On this page

AWS PrivateLink

Overview

Dremio Cloud engines may be configured for greater security when connecting back to Dremio using AWS PrivateLink. PrivateLink allows for the easy connection to services like Dremio Cloud across varying accounts and virtual private clouds (VPC) configurations for a simplified network architecture.

Configuring the Security Group

For ease of configuration, we recommend provisioning the AWS PrivateLink within your existing Dremio security group. You must add inbound rules to the security group to allow communication between Dremio Cloud and the network interface for AWS PrivateLink. For additional information, see Security groups for your VPC.

To create or edit a security group and add both inbound and outbound rules, perform the steps outlined on the Creating an AWS Security Group topic.

Configuring Your Dremio Manual Installation

To use the PrivateLink with a new manual installation flow of Dremio, you'll need to obtain a VPC endpoint ID for the Network Settings section of the Cloud Connection step.

Creating a Cloud & VPC Endpoint

Dremio connects with VPCs using Clouds, which must be configured to your AWS account and VPC Endpoint. Preventing the exposure of your traffic outside your VPC and its associated services entails creating endpoints to serve as authorized traffic destinations. This effectively creates an elastic network interface within your subnet where each endpoint's private IP address serves as entry points for traffic bound to a specific service, such as Dremio.

For information on these processes, see Managing Clouds.

What Next

require encrypted communication, even within a private network, you'll need to enable the **Encrypt connection** setting on a source-by-source basis for any existing sources.

Troubleshooting

I'm receiving the following error: private-dns-enabled cannot be set because there is already a conflicting DNS domain for "X" in the VPC "Y".

If you encountered the following error while creating an endpoint for Dremio, this means that the Dremio-provided service name you used is already in use. Check any existing endpoints to ensure whether the same service name is already in use. Should no other endpoint exist with the same service name, contact Dremio's Infrastructure team for additional assistance.

My Dremio Cloud Engines are displaying an error about how they cannot access the AWS endpoint.

This error typically appears from the Dremio project's **Engines** screen when access to the AWS endpoint is disrupted or broken off completely. Most often, this happens when the endpoint used by Dremio is either deleted or the security group is altered incorrectly. As a result, Dremio will be unable to process any further queries until the endpoint issue is resolved.

My AWS endpoint was deleted.

If your AWS endpoint was somehow deleted, it cannot be restored. You must manually recreate a VPC Endpoint.

Additional Information

- VPC endpoints: Virtual devices used to facilitate secure connections between a VPC and supported services, like Dremio Cloud or a data source.

Was this page helpful? Yes No