Certainly! Here’s a detailed guide for setting up AWS PrivateLink between a service provider account (your AWS account) and a consumer (vendor) account:

### Service Provider Account (Your AWS Account)

1. \*\*Create a Network Load Balancer (NLB)\*\*:

- \*\*Navigate to the EC2 Console\*\* and go to \*\*Load Balancers\*\*.

- Click \*\*Create Load Balancer\*\* and choose \*\*Network Load Balancer\*\*.

- Configure the load balancer:

- \*\*Name\*\*: Enter a name for your NLB.

- \*\*Scheme\*\*: Choose \*\*Internal\*\* (if the service is internal) or \*\*Internet-facing\*\*.

- \*\*Listeners\*\*: Set up listeners for the ports on which your service is running.

- \*\*Availability Zones\*\*: Select the availability zones where your service is running.

- \*\*Create Target Groups\*\*:

- Define target groups with the instances or IP addresses that will handle the traffic.

- Register the targets (EC2 instances or IP addresses) with the target group.

- \*\*Review and Create\*\* the NLB.

2. \*\*Create a VPC Endpoint Service\*\*:

- Go to the \*\*VPC Console\*\* and navigate to \*\*Endpoint Services\*\*.

- Click \*\*Create Endpoint Service\*\*.

- \*\*Select Network Load Balancer\*\*: Choose the NLB you created.

- \*\*Enable Private DNS Name\*\* (optional): If you want to use a private DNS name.

- \*\*Configure Service Permissions\*\*:

- Allow connections from specific AWS accounts or VPCs.

- Add the AWS account ID of the consumer (vendor) account if known.

- \*\*Create\*\* the endpoint service.

3. \*\*Approve Endpoint Connection Requests\*\*:

- Go to the \*\*VPC Console\*\* and navigate to \*\*Endpoint Connections\*\*.

- You will see connection requests from the consumer account.

- \*\*Accept\*\* the connection requests.

4. \*\*Security Groups and Network ACLs\*\*:

- Ensure that the security groups associated with the NLB allow traffic on the relevant ports.

- Ensure network ACLs are configured to permit traffic as needed.

5. \*\*(Optional) Enable Logging\*\*:

- Enable logging for the Network Load Balancer and VPC Flow Logs for monitoring and debugging.

### Consumer (Vendor) Account

1. \*\*Create a VPC Endpoint\*\*:

- Go to the \*\*VPC Console\*\* and navigate to \*\*Endpoints\*\*.

- Click \*\*Create Endpoint\*\*.

- \*\*Service Category\*\*: Choose \*\*Find service by name\*\*.

- \*\*Service Name\*\*: Enter the service name provided by the service provider. It should be in the format `com.amazonaws.region.vpce-svc-xxxxxxxxxxxx`.

- \*\*VPC and Subnets\*\*: Select the VPC and subnets where you want the endpoint to be placed.

- \*\*Configure Security Groups\*\*: Attach security groups to the endpoint that allow outbound traffic to the NLB.

- \*\*Review and Create\*\* the endpoint.

2. \*\*Verify the Endpoint Connection\*\*:

- Go to the \*\*VPC Console\*\* and navigate to \*\*Endpoints\*\*.

- Check the \*\*Endpoint State\*\*. It should be `Available` if everything is configured correctly.

3. \*\*Testing Connectivity\*\*:

- Use tools like `curl` or `nc` from within the VPC to test connectivity to the service endpoint.

- Verify that the traffic is routing correctly and that you can reach the service exposed by the NLB.

4. \*\*Security Groups and Network ACLs\*\*:

- Ensure that security groups allow traffic from your VPC endpoint.

- Check network ACLs to ensure they permit traffic between the endpoint and the service.

### Summary

- \*\*Service Provider Account\*\*: Set up a Network Load Balancer, create an endpoint service, and approve connection requests.

- \*\*Consumer Account\*\*: Create a VPC endpoint to connect to the service provider’s endpoint service and ensure proper security and connectivity.

If you have specific configurations or need further details on any step, just let me know!

Sure! Here’s an updated document that includes VPC and subnet creation as part of the setup process:

---

# AWS PrivateLink Setup Documentation

## Service Provider Account

1. \*\*Create a VPC and Subnets\*\*

- \*\*Action Taken\*\*: A Virtual Private Cloud (VPC) and necessary subnets were created to host the service resources.

2. \*\*Create a Network Load Balancer (NLB)\*\*

- \*\*Action Taken\*\*: A Network Load Balancer was set up to route traffic to the service resources within the VPC.

3. \*\*Create a VPC Endpoint Service\*\*

- \*\*Action Taken\*\*: The NLB was associated with a VPC Endpoint Service to privately expose the service.

4. \*\*Approve Endpoint Connections\*\*

- \*\*Action Taken\*\*: Connection requests from the consumer account were reviewed and accepted.

5. \*\*Configure Security\*\*

- \*\*Action Taken\*\*: Security groups and network ACLs were configured to allow necessary traffic to and from the NLB.

## Consumer (Vendor) Account

1. \*\*Create a VPC and Subnets\*\*

- \*\*Action Taken\*\*: A Virtual Private Cloud (VPC) and necessary subnets were created for the applications.

2. \*\*Create a VPC Endpoint\*\*

- \*\*Action Taken\*\*: A VPC Endpoint was established to connect to the service provider’s VPC Endpoint Service.

3. \*\*Verify Connection\*\*

- \*\*Action Taken\*\*: The status of the VPC Endpoint was verified, and connectivity to the service was tested.

4. \*\*Configure Security\*\*

- \*\*Action Taken\*\*: Security groups and network ACLs were adjusted to permit traffic to and from the VPC Endpoint.

---

This document outlines that all necessary steps for setting up AWS PrivateLink, including the creation of VPCs and subnets, were completed to ensure secure and private communication between the service provider and the consumer.