** | -- |

| Domain | Status | Creation ti |
|---|---|---|
| string | Creating | xx |
| string | Succeed | xx |

## 2.2.6 Delete a private link connection

1. **Confirmation Step**: Triggers a pop-up confirmation dialog to prevent accidental deletion (e.g., "Are you sure you want to delete this Private Link Connection? ").

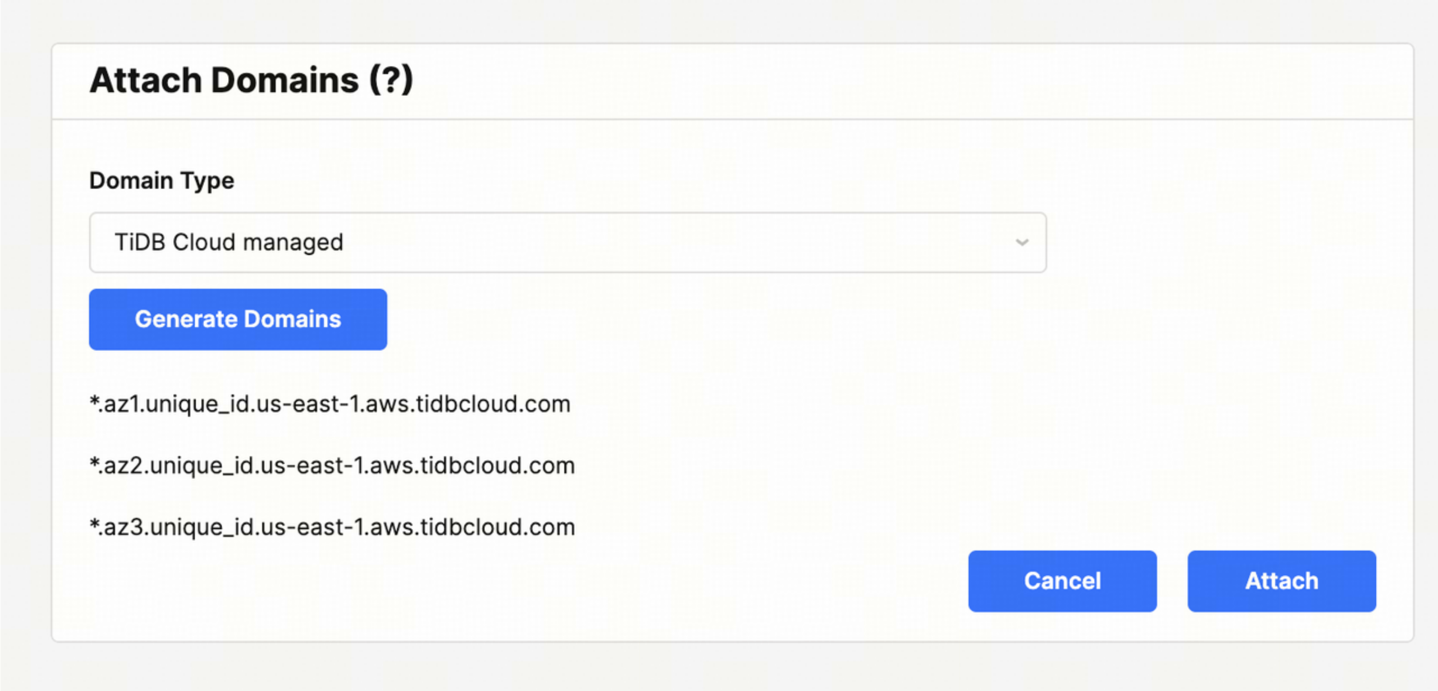
2. **Deletion Restriction**: Cannot delete a connection if it has attached domains (users must detach all domains first， we can gray the delete button in this case).

### 2.2.7 Attach domains

Attach domains diffs from different private link connection type!

AWS endpoint service

- TiDB Cloud managed
  - Only allow clicks to generate domains; not allowed to be customized by users
- Confluent Cloud
  - Input the unique_id to generate domains
- Others



Attach Domains (?)

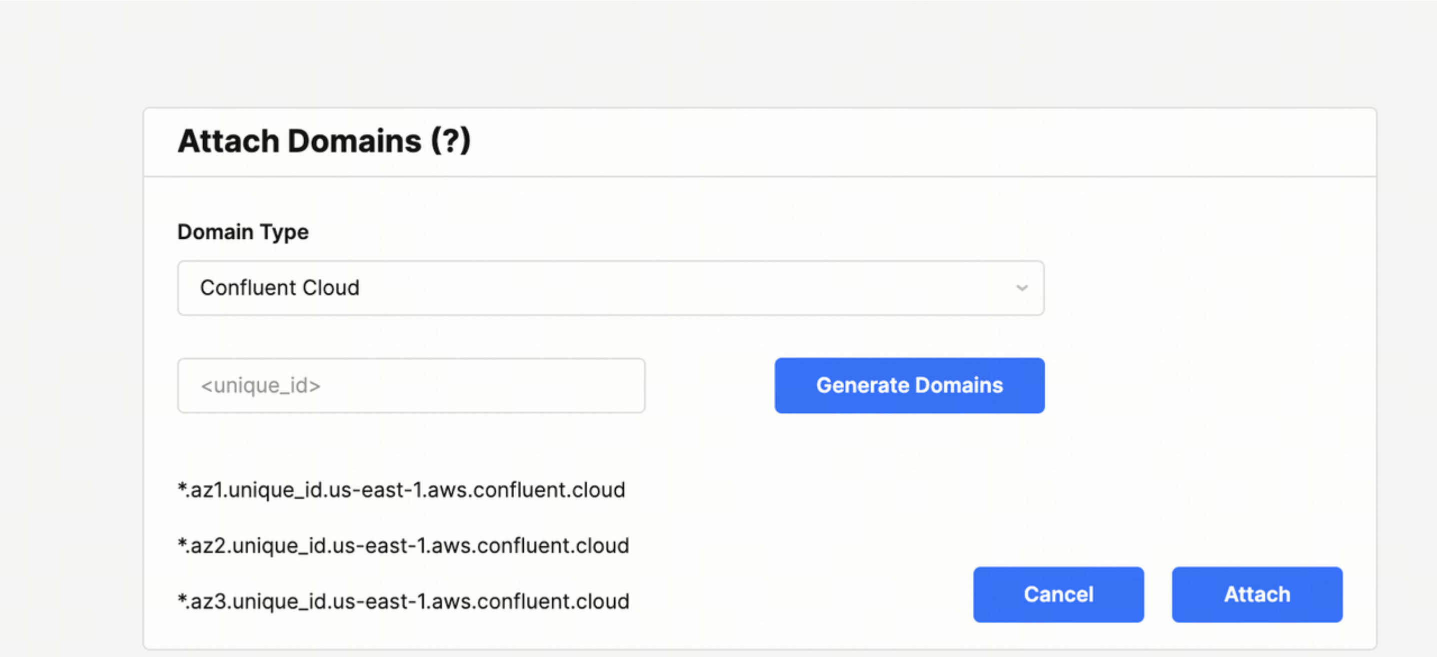
Domain Type

TiDB Cloud managed

*.az1.unique_id.us-east-1.aws.tidbcloud.com

*.az2.unique_id.us-east-1.aws.tidbcloud.com

*.az3.unique_id.us-east-1.aws.tidbcloud.com


Attach Domains (?)

Domain Type

Confluent Cloud

<unique_id>

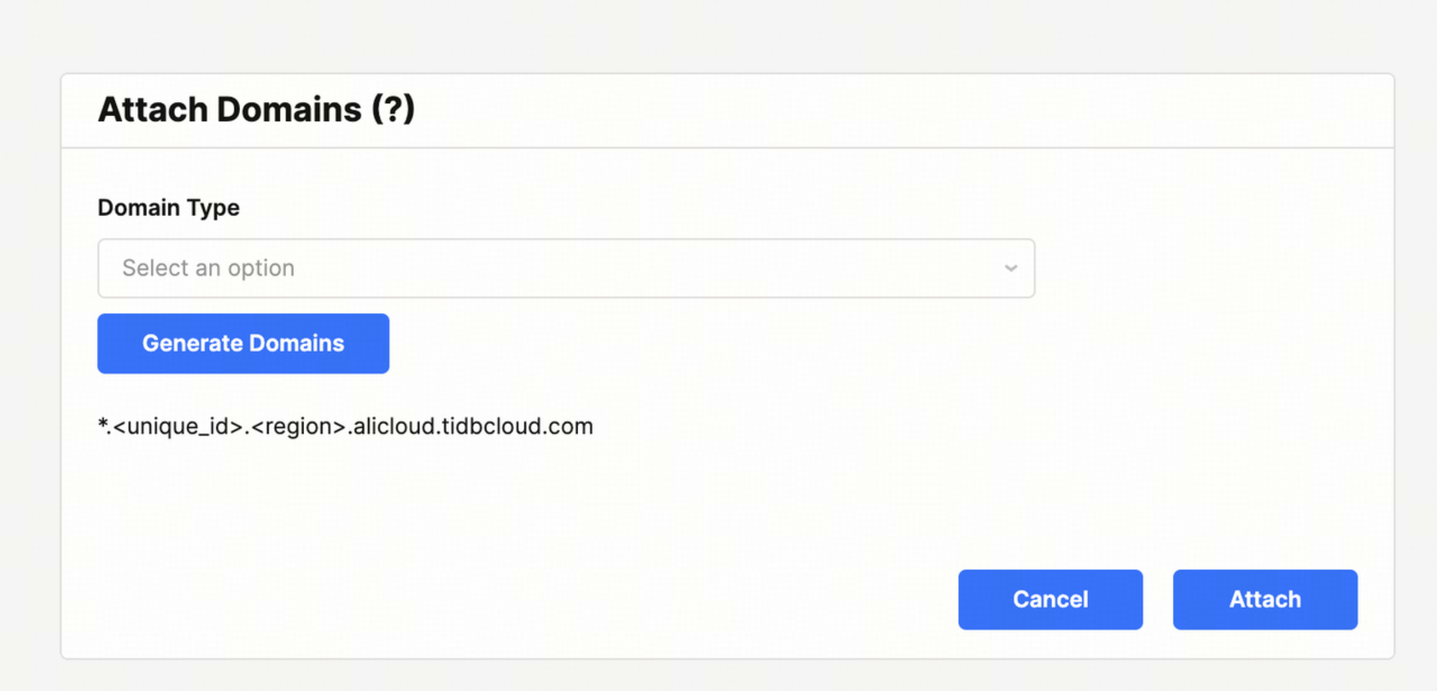
*.az1.unique_id.us-east-1.aws.confluent.cloud

*.az2.unique_id.us-east-1.aws.confluent.cloud

*.az3.unique_id.us-east-1.aws.confluent.cloud

AliCloud endpoint service

- TiDB Cloud managed: without azs


Attach Domains (?)

Domain Type

Select an option

*.<unique_id>.<region>.alicloud.tidbcloud.com

> **Currently, a private link can only attach domains once.**
>
> **If one wants to update the domains, they need to detach existing domains first.**

## 2.2.8 Detach domains

**Confirmation Step**: Triggers a pop-up dialog with the list of domains to be detached (e.g., "Are you sure you want to detach the following domains: xx,xx,xx

## 2.3 Private Link Connection Lifecycle

1. **Creation Restriction**: A Private Link Connection can only be created for a **running TiDB Cloud cluster** (cannot be created for stopped/paused clusters).
2. **Deletion Precondition**: All attached domains must be detached before deleting a Private Link Connection.
3. **Cluster Deletion Precondition**: All Private Link Connections associated with a cluster must be deleted before deleting the cluster.

## 2.4 Links

TODO