User Guide

AWS Local Zones

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.

Managing 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 for AWS Local Zones

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.

AWS Local Zones concepts

These are the essential concepts in AWS Local Zones:

- **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.
- **Group Long Name** — The Local Zone group name.
- **Network Border Group** — A unique group from which AWS advertises public IP addresses. It consists of Availability Zones, Local Zones, or Wavelength Zones. A pool of public IP addresses can be explicitly allocated for use in a network border group. Once provisioned, IP addresses cannot move between network border groups. For example, the `us-west-2-lax-1` network border group consists of two Local Zones in Los Angeles, and the `us-east-1-bos-1` network border group consists of a single Local Zone in Boston. You can move an IP address between the two Los Angeles Local Zones, but you cannot move an IP address from a Los Angeles Local Zone to the Boston Local Zone.

  When creating a subnet, you will find the network border group for the Local Zones in the **Availability Zone** drop-down list.
- **Parent Region** — The Region that handles some of the Local Zone and Wavelength Zone control plane operations, such as API calls.
- **Parent Zone ID** — The ID of the zone that handles some of the Local Zone and Wavelength Zone control plane operations, such as API calls
- **Geography** — The geography for a Local Zone is the specific physical location of its infrastructure. This information can help you meet your regulatory, compliance, and operational requirements.

For more information, see:

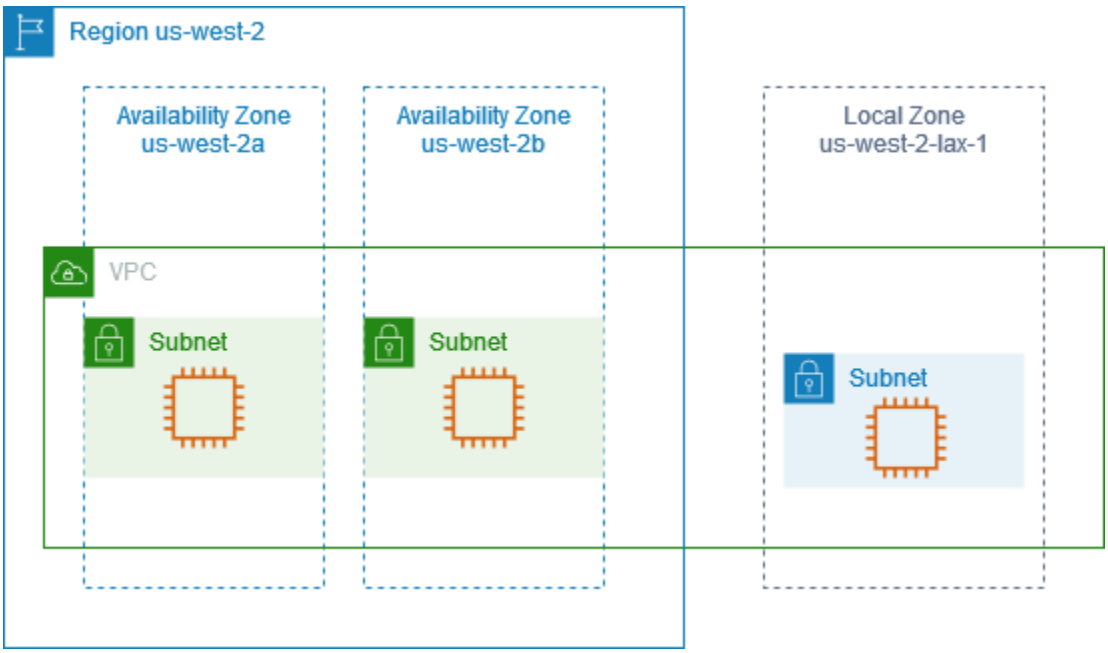
- AWS Site-to-Site VPN concepts in the *AWS Site-to-Site VPN User Guide*.
- Route table concepts in the *Amazon VPC User Guide*.

How AWS 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 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*.

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.



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

- Amazon EBS snapshots storage vary depending on the Local Zone selected, see AWS Local Zones features.

- Default encryption behavior of Amazon EBS volume varies depending on the Local Zone selected, see AWS Local Zones features.
- 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.
- You cannot select a subnet from a Local Zone while creating a Cloud WAN or transit gateway VPC attachment. Doing so will result in an error.
- Traffic that is destined for a subnet in a Local Zone using 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 Direct Connect between your on-premises locations and the Local Zone. For more information on building resilience with Direct Connect, see Direct Connect Resiliency Recommendations.
- The following Local Zones support IPv6: `us-east-1-atl-2a`, `us-east-1-chi-2a`, `us-east-1-dfw-2a`, `us-east-1-iah-2a`, `us-east-1-mia-2a`, `us-east-1-nyc-2a`, `us-west-2-lax-1a`, `us-west-2-lax-1b`, and `us-west-2-phx-2a`.
- The following Local Zones support edge association with virtual private gateway (VGW): `us-east-1-atl-2a`, `us-east-1-chi-2a`, `us-east-1-dfw-2a`, `us-east-1-iah-2a`, `us-east-1-mia-2a`, `us-east-1-nyc-2a`, `us-west-2-lax-1a`, `us-west-2-lax-1b`, and `us-west-2-phx-2a`.

  To understand edge association and other route-table concepts, see Route table concepts in the *Amazon VPC User Guide*.

  To understand virtual private gateway and other AWS Site-to-Site VPN concepts, see Concepts in the *AWS Site-to-Site VPN User Guide*.
- 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 an internet gateway and a Local Zone.

- 1500 bytes between Direct Connect and all Local Zones except:
  - 8500 bytes for `us-east-1-atl-2a`, `us-east-1-chi-2a`, `us-east-1-dfw-2a`, `us-east-1-iah-2a`, `us-west-2-lax-1a`, `us-west-2-lax-1b`, `us-east-1-mia-2a`, `us-east-1-nyc-2a`, and `us-west-2-phx-2a`
- 1300 bytes between an Amazon EC2 instance in a Local Zone and an Amazon EC2 instance in the Region for all Local Zones except:
  - 9001 bytes for `us-west-2-lax-1a` and `us-west-2-lax-1b`
  - 8801 bytes for `us-east-1-atl-2a`, `us-east-1-chi-2a`, `us-east-1-dfw-2a`, `us-east-1-iah-2a`, `us-east-1-mia-2a`, `us-east-1-nyc-2a`, and `us-west-2-phx-2a`

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

Available Local Zones

AWS Local Zones is available around the world. Find the Local Zone closest to you.

The following terms are identifying details associated with a Local Zone.

- Group Long Name - The name for a group of Local Zones.
- Local Zone Name - The name of the Local Zone.
- Local Zone ID - The ID of the Local Zone. The ID is the code of the Local Zone's parent Region followed by an identifier for its location. For example, `us-west-2-lax-1a` is in Los Angeles where `us-west-2` is the parent Region code and `lax-1a` is the location identifier.
- Network Border Group - A unique group from which AWS advertises public IP addresses.
- Parent Region Name - The name of the AWS Region for the Local Zone.
- Parent Zone ID - The ID of the parent AWS zone that handles some of the Local Zone control plane operations, such as API calls.
- Geography - The geography for a Local Zone is the specific physical location of its infrastructure.

For more information on Local Zone terms, see Concepts

List of Local Zones

Locate the Local Zone closest to you.

AWS Local Zones

- North America
- South America
- Africa
- Asia Pacific
- Europe
- Middle East

North America

The following Local Zones are available in North America:

Local Zone Group Long Name	Local Zone Name	Local Zone ID	Network Border Group	Parent Region Name	Parent Zone ID	Geography
México (Querétaro)	us-east-1-qro-1a	use1-qro1-az1	us-east-1-qro-1	us-east-1	use1-az1	Mexico
US East (Atlanta) 2	us-east-1-atl-2a	use1-atl2-az1	us-east-1-atl-2	us-east-1	use1-az5	Georgia, United States of America
US East (Atlanta) *	us-east-1-atl-1a	use1-atl1-az1	us-east-1-atl-1	us-east-1	use1-az4	Georgia, United States of America
US East (Boston)	us-east-1-bos-1a	use1-bos1-az1	us-east-1-bos-1	us-east-1	use1-az4	Massachusetts, United States of America
US East (Chicago) 2	us-east-1-chi-2a	use1-chi2-az1	us-east-1-chi-2	us-east-1	use1-az6	Illinois, United States of America
US East (Chicago)*	us-east-1-chi-1a	use1-chi1-az1	us-east-1-chi-1	us-east-1	use1-az5	Illinois, United States

Local Zone Group Long Name	Local Zone Name	Local Zone ID	Network Border Group	Parent Region Name	Parent Zone ID	Geography
						of America
US East (Dallas) 2	us-east-1-dfw-2a	use1-dfw2-az1	us-east-1-dfw-2	us-east-1	use1-az4	Texas, United States of America
US East (Dallas)*	us-east-1-dfw-1a	use1-dfw1-az1	us-east-1-dfw-1	us-east-1	use1-az1	Texas, United States of America
US East (Houston) 2	us-east-1-iah-2a	use1-iah2-az1	us-east-1-iah-2	us-east-1	use1-az2	Texas, United States of America
US East (Houston)*	us-east-1-iah-1a	use1-iah1-az1	us-east-1-iah-1	us-east-1	use1-az6	Texas, United States of America
US East (Kansas City) 2	us-east-1-mci-1a	use1-mci1-az1	us-east-1-mci-1	us-east-1	use1-az2	Missouri, United States of America

Local Zone Group Long Name	Local Zone Name	Local Zone ID	Network Border Group	Parent Region Name	Parent Zone ID	Geography
US East (Miami) 2	us-east-1-mia-2a	use1-mia2-az1	us-east-1-mia-2	us-east-1	use1-az6	Florida, United States of America
US East (Miami)*	us-east-1-mia-1a	use1-mia1-az1	us-east-1-mia-1	us-east-1	use1-az2	Florida, United States of America
US East (Minneapolis)	us-east-1-msp-1a	use1-msp1-az1	us-east-1-msp-1	us-east-1	use1-az5	Minnesota, United States of America
US East (New York City) 2	us-east-1-nyc-2a	use1-nyc2-az1	us-east-1-nyc-2	us-east-1	use1-az5	New Jersey, United States of America
US East (New York City)*	us-east-1-nyc-1a	use1-nyc1-az1	us-east-1-nyc-1	us-east-1	use1-az5	New Jersey, United States of America

Local Zone Group Long Name	Local Zone Name	Local Zone ID	Network Border Group	Parent Region Name	Parent Zone ID	Geography
US East (Philadelphia)	us-east-1-phl-1a	use1-phl1-az1	us-east-1-phl-1	us-east-1	use1-az1	Pennsylvania, United States of America
US West (Denver)	us-west-2-den-1a	usw2-den1-az1	us-west-2-den-1	us-west-2	usw2-az4	Colorado, United States of America
US West (Honolulu)	us-west-2-hnl-1a	usw2-hnl1-az1	us-west-2-hnl-1	us-west-2	usw2-az3	Hawaii, United States of America
US West (Las Vegas)	us-west-2-las-1a	usw2-las1-az1	us-west-2-las-1	us-west-2	usw2-az3	Nevada, United States of America
US West (Los Angeles)	us-west-2-lax-1a	usw2-lax1-az1	us-west-2-lax-1	us-west-2	usw2-az2	California, United States of America

Local Zone Group Long Name	Local Zone Name	Local Zone ID	Network Border Group	Parent Region Name	Parent Zone ID	Geography
US West (Los Angeles)	us-west-2-lax-1b	usw2-lax1-az2	us-west-2-lax-1	us-west-2	usw2-az4	California, United States of America
US West (Phoenix) 2	us-west-2-phx-2a	usw2-phx2-az1	us-west-2-phx-2	us-west-2	usw2-az2	Arizona, United States of America
US West (Phoenix)*	us-west-2-phx-1a	usw2-phx1-az1	us-west-2-phx-1	us-west-2	usw2-az2	Arizona, United States of America
US West (Portland)*	us-west-2-pdx-1a	usw2-pdx1-az1	us-west-2-pdx-1	us-west-2	usw2-az3	Oregon, United States of America
US West (Seattle)	us-west-2-sea-1a	usw2-sea1-az1	us-west-2-sea-1	us-west-2	usw2-az1	Washington, United States of America

* Contact Support to request access.

South America

The following Local Zones are available in South America:

Local Zone Group Long Name	Local Zone Name	Local Zone ID	Network Border Group	Parent Region Name	Parent Zone ID	Geography
Argentina (Buenos Aires)	us-east-1-bue-1a	use1-bue1-az1	us-east-1-bue-1	us-east-1	use1-az2	Argentina
Chile (Santiago)	us-east-1-scl-1a	use1-scl1-az1	us-east-1-scl-1	us-east-1	use1-az1	Chile
Peru (Lima)	us-east-1-lim-1a	use1-lim1-az1	us-east-1-lim-1	us-east-1	use1-az2	Peru

Africa

The following Local Zones are available in Africa:

Local Zone Group Long Name	Local Zone Name	Local Zone ID	Network Border Group	Parent Region Name	Parent Zone ID	Geography
Nigeria (Lagos)	af-south-1-los-1a	afs1-los1-az1	af-south-1-los-1	af-south-1	afs1-az1	Nigeria

Asia Pacific

The following Local Zones are available in Asia Pacific:

Local Zone Group Long Name	Local Zone Name	Local Zone ID	Network Border Group	Parent Region Name	Parent Zone ID	Geography
Australia (Perth)	ap-southeast-2-per-1a	apse2-per1-az1	ap-southeast-2-per-1	ap-southeast-2	apse1-az1	Australia
India (Delhi)	ap-south-1-del-1a	aps1-del1-az1	ap-south-1-del-1	ap-south-1	aps1-az3	India
India (Kolkata)	ap-south-1-ccu-1a	aps1-ccu1-az1	ap-south-1-ccu-1	ap-south-1	aps1-az1	India
New Zealand (Auckland)*	ap-southeast-2-akl-1a	apse2-akl1-az1	ap-southeast-2-akl-1	ap-southeast-2	apse2-az2	New Zealand
Philippines (Manila)	ap-southeast-1-mnl-1a	apse1-mnl1-az1	ap-southeast-1-mnl-1	ap-southeast-1	apse1-az1	Philippines
Taiwan (Taipei)*	ap-northeast-1-tpe-1a	apne1-tpe1-az1	ap-northeast-1-tpe-1	ap-northeast-1	apne1-az2	Taiwan
Thailand (Bangkok)	ap-southeast-1-bkk-1a	apse1-bkk1-az1	ap-southeast-1-bkk-1	ap-southeast-1	apse1-az1	Thailand

Europe

The following Local Zones are available in Europe:

Local Zone Group Long Name	Local Zone Name	Local Zone ID	Network Border Group	Parent Region Name	Parent Zone ID	Geography
Denmark (Copenhagen)	eu-north-1-cph-1a	eun1-cph1-az1	eu-north-1-cph-1	eu-north-1	eun1-az2	Denmark
Finland (Helsinki)	eu-north-1-hel-1a	eun1-hel1-az1	eu-north-1-hel-1	eu-north-1	eun1-az1	Finland
Germany (Hamburg)	eu-central-1-ham-1a	euc1-ham1-az1	eu-central-1-ham-1	eu-central-1	euc1-az3	Germany
Poland (Warsaw)	eu-central-1-waw-1a	euc1-waw1-az1	eu-central-1-waw-1	eu-central-1	euc1-az3	Poland

Middle East

The following Local Zones are available in the Middle East:

Local Zone Group Long Name	Local Zone Name	Local Zone ID	Network Border Group	Parent Region Name	Parent Zone ID	Geography
Oman (Muscat)	me-south-1-mct-1a	mes1-mct1-az1	me-south-1-mct-1	me-south-1	mes1-az1	Oman

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

Find your Local Zones using the AWS CLI

Use the describe-availability-zones command to get a details of the Local Zones available in a specific Region, for your account.

The following example shows how to run the `describe-availability-zones` command:

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

The following example shows an output of the `describe-availability-zones` command:


```
{
            "State": "available",
            "OptInStatus": "opted-in",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2-lax-1a",
            "ZoneId": "usw2-lax1-az1",
            "GroupName": "us-west-2-lax-1",
            "NetworkBorderGroup": "us-west-2-lax-1",
            "ZoneType": "local-zone",
            "ParentZoneName": "us-west-2a",
            "ParentZoneId": "usw2-az2",
            "GroupLongName": "US West (Los Angeles)"
        },
        {
            "State": "available",
            "OptInStatus": "opted-in",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2-lax-1b",
            "ZoneId": "usw2-lax1-az2",
            "GroupName": "us-west-2-lax-1",
            "NetworkBorderGroup": "us-west-2-lax-1",
            "ZoneType": "local-zone",
            "ParentZoneName": "us-west-2d",
            "ParentZoneId": "usw2-az4",
            "GroupLongName": "US West (Los Angeles)"
        }
```

Getting started with AWS Local Zones

To get started with AWS Local Zones, you must first opt-in to a Local Zone through the AWS Global View 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: Opt-in to a Local Zone

You can use the AWS Global View console or a command line interface to determine which Local Zones are available for your account. Then opt in to the Local Zone that you want to use.

AWS Global View console

To opt in to a Local Zone

1. Sign in to the AWS Global View console.
2. From the navigation pane, choose **Regions and Zones**.
3. Choose the **Local Zones** tab.
4. Find the Local Zone that you want to enable. You can scroll down the list or enter a term in the Search field.
5. Select the row for the Local Zone.
6. Choose **Opt-in**.
7. You will be asked to enable the parent Region of the Local Zone. Choose **Enable Region**.
8. On the **Enable Region** pop-up, choose **Enable Region**.
9. From the **Local Zones** tab on the **Regions and Zones** page, select the Local Zone and choose **Opt-in**.
10. On the **Opt-in Zone group** pop-up, choose **Opt-in Zone group**.

    You can now use the Local Zone.

AWS CLI

To opt in to a Local Zone

1. 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
```

2. 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 for the subnet from the range of your VPC. You can optionally specify an IPv6 CIDR block for a subnet if there is an IPv6 CIDR block associated with the VPC. You can specify the Local Zone where the subnet resides. You can have multiple subnets in the same Local Zone.

Console

To add a Local Zone subnet to a VPC

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 ID**, 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 the IPv4 CIDR block for the subnet.
9. (Optional) Specify an IPv6 CIDR block for the subnet. This option is available only if an IPv6 CIDR block is associated with the VPC.
10. (Optional) To add a tag, enter the tag key and tag value. Choose **Add new tag** to add another tag.
11. Choose **Create subnet**.

AWS CLI

To add a Local Zone subnet to a VPC

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 Amazon EC2 instance in a Local Zone.

Console

To launch an Amazon EC2 instance in a Local Zone subnet

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, under **Instances**, choose **Instance Types**.
3. In the search field, choose **Availability zones**, choose **Contains**, and then enter the zone name (for example, `us-west-2-lax-1`.) Select the first item, or whichever item has just this zone ID and the Availability Zones for the parent Region.
4. Select one of the instance types, and then choose **Actions**, **Launch instance**.

5. Under **Name and tags**, enter a descriptive 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.
6. Under **Application and OS Images (Amazon Machine Image)**, do the following:
   a. Select an operating system for your instance.
   b. Select the **Amazon Machine Image (AMI)**. An *Amazon Machine Image (AMI)* is a basic configuration that serves as a template for your instance.
   c. Select the **Architecture**.
7. Under **Key pair (login)**, choose an existing key pair or create a new one. This is required if you want to connect to your EC2 instance.
8. Next to **Network settings**, choose **Edit**, and then:
   a. Select your VPC.
   b. Select your Local Zone subnet.
   c. Enable or disable **Auto-assign public IP**.
   d. Create a security group or select an existing one.
9. You can keep the default selections for the other configuration settings for your instance. To determine the storage types that are supported, see the *Compute and storage* section in AWS Local Zones features.
10. Review a summary of your instance configuration in the **Summary** panel, and when you're ready, choose **Launch instance**.
11. A confirmation page lets you know that your instance is launching. Choose **View all instances** to close the confirmation page and return to the console.
12. On the **Instances** screen, you can view the status of the launch. It takes a short time for an instance to launch. When you launch an instance, its initial state is `pending`. After the instance starts, its state changes to `running` and it receives a public DNS name. If the **Public IPv4 DNS** column is hidden, choose the settings icon () in the top-right corner, turn on **Public IPv4 DNS**, and choose **Confirm**.
13. It can take a few minutes for the instance to be ready for you to connect to it. Check that your instance has passed its status checks; you can view this information in the **Status check** column.

AWS CLI

To get the instance types supported in a Local Zone

Use the describe-instance-types command.

```
aws ec2 describe-instance-type-offerings \
    --filters Name=location,Values=us-west-2-lax-1a \
    --location-type availability-zone \
    --query InstanceTypeOfferrings[*].InstanceType
```

To launch an EC2 instance in a Local Zone subnet

Use the run-instances command.

```
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

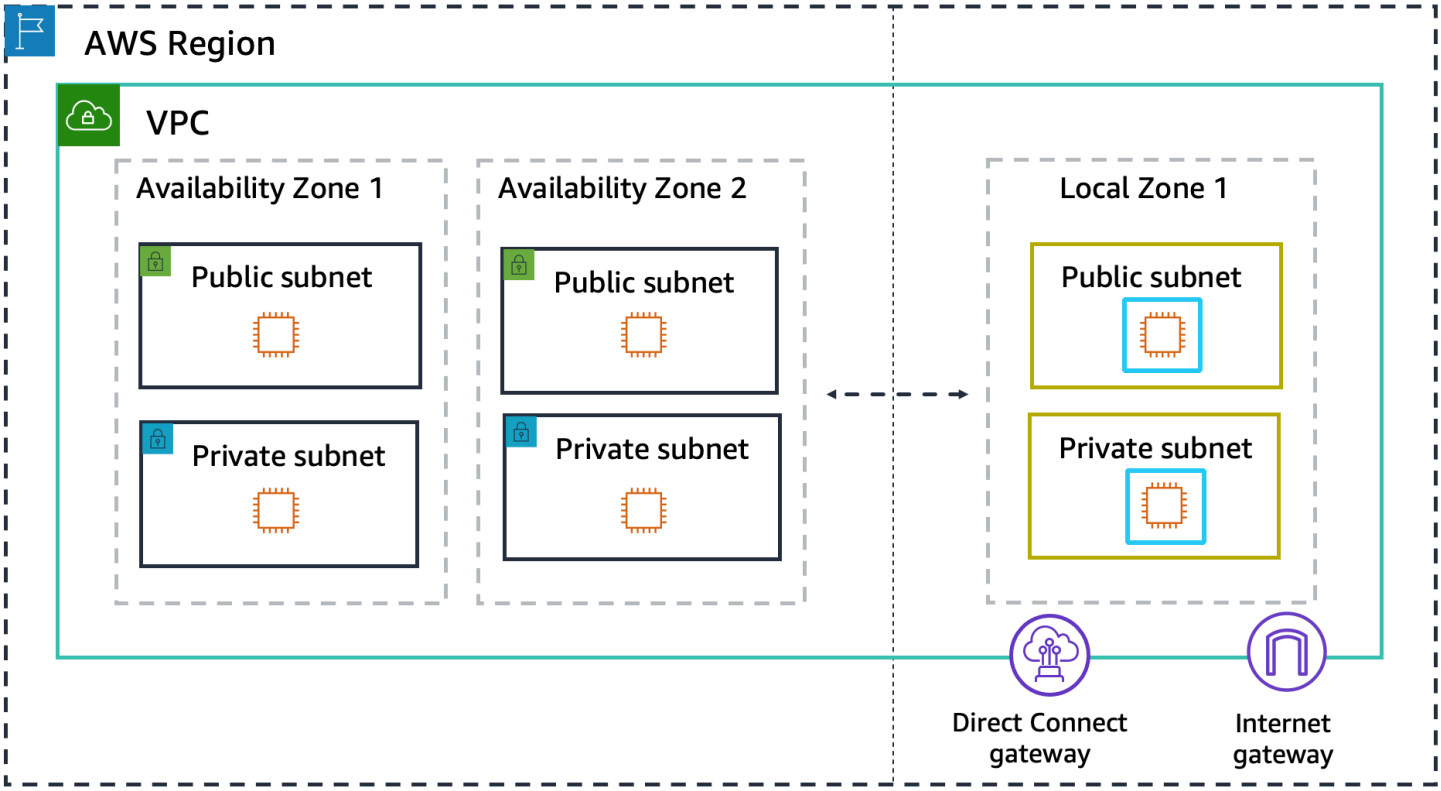
When you are finished with a Local Zone, delete the resources in the Local Zone. To disable a zone group, you must contact AWS Support. Open a case titled "Disable zone group" and provide the name of the zone group.

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, and 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

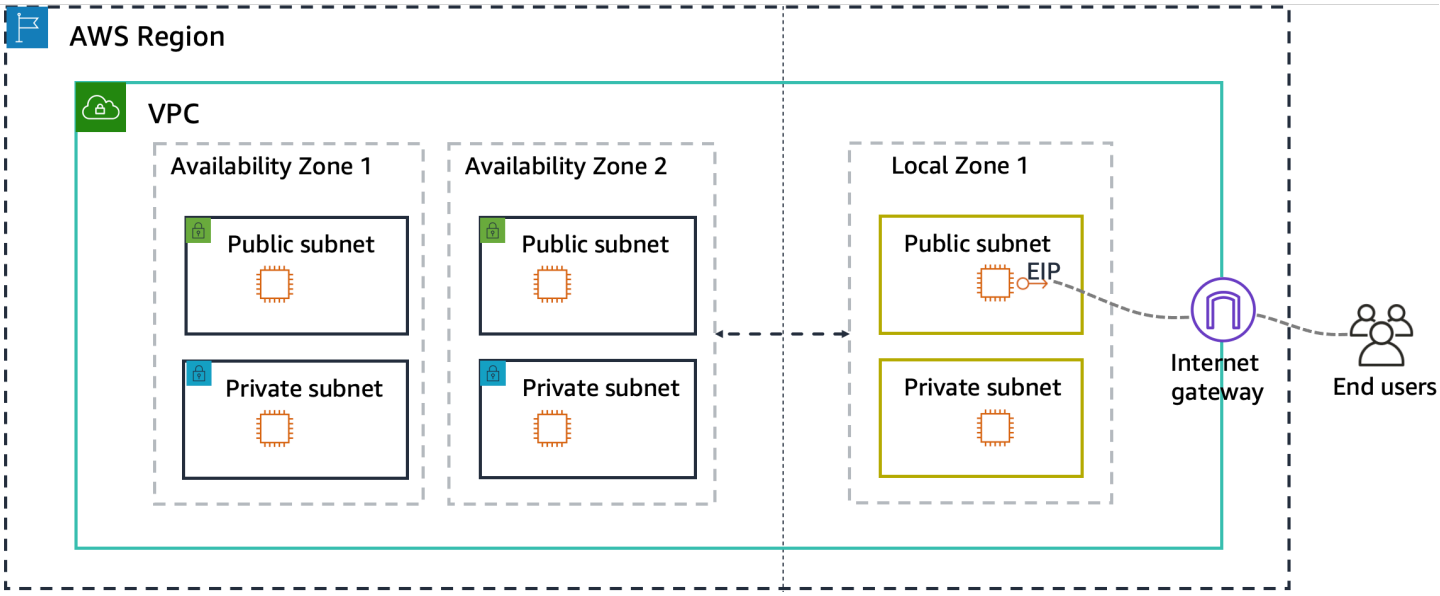
- Internet gateway connection in Local Zones

- NAT gateway connection in Local Zones
- VPN connection in Local Zones
- Direct Connect in Local Zones
- Transit gateway connection between Local Zones
- Transit gateway connection in Local Zones

Internet gateway connection in Local Zones

Internet gateways provide two-way public connectivity to applications running in AWS Regions and/or in Local Zones. For more information, see Internet gateways in the *Amazon VPC User Guide*.

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 public-facing applications to be closer to end users than an AWS Region can provide.



For your private applications that require outbound-only connectivity to the internet, use a NAT gateway.

NAT gateway connection in Local Zones

A NAT gateway is a Network Address Translation (NAT) service. It allows your Amazon VPC resources in your private subnets to securely access services outside the subnet, including the

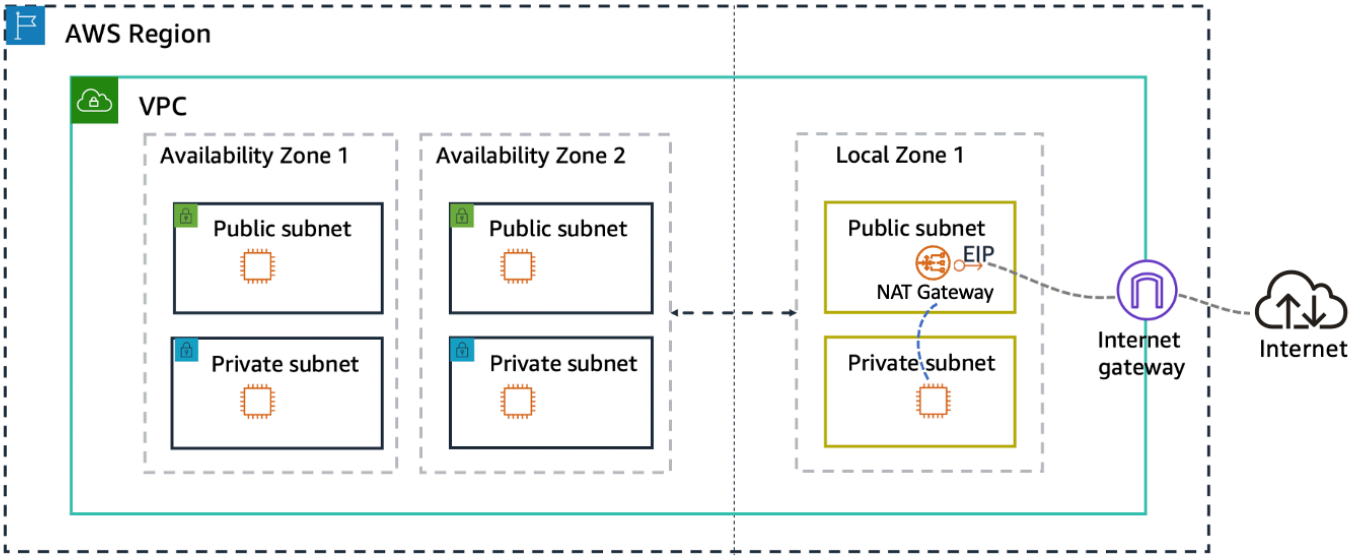
internet, while keeping those private resources inaccessible to any unsolicited traffic. For a list of Local Zones that support NAT gateways, see AWS Local Zones features.

To use NAT gateway to access the internet from your private resources, instantiate your NAT gateway in the public subnet and then route your internet traffic (`0.0.0.0/0` or `::/0`) from the private subnet to the NAT gateway. The NAT gateway translates the private IP address of the traffic coming from your private subnet to the EIP associated with it so that your private resources can access the internet securely.

The NAT gateway only accepts the response traffic from the destinations that are accessed and drops any unsolicited inbound connections. This keeps your private resources inaccessible from the internet.

For more information, see NAT gateways in the *Amazon VPC User Guide*.

The following image shows the traffic flow from a private subnet in a Local Zone to a NAT gateway in a public subnet in the same Local Zone, then to an internet gateway, and to the internet.

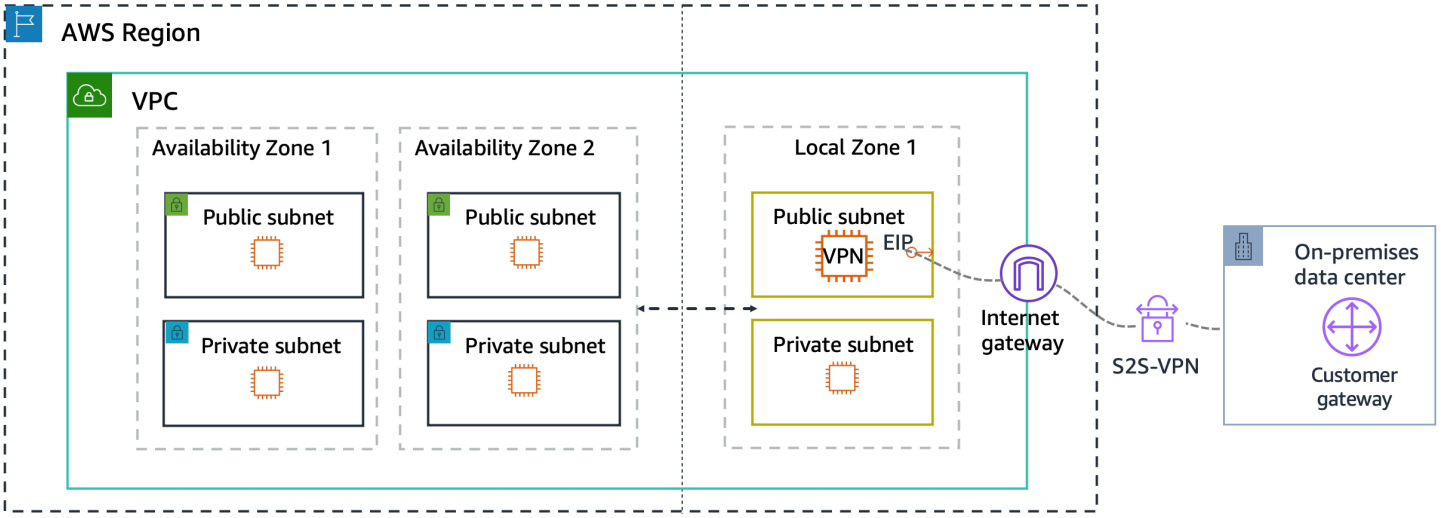


VPN connection in Local Zones

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 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.

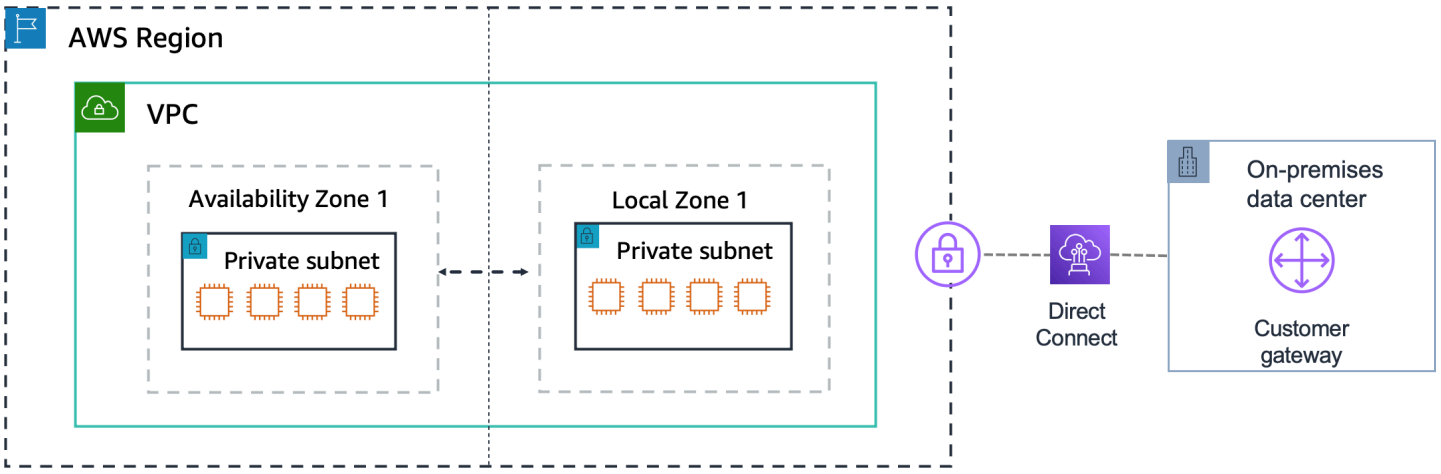


Direct Connect in Local Zones

With 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. 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.

For more information, see the Direct Connect User Guide.

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



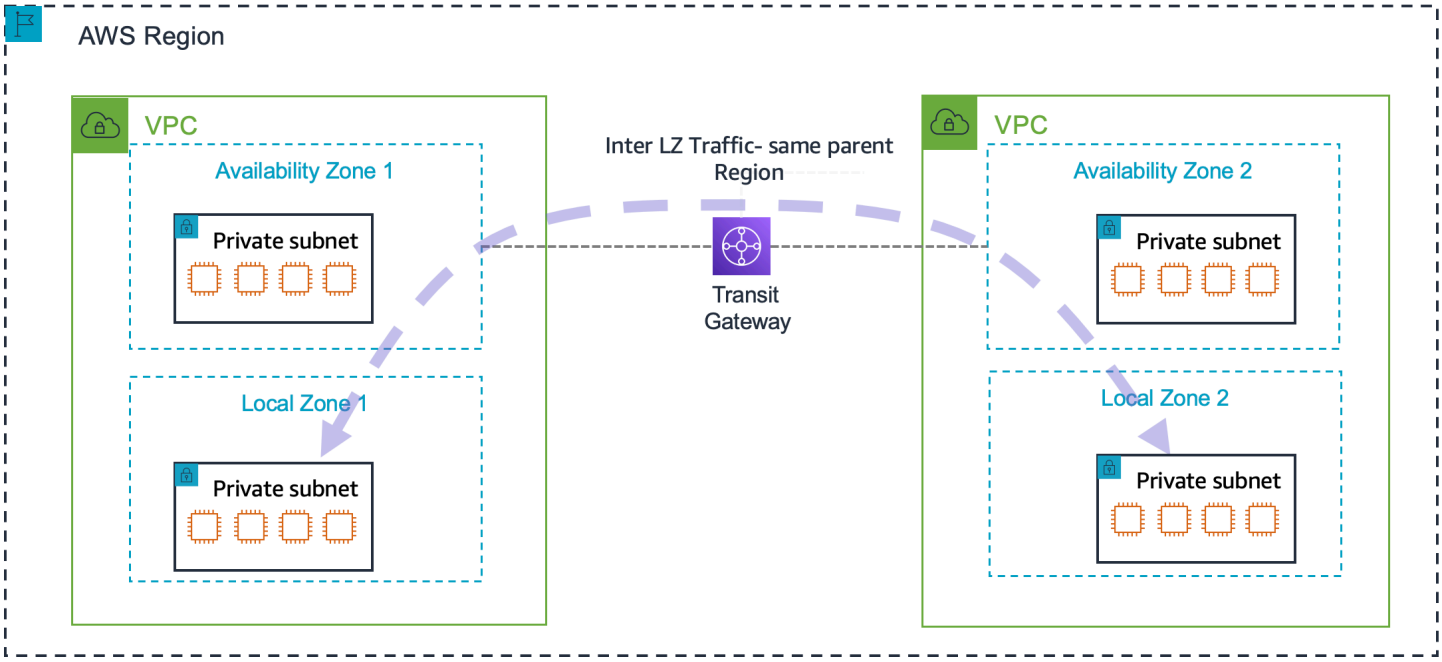
During a hybrid cloud migration, you can migrate your applications to Local Zones while using Direct Connect to communicate back to other parts of your applications in the data center. An example is migrating the front end of an application to Amazon EC2, Amazon ECS, or Amazon EKS in a Local Zone and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

Transit gateway connection between Local Zones

A transit gateway can be used to connect one Local Zone to another within the same parent Region. For more information about transit gateways, see Connect your VPC to other VPCs and networks using a transit gateway in the *Amazon VPC User Guide*.

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

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



Considerations

- You must create a transit gateway attachment in the parent zone.
- You can't connect a Local Zone to another Local Zone or Outpost that is within the same VPC.

Parent zone

You can use the AWS Global View console or the command line interface to get the parent zone details for a Local Zone.

AWS Global View console

To get the parent zone details for a Local Zone

1. Sign in to the AWS Global View console.
2. From the navigation pane, choose **Regions and Zones**.
3. Choose the **Local Zones** tab.
4. Find the Local Zone.
5. Scroll to see the **Parent Zone name** and **Parent Zone ID** for the Local Zone.

AWS CLI

To get the parent zone details for a Local Zone

Use the describe-availability-zones command. The following example uses a Local Zone in Los Angeles.

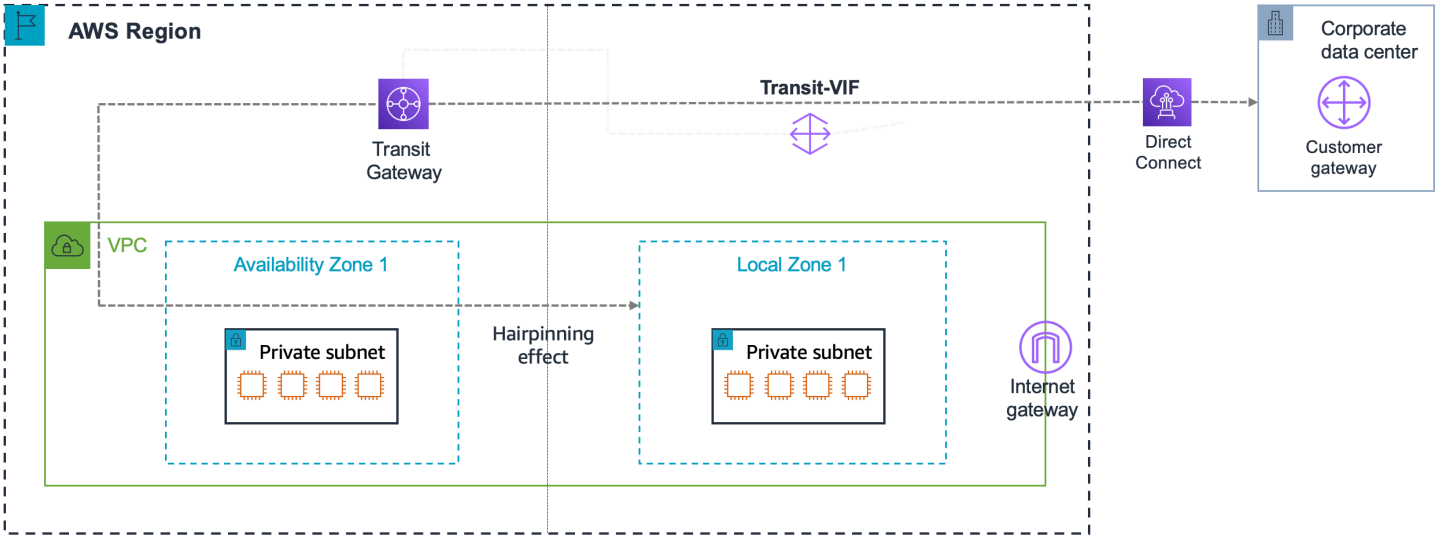
```
aws ec2 describe-availability-zones \
  --zone-names us-west-2-lax-1a \
  --query 'AvailabilityZones[0].ParentZoneName' \
  --region us-west-2 \
  --output text
```

Transit gateway connection in Local Zones

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

For more information about transit gateways, see Connect your VPC to other VPCs and networks using a transit gateway in the *Amazon VPC User Guide*.

The following diagram shows the connection from the customer gateway over the Direct Connect into the transit gateway 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 transit gateway 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.

AWS managed policies for AWS Local Zones

An AWS managed policy is a standalone policy that is created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases so that you can start assigning permissions to users, groups, and roles.

Keep in mind that AWS managed policies might not grant least-privilege permissions for your specific use cases because they're available for all AWS customers to use. We recommend that you reduce permissions further by defining customer managed policies that are specific to your use cases.

You cannot change the permissions defined in AWS managed policies. If AWS updates the permissions defined in an AWS managed policy, the update affects all principal identities (users, groups, and roles) that the policy is attached to. AWS is most likely to update an AWS managed policy when a new AWS service is launched or new API operations become available for existing services.

For more information, see AWS managed policies in the *IAM User Guide*.

AWS managed policy: AWSZoneGroupAccessManagementServiceRolePolicy

The `AWSZoneGroupAccessManagementServiceRolePolicy` policy is attached to the `AWSServiceRoleForZoneGroupAccessManagement` service-linked role that allows an administrator to enable Zone Groups on behalf of their entire organization, automatically opting-in all existing member accounts and new accounts joining the organization. You cannot attach this policy to your users, groups, or roles.

Permissions details

This policy includes the following permissions.

- `DescribeOrganization` – View organization details.
- `DescribeOrganizationalUnit` – View organizational unit information.
- `DescribeAccount` – View account details.
- `ListAccounts` – List all accounts in the organization.
- `ListParents` – List parent containers.

- `ListAWSServiceAccessForOrganization` – List AWS service access status.
- `ListChildren` – List child resources.
- `ListDelegatedAdministrators` – List delegated administrators.

To view details for this policy, see AWSZoneGroupAccessManagementServiceRolePolicy in the *AWS Managed Policy Reference*.

AWS Local Zones updates to AWS managed policies

View details about updates to AWS managed policies for AWS Local Zones since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS Local Zones Document history page.

Change	Description	Date
AWSZoneGroupAccessManagementServiceRolePolicy – New policy	Added a new AWS managed policy that allows an administrator to enable Zone Groups on behalf of their entire organization, automatically opting-in all existing member accounts and new accounts joining the organization.	June 30, 2025

Document history for the AWS Local Zones user guide

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

Change	Description	Date
Geography field	The Geography for a Local Zone is the specific physical location of its infrastructure.	March 25, 2025
Group Long Name field	Group Long Name is the name of the Local Zone group.	March 11, 2025
New Local Zone launch	A new Local Zone is now available in US East (New York City).	January 8, 2025
New Local Zone launch	A new Local Zone is now available in US West (Honolulu).	April 29, 2024
New Local Zone launch	A new Local Zone is now available in US East (Miami) 2.	March 28, 2024
New Local Zone launch	A new Local Zone is now available in US East (Atlanta) 2.	February 26, 2024
New Local Zone launch	A new Local Zone is now available in US East (Houston) 2.	February 5, 2024
New Local Zone launch	A new Local Zone is now available in US East (Chicago) 2.	January 30, 2024

New Local Zone launch	A new Local Zone is now available in US East (Dallas) 2.	November 13, 2023
NAT gateways	NAT gateways are now available in select Local Zones.	August 17, 2023
New Local Zone launch	A new Local Zone is now available in US West (Phoenix) 2.	July 27, 2023
Initial release	Initial release of the AWS Local Zones User Guide	November 17, 2022