AWS Local Zones

User Guide

AWS Local Zones: User Guide

Table of Contents

What is AWS Local Zones?

AWS Local Zones places compute, storage, database, and other select AWS resources close to large population and industry centers. You can use Local Zones to provide your users with low-latency access to your applications.

Why use AWS Local Zones?

Here are some reasons to use AWS Local Zones.

- **Run low-latency applications at the edge** — Build and deploy applications close to end users to enable real-time gaming, live streaming, augmented and virtual reality (AR/VR), virtual workstations, and more.
- **Simplify hybrid cloud migrations** — Migrate your applications to a nearby AWS Local Zone, while still meeting the low-latency requirements of hybrid deployment.
- **Meet stringent data residency requirements** — Comply with state and local data residency requirements in sectors such as healthcare, financial services, iGaming, and government.

Local Zones concepts

The following are the key concepts:

- **Local Zone** — An extension of an AWS Region in geographic proximity to your users, where the Local Zone infrastructure is deployed.
- **VPC** — A virtual private cloud (VPC) is a virtual network that closely resembles a traditional network that you'd operate in your own data center. You create subnets in your VPCs and deploy AWS resources, such as Amazon EC2 instances, in your subnets. A VPC can span Availability Zones, Local Zones, and Wavelength Zones.
- **Local Zone subnet** — A subnet that you create in a Local Zone. You can deploy supported AWS resources in your Local Zone subnets.
- **Network Border Group** — A unique set of Availability Zones, Local Zones, or Wavelength Zones from which AWS advertises IP addresses.

Deploying in Local Zones

You can manage your AWS resources in a Local Zone using the following options:

- **AWS Management Console** — Provides a web interface that you can use to manage your Local Zones and create resources in your Local Zones.
- **AWS Command Line Interface (AWS CLI)** — Provides commands for a broad set of AWS services, including Amazon VPC, and is supported on Windows, macOS, and Linux. The services that you use in Local Zones continue to use their own namespaces. For example, Amazon EC2 uses the "ec2" namespace, and Amazon EBS uses the "ebs" namespace. For more information, see AWS Command Line Interface.
- **AWS SDKs** — Provides language-specific APIs and takes care of many of the connection details, such as calculating signatures, handling request retries, and handling errors. For more information, see AWS SDKs.

Pricing

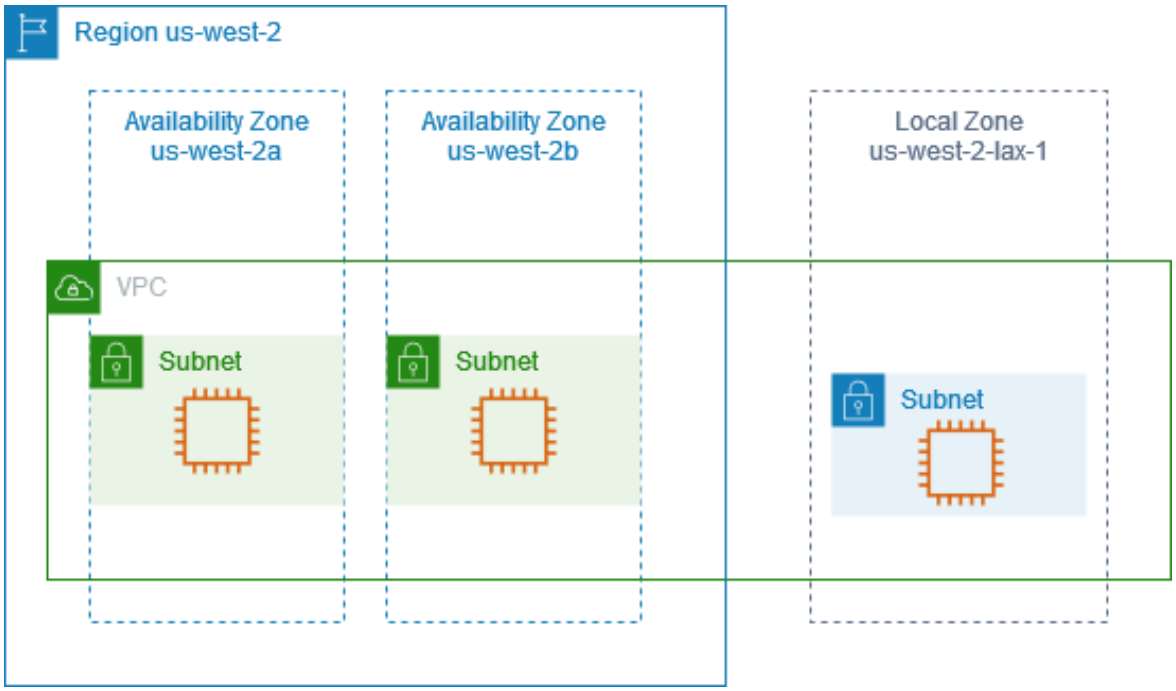
There's no additional charge for enabling Local Zones. You pay only for the resources that you deploy in your Local Zones. AWS resources in Local Zones have different prices than they do in parent AWS Regions. For more information, see AWS Local Zones pricing.

How Local Zones work

A Local Zone is an extension of an AWS Region in geographic proximity to your users. Local Zones have their own connections to the internet and support AWS Direct Connect, so that resources created in a Local Zone can serve applications that require low latency.

To use a Local Zone, you must first enable it. Next, you create a subnet in the Local Zone. Finally, you launch resources in the Local Zone subnet. For more detailed instructions, see *Getting started* (p. 5).

The following diagram illustrates an account with a VPC in the AWS Region `us-west-2` that is extended to the Local Zone `us-west-2-lax-1`. Each zone in the VPC has one subnet, and each subnet has one EC2 instance.



Available Local Zones

The code for a Local Zone is the Region code of its parent Region, followed by an identifier that indicates its physical location. For example, `us-west-2-lax-1` is in Los Angeles.

Local Zones are available in the following Regions:

- US East (N. Virginia)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Tokyo)
- Europe (Frankfurt)

For the complete list of supported and announced Local Zones, see AWS Local Zones Locations.

AWS resources supported in Local Zones

Creating a resource in a Local Zone subnet puts it close to your users. For a list of services with resources that are supported in Local Zones, see AWS Local Zones features.

Considerations

- Local Zone subnets follow the same routing rules as Availability Zone subnets, including the use of route tables, security groups, and network ACLs.
- Outbound internet traffic leaves a Local Zone from the Local Zone.
- Network traffic will hairpin to the AWS Region when connecting from an on-premises location into a Local Zone using a Transit Gateway.
- Traffic within the US that is destined for a subnet in a Local Zone using AWS Direct Connect does not travel through the parent Region of the Local Zone. Instead, traffic takes the shortest path to the Local Zone. This decreases latency and helps make your applications more responsive.

  If you require a more resilient connection, implement more than one AWS Direct Connect between your on-premises locations and the Local Zone. For more information on building resilience with AWS Direct Connect, see AWS Direct Connect Resiliency Recommendations.
- The only Local Zones that support IPv6 are `us-west-2-lax-1a` and `use-west-2-lax-1b`.
- You cannot create VPC endpoints inside Local Zone subnets.
- The AWS Site-to-Site VPN is not available in Local Zones. Use a software-based VPN to establish a site-to-site VPN connection into a Local Zone.
- Generally, the Maximum Transmission Unit (MTU) is as follows:
  - 9001 bytes between Amazon EC2 instances in the same Local Zone.
  - 1500 bytes between internet gateway and a Local Zone.
  - 1468 bytes between AWS Direct Connect and a Local Zone.
  - 1300 bytes between an Amazon EC2 instance in a Local Zone and an Amazon EC2 instance in the Region.

Resources

Learn how to get started with AWS Local Zones with the following resources:

- Getting started
- Get Started Deploying Low Latency Applications with AWS Local Zones

Getting started with AWS Local Zones

To get started with AWS Local Zones, you must first enable a Local Zone through the Amazon EC2 console or the AWS CLI. Next, create a subnet in a VPC in the parent Region, specifying the Local Zone when you create it. Finally, create AWS resources in the Local Zone subnet.

Tasks

Step 1: Enable a Local Zone

You can use the Amazon EC2 console or a command line interface to determine which Local Zones are available for your account, and then enable the Local Zone that you want to use.

To enable a Local Zone using the console

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. From the navigation bar, choose the **Regions** selector and then choose the parent Region.
3. On the navigation pane, choose **EC2 Dashboard**.
4. In the upper-right corner of the page, choose **Account attributes**, **Zones**.
5. For the Local Zone to enable, choose **Manage**.
6. For **Zone group**, choose **Enabled**.
7. Choose **Update zone group**.

To enable a Local Zone using the AWS CLI

Use the describe-availability-zones command as follows to describe all Local Zones in the specified Region.

```
aws ec2 describe-availability-zones \
  --region us-west-2 \
  --filters Name=zone-type,Values=local-zone \
  --all-availability-zones
```

Use the modify-availability-zone-group command as follows to enable a specific Local Zone.

```
aws ec2 modify-availability-zone-group \
  --region us-west-2 \
  --group-name us-west-2-lax-1 \
  --opt-in-status opted-in
```

Step 2: Create a Local Zone subnet

When you add a subnet, you must specify an IPv4 CIDR block from the VPC IPv4 CIDR block. If the VPC has an IPv6 CIDR block, you can specify an IPv6 CIDR block from the VPC IPv6 CIDR block. You can specify the Local Zone where the subnet resides. You can have multiple subnets in the same Local Zone.

To add a Local Zone subnet to a VPC using the console

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. From the navigation bar, choose the **Regions** selector and then choose the parent Region.
3. In the navigation pane, choose **Subnets**.
4. Choose **Create subnet**.
5. For **VPC**, select the VPC.
6. For **Subnet name**, enter a name for your subnet. Doing so creates a tag with a key of `Name` and the value that you specify.
7. For **Availability Zone**, choose the Local Zone that you enabled.
8. Specify an IPv4 CIDR block for the subnet.
9. (Optional) To add a tag, choose **Add new tag** and enter the tag key and tag value.
10. Choose **Create subnet**.

To add a Local Zone subnet to a VPC using the AWS CLI

Use the create-subnet command as follows to create a subnet for the specified VPC in the specified Local Zone.

```
aws ec2 create-subnet \
  --region us-west-2 \
  --availability-zone us-west-2-lax-1a \
  --vpc-id vpc-081ec835f303f720e
```

Step 3: Create a resource in your Local Zone subnet

After you create a subnet in a Local Zone, you can deploy AWS resources in the Local Zone. For example, the following procedure shows how to launch an EC2 instance in a Local Zone.

To launch an EC2 instance in a Local Zone subnet using the console

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Choose **Launch instance**.
3. For **Name and tags**, enter a name for the instance (for example, *my-lz-instance*). Doing so creates a tag with a key of `Name` and the value that you specify.
4. For **Application and OS Images (Amazon Machine Image)**, choose an operating system for your instance.
5. For **Instance type**, select an instance type that's supported in a Local Zone, such as `t3.micro`.
6. For **Key pair (login)**, choose an existing key pair or create a new one.
7. For **Network settings**, choose **Edit**, and then select your VPC, Local Zone subnet, and security group.
8. When you are finished configuring your instance, choose **Launch instance**.

To launch an EC2 instance in a Local Zone subnet using the AWS CLI

Use the run-instances command as follows to launch an instance in the specified Local Zone subnet.

```
aws ec2 run-instances \
  --region us-west-2 \
  --subnet-id subnet-08fc749671b2d077c \
  --instance-type t3.micro \
  --image-id ami-0abcdef1234567890 \
  --security-group-ids sg-0b0384b66d7d692f9 \
  --key-name my-key-pair
```

Step 4: Clean up

When you are finished with a Local Zone, you can disable it. Before you can disable a Local Zone, you must delete the resources in the Local Zone.

To disable a Local Zone using the console

1. On the navigation pane, choose **EC2 Dashboard**.
2. In the upper-right corner of the page, choose **Account attributes**, **Zones**.
3. For the Local Zone to enable, choose **Manage**.
4. For **Zone group**, choose **Disabled**.
5. Choose **Update zone group**.

To disable a Local Zone using the AWS CLI

Use the modify-availability-zone-group command as follows to disable a specific Local Zone.

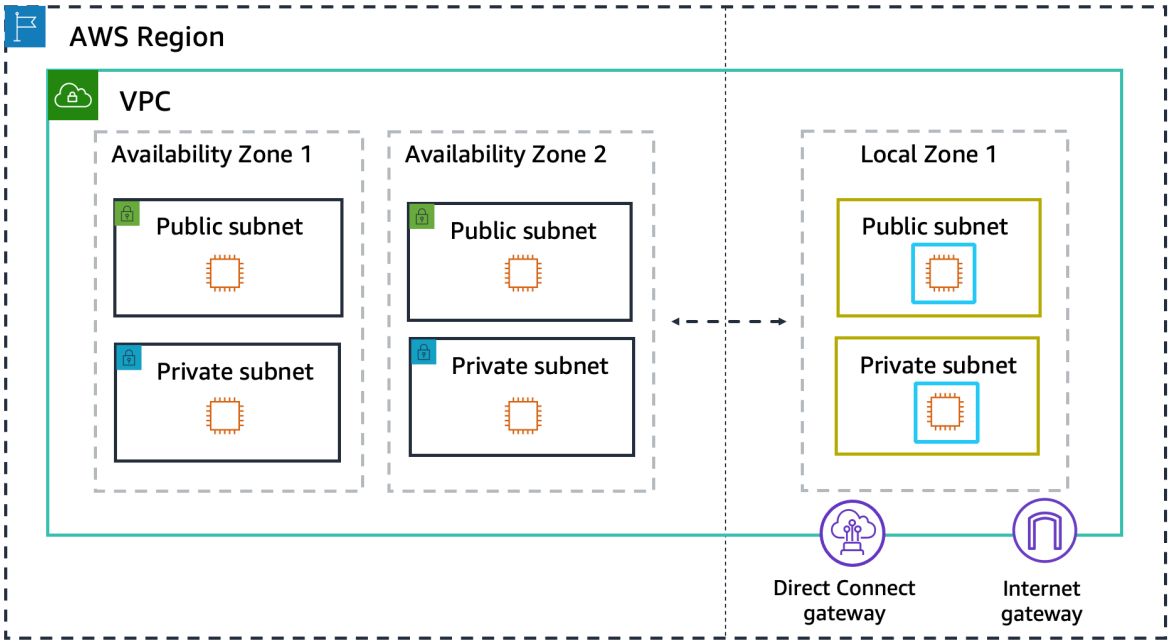
```
aws ec2 modify-availability-zone-group \
  --region us-west-2 \
  --group-name us-west-2-lax-1 \
  --opt-in-status not-opted-in
```

Connectivity options for Local Zones

There are many ways to connect users and applications to resources running in a Local Zone.

You build Local Zones into your network architecture in the same way you choose an Availability Zone. Your workloads use the same application programming interfaces (APIs), security models, and toolsets. You can extend any VPC from a parent Region into a Local Zone by creating a new subnet and assigning it to the Local Zone. When you create a subnet in AWS Local Zones, we extend your VPC to that Local Zone and your VPC treats the subnet the same as any subnet in any other Availability Zone and automatically adjusts any relevant gateways and route tables.

The following diagram shows a network with resources running in two Availability Zones and in a Local Zone within an AWS Region. The Local Zone network can have public or private subnets, internet gateways (IGW), and AWS Direct Connect gateways (DXGW). Workloads running in the Local Zone can directly access workloads or AWS services that live in any AWS Region.



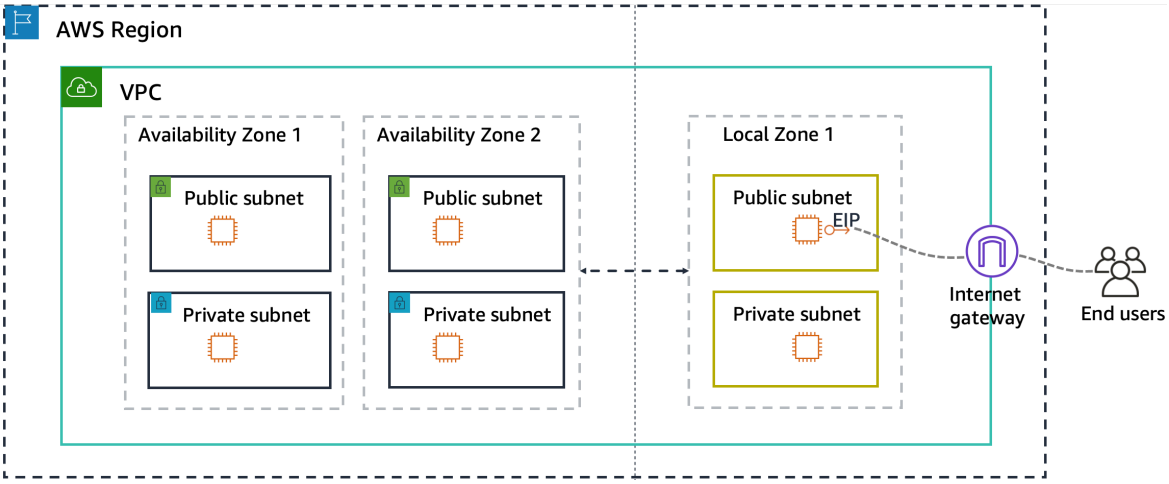
The following sections explain the different ways to connect to resources in a Local Zone.

Connection options

Internet gateway connection to the internet

Internet gateways provide public connectivity to applications running in AWS Regions and/or in Local Zones.

In the following diagram, end users access a public-facing application in Local Zone 1. Traffic goes directly to the internet gateway in Local Zone 1 without going through the parent AWS Region. Use this type of connectivity for low-latency use-cases where you want your applications to be closer to end users than an AWS Region can provide.

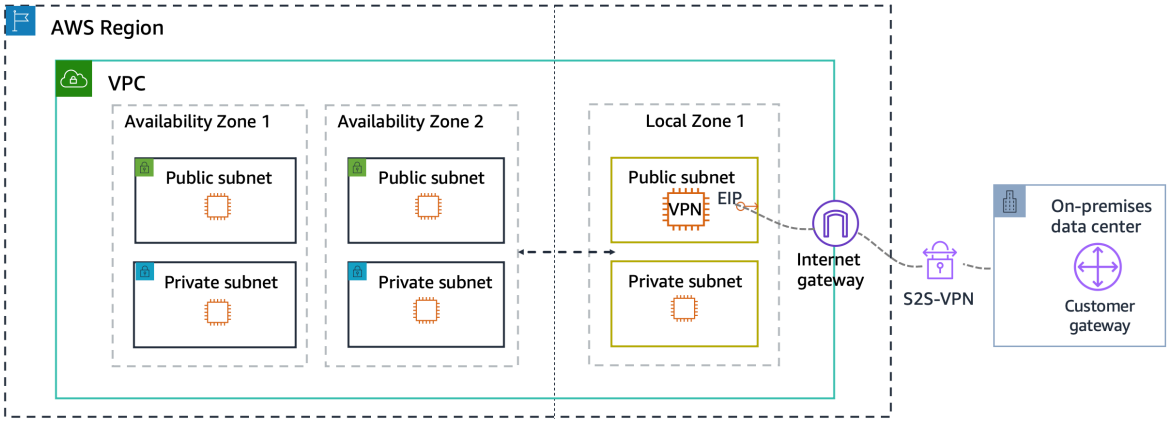


Note
Unlike internet gateways, NAT gateways live in the AWS Region. If NAT is required in the Local Zone, or if traffic must ingress and egress directly from the Local Zone, use NAT instances. For more information, see NAT instances in the *Amazon VPC User Guide*.

Amazon EC2-based VPN connection to a data center

A VPN connection can provide secure, two-way communication between workloads running in an on-premises data center and a Local Zone. For Local Zones, you must deploy a software-based VPN solution on an Amazon EC2 instance. Visit the AWS Marketplace and find VPN solutions that are ready to run on an Amazon EC2 instance. You'll also need to deploy an internet gateway so that you can establish your site-to-site VPN connection.

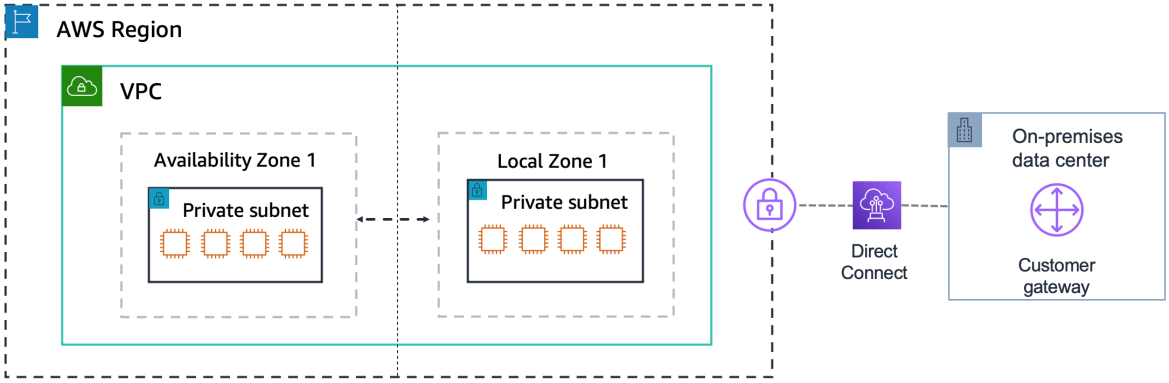
The following diagram shows a data center connected to Local Zone 1 by a software-based VPN solution running on an Amazon EC2 instance in Local Zone 1. This allows for encrypted connectivity from the data center directly into the Local Zone without traffic going through the parent Region.



AWS Direct Connect connection to a data center

With AWS Direct Connect, you transfer data privately and directly from your data center into and out of Local Zones using a Public Virtual Interface (VIF) or Private VIF. AWS Direct Connect provides similar benefits to using a software-based VPN on Amazon EC2, but bypasses the public internet and reduces the overheard required to manage the connection to Local Zones.

The following diagram shows an AWS Direct Connect connection between a Local Zones and data center.

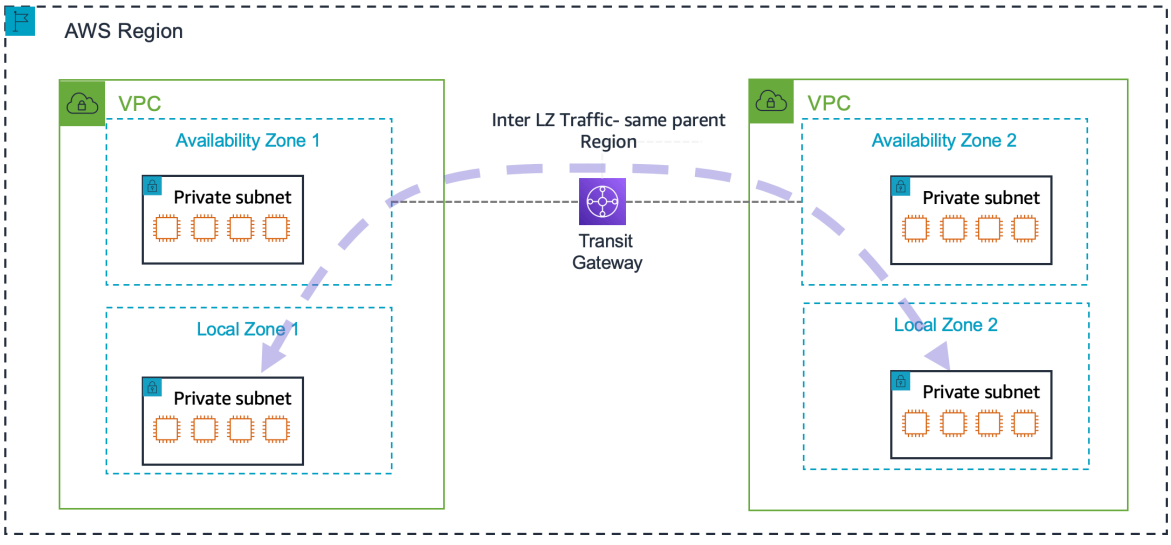


During a hybrid cloud migration, you can migrate your applications to Local Zones while using AWS Direct Connect to communicate back to other parts of your applications in the data center. An example is migrating the front end of an application to Amazon EC2, Amazon ECS, or Amazon EKS in a Local Zone and having the back-end database remain in the data center. Eventually, you can migrate the database to the Local Zone and the entire application to an AWS Region.

AWS Transit Gateway connection between Local Zones

AWS Transit Gateway can be used to connect one Local Zone to another within the same parent Region.

The following diagram shows the TGW connection between two Local Zones in the same Region.

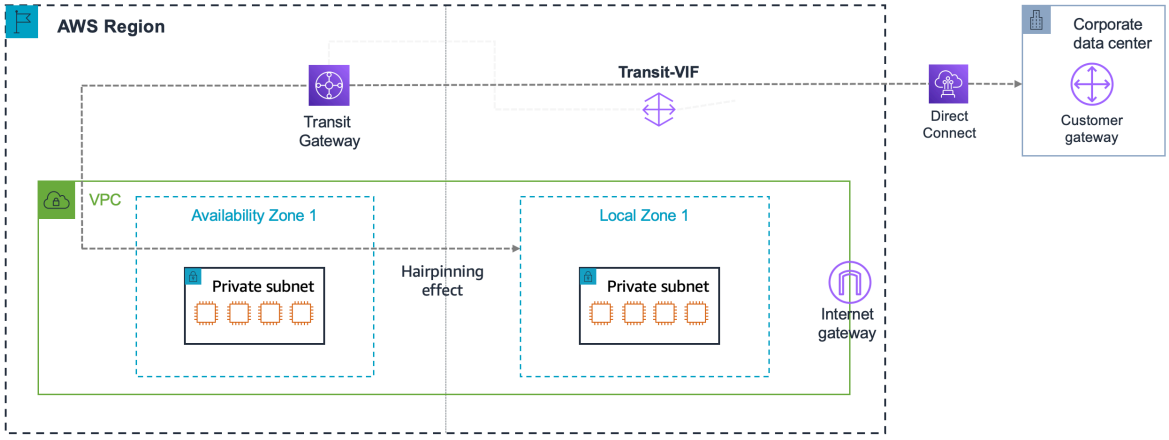


A TGW connection between Local Zones is useful when you have workloads in different Local Zones and also require network connectivity between them.

AWS Transit Gateway connection to a data center

AWS Transit Gateway (TGW) connects your Amazon Virtual Private Cloud and on-premises networks through a central hub. TGW live in AWS Regions. While you can use TGW to connect data centers to a Local Zone, this is not a direct connection.

The following diagram shows the connection from the customer gateway over the Direct Connect into the TGW in the AWS Region using a Transit VIF. From there, it connects to the VPC to enable traffic to the Local Zone.



When you use this connectivity option for Local Zones, all traffic from the data center to the Local Zone will first go to the parent Region (also known as “hairpinning”) of the destination Local Zone and then to the Local Zone. Using a TGW to connect to a Local Zone from your premises is not an ideal path since your data must travel to the Region first, increasing latency.

Document history for the AWS Local Zones User Guide

The following table describes the documentation releases for AWS Local Zones.

Change	Description	Date
Initial release (p. 12)	Initial release of the AWS Local Zones User Guide	November 17, 2022