AWS Foundation

ORGANISATIONS,GA, ENI & BACKUP

Agenda

1. Introduction Global Accelerator
2. Global Accelerator Components
3. Introduction to AWS Organizations
4. Starting off with Organizations
5. Elastic Network Interfaces
6. Elastic Network Adapter
7. Elastic Fabric Adapter
8. Introduction to CloudFront
9. CloudFront v/s Global Accelerator

Introduction to Global Accelerator

Introduction to Global Accelerator

AWS Global Accelerator is a service that improves the availability and performance of our applications with local or global users

It provides static IP addresses that will act as a fixed entry point to our application endpoints on EC2, Beanstalk, or load balancers

Introduction to Global Accelerator

How does Global Accelerator work?

User

Traffic from our user's client is sent to AWS Global Accelerator

Edge Location

Our user's traffic enters the AWS global network at the closest edge location

AWS Global Accelerator

AWS Global Accelerator directs traffic to the optimal endpoint based on proximity to the client, health, and endpoint weights

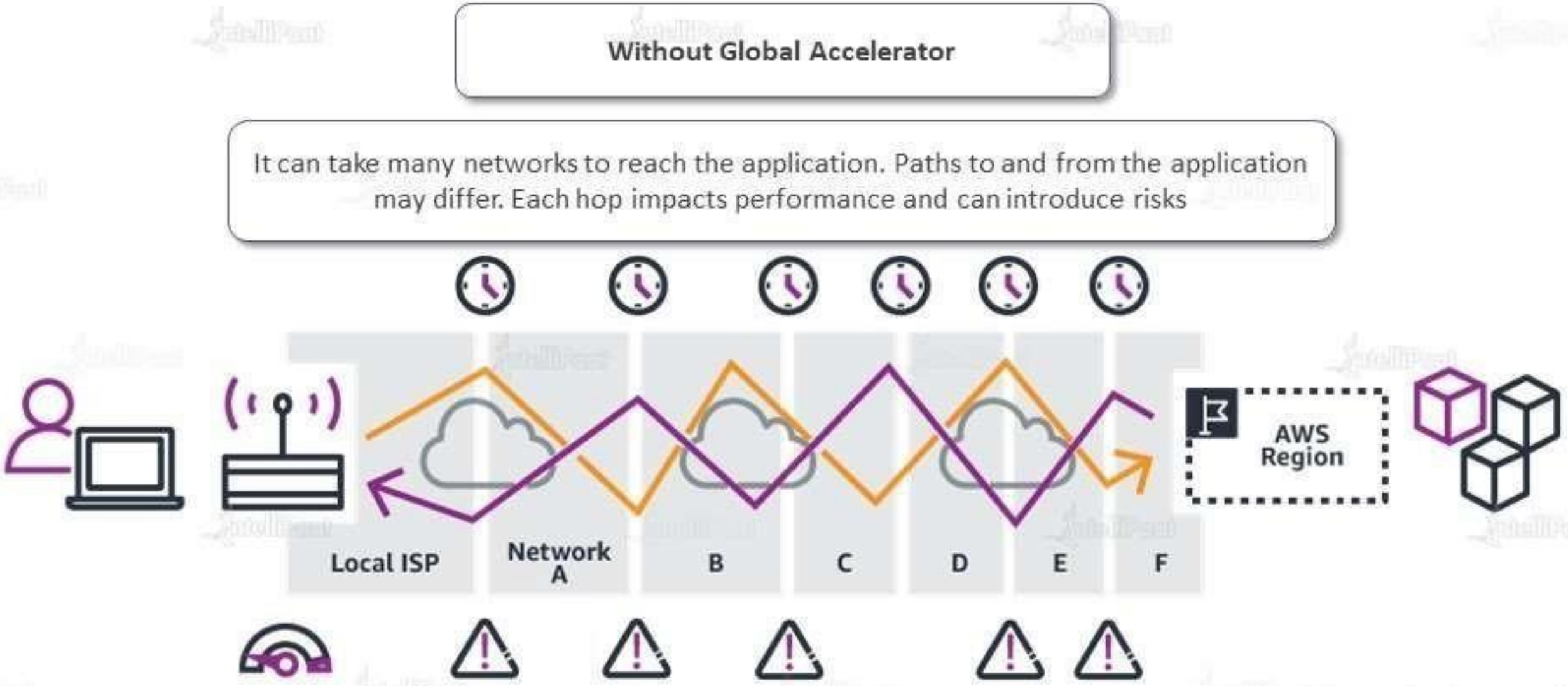
Endpoint Group

Our user's traffic traverses the AWS global network to the optimal endpoint group in an AWS region. Each endpoint group includes one or more application endpoints

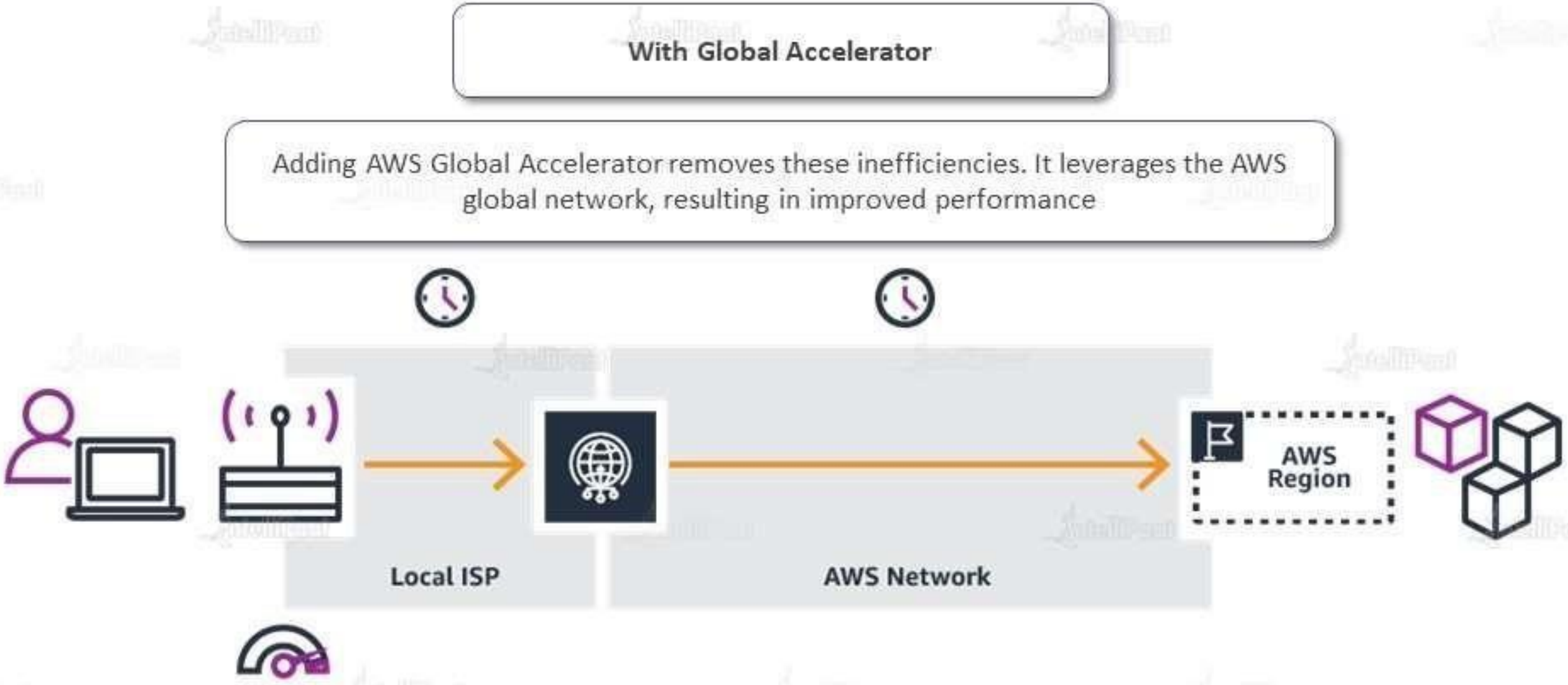
Endpoints

AWS Global Accelerator ensures that the traffic is routed to the appropriate endpoint based on performance and policies that we can configure

Introduction to Global Accelerator



Introduction to Global Accelerator



Introduction to Global Accelerator

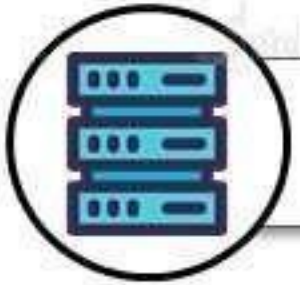
Benefits of Using Global Accelerator

Instant regional failover

High availability

No variability around clients that cache IP addresses

Improved performance



Easy manageability

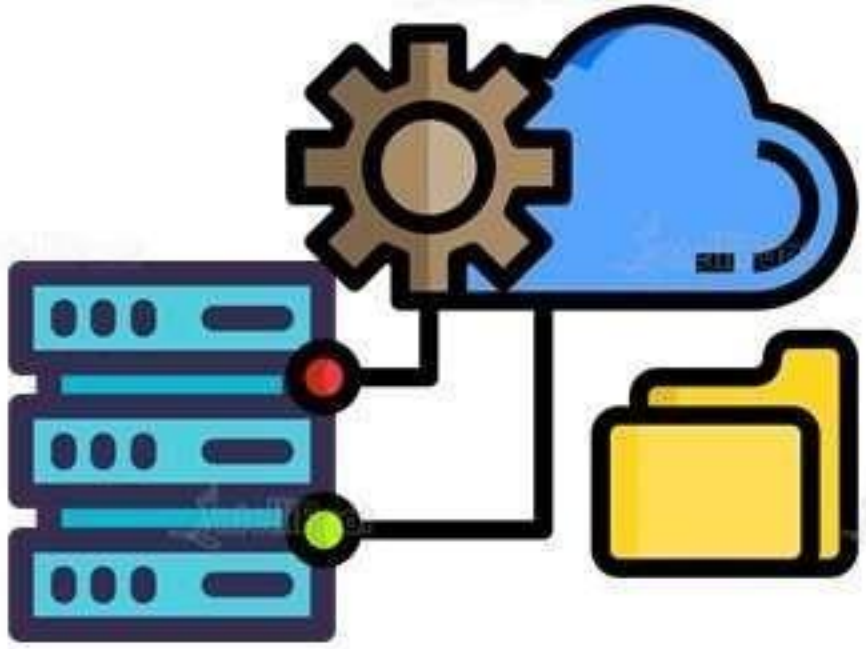
Fine-grained control

Introduction to Global Accelerator

There is **BYOIP** (Bring Your Own IP address) facility in Global Accelerator. This lets us use our own IP address as the entry point static IP

How does this help?

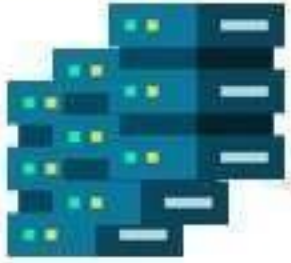
This allows us to move our on-premises applications that have hardcoded IP address dependencies to AWS, without making any client-facing changes



Introduction to Global Accelerator

Use Cases

Scales for Increased Application Utilization



When app usage grows, the number of IPs to manage also increases. Global Accelerator takes care of scaling our network up or down

Protects the Applications

While making our ELB or EC2 instances Internet-facing, the exposure to attacks increases. Using GA, we can use an internal ALB or a private instance as an endpoint

Global Accelerator Components

Global Accelerator Components

Static IP Addresses

Global Accelerator provides two static IP addresses as endpoints or we can use a BYOIP address

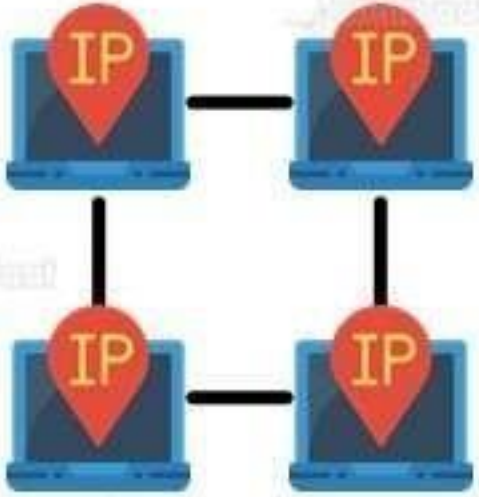
Accelerator

It directs traffic to healthy endpoints over the AWS global network to increase availability and performance

Global Accelerator Components

Network Zone

A network zone is an isolated unit with its own set of physical infrastructure, so if an IP becomes unavailable, we can try another IP in another network zone



Listener

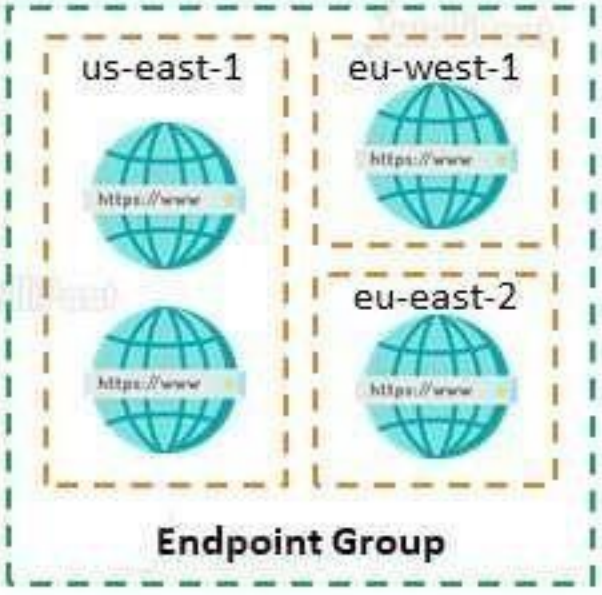
Processes inbound connections from clients to Global Accelerator, based on the port (or port range) and the protocol (TCP and UDP) that we configure

Port 80

Global Accelerator Components

Endpoint Groups

Every endpoint group is associated with a region. There will be one or more endpoint groups in a region

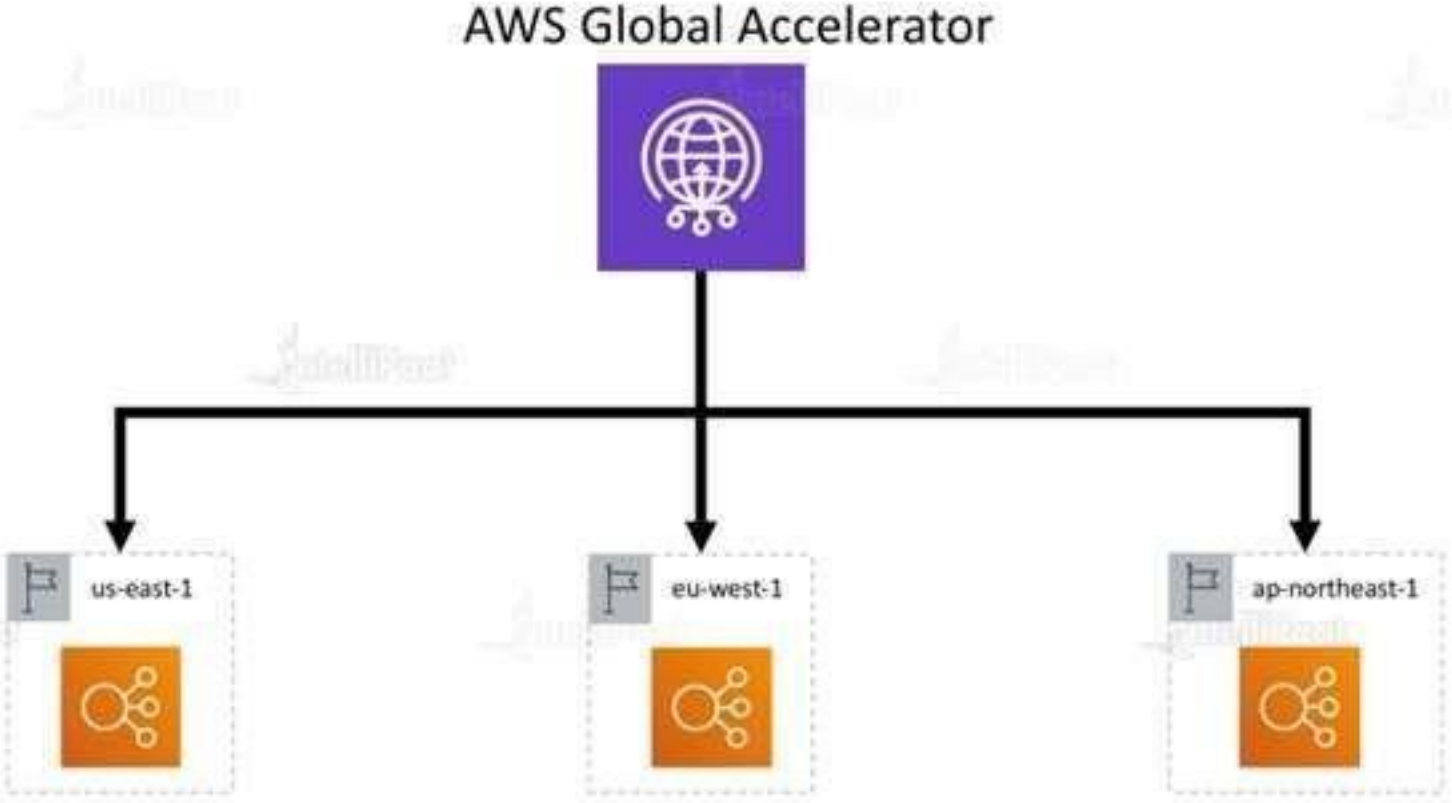


Endpoints

Endpoints can be NLB, ALB, EC2 instances, or Elastic IP addresses. Traffic is routed to the endpoint according to the configuration we provide

Global Accelerator Components

Let's take an example. Here, we are connecting three load balancers, which are in three different locations with common endpoints



Global Accelerator Components

Global Accelerator Components

Quotas

- Accelerators for each AWS account: 20
- Listeners for each Accelerator: 10
- Port ranges for each listener: 10
- Endpoints for each endpoint group: 10
- Tags for each Accelerator: 50

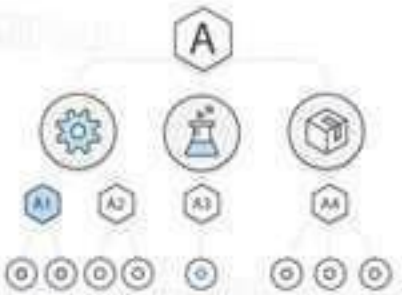
Pricing

- Global Accelerator is not available in the free tier
- There is a fixed fee for a full or partial hour usage of GA with a charge of $0.025 until it is detected

Introduction to AWS Organizations

Introduction to AWS Organizations

AWS Organization is a tool that lets us centrally manage multiple AWS accounts added to our 'organization'



AWS Organizations

If we are the administrator of an organization, then we can invite the existing AWS accounts to join Organizations or we can create accounts in Organizations directly

Introduction to AWS Organizations

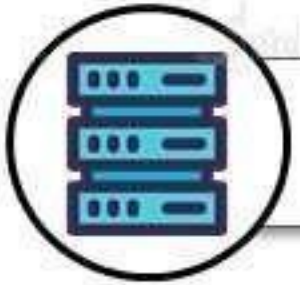
AWS Organizations Features

Centralized management

Consolidated billing for all member accounts

Control over the accounts' usage of services or APIs

Integration with AWS IAM



Consistent data replication, eventually

Standardized tags across accounts

Introduction to AWS Organizations

Pricing of AWS Organizations

There are no additional charges for AWS Organizations!

The charges apply to only the usage of other AWS resources by all member accounts

Introduction to AWS Organizations

Ways to Access AWS Organizations

AWS Management Console

Organizations can be accessed through the browser-based AWS Management Console to manage resources

AWS Command-line Tools

With AWS CLI, we can use the system's command line to access Organizations using commands. It is faster than console

AWS CLI

Introduction to AWS Organizations

Ways to Access AWS Organizations

AWS SDKs

SDKs have libraries that can be used to write code as well as access AWS Organizations

HTTPS Query API

It gives programmatic access to AWS Organizations and its services. We can issue HTTPs requests directly to a service

Introduction to AWS Organizations

AWS Organizations Quotas

Max. and Min. Values

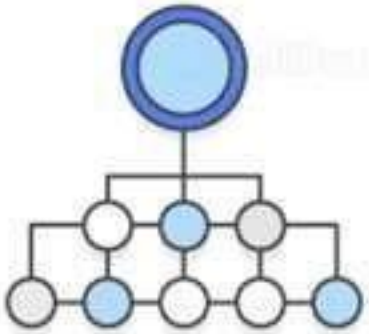
- Number of roots in an Organization: 1
- Number of OUs in an Organization: 1,000
- Number of policies in an Organization: 1,000
- OU maximum nesting in a root: 5
- Number of member accounts that can be can created concurrently: 5

Expiration Time for Handshakes

- Invitation to join an Organization: 15 days
- Request to enable all features in an Organization: 90 days
- Handshake is deleted and no longer appears in lists: 30 days

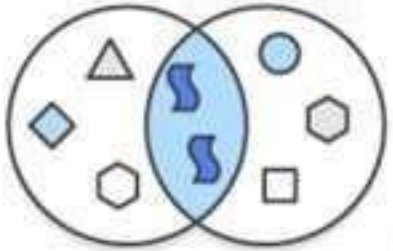
Introduction to AWS Organizations

How does AWS IAM work with Organizations?



Creates groups of AWS accounts with AWS Organizations

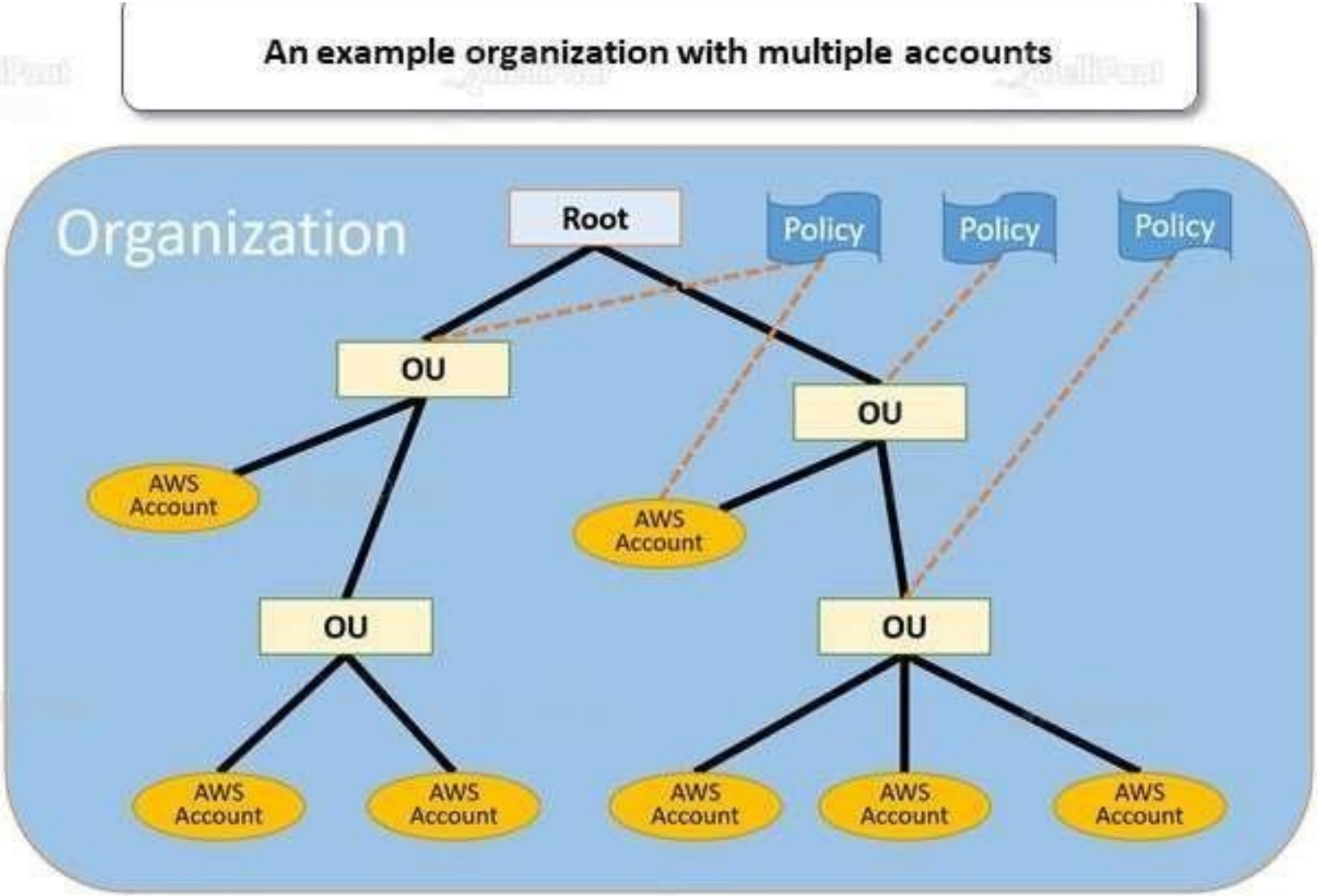
Attaches service control policies (SCPs) to those groups to centrally control AWS service use



Entities in AWS accounts can only use the AWS services allowed by both SCP and AWS IAM policies for each account

AWS Organizations Concepts

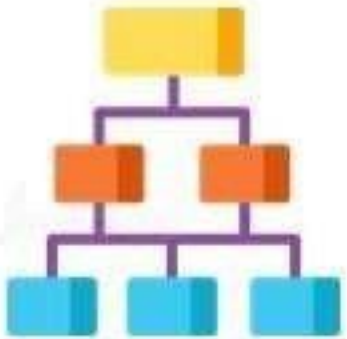
AWS Organizations Concepts



AWS Organizations Concepts

- Organization
- Root
- Organization Unit (OU)
- Account
- Invitation
- Handshake

Organizations can be used to consolidate multiple AWS accounts so that we can administer them all as a single unit

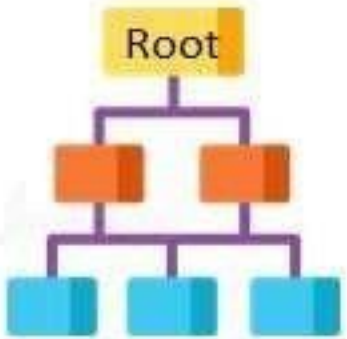


An organization will have one master account and zero or more member accounts. We can organize our organization in an hierarchical order with a root on the top

AWS Organizations Concepts

- Organization
- Root
- Organization Unit (OU)
- Account
- Invitation
- Handshake

This is the master account for all subaccounts. It we apply a policy to root, it will be applied to all the member accounts and organization units

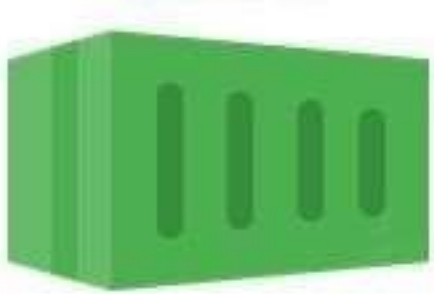


We can have only one root and that will be automatically created when we create an organization

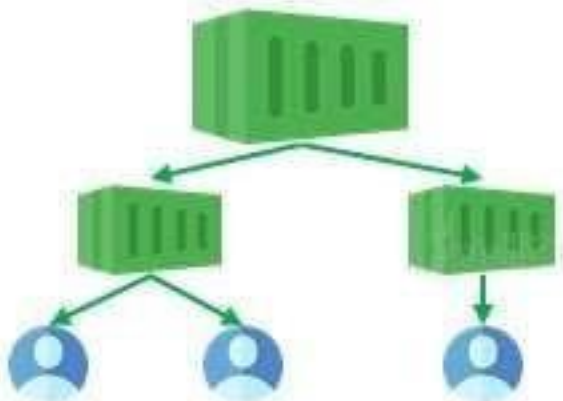
AWS Organizations Concepts

- Organization
- Root
- Organization Unit (OU)
- Account
- Invitation
- Handshake

A container for accounts within a root. An OU can contain other OUs and this is what enables the tree-like hierarchy that ends in accounts



Organization Unit (OU)



If we attach a policy to an OU, this affects all the other OUs under it, as well as to the member accounts

AWS Organizations Concepts

- Organization
- Root
- Organization Unit (OU)
- Account
- Invitation
- Handshake

An account is basically an AWS account that contains AWS resources. We can apply policies to the account only to control that account's resources

Master Account

This account creates the organization and we can administer using it

Member Account

All other accounts in member accounts. They can be part of only one organization

AWS Organizations Concepts

- Organization
- Root
- Organization Unit (OU)
- Account
- **Invitation**
- Handshake

This is the process of asking another AWS account to join our organization. Only a master account can send out an invite. If they accept, they become a member

AWS Organizations Concepts

- Organization
- Root
- Organization Unit (OU)
- Account
- Invitation
- Handshake

Handshake is a multi-step process of sharing information between two accounts/parties. Handshakes are used to send out invitations and get back acknowledgement

We can work with handshakes directly if we are working with the organization's API or AWS CLI tools

Starting with Organizations

Starting with Organizations

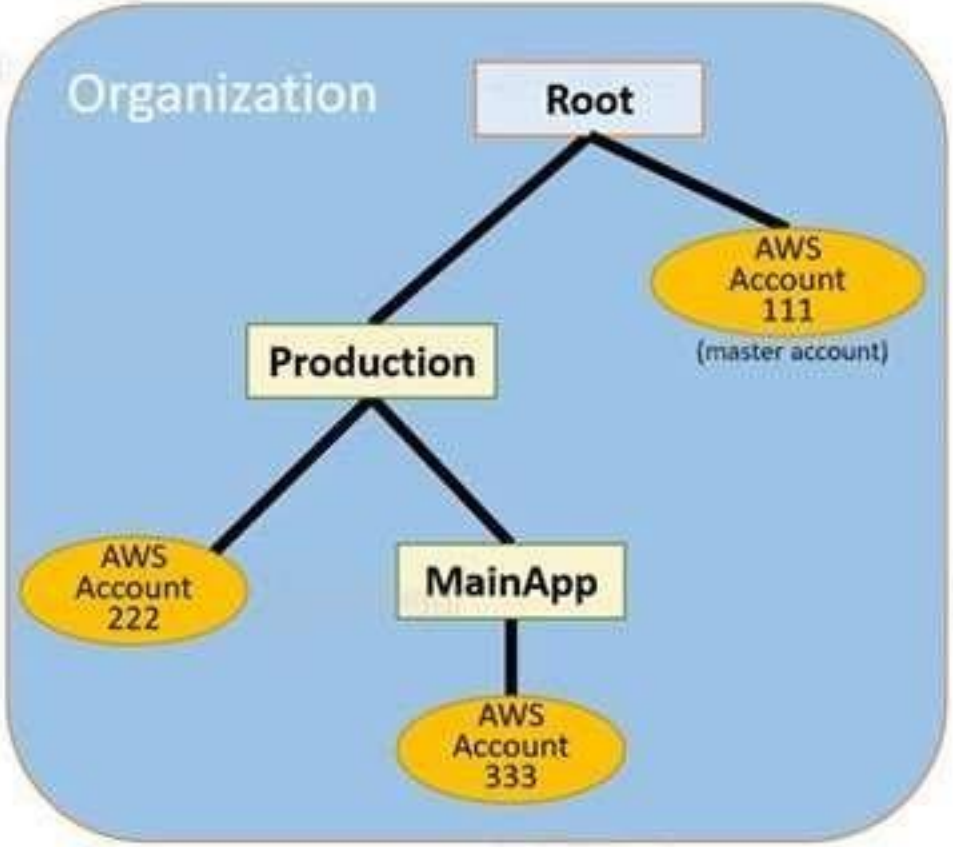
Starting with Organizations

Step 1: Create an Organization

1. Open the AWS Management Console, and then choose our **account name** from the navigation bar
2. Choose **My Organization**
3. Choose **Create Organization**
4. Choose **Enable all features** or **Enable only consolidated billing**
5. Choose **Create**

Starting with Organizations

Step 2: Create Organizational Units



Starting with Organizations

Step 3: Create Service Control Policies

First, enable SCP

Then, check out the SCPs in the IAM console

Starting with Organizations

Step 4: Test Restrictions

1. AWS Organizations denies any attempt to perform an action in any service that isn't in the allow list
2. AWS Organizations denies any attempt to perform an action that isn't in the allow list policy and any action that is in the deny list policy
3. Test the master account to check if any of these rules affect the root account; they shouldn’t affect the root account

Elastic Network Interface

Elastic Network Interface

Elastic Network Interface

An elastic network interface (ENI) is a logical networking component in a VPC that represents a virtual network card. When we move a network interface from one instance to another, network traffic is redirected to the new instance

Elastic Network Interface

IP Addresses per Network Interface per Instance Type

Instance Type	Maximum NIs	Private IPv4 Addresses per Interface	IPv6 Addresses per Interface
a1.xlarge	4	15	15
c1.medium	2	6	IPv6 not supported
t2.micro	2	2	2
t2.small	3	4	4
t2.medium	3	6	6
z1d.metal	15	50	50

Elastic Network Interface

When do we need a network interface?

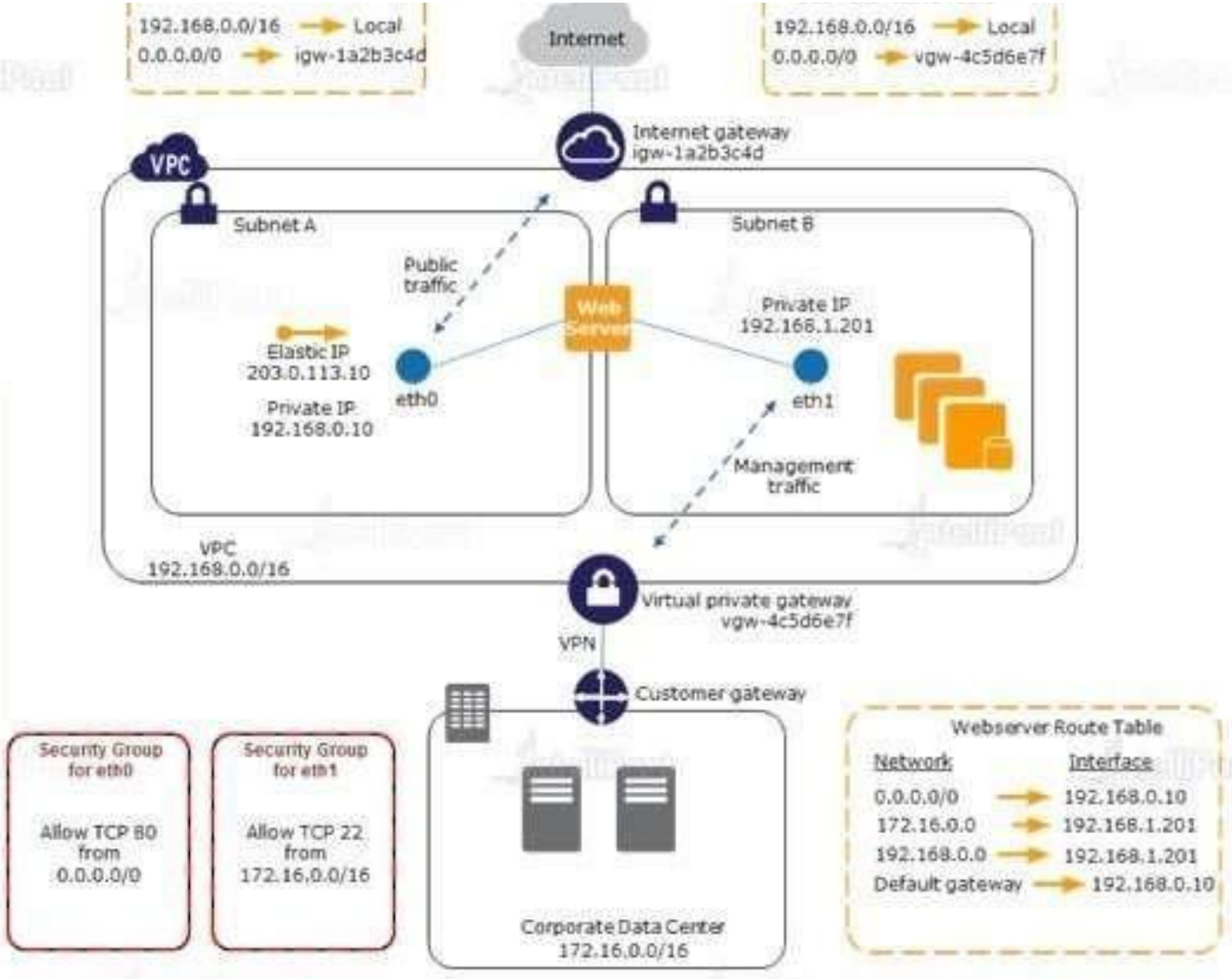
We will have to attach multiple network interfaces in the following scenarios:

1. Creating a management network
2. Using network and security appliances in our VPC
3. Creating dual-homed instances with workloads/roles on distinct subnets
4. Creating a low-budget, high-availability solution

Elastic Network Interface

Scenario Example

We can create a management network using network interfaces. In this scenario, the primary network interface (eth0) on the instance handles public traffic, and the secondary network interface (eth1) handles backend management traffic and is connected to a separate subnet in our VPC that has more restrictive access controls



Elastic Network Adapter

Elastic Network Adapter

Elastic Network Adapter

Amazon EC2 provides enhanced networking capabilities through the elastic network adapter (ENA). It supports network speeds up to 100 GBps for the supported instance types

Elastic Network Adapter

All the available instance types

A1, C5, C5d, C5n, F1, G3, G4, H1, I3, I3en, Inf1, m4.16xlarge, M5, M5a, M5ad, M5d, M5dn, M5n, P2, P3, R4, R5, R5a, R5ad, R5d, R5dn, R5n, T3, T3a, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, u-18tb1.metal, u-24tb1.metal, X1, X1e, and z1d instances

All the available AMIs

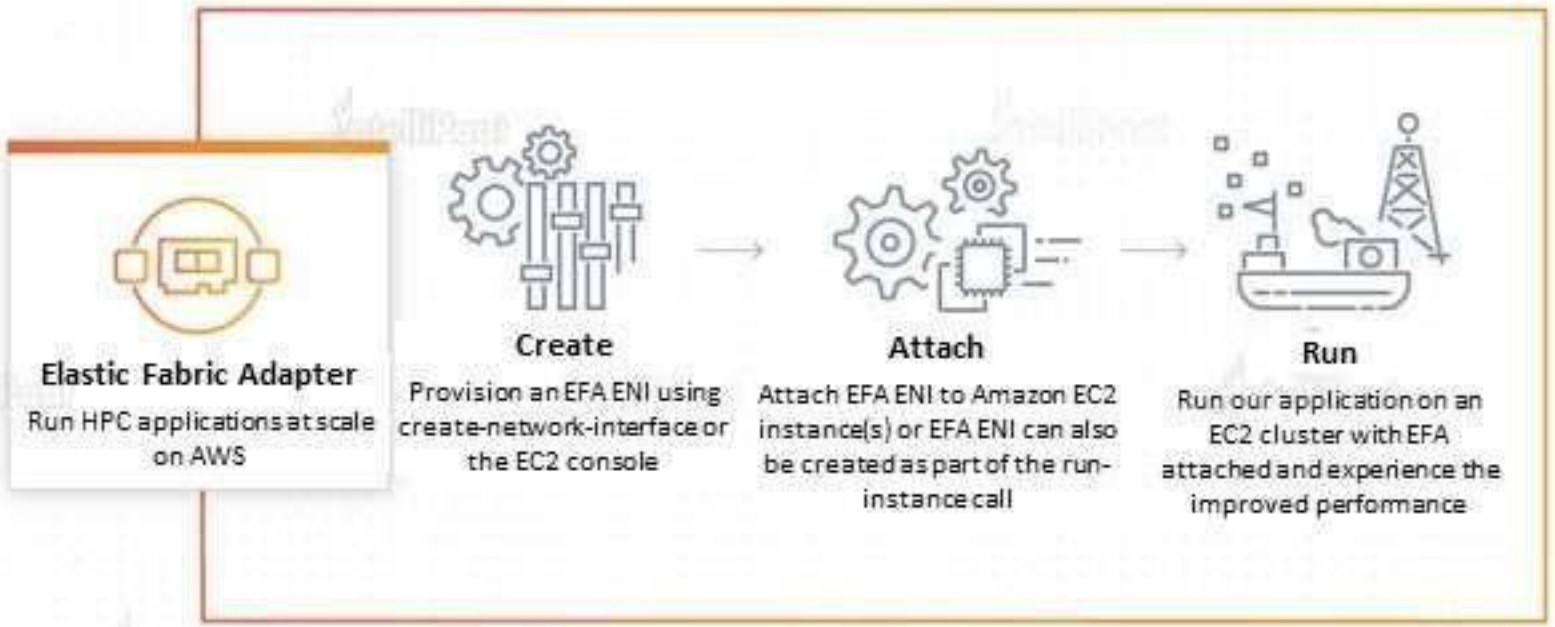
1. Amazon Linux 2
2. Amazon Linux AMI 2018.03
3. Ubuntu 14.04 (with linux-aws kernel) or later
4. Red Hat Enterprise Linux 7.4 or later
5. SUSE Linux Enterprise Server 12 SP2 or later
6. CentOS 7.4.1708 or later
7. FreeBSD 11.1 or later
8. Debian GNU/Linux 9 or later

Elastic Fabric Adapter

Elastic Fabric Adapter

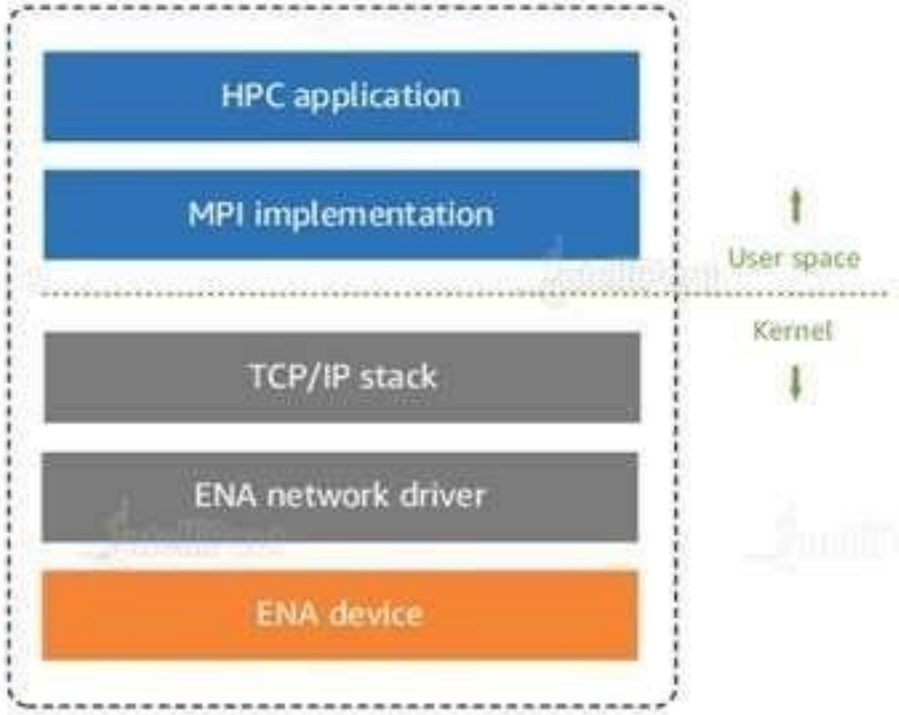
Elastic Fabric Adapter

The network device that we can attach to our Amazon EC2 instance to accelerate High Performance Computing (HPC) and Machine Learning applications

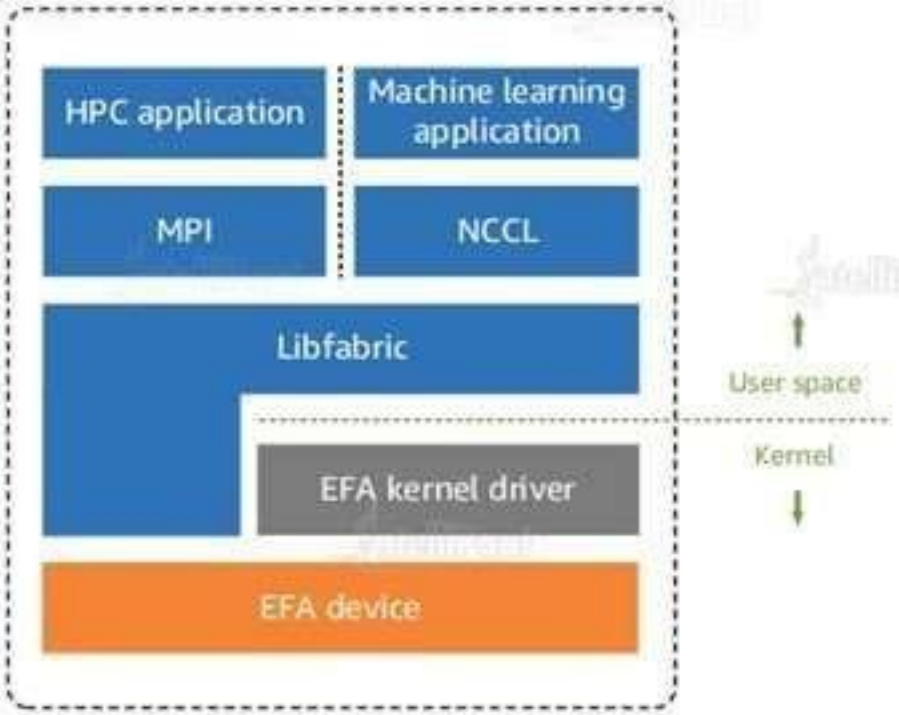


Elastic Fabric Adapter

To put it simply, an EFA is an ENA with added functionalities. It provides an additional OS-bypass function, which allows HPC and ML apps to directly communicate over a network interface to achieve low latency



Traditional HPC software stack in EC2



HPC software stack in EC2 with EFA

Elastic Fabric Adapter

Difference Between EFAs and ENAs

ENAs provide traditional IP networking features that are required to support VPC networking

EFAs provide all of the same traditional IP networking features as ENAs, and they also support OS-bypass capabilities

Elastic Fabric Adapter

Supported Instance Types

c5n.18xlarge, c5n.metal, i3en.24xlarge, i3en.metal, inf1.24xlarge, m5dn.24xlarge, m5n.24xlarge, r5dn.24xlarge, r5n.24xlarge, and p3dn.24xlarge

Supported AMIs

1. Amazon Linux 2
2. Amazon Linux
3. RHEL 7.6
4. RHEL 7.7
5. CentOS 7
6. Ubuntu 16.04
7. Ubuntu 18.04

Elastic Fabric Adapter

What are the limitations of EFAs?

- We can attach only one EFA per instance
- We cannot send EFA traffic from one subnet to another subnet. Only the normal IP traffic can be sent. EFA OS-bypass traffic is limited to a single subnet
- EFA OS-bypass traffic cannot be routed, only the IP traffic from EFA can be routed
- A security group that allows inbound and outbound traffic to and from the security group itself should be attached to an EFA

AWS CloudFront

AWS CloudFront

Amazon CloudFront is an Amazon Web Services content delivery network. Content delivery networks provide a globally distributed network of proxy servers that cache content, such as web videos or other bulky media, closer to consumers, improving access speed to the content.

AWS CloudFront
Vs
Global Accelerator

IntelliPaat

Differences

CloudFront

- CloudFront employs multiple sets of dynamically changing IP addresses.
- CloudFront pricing is primarily determined by data transfer out & HTTP requests.
- CloudFront caches content using Edge locations .
- CloudFront is optimized for HTTP Protocol

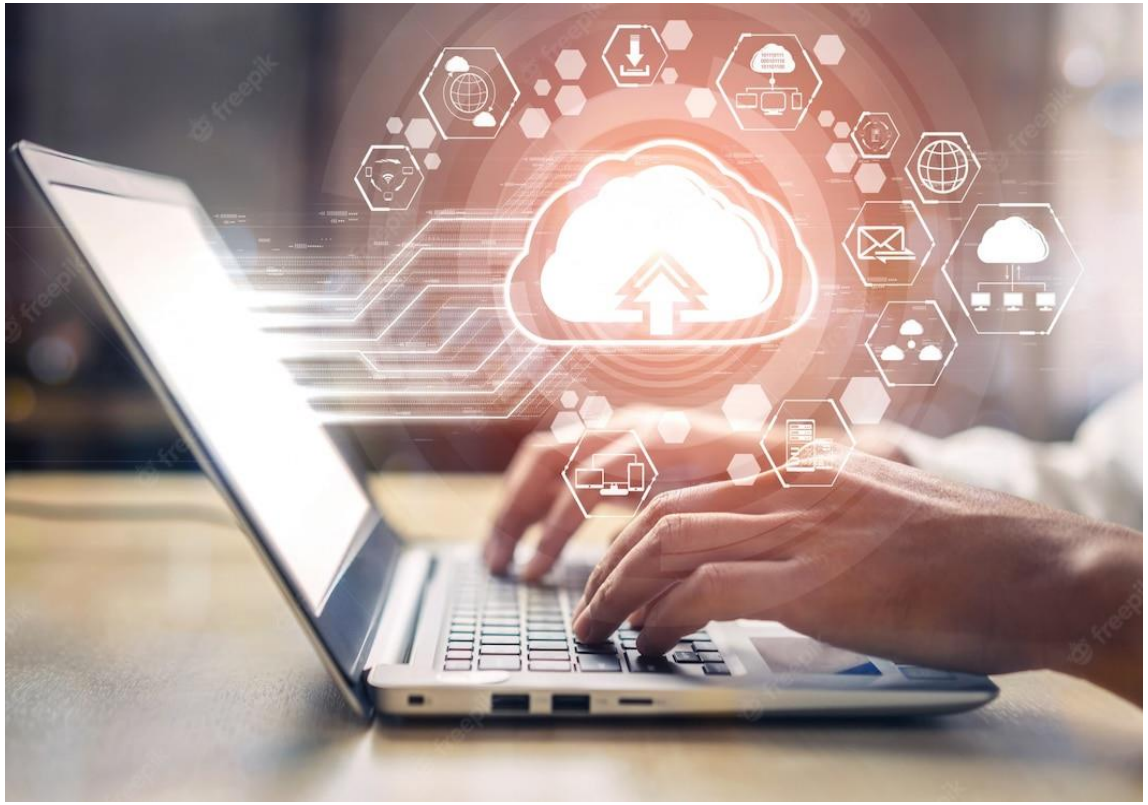
Global Accelerator

- Global Accelerator provides a fixed entry point to your applications via a set of static IP addresses
- Global Accelerator charges a fixed hourly fee as well as incremental charge over your standard Data Transfer rates.
- Global Accelerator uses edge locations to find the best path to the nearest regional endpoint
- Global Accelerator is ideal for both HTTP and non HTTPprotocol such as Tcp & Udp .

AWS Backup

AWS Backup

AWS Backup Service can be used to centralize and automate data protection across multiple AWS services and hybrid workloads. AWS Backup provides a low-cost, fully managed, policy-based service that simplifies data protection at scale. AWS Backup also assists you in meeting regulatory compliance and business data protection policies.



AWS Backup

Advantages of AWS Backup

- Manage backups centrally
- Backup procedures should be automated.
- Increase backup compliance.

.

India: +91-7847955955

US: 1-800-216-8930 (TOLL FREE)

support@intellipaat.com

24/7 Chat with Our Course Advisor