Architecture Diagrams

Centralizing Amazon VPC Endpoints with AWS Transit Gateway

Centralizing Amazon VPC Endpoints with AWS Transit Gateway: Architecture Diagrams

Table of Contents

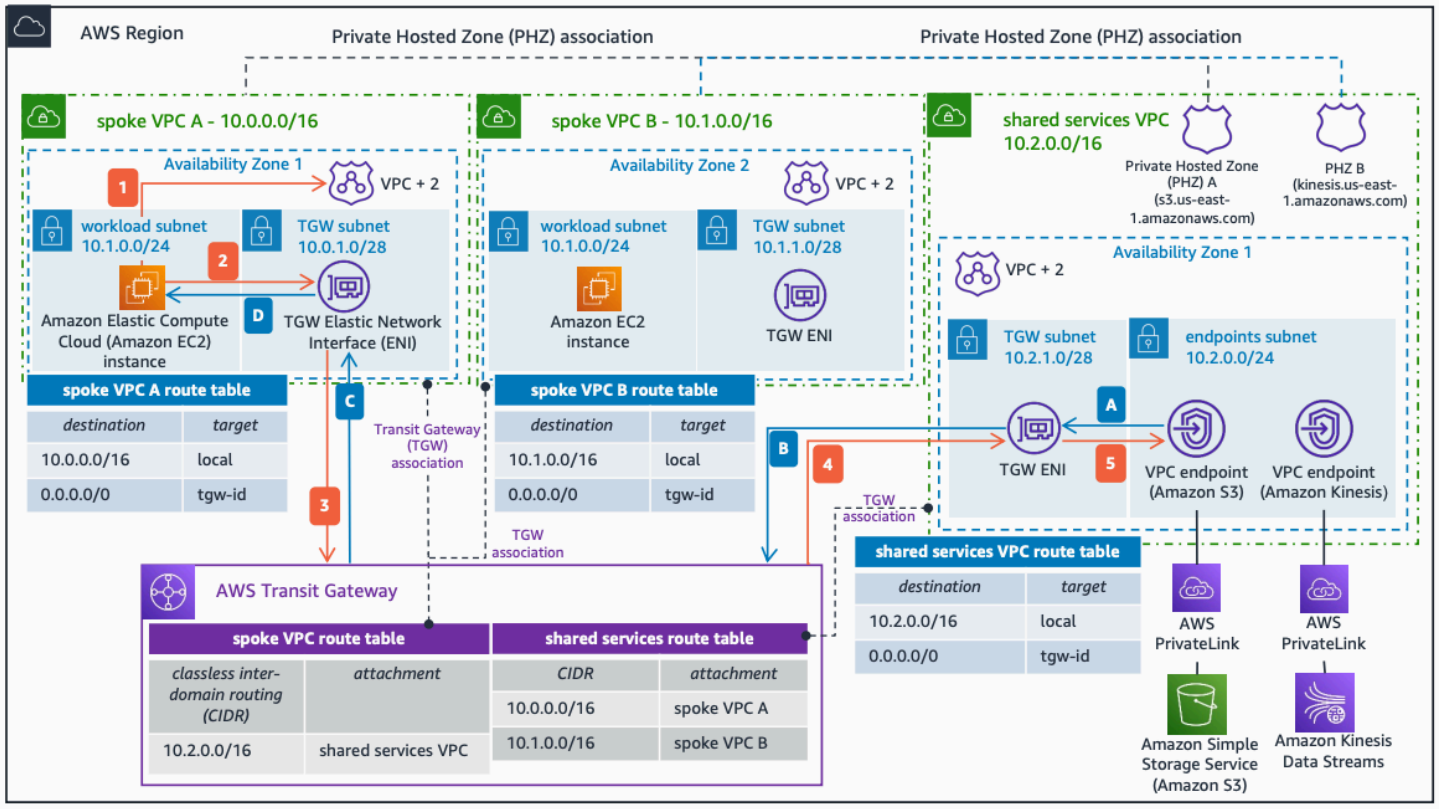
Centralized endpoint access 1
Centralizing Amazon VPC endpoint access architecture 1
Further reading 2
Diagram history 2
On-premises access 4
Accessing Amazon VPC endpoints from on-premises architecture 4
Further reading 5
Diagram history 5

Centralizing Amazon VPC Endpoint Access with AWS Transit Gateway

Publication date: **March 25, 2022 (Diagram history)**

This architecture centralizes Amazon VPC interface endpoints in a shared services VPC using AWS Transit Gateway. You create custom Amazon Route 53 private hosted zones and associate them to all VPCs that consume these endpoints.

Centralizing Amazon VPC endpoint access architecture



The following steps describe the data flow in this architecture:

1. An Amazon Elastic Compute Cloud instance in **spoke VPC A** resolves the Amazon Simple Storage Service domain name by querying the VPC+2 resolver. Private hosted zone A associates with **spoke VPC A** to complete domain resolution.
2. The instance sends the traffic to the Transit Gateway ENI as per the **spoke VPC A** route table.
3. The traffic forwards to AWS Transit Gateway.

4. The **Transit Gateway spoke VPC route table** forwards the traffic to the **shared services VPC**.
5. The Transit Gateway ENI in the shared services VPC forwards the traffic to the corresponding interface endpoint connecting to Amazon S3.

The return path follows these steps:

A. The VPC endpoint sends the response back to the Transit Gateway ENI.

B. The traffic forwards to AWS Transit Gateway.

C. The **Transit Gateway shared services route table** sends the traffic to **spoke VPC A**.

D. The Transit Gateway ENI delivers the response to the destination Amazon EC2 instance.

For more information about interface endpoints and AWS PrivateLink, see Access an AWS service using an interface VPC endpoint.

To see an example of this architecture in Terraform, see AWS Hub and Spoke Architecture with Shared Services VPC.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	March 25, 2022
Initial publication	Reference architecture diagram first published.	March 25, 2022

Note

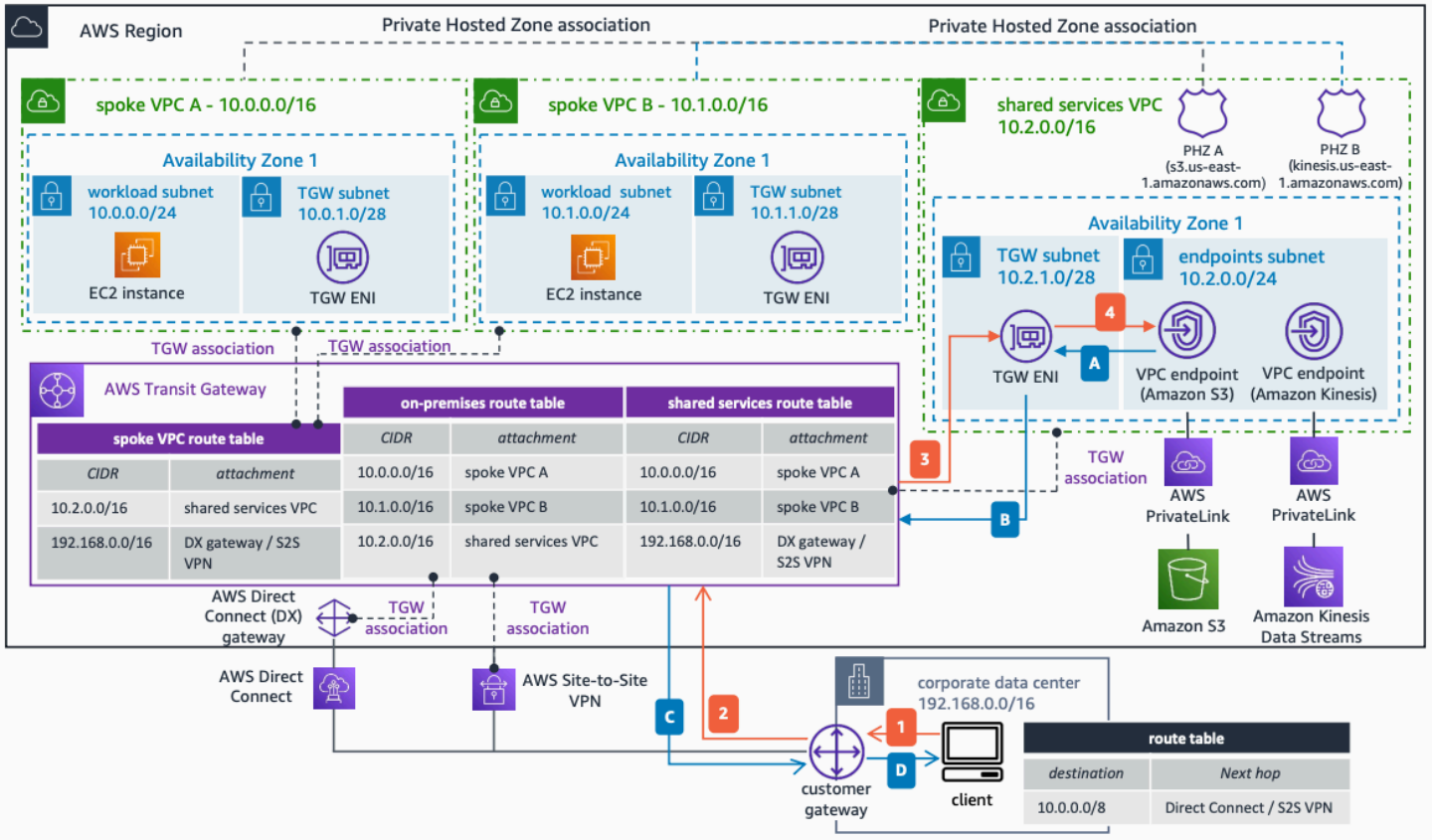
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

Accessing Amazon VPC Endpoints from On-Premises Environments

Publication date: **March 25, 2022 (Diagram history)**

This architecture uses AWS Transit Gateway to access interface Amazon VPC endpoints from on-premises environments. It uses AWS Direct Connect or AWS Site-to-Site VPN as transport between AWS and the corporate data center.

Accessing Amazon VPC endpoints from on-premises architecture



The following steps describe the data flow in this architecture:

1. A client in the corporate data center sends the request through the customer gateway. It resolves the DNS name to obtain the private IP address of the VPC endpoint.

2. The traffic sends to AWS Transit Gateway through an AWS Direct Connect link or an AWS Site-to-Site VPN connection.
3. The **Transit Gateway on-premises route table** forwards the traffic to the **shared services VPC**.
4. The Transit Gateway ENI forwards the traffic to the VPC endpoint.

The return path follows these steps:

A. The VPC endpoint sends the response back to the Transit Gateway ENI.

B. The traffic forwards to AWS Transit Gateway.

C. The **Transit Gateway shared services route table** sends the traffic to the corporate data center through the Direct Connect link or Site-to-Site VPN connection.

D. The response arrives at the on-premises client.

For more information about centralizing AWS PrivateLink endpoints with AWS Transit Gateway, see the Integrating AWS Transit Gateway with AWS PrivateLink and Amazon Route 53 Resolver blog post.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	March 25, 2022

Initial publication	Reference architecture diagram first published.	March 25, 2022

Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.