CSYE 6225 – Network Structures & Cloud Computing

Team Members:

Neel Indap

Nishant Gohel

Kunal Chugh

Virtual Machines OS Support

OS	AWS	Azure	GCP
Windows Server	Windows Server 2003 SP1 Windows Server 2003 R2 Windows Server 2008 Microsoft Windows Server 2012	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016	Windows-1709-core Windows-1709-core-for-containers Windows-2016 Windows-2016-core Windows-2012-r2 Windows-2012-r2-core Windows-2008-r2
CentOS	CentOS x64 5.1-5.11 CentOS x64 6.1-6.6 CentOS x64 7.0-7.1	CentOS 6 CentOS 7	CentOS 6,7
Red Hat Enterprise Linux (RHEL)	RHEL x64 5.1-5.11 RHEL x64 6.1-6.6 RHEL x64 7.0-7.1	RHEL 6 RHEL 7	RHEL 6 RHEL 7
Debian	Debian x64 6.0.0-6.0.8 Debian x64 7.0.0-7.2.0	Debian 6 Debian 7	Debian 8 Debian 9
Ubuntu	Ubuntu x64 12.04, 12.10 Ubuntu x64 13.04, 13.10 Ubuntu x64 14.04, 14.10	Ubuntu 12.04, 14.04, 16.04, 16.10	Ubuntu-16.04-lts Ubuntu-14.04-lts Ubuntu-17.10
SUSE Linux Enterprise Server (SLES)	Not Available	SLES 11 SLES 12	SLES 11 SLES 12
Oracle Linux	Not Available	Version 6, 7	Not Available

Relational Database Support

AWS	Azure	GCP
Amazon Aurora PostgreSQL MySQL MariaDB Oracle Microsoft SQL Server	Windows Azure SQL DB SQL Server Oracle MySQL SQL Compact PostgreSQL	Cloud SQL - by MSQL (currently in beta and support for MySQL 5.6 and 5.7) Cloud Spanner

NoSQL Database Support

Types	AWS	Azure
Key/Value	Memcached Redis Aerospike	Windows Azure Blob Storage Windows Azure Table Storage Windows Azure Cache Redis Memcached Riak
Column Family	Cassandra Hbase	Cassandra HBase
Document	Amazon DynamoDB MongoDB MarkLogic Couchbase	MongoDB RavenDB CouchDB
Graph	Neo4J Amazon Neptune OrientDB GraphDB	Neo4J

- Google Cloud supports following databases

1. Google cloud BigTable
2. Google cloud datastore
3. Firebase Realtime Database
4. Cloud Firestore for Firebase

Deployment Tools

AWS	Azure	GCP
AWS Elastik Beanstalk AWS CloudFormation AWS OpsWorks AWS CodeCommit AWS CodePipeline AWS CodeDeploy Amazon EC2 Container Service	Microsoft Azure Resource Manager Template and Classic	Google Cloud Deployment Manager

DNS

AWS	Azure	GCP
Route 53	Azure DNS	Cloud DNS

Security Groups- AWS

- AWS “Security Groups” helps protecting instances by configuring inbound and outbound rules. Users can configure what ports to open to accept traffic from what source and similarly configure outbound ports from EC2 instances.
- AWS allows us to create 200 Security groups per VPC, for example if you have 5 VPCs you can create 200 * 5 = 1000 Security groups totally, but Security groups in both clouds cannot span regions.

Security Groups – Azure

- Azure’s naming convention is “Network Security Group” is currently available only for Regional Virtual Networks and not available for that has Affinity Group Associated. You can have max 100 NSGs per subscription
- Unlike AWS, Network Security Group of Azure can be associated to VM Instance, Subnets. Azure currently doesn’t offer user interface to add/edit security groups, so users must use PowerShell and REST APIs to setup the same

Security Group - Google Cloud

- Compute Engine uses firewall rules to secure Compute Engine virtual machine instances and networks. You create a rule by specifying the source IP address range, protocol, ports, or user-defined tags that represent source and target groups of virtual machines instances. However, Compute Engine firewall rules can’t block outbound traffic. To do that, you can use a different kind of technology, such as iptables.

VPC - AWS

- Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.
- You can launch your AWS resources, such as Amazon EC2 instances, into your VPC. You can configure your VPC by modifying its IP address range, create subnets, and configure route tables, network gateways, and security settings.
- The original release of Amazon EC2 supported a single, flat network that's shared with other customers called the *EC2-Classic* platform. Earlier AWS accounts still support this platform, and can launch instances into either EC2-Classic or a VPC. Accounts created after 2013-12-04 support EC2-VPC only

VPC – AWS cont..

- By launching your instances into a VPC instead of EC2-Classic, you gain the ability to:
  - Assign static private IPv4 addresses to your instances that persist across starts and stops
  - Optionally associate an IPv6 CIDR block to your VPC and assign IPv6 addresses to your instances
  - Assign multiple IP addresses to your instances
  - Define network interfaces, and attach one or more network interfaces to your instances
  - Change security group membership for your instances while they're running
  - Control the outbound traffic from your instances (egress filtering) in addition to controlling the inbound traffic to them (ingress filtering)
  - Add an additional layer of access control to your instances in the form of network access control lists (ACL)
  - Run your instances on single-tenant hardware

VPC - Azure

- In 2013,Azure introduced many new services and importantly Virtual Networks, “a Logically Isolated network” the VPC version of Azure within its Datacenter. Azure’s Virtual Network resembles VPC in many aspects and in fact behaves similar in many cases but there are few differences as well.
- Resources within the virtual network can communicate with each other privately, through private IP addresses.
- On-premises resources can access resources in a virtual network using private IP addresses over a Site-to-Site VPN (VPN Gateway) or ExpressRoute.
- Service instances in a virtual network are fully managed by the Azure service, to monitor health of the instances, and provide required scale, based on load.

VPC – Azure cont..

- Services that can be deployed into Azure virtual network
  - Service fabric
  - Virtual machine scale sets
  - HDInsight
  - App Service Environment
  - RedisCache
  - API Management
  - VPN Gateway
  - Application Gateway (internal)
  - Azure Container Service Engine
  - Azure Active Directory Domain Services
  - Azure Batch

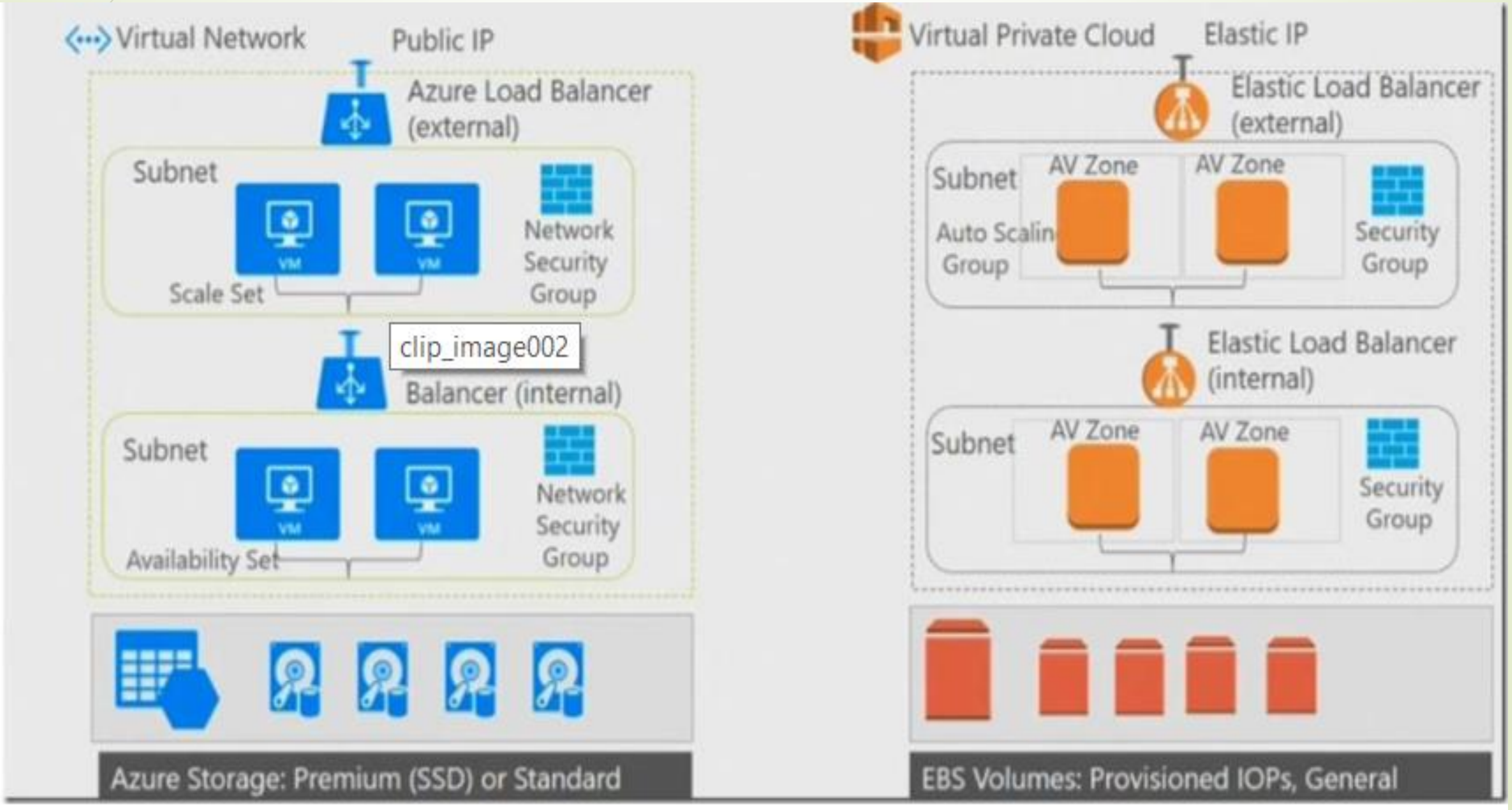
VPC – Google Cloud

- Cloud Virtual Networks can contain up to 7000 virtual machine instances. Unlike AWS and Azure, networks can encompass resources (subnets) deployed across multiple regions and reduces the need for complex VPN and network peering configuration
- Google Cloud VPN securely connects your on-premises network to your Google Cloud Platform (GCP) Virtual Private Cloud (VPC) network through an IPsec VPN connection. Traffic traveling between the two networks is encrypted by one VPN gateway, then decrypted by the other VPN gateway. This protects your data as it travels over the Internet.

VPC – Cloud cont…

- Cloud VPN provides a 99.9% service availability.
- Cloud VPN supports site-to-site VPN. You can have multiple tunnels to a single VPN gateway. In other words, you can connect multiple on-premises networks using multiple on-premises gateways to the same VPC network.
- Cloud VPN supports both static routes and dynamic routes
- Cloud VPN supports both IKEv1 and IKEv2 using a shared secret

Azure vs AWS


Virtual Network
Public IP
Azure Load Balancer (external)
Subnet
VM
VM
Network Security Group
Scale Set
clip_image002
Balancer (internal)
Subnet
VM
VM
Network Security Group
Availability Set
Azure Storage: Premium (SSD) or Standard
Virtual Private Cloud
Elastic IP
Elastic Load Balancer (external)
Subnet
AV Zone
AV Zone
Auto Scalin Group
Security Group
Elastic Load Balancer (internal)
Subnet
AV Zone
AV Zone
Security Group
EBS Volumes: Provisioned IOPs, General

Subnets - AWS

- An AWS VPC spans all the Availability Zones (AZs) in that region, hence, subnets in AWS VPC are mapped to Availability Zones (AZs). A subnet must only belong to one AZ and cannot span Azs
- AWS VPC subnets can either be private or public.
- WS creates a default VPC and subnets for each region. This default VPC has subnets for each region where the VPC resides, and any image (EC2 instance) deployed to this VPC will be assigned a public IP address and hence has internet connectivity
- AWS has matured tools like their management portal, Cloud Formation Templates, CLIs and programmable APIs to launch subnets.

Subnets – Azure

- Azure VNet subnets are defined by the IP Address block assigned to it
- Azure VNet does not provide a default VNet and does not have private or public subnet as in AWS VPC. Resources connected to a VNet have access to the Internet, by default.
- Azure Virtual Network also allows us to create subnets of any quantity using the Management portal, PowerShell, CLI.

Subnets - GCP

- Unlike AWS and Azure, Google do not constrain the private IP address ranges of subnets to the address space of the parent network. It is therefore possible to have one subnet with a range of 10.240.0.0/16 and another with 192.168.0.0/16 on the same network. While the network can span multiple regions, individual subnets must belong to a single region. Default network routes allow connectivity to/from the internet to each subnet and between subnets. Additional routes can be added to override these defaults where required.

Routing Table – AWS

- AWS uses the route table to specify the allowed routes for outbound traffic from the subnet. All subnets created in a VPC is automatically associated with the main routing table, hence, all subnets in a VPC can allow traffic from other subnets unless explicitly denied by security rules

Routing Table - Azure

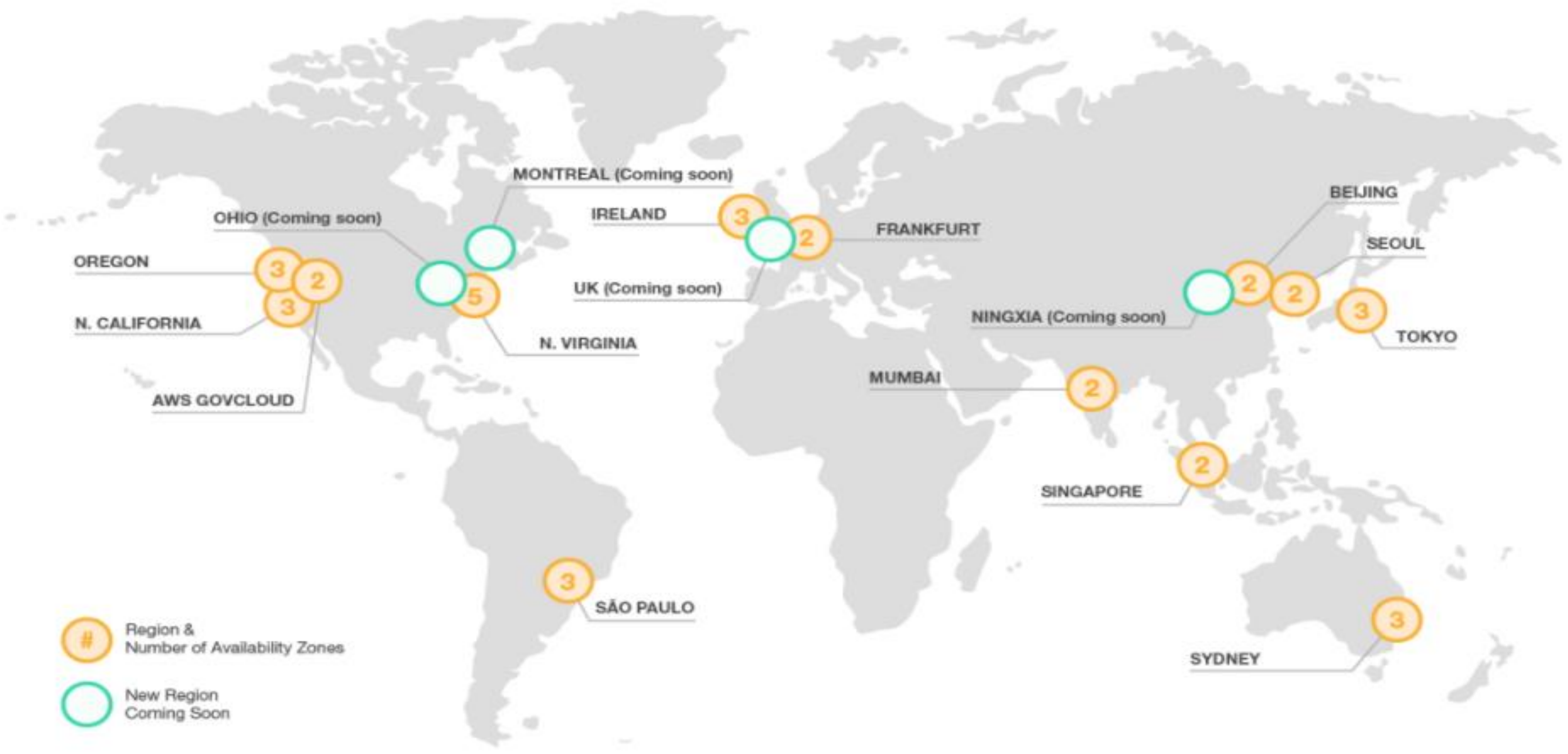
- Windows Azure provides default routing across subnets within a single virtual network, but does not provide any type of network ACL capability with respect to internal IP addresses. So in order to restrict access to machines within a single virtual network, those machines must leverage Windows Firewall with Advanced Security
- In a hybrid setup, Azure VNet may use any of the three route tables – UDR, BGP and System routing tables.
- In Azure VNet, the subnet relies on the system routes for its traffic until a route table is explicitly associated with a subnet.

Routing Table – GCP

- Two routes are created at network creation time.
  - A default route for Internet Traffic (0/0)
  - Virtual network route for destination IP range within IPv4 range of networks

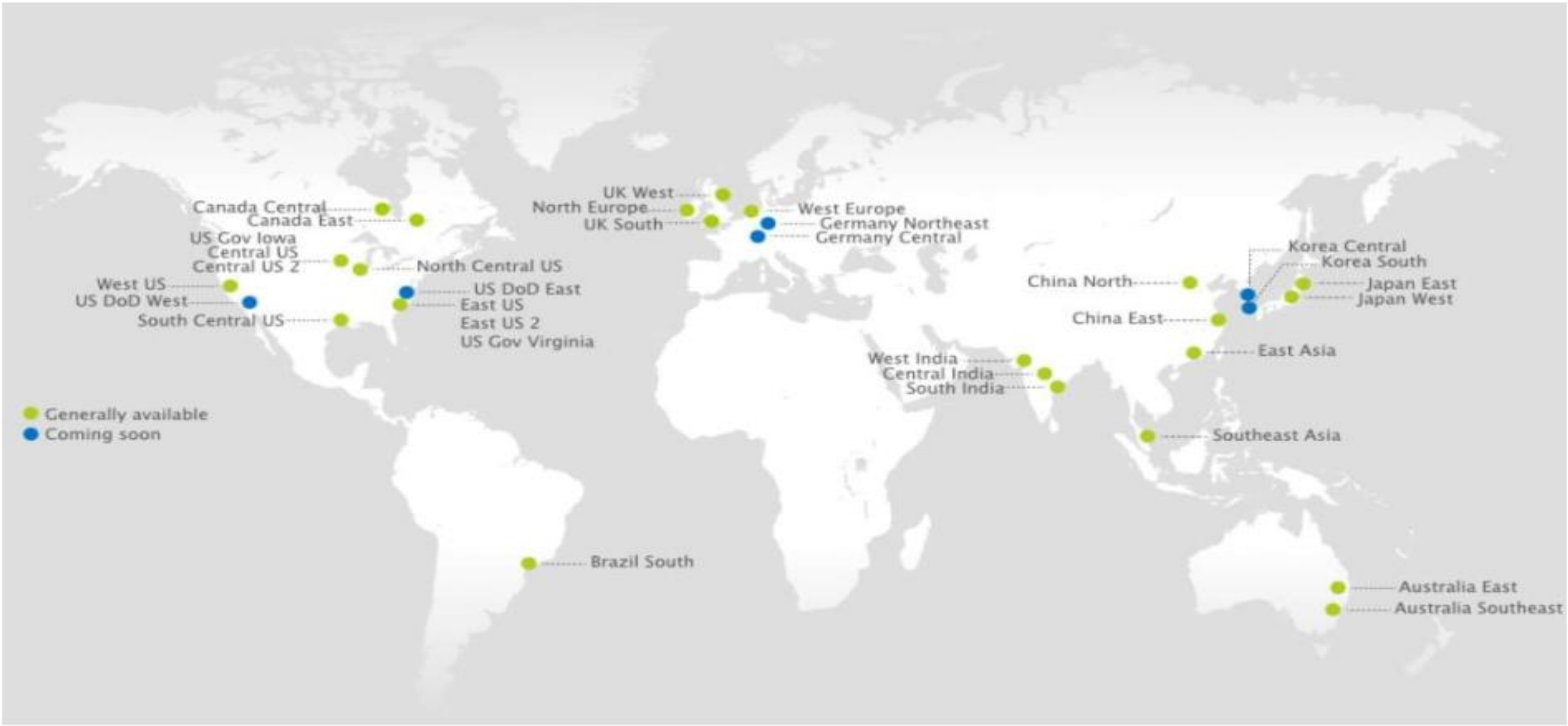
- Each route in the routes collection may apply to zero or more instances. GCP applies a route to an instance if the tag applied to the route and the tag applied to that instance match. If the route has no tag, then the route applies to all instances in the network

AWS Location Worldwide



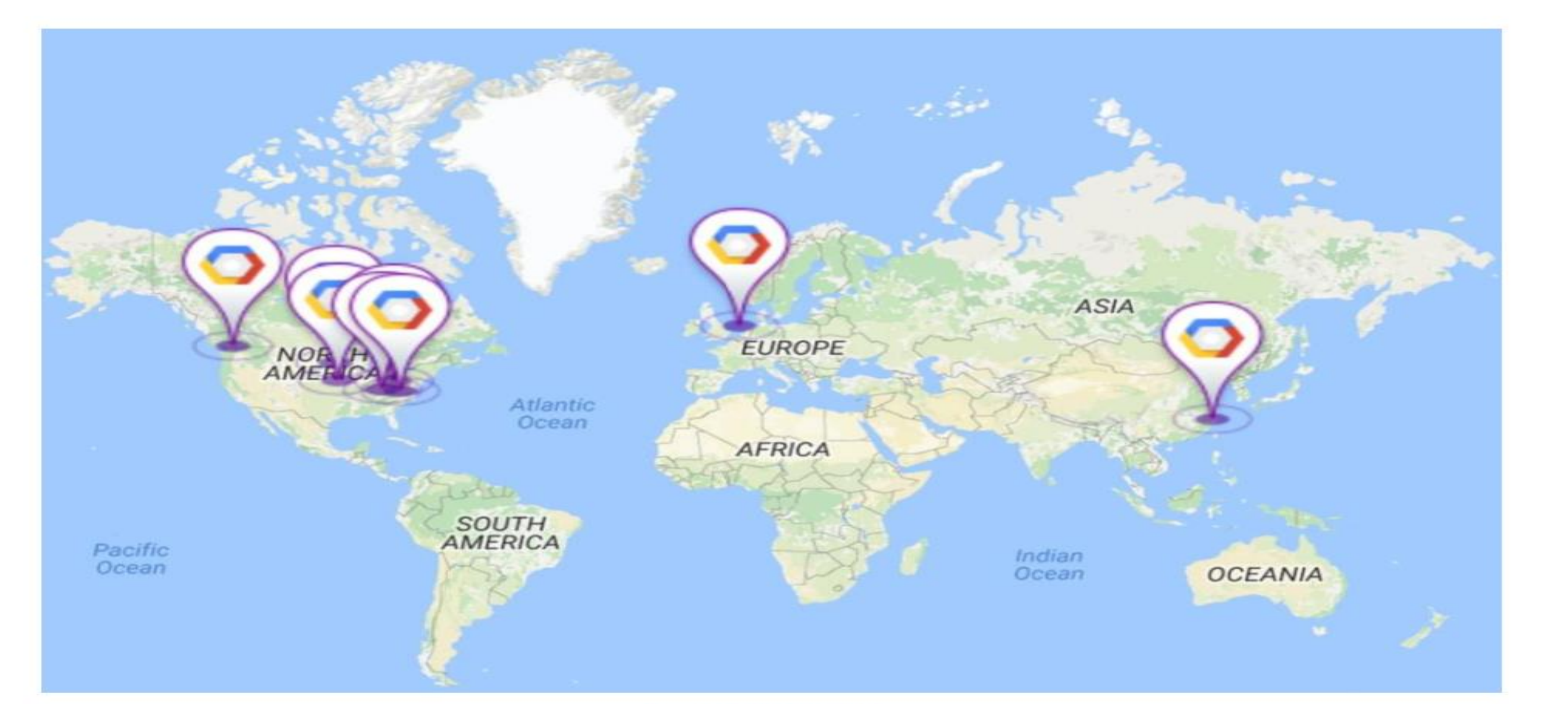
AWS locations. Diagram by Amazon

Azure Location Worldwide



Azure locations. Diagram by Microsoft

GCP Location Worldwide



Google Cloud locations