



AWS Secure Environment Accelerator (SEA)

Atelier d'introduction

Louis Caron

loucaron@amazon.com

Février 2021

Agenda

- ❖ La solution à haut niveau
- ❖ Revue de l'architecture de AWS Secure Environment Accelerator (SEA)
- ❖ Liste des requis
- ❖ Qu'est-ce qu'un "State Machine"
- ❖ Fonctionnement de AWS SEA "Accelerator State Machine"
- ❖ Les grandes étapes de l'installation
- ❖ Demo & revue du fichier "config.json"

La solution à haut niveau

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Sommaire des fonctionnalités (1/3)



- **Organisation AWS avec plusieurs comptes:**

- Une [AWS Organization](#) est une structure de regroupement pour un certain nombre de comptes AWS distincts qui sont contrôlés par une seule entité client. Cela fournit une facturation consolidée, des unités organisationnelles et facilite le déploiement de garde-corps pan-organisationnels tels que les journaux AWS CloudTrail et les stratégies de contrôle des services. Les comptes séparés fournissent une isolation solide du plan de contrôle et du plan de données entre les charges de travail et / ou les environnements.

- **Chiffrement:**

- [AWS KMS](#) avec les clés CMK gérées par le client est largement utilisé pour toutes les données stockées au repos, dans les compartiments S3, les volumes EBS, le chiffrement RDS.

- **Politiques de contrôle des services:**

- [SCP](#) fournit un mécanisme de balises de sécurité principalement utilisé pour refuser des catégories entières d'opérations d'API au niveau d'un compte AWS, d'une unité d'organisation ou d'une organisation. Ceux-ci peuvent être utilisés pour garantir que les charges de travail sont déployées uniquement dans des régions prescrites, garantir que seuls les services de la liste blanche sont utilisés ou empêcher la désactivation des contrôles de détection / prévention. Des SCP normatifs sont fournis.

Sommaire des fonctionnalités (2/3)



- **Réseau centralisé et isolé:**
 - Clouds privés virtuels (VPC) sont utilisés pour créer une isolation du plan de données entre les charges de travail, centralisée dans un compte de réseau partagé. La connectivité aux environnements sur site, la sortie Internet, les ressources partagées et les API AWS sont médiatisées à un point central d'entrée / sortie via l'utilisation de Passerelle de transit, VPN de site à site, Pare-feu de nouvelle génération et AWS Direct Connect (le cas échéant).
- **Gestion DNS centralisée:**
 - Amazon Route 53 est utilisé pour fournir des zones hébergées publiques et privées unifiées dans l'environnement cloud. Les résolveurs de Amazon Route 53 entrants et sortants étendent cette vue unifiée du DNS aux réseaux locaux.
- **Journalisation complète:**
 - AWS CloudTrail les journaux sont activés à l'échelle de l'organisation pour assurer l'auditabilité dans l'environnement cloud. Amazon CloudWatch Les journaux, pour les applications, ainsi que les journaux de flux VPC, sont centralisés et la suppression est empêchée via les SCP.

Sommaire des fonctionnalités (3/3)



- **Contrôles de sécurité détective:**
 - Des menaces de sécurité potentielles sont apparues dans l'environnement cloud via le déploiement automatique de contrôles de sécurité de détection tels que [Amazon GuardDuty](#), [AWS Config](#), et [AWS Security Hub](#).
- **Authentification unique (SSO):**
 - AWS SSO est utilisé pour fournir une hypothèse de rôle IAM authentifié par AD dans les comptes de l'organisation pour les mandataires autorisés.

Implémentation automatisée de balises de sécurité techniques

#	Balises de sécurité	Couverture de AWS SEA
1	Protéger le compte administrateur racine / global	✓
2	Gestion des privilèges administratifs	✓
3	Accès à la console cloud	✓
4	Comptes de surveillance d'entreprise	✓
5	Emplacement des données	✓
6	Protection des données au repos	✓
7	Protection des données en transit	✓
8	Segmenter et séparer	✓
9	Services de sécurité réseau	✓
10	Services de cyberdéfense	✓
11	Journalisation et surveillance	✓
12	Configuration du Marketplace	✓

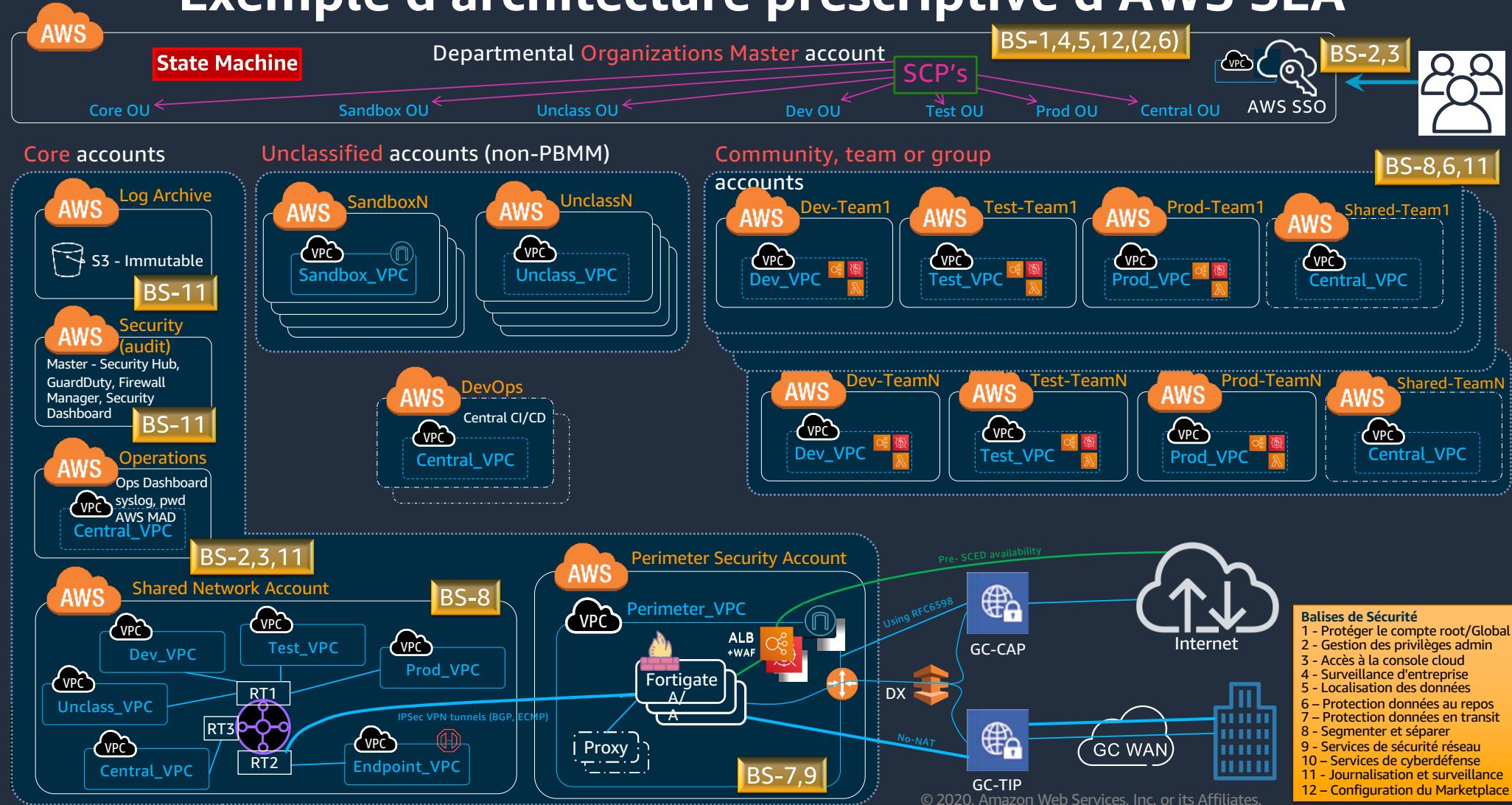
© 2021, Amazon Web Services, Inc. or its Affiliates.

* Certains garde-corps nécessitent un suivi manuel



Exemple d'architecture prescriptive d'AWS SEA

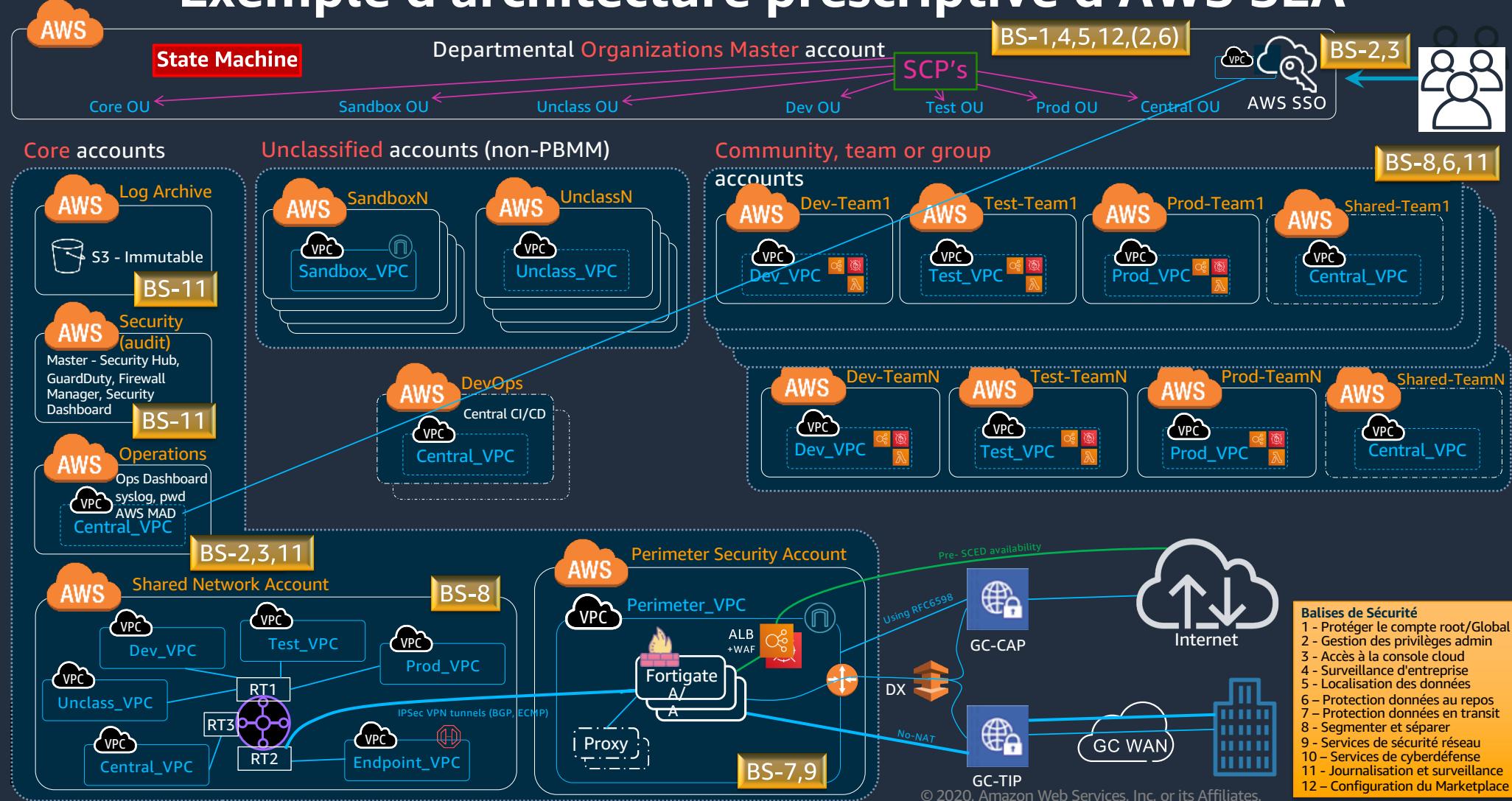
v1.2c



© 2020, Amazon Web Services, Inc. or its Affiliates.

Exemple d'architecture prescriptive d'AWS SEA

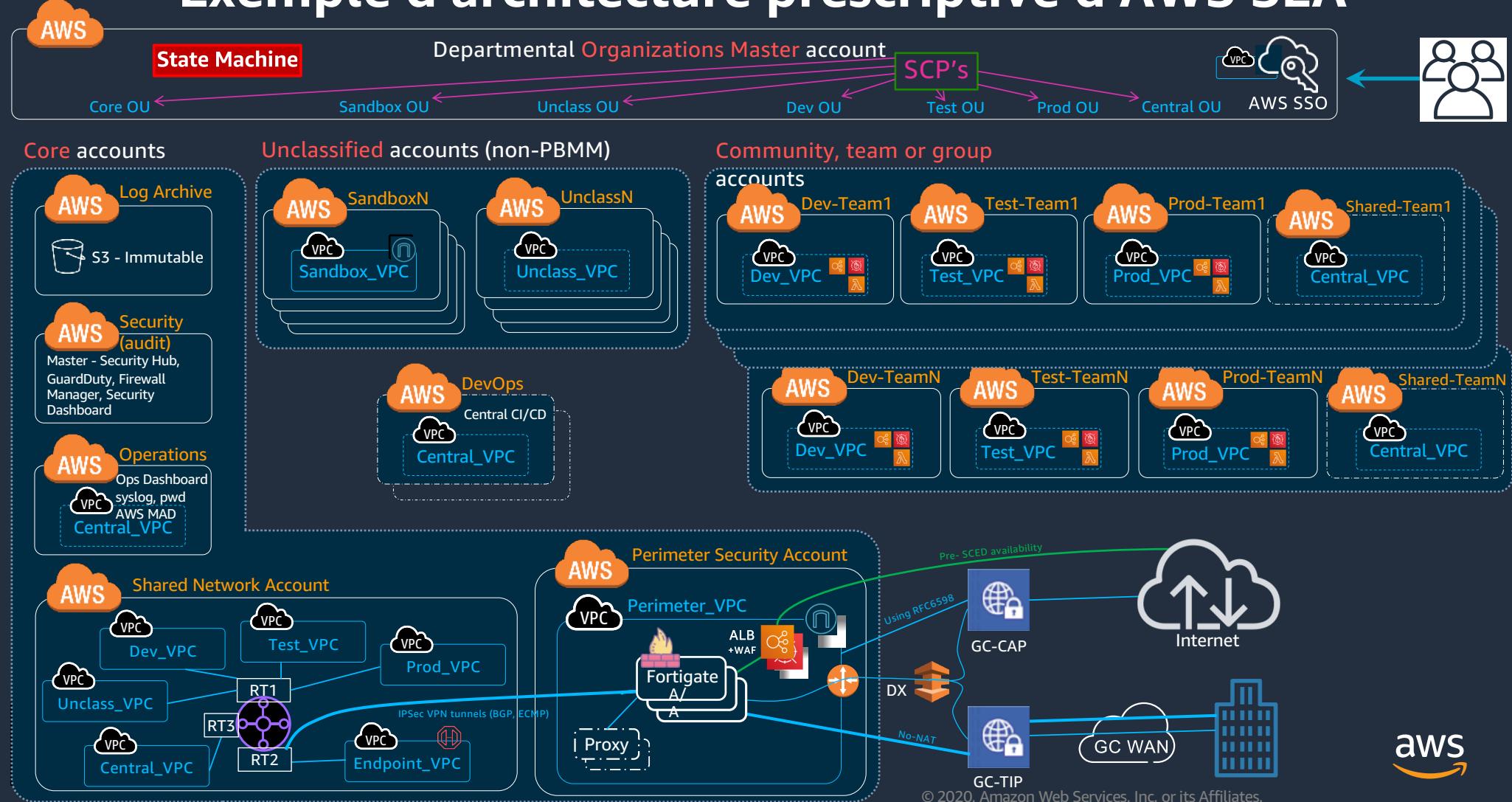
v1.2c



© 2020, Amazon Web Services, Inc. or its Affiliates.

Exemple d'architecture prescriptive d'AWS SEA

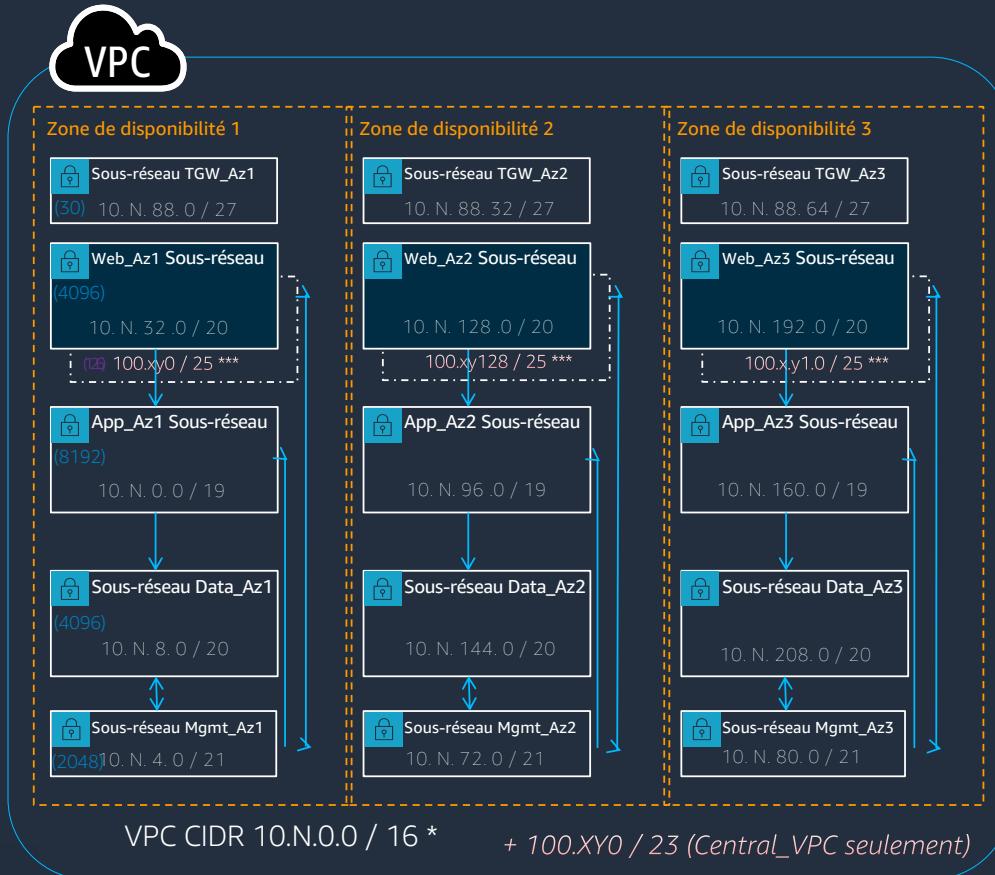
v1.2c



Conception de VPC standard AWS Accelerator v1.2

(Utilisé pour Dégager, Dev, Test, Prod, VPC centraux) - **Classe B**

(L'option demi-classe B existe)



REMARQUE: les sous-réseaux ne sont PAS des ZIP. Les groupes de sécurité sont utilisés comme limite de zonage / ZIP. Cette conception tire parti du concept de nombreux micro-ZIP, potentiellement un par application, par zone.

REMARQUE: les sous-réseaux TGW ne sont pas partagés. Sandbox_VPC supprime les sous-réseaux TGW, les sous-réseaux Web deviennent publics avec IGW et NATGW pour les sous-réseaux privés. Sous-réseaux du VPC central RFC6598 nommés GCWide_azX.

* Nous attribuons un full / 16 à chaque VPC (c'est-à-dire 10.10.0.0/16 pour Dev, 10.11.0.0/16 pour Test, etc.). Le client peut éventuellement utiliser d'autres blocs CIDR RFC1918. Il est essentiel que ces plages CIDR n'entrent pas en conflit avec les plages CIDR d'un département sur site car il n'y a PAS de NAT'ing pour les communications sol-cloud (marquer comme «utilisé pour le cloud» dans le système IPA).

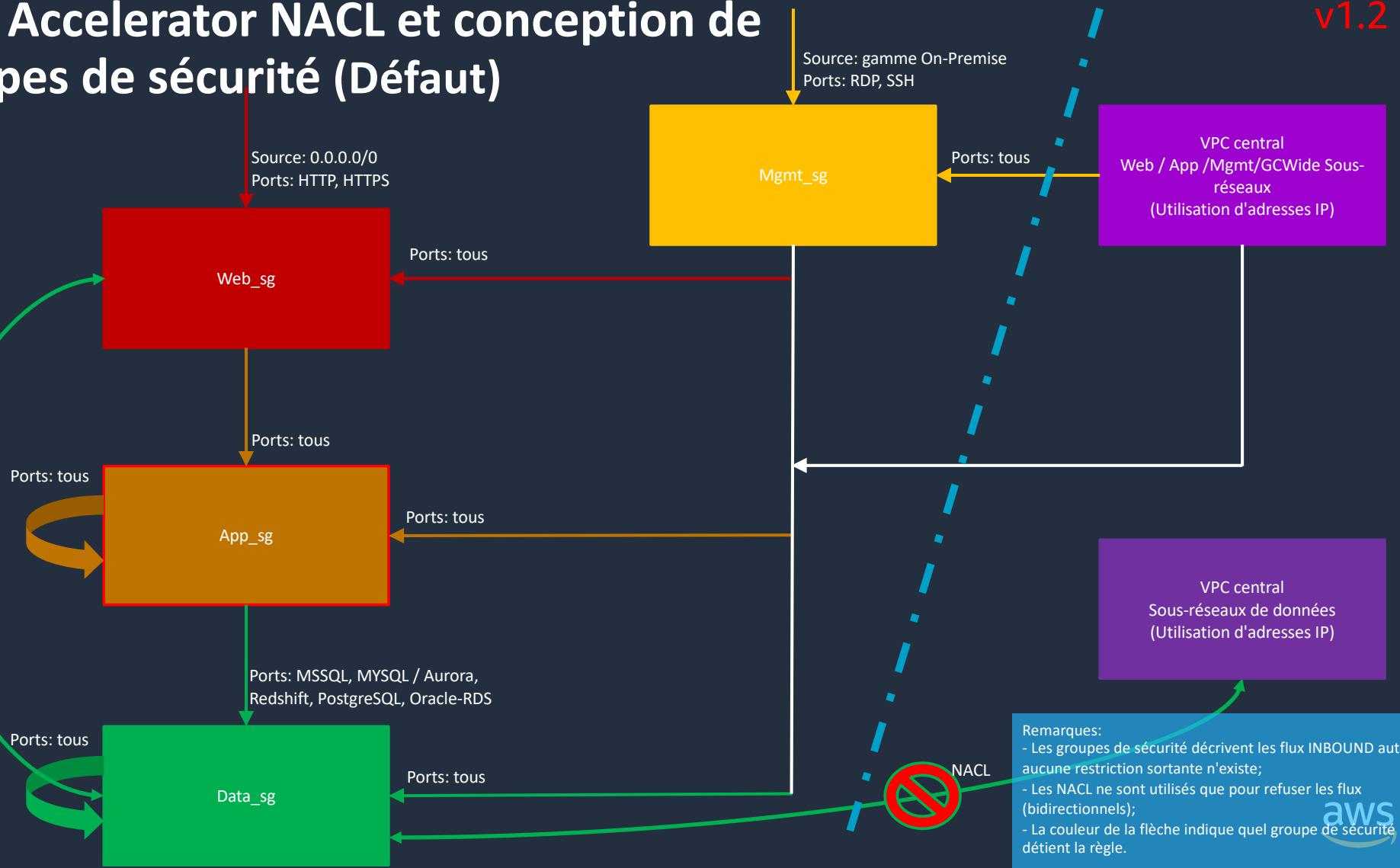
** Remarque: 10.N.224.0 / 19, 10.N.88.96-10.N.95.255, et 100.xy1.128 / 25 sont disponibles pour une affectation future.

*** Le CIDR VPC central a été étendu avec une plage CIDR RFC6598 (sous-réseaux Web internes) pour héberger MAD et d'autres services qui peuvent nécessiter un accès inter-départements.

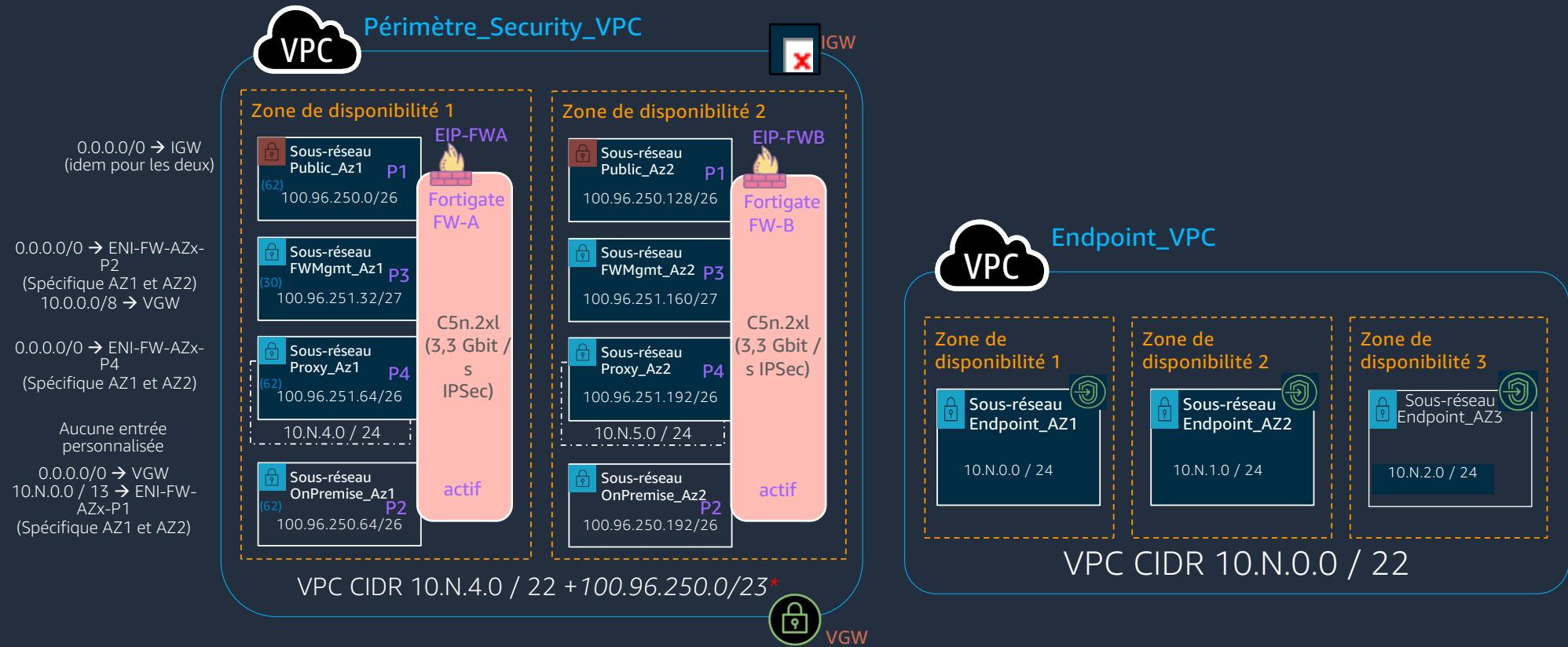


AWS Accelerator NACL et conception de groupes de sécurité (Défaut)

v1.2



Conceptions de VPC spécialisés AWS Accelerator v1.2



* 100.96.250.0/23 est un exemple de bloc RFC6598, les clients doivent chacun utiliser leur propre bloc attribué par SSC. Les ministères ont également besoin que SSC attribue des ASN BGP uniques.

** Remarque: 10.n.4.0 / 22 doit être utilisé pour créer un VPC car vous ne pouvez pas étendre un bloc de sous-réseau 100. *

*** 100.96.252.0/23 supplémentaires nécessaires pour le réseau de superposition (Fortigates à l'intérieur du tunnel VPN). Avant que GCCAP ne soit disponible, le sous-réseau public contiendra des ELB pour les applications publiques.

**** Adresses disponibles restantes: 100.96.251.0/27 et 100.96.251.128/27 (32 par AZ)



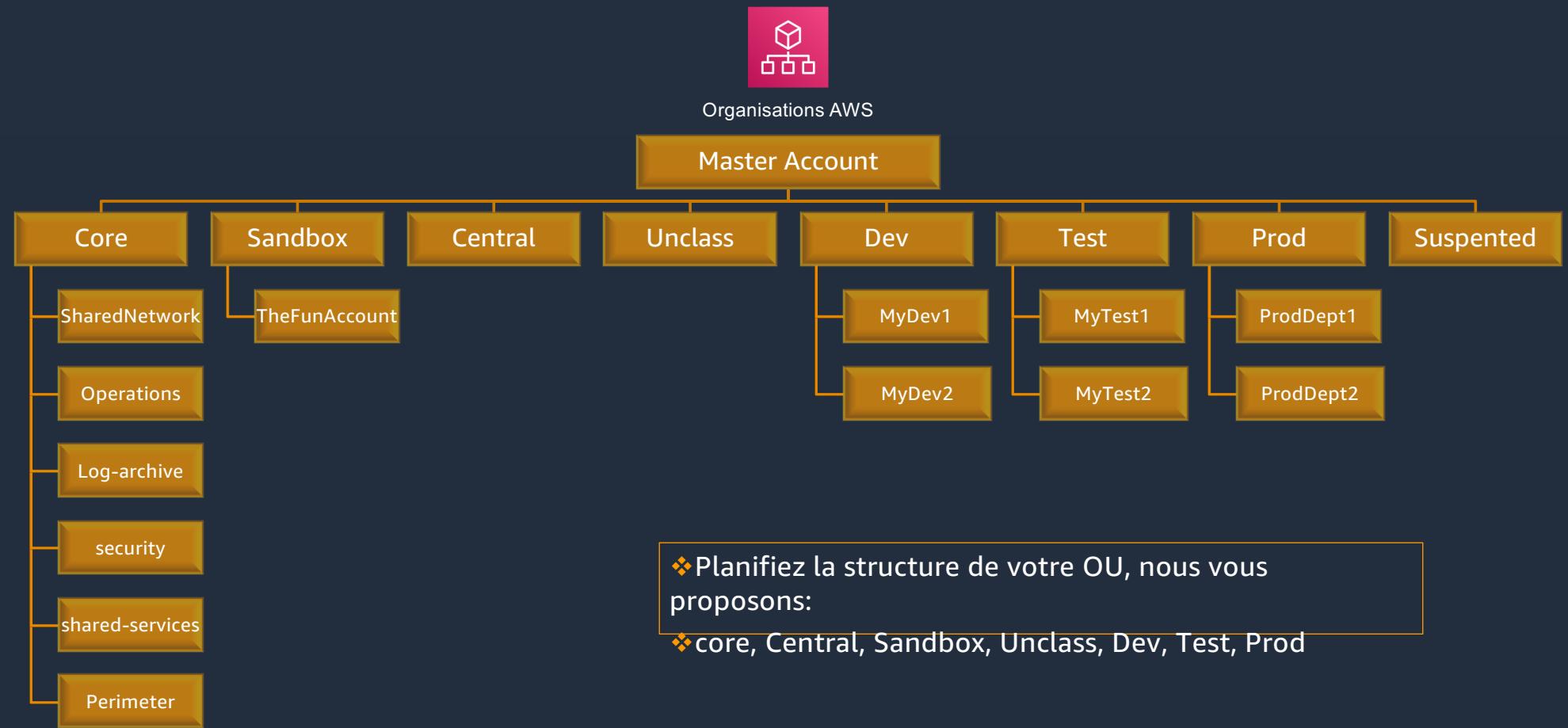
Liste des requis

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Configuration AWS SEA pour la production - Informations requises

CECI NÉCESSITE UNE PRÉPARATION ET UNE PLANIFICATION EXTENSIVES



Configuration SEA pour la production - Informations requises

CECI NÉCESSITE UNE PRÉPARATION ET UNE PLANIFICATION EXTENSIVES

1. Planifiez la structure de votre OU, nous vous suggérons:
 - core, Central, Sandbox, Unclass, Dev, Test, Prod
2. 6 * blocs d'adresses RFC1918 de classe B (CIDR) qui n'entrent pas en conflit avec vos réseaux sur site
 - (un pour chaque OU, sauf Sandbox qui n'est pas routable)
 - la plage de classe B "principale" sera divisée pour prendre en charge le VPC Endpoint et le VPC de périmètre
3. 2 * blocs d'adresses RFC6598 / 23 (exigence du gouvernement du Canada (GC) uniquement)
 - (MAD, sous-couche de périmètre) (les clients non GC peuvent utiliser l'espace d'adressage de la plage CIDR principale)
4. 2 * BGP ASN (TGW, FW Cluster) (un troisième est requis si vous déployez un VGW pour la connectivité DX)
5. Un nom de domaine Windows unique (deptaws/dept.aws, deptcloud/dept.cloud, etc.)
6. Noms de domaine DNS et adresses IP de serveur DNS pour les zones DNS privées sur site nécessitant une résolution cloud
7. Domaine DNS pour une zone publique hébergée dans le cloud "public": ["dept.cloud-nuage.canada.ca"]
8. Domaine DNS pour une zone privée hébergée dans le cloud "privée": ["dept.cloud-nuage.gc.ca"]
9. Certificat TLS Wildcard pour chacune des 2 zones précédentes
10. 2 * licences de pare-feu Fortinet FortiGate
11. Nous recommandons également au moins 20 ALIASES de messagerie uniques associées à une seule boîte aux lettres, jamais utilisées auparavant pour ouvrir des comptes AWS, de sorte que vous n'ayez pas besoin de demander de nouveaux alias de messagerie chaque fois que vous devez créer un nouveau compte AWS.

Les grandes étapes de l'installation

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Exigences de base

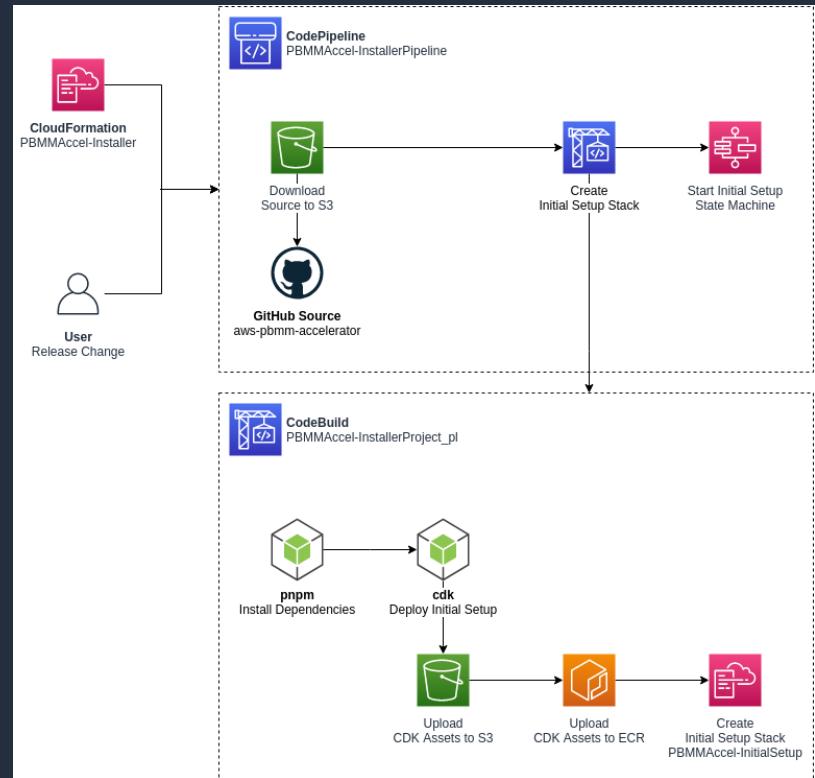
- ❖ Le déploiement d'**AWS SEA** nécessite l'assistance de votre équipe de compte AWS locale. Tentatives de déploiement de l'accélérateur sans le support de votre AWS SA, TAM, ProServe, ou l'installation échouera car les nouveaux comptes AWS n'ont pas de quotas appropriées établies pour faciliter l'installation.
- ❖ L'installation de l'architecture native de **AWS SEA** est prescriptive. Elle nécessite une augmentation de vos quotas pour prendre en charge un minimum de 6 comptes AWS dans **AWS Organizations**, plus, tous les comptes de charge de travail supplémentaires requis.

Les grandes étapes de l'installation

1. Créer les divers fichiers de configuration et les déposer dans un **Bucket S3**
2. Démarrage de l'installation via **CloudFormation**
3. Initialisation du "Accelerator State Machine" via l'utilisation de **AWS CodeCommit**, **AWS CodeBuild** et **AWS CodePipeline**
4. Exécution du "Accelerator State Machine" en utilisant les **AWS Step Functions**
5. Les configurations manuelles pour finaliser l'installation

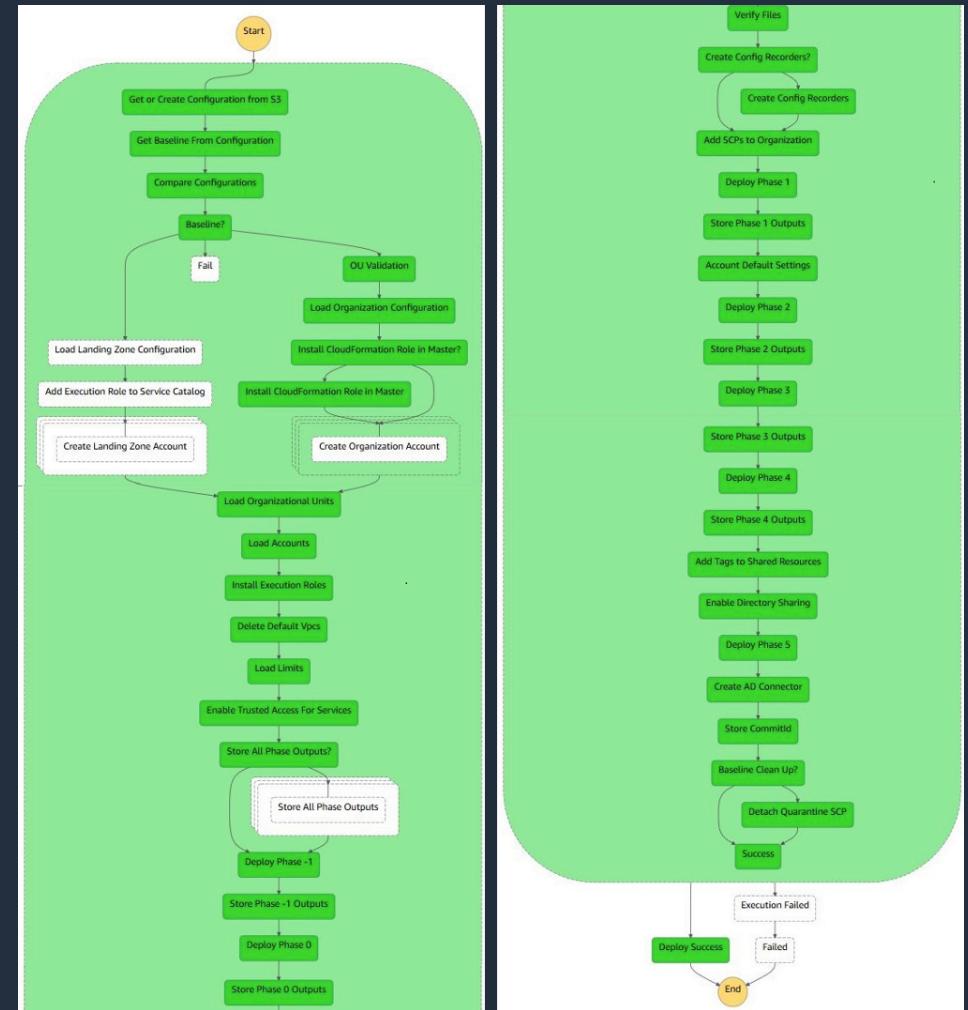
Les grandes étapes de l'installation

1. Créer les divers fichiers de configuration et les déposer dans un **Bucket S3**
2. Démarrage de l'installation via **CloudFormation**
3. Initialisation du “Accelerator State Machine” via l'utilisation de **AWS CodeCommit**, **AWS CodeBuild** et **AWS CodePipeline**



Les grandes étapes de l'installation

4. Exécution du "Accelerator State Machine" en utilisant les AWS Step Functions



Les grandes étapes de l'installation

5. Les configurations manuelles pour finaliser l'installation

- Changer les mots de passe des comptes root et Firewall
- Initialiser MFA pour chaque comptes root

The screenshot shows the AWS Organizations console and a 'Switch Role' dialog box.

AWS Organizations Console: Shows a list of accounts under 'My Account'. One account, 'security' (Email: ioucaron+pbmmT-sec@amazon.com, Account ID: 195086257040), is highlighted with an orange oval. The 'Switch Role' button is circled in green.

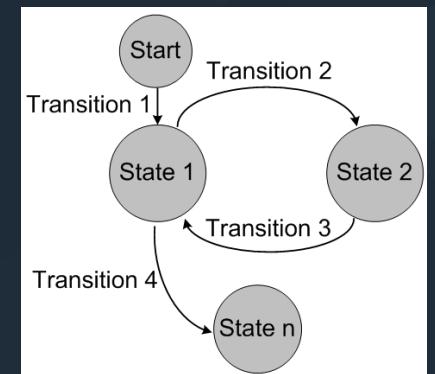
Switch Role Dialog: A modal window titled 'Switch Role'. It contains fields for 'Account*' (set to 012345678901) and 'Role*' (set to PBMMAccel-PipelineRole). Other fields include 'Display Name' (DevAcct), 'Color' (selected color palette), and a 'Switch Role' button.

Right Panel: Shows the user is logged in as Admin (Account: 3420-0203-3641). It displays 'Role History' with a red bar indicating the current role: DevAcct (PBMMAccel-PipelineRole). It also lists 'Currently active as: PBMMAccel-PipelineRole' and 'Account: 6694-2100-9277'. Navigation links include My Account, My Organization, My Service Quotas, My Billing Dashboard, Orders and Invoices, and Back to Admin. A 'Sign Out' link is at the bottom.

Qu'est-ce qu'un "State Machine"

Qu'est-ce qu'un "State Machine"

Un "State Machine" (Une machine à états) est un concept utilisé dans la conception de programmes informatiques ou de logique numérique. Une machine à états finis est composée d'un nombre fini d'états, de transitions et d'actions qui peuvent être modélisés avec des graphiques de flux, où le chemin de la logique peut être détecté lorsque les conditions sont remplies.



Fonctionnement du “Accelerator State Machine”

Accelerator State Machine

- ❖ L'accélérateur se compose d'une machine à état finis primaire PBMMaccel-MainStateMachine_SM et de neuf machines d'état secondaire supportant (à partir de la version 1.2.1). Le client exécute seulement PBMMaccel-MainStateMachine_SM. Tous les dépannages commenceront généralement par PBMMaccel-MainStateMachine_SM.

Step Functions > State machines

State machines (9)

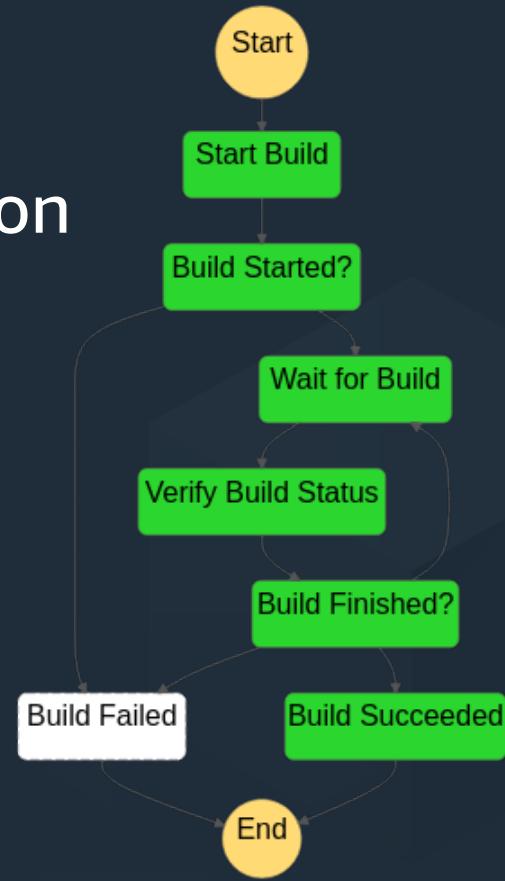
Create state machine

Name	Type	Creation date	Status	Logs	Running	Succeeded	Failed	Timed out	Aborted
PBMMaccel-MainStateMachine_sm	Standard	Aug 31, 2020 05:50:56.255 PM	Active	-	0	2	0	0	0
PBMMaccel-CodeBuild_sm	Standard	Aug 31, 2020 05:50:30.127 PM	Active	-	0	14	0	0	0
PBMMaccel-InstallRoles_sm	Standard	Aug 31, 2020 05:50:29.159 PM	Active	-	0	2	0	0	0
PBMMaccel-CreateAdConnector_sm	Standard	Aug 31, 2020 05:50:27.909 PM	Active	-	0	2	0	0	0
PBMMaccel-InstallCfnRoleMaster_sm	Standard	Aug 31, 2020 05:50:27.811 PM	Active	-	0	2	0	0	0
PBMMaccel-OrgCreateAccount_sm	Standard	Aug 31, 2020 05:50:27.749 PM	Active	-	0	16	0	0	0
PBMMaccel-DeleteDefaultVpcs_sfn	Standard	Aug 31, 2020 05:50:27.364 PM	Active	-	0	2	0	0	0
PBMMaccel-CreateConfigRecorder_sfn	Standard	Aug 31, 2020 05:50:27.312 PM	Active	-	0	2	0	0	0
PBMMaccel-ALZCreateAccount_sm	Standard	Aug 31, 2020 05:50:26.779 PM	Active	-	0	0	0	0	0



Fonctionnement du “Accelerator State Machine”

- ❖ Consiste en 6 phases d'installation



Fonctionnement du “Accelerator State Machine”

- ❖ Lors d'une erreur, l'installation arrête et envoie une notification à l'administrateur via courrier
- ❖ Le paramétrage complet de la solution se fait via le fichier "config.json"
- ❖ Le "Accelerator State Machine" génère dynamique des scripts **AWS CloudFormation** via l'utilisation du **CDK**
 - **AWS CloudFormation** est utilisé pour faire les installations et configurations
 - Le code du "Accelerator State Machine" s'exécute sous forme de fonction **Lambda** en utilisant **AWS Step Functions** pour en faire l'orchestration



Fonctionnement du “Accelerator State Machine”

- ❖ On utilise plusieurs phase de déploiement due à une restriction de **AWS CloudFormation** qui nous empêche de faire des références entre les comptes et Regions et d'utiliser des noms similaires pour le nom des Stacks à travers différentes Regions.
- ❖ Échange d'information entre les Phases d'installation est fait via **AWS SecretManager** et **S3** durant l'installation
- ❖ Toutes les ressources partagés utilisent des **Tags** pour permettre de les identifier

Fonctionnement du “Accelerator State Machine”

- ❖ La machine d'état peut être arrêtée et redémarrée à tout moment. L'accélérateur a été conçu pour être en mesure de revenir à un état stable, de sorte que la machine d'état peut être arrêtée ou échouer pour une raison quelconque
- ❖ L'accélérateur est idempotent - il peut être exécuté autant ou aussi peu de fois que vous le souhaitez sans effet négatif.
- ❖ La machine d'état, utilisant principalement les capacités du CDK, évaluera les delta entre l'ancienne configuration précédemment déployée et la nouvelle configuration et mettra à jour l'environnement le cas échéant.



Fonctionnement du “Accelerator State Machine”

La machine d'état s'exécutera :

- automatiquement après chaque exécution du pipeline de code (nouvelles installations, mises à niveau de code ou exécutions manuelles de pipeline)
- automatiquement lorsque de nouveaux comptes AWS sont déplacés vers une unité d'organisation de contrôleur Accelerator dans les organisations AWS
- quand quelqu'un le démarre manuellement : **Step Functions**, PBMMaccel-MainStateMachine_SM, Start Execution, Start Execution (laisser les valeurs par défaut dans le nom et la zone json)



Fonctionnement du “Accelerator State Machine”

- ❖ La machine d'état empêche les utilisateurs d'effectuer accidentellement certaines modifications majeures, en particulier des modifications de plate-forme AWS non prises en charge, des modifications qui ne seront pas déployées ou des modifications qui pourraient être catastrophiques pour les utilisateurs.
- ❖ Si quelqu'un sait exactement ce qu'il fait et quelles sont les conséquences de ces changements, nous offrons la possibilité de passer outre à ces vérifications.
- ❖ Les clients doivent s'attendre à ce que les articles que nous avons bloqués ne puissent être modifiés après l'installation de l'accélérateur.



Demo & Revue du fichier “config.json”

Full PBMM configuration [file](#) (config.example.json)

❖ Le fichier de configuration PBMM complet basé sur les commentaires des clients qui migraient vers AWS à grande échelle et à un rythme rapide. Des clients de cette nature ont indiqué qu'ils ne souhaitaient pas avoir à augmenter leurs pare-feu de périmètre ou à ajouter des points de terminaison d'interface lorsque leurs développeurs commencent à utiliser de nouveaux services AWS. Ce sont les deux composants les plus dispendieuses de la solution d'architecture déployée.

Light weight PBMM configuration [file](#) (config-lite-example.json)

(Recommended for most new PBMM customers)

❖ Pour réduire les coûts de la solution et permettre aux clients de devenir des capacités AWS plus avancées, nous avons créé cette configuration plus légère qui ne sacrifie pas les fonctionnalités, mais pourrait limiter les performances. Ce fichier de configuration:

- déploie uniquement les 6 points de terminaison d'interface centralisés requis (en supprime 56). Tous les services restent accessibles à l'aide des points de terminaison publics AWS, mais nécessitent de traverser les pare-feu de périmètre
- supprime les points de terminaison de l'interface VPC de périmètre
- réduit la taille des instances Fortigate de c5n.2xl à c5n.xl (VM08 à VM04)
- supprime le Unclass OU et le VPC

❖ L'accélérateur permet aux clients d'ajouter ou de modifier facilement cette fonctionnalité à l'avenir, au fur et à mesure des besoins, sans aucun impact

Ultra-Light sample configuration [file](#) (config.ultralite-example.json)

❖ Ce fichier de configuration a été créé pour représenter un déploiement d'accélérateur extrêmement minimaliste, simplement pour démontrer l'art du possible pour une configuration extrêmement simple. Cette configuration a:

- pas de comptes de réseau partagé ou de périmètre
- pas d'objets de mise en réseau (VPC, TGW, ELB, SG, NACL, points de terminaison) ou route53 (zones, résolveurs)
- pas de AD géré, de connecteur AD, de cluster rsyslog, d'hôte RDGW ou de pare-feu tiers
- active / déploie les services de sécurité AWS uniquement dans 2 régions (ca-central-1, us-east-1) (non recommandé)
- déploie uniquement 2 règles de configuration AWS avec correction SSM
- renommée des noms de compte d'archivage de journaux (journaux), de sécurité (audit) et d'opérations (Ops)

Multi-Region sample configuration [file](#) (config.multi-region-example.json)

❖ Ce fichier de configuration a été créé pour représenter une version multirégionale plus avancée du fichier de configuration Full PBMM. Cette configuration:

- ajoute un TGW dans us-east-1, appairé au TGW dans ca-central-1
- ajoute des routes statiques TGW, y compris plusieurs exemples de routes statiques factices
- ajoute un VPC Endpoint central dans us-east-1 avec des points de terminaison us-east-1 configurés
- ajoute un VPC partagé pour tous les comptes UnClass OU dans us-east-1, connecté au TGW us-east-1 (accessible via ca-central-1)
 - crée des zones et des règles de résolveur supplémentaires
- Envoie us-east-1 CloudWatch Logs au compartiment central d'archivage de journaux S3 dans ca-central-1
- Déploie des documents SSM sur us-east-1 et corrige les règles configurées dans UnClass OU
- ajoute un VPC spécifique au compte local, dans us-east-1, dans le compte MyUnClass et le connecte au TGW us-east-1 (c'est-à-dire partage le TGW)
 - VPC de compte local configuré pour utiliser des points de terminaison centraux, associe les zones hébergées centralisées appropriées au VPC (crée également 5 points de terminaison locaux)
- ajoute un VGW pour DirectConnect au VPC de périmètre
- ajoute la 3e AZ dans ca-central-1 (MAD & ADC dans AZ a et b)

Où trouver AWS SEA dans GitHub?

❖ Site GitHub principal:

- <https://github.com/aws-samples/aws-secure-environment-accelerator>

❖ Gabarit du fichier de configuration:

- https://github.com/aws-samples/aws-secure-environment-accelerator/tree/master/reference-artifacts/SAMPLE_CONFIGS

❖ Description des divers fichiers de configuration:

- <https://github.com/aws-samples/aws-secure-environment-accelerator/blob/master/docs/installation/customization-index.md>



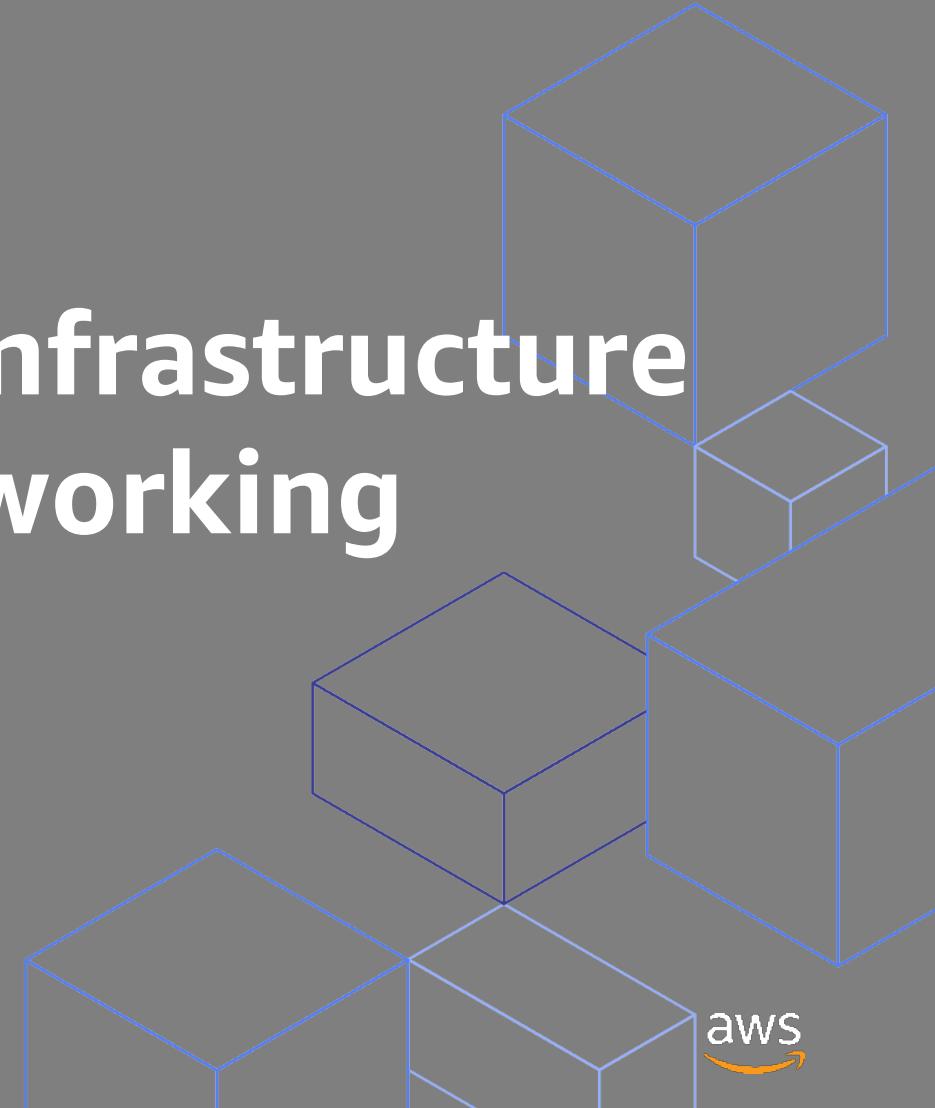
Questions?

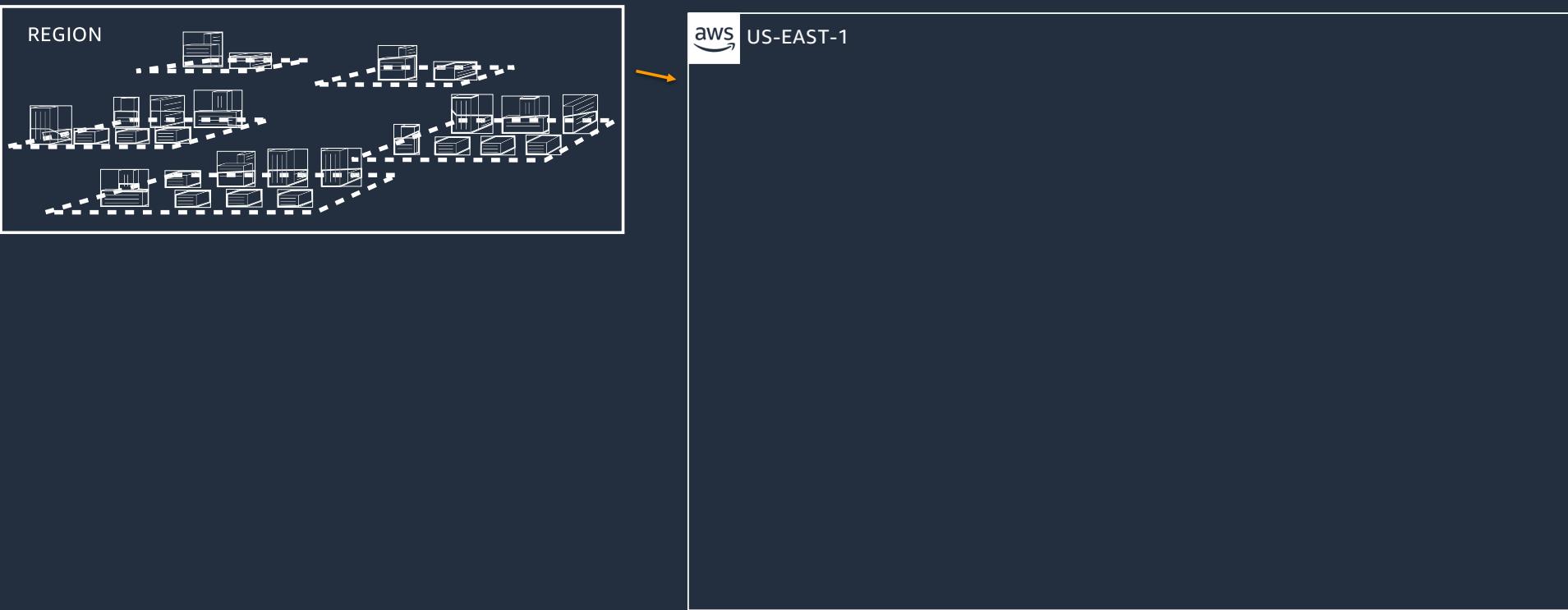
Louis Caron
loucaron@amazon.com



Annexes

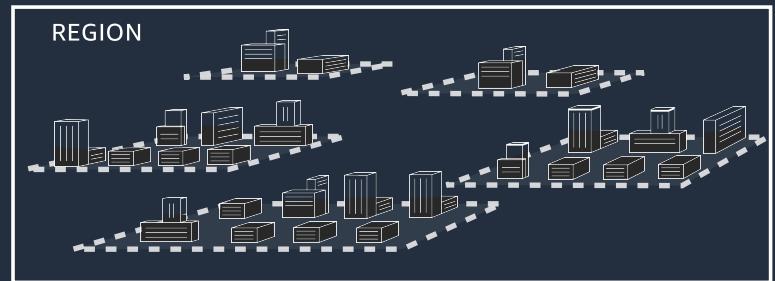
Mapping Physical Infrastructure to logical AWS networking constructs



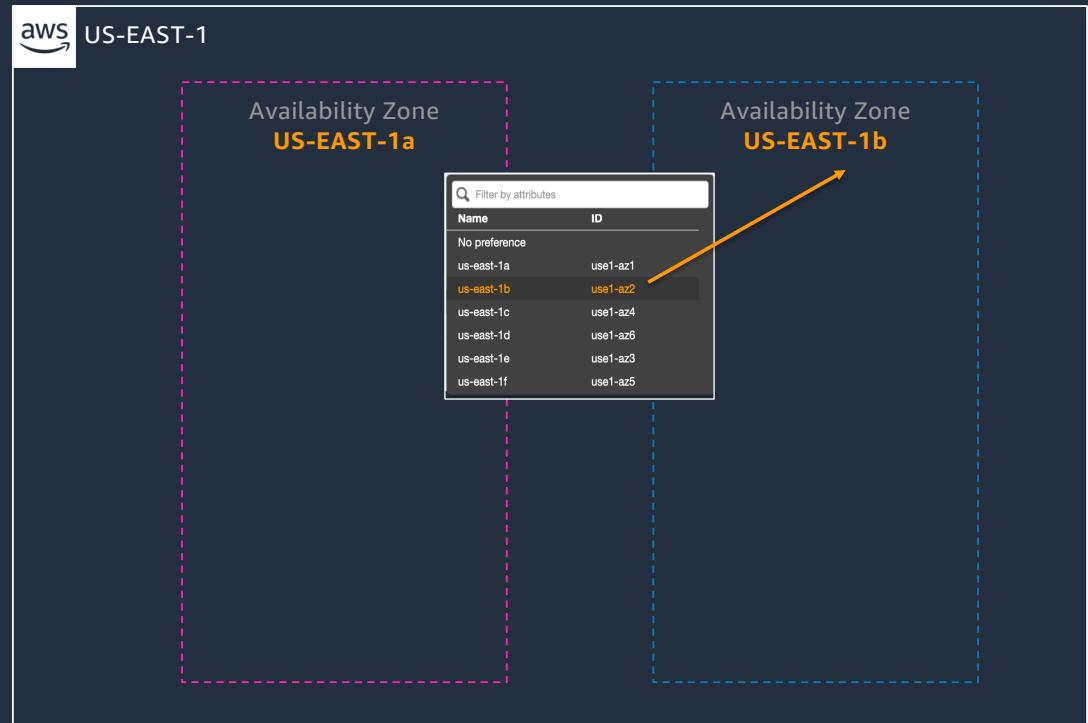


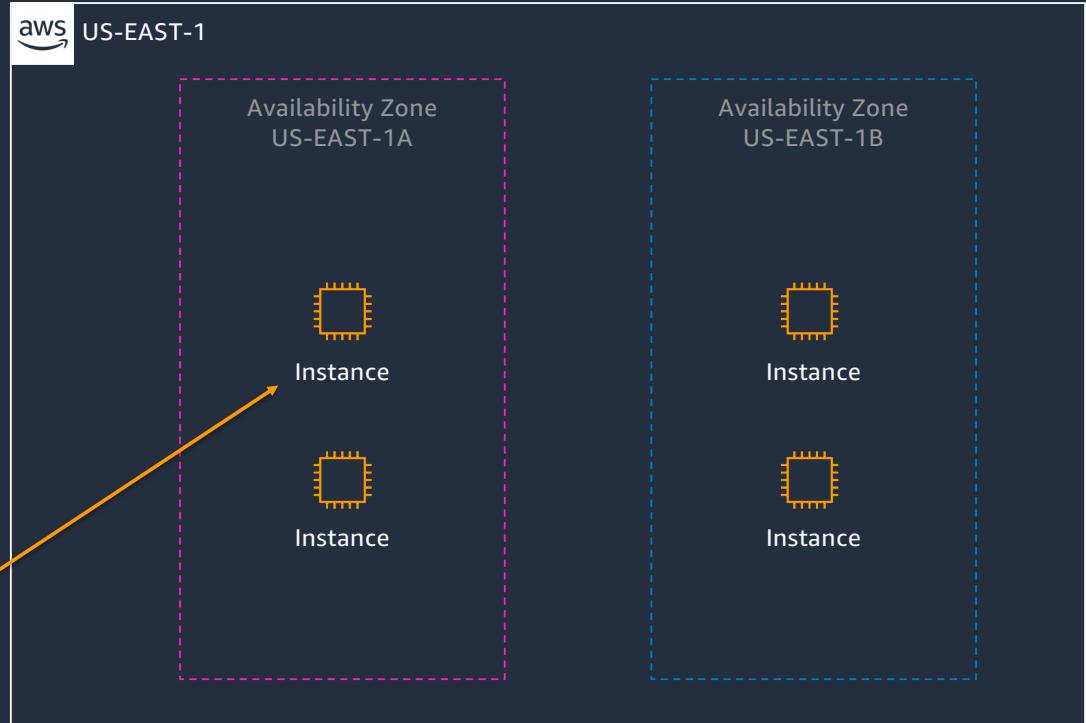
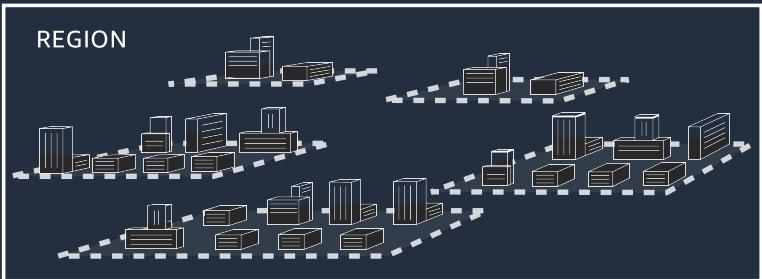
© 2021, Amazon Web Services, Inc. or its Affiliates.





AVAILABILITY ZONE



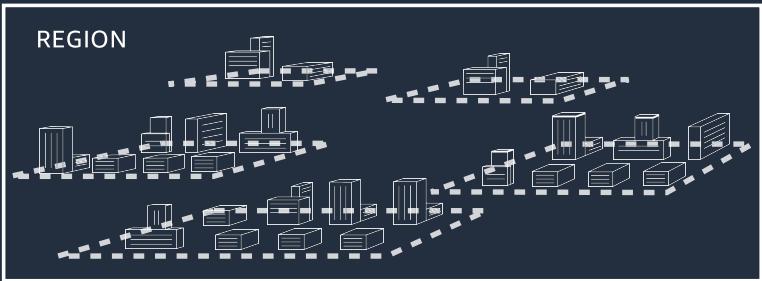


DATA CENTER, RACK, HOST



© 2021, Amazon Web Services, Inc. or its Affiliates.

aws
amazon



DATA CENTER, RACK, HOST



Amazon Virtual Private Cloud

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Amazon VPC - Virtual Private Cloud

Provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define

Bring your own network



IP Addresses



Subnets



Network Topology

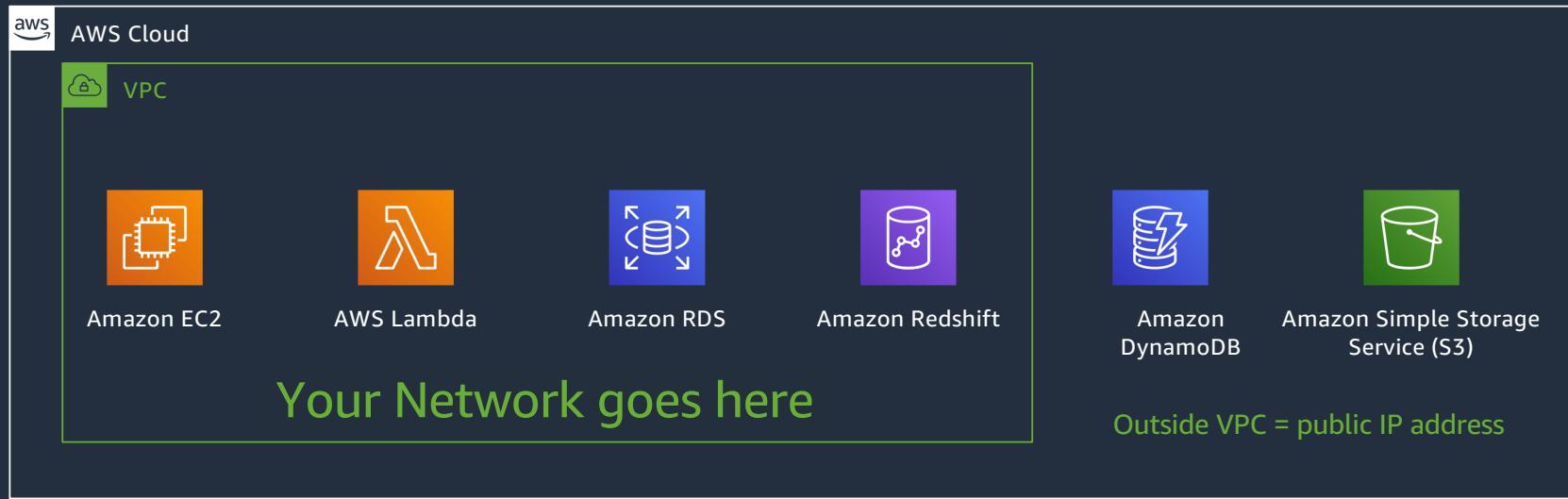


Routing Rules



Security Rules

Amazon Virtual Private Cloud (VPC)

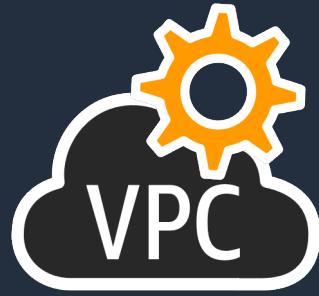


Setting up an Internet connected VPC

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Steps for Creating an Internet-connected VPC



Choosing an address range



Creating subnets in Availability Zones



Creating a route to the Internet



Authorizing traffic to/from the VPC

Choosing an IP address range

CIDR notation review

CIDR range example:

172.31.0.0/16

1010 1100 0001 1111 0000 0000 0000 0000



Choosing an IP address range for your VPC



VPC



Avoid ranges that overlap with other networks to which you might connect

172.31.0.0/16

Recommended:
RFC1918 range

Private IP address range for your VPC – IPv4

- "CIDR" Range ?
 - Classless Inter-domain Routing
 - No more Class A, B, C
- RFC1918
 - 192.168.0.0 /16
 - 172.16.0.0 /12
 - 10.0.0.0 /8
- How Big ?

© 2021, Amazon Web Services, Inc. or its Affiliates.

Updated by: [6761](#) BEST CURRENT PRACTICE
Network Working Group Errata Exist
Request for Comments: [1918](#) Y. Rekhter
Obsoletes: [1627](#), [1597](#) Cisco Systems
BCP: 5 B. Moskowitz
Category: Best Current Practice Chrysler Corp.
D. Karrenberg RIPE NCC
G. J. de Groot RIPE NCC
E. Lear Silicon Graphics, Inc.
February 1996

Address Allocation for Private Internets

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

1. Introduction

For the purposes of this document, an enterprise is an entity autonomously operating a network using TCP/IP and in particular determining the addressing plan and address assignments within that network.

This document describes address allocation for private internets. The allocation permits full network layer connectivity among all hosts inside an enterprise as well as among all public hosts of different enterprises. The cost of using private internet address space is the potentially costly effort to renumber hosts and networks between public and private.

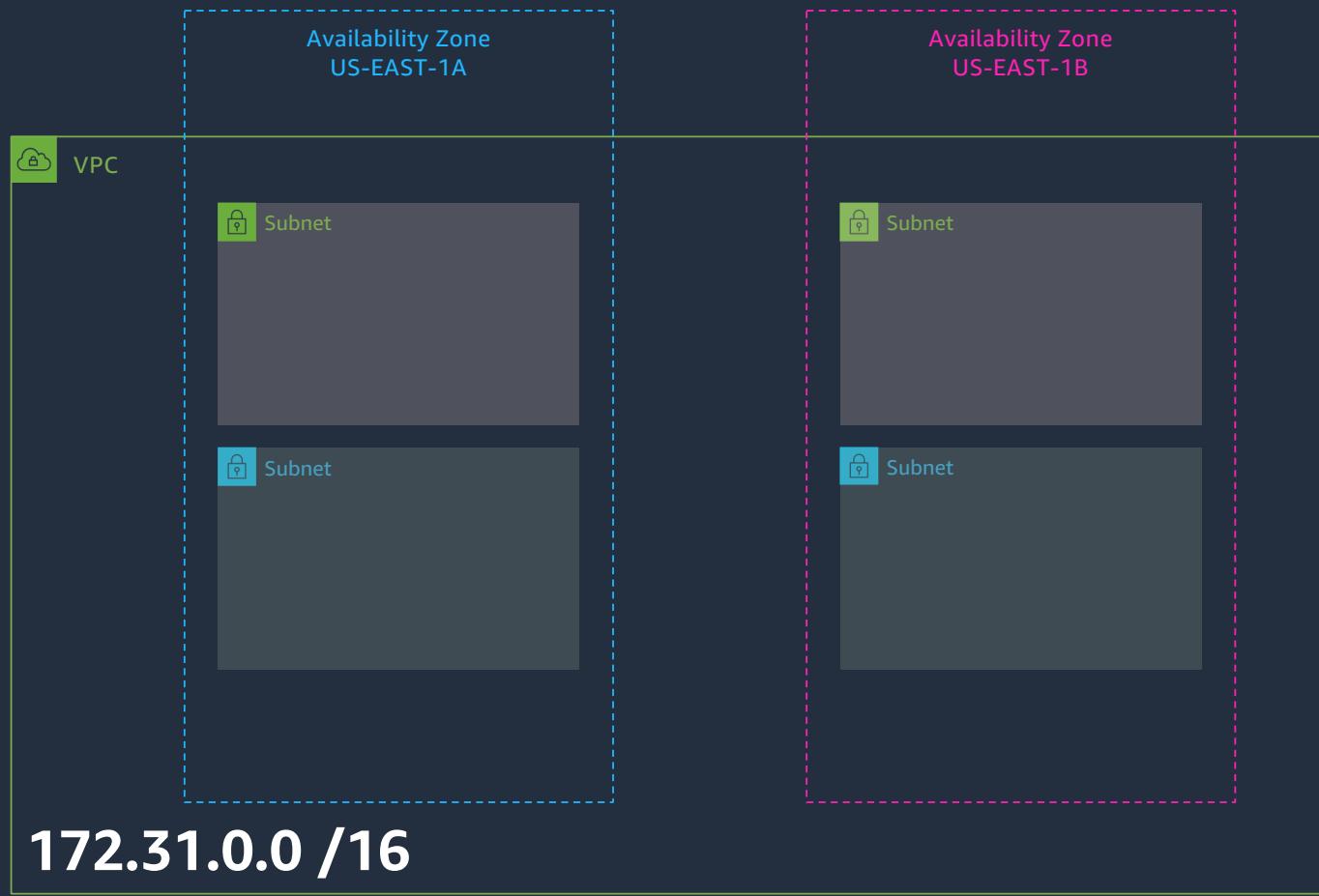
VPC IPv4 address space design considerations

- Bring your own addressing plan
- Plan for future expansion to additional Regions & Availability Zones
- Consider connectivity to corporate networks
- Avoid overlapping IP space
- Consider subnet design
 - VPC CIDR cannot be modified once created
 - New CIDRs can be added for expansion
 - Choose VPC CIDR ranges :

/16 = largest address space for VPC

/28 = smallest address space for VPC

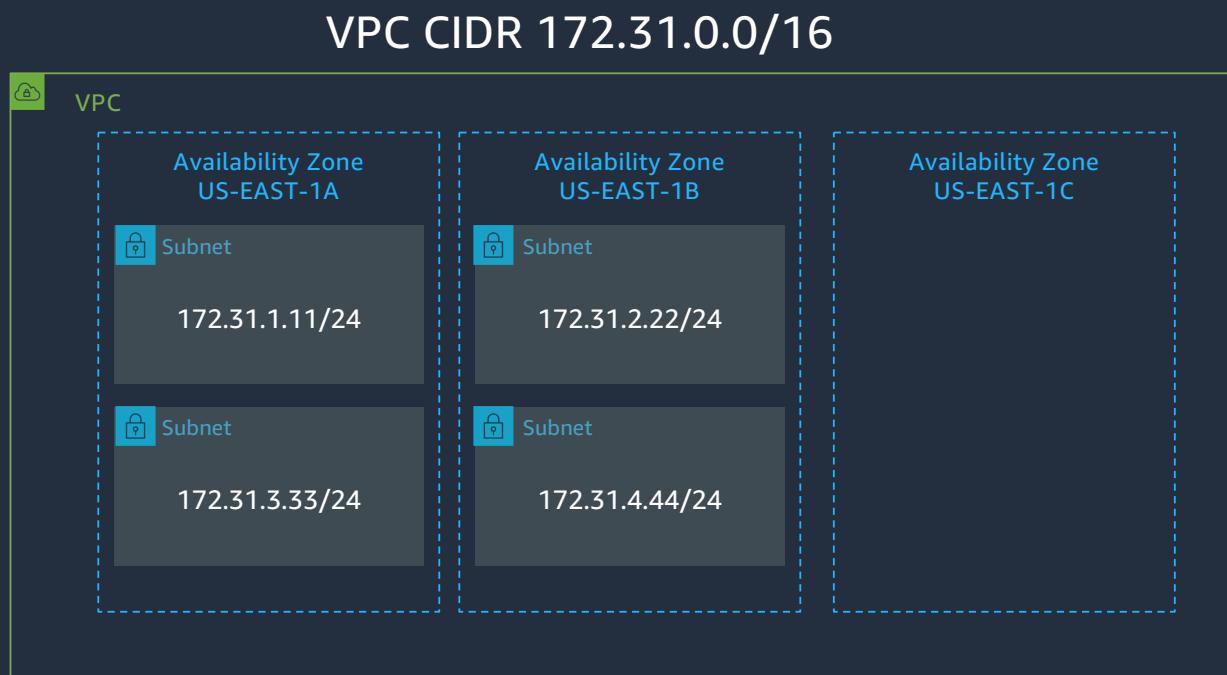
VPC CIDR /16



© 2021, Amazon Web Services, Inc. or its Affiliates.

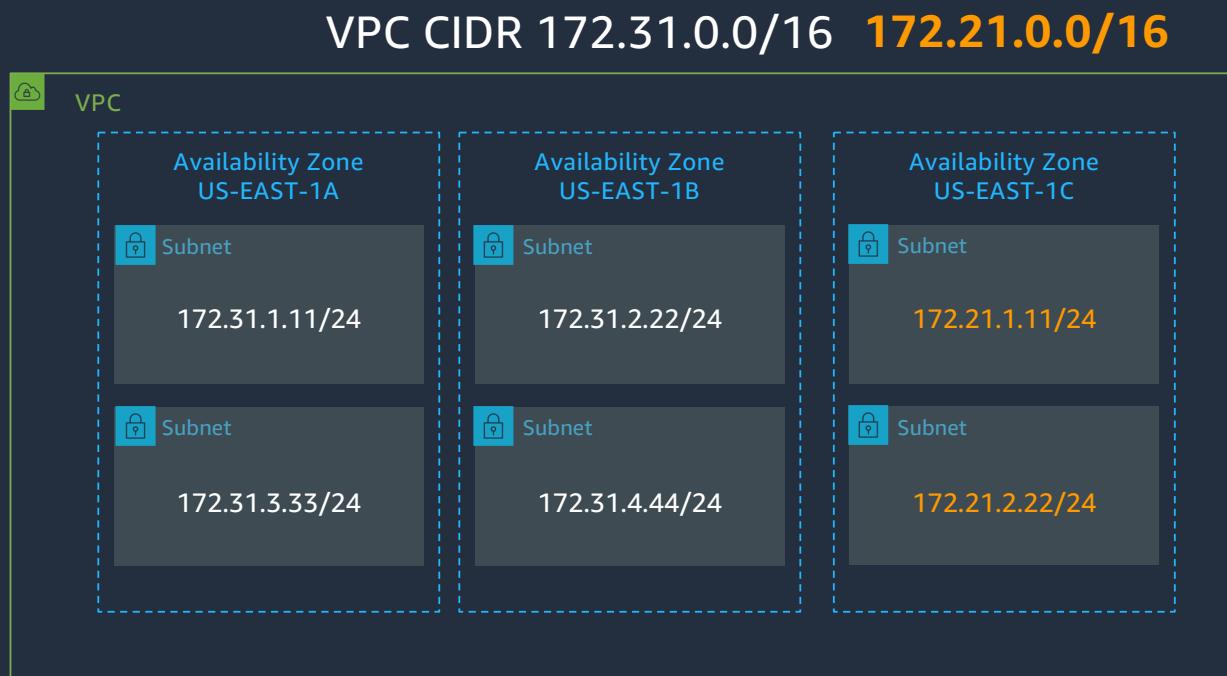


Expand your existing Amazon VPC



Initial VPC CIDR:
172.31.0.0/16

Add Secondary CIDR Range to VPC



Initial VPC CIDR:
172.31.0.0/16

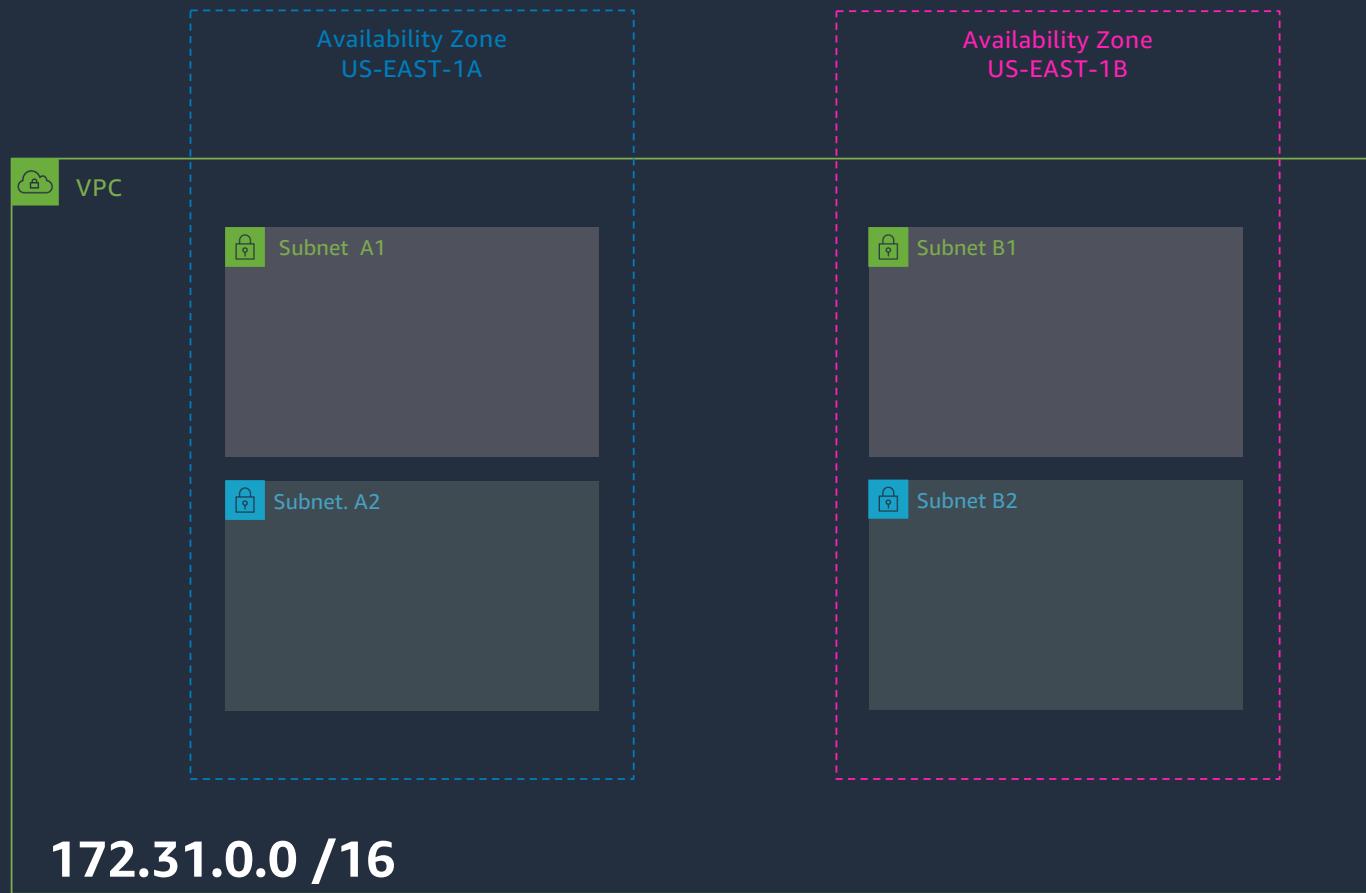
Additional VPC CIDR:
172.21.0.0/16

Create Subnets in Availability Zones

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



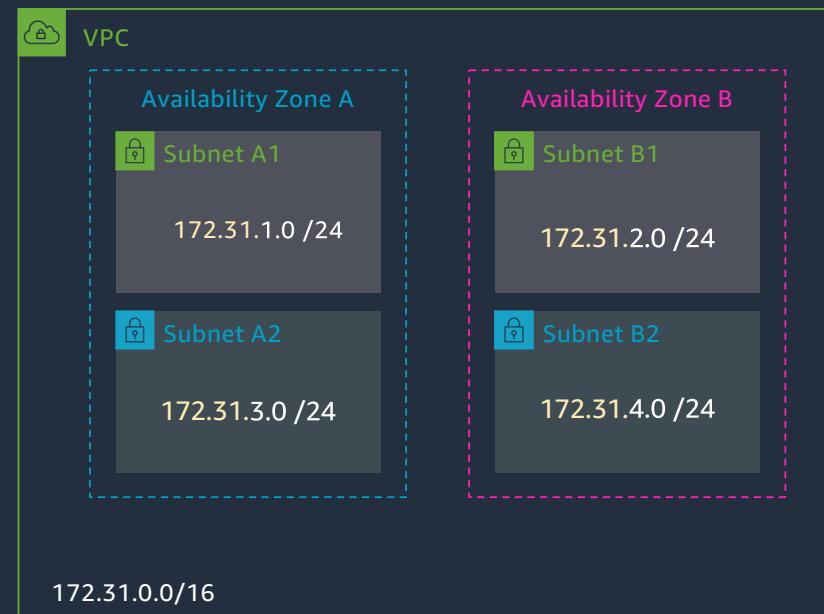
Subnets



How to segment my networks inside a VPC?

VPC Subnets

- You can add one or more subnets in each Availability Zone
- AZs provides fault isolations
- Subnets are allocated as a subset of the VPC CIDR range
- Even distribution of IP space across AZs
- Use at least 2 AZs
- How big? How many?



Subnets are AZ specific

VPC and Subnet recommendations



/16 VPC or smaller from private IPv4 address ranges

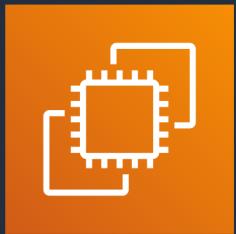
At least /24 subnets (251 usable addresses)

Use multiple Availability Zones per VPC through multiple subnets



You can expand your VPC by adding additional IP address ranges

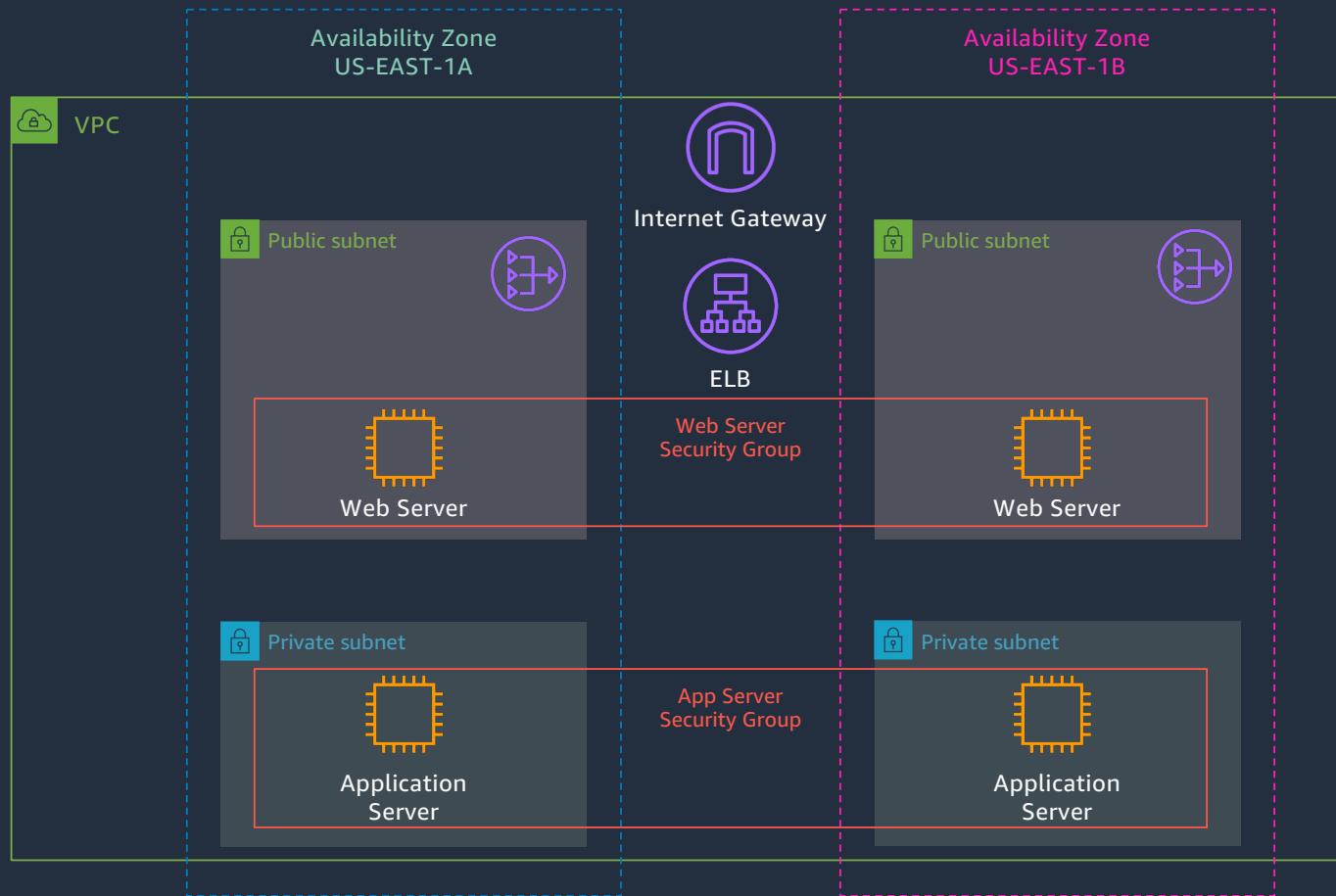
EC2 instances



Public and Private Subnets

- **Public Subnet**
 - A subnet whose traffic is routed to an Internet Gateway.
 - Allows the use of Elastic IPs and Public IPs addresses
 - Useful as DMZ infrastructure for web servers & internet ELBs
 - EC2 instances will get both Private IP and Public IP
- **Private Subnet**
 - Subnet that DOES NOT have route to Internet Gateway.
 - Can indirectly route to Internet via NAT instance or NAT gateway.
 - NAT devices reside in a public subnet
 - Useful for application servers and databases
 - EC2 instances will be assigned Private IP in subnet range

Example Web Application

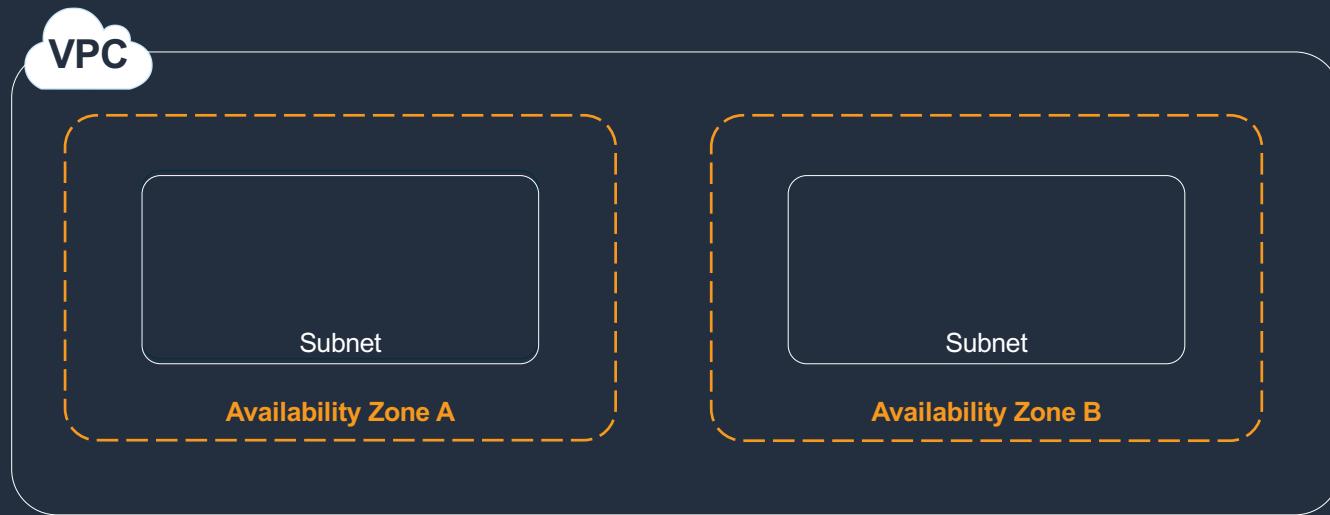


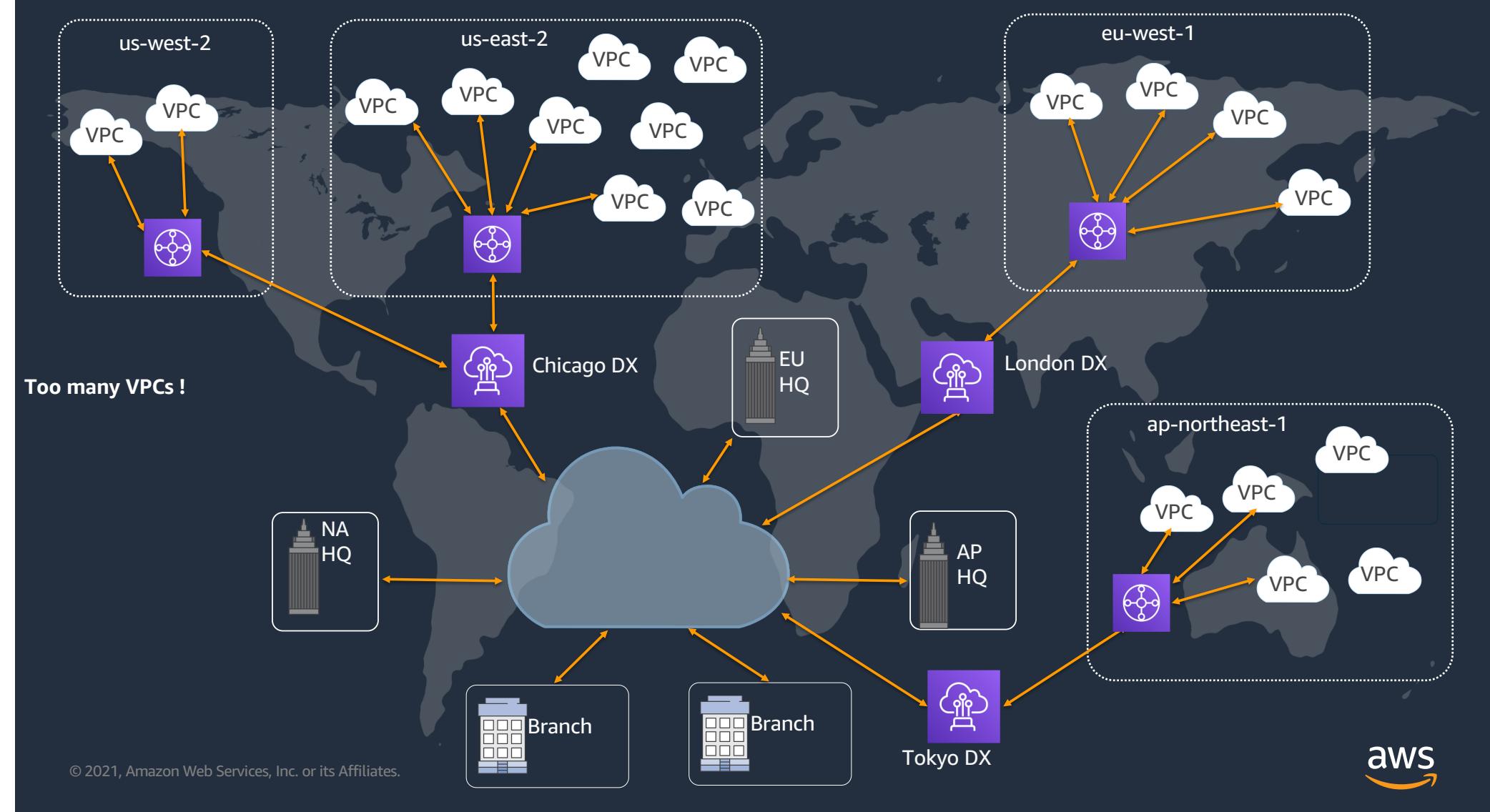
Multi-VPC Network Infrastructure

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



From one VPC





Account and VPC segmentation

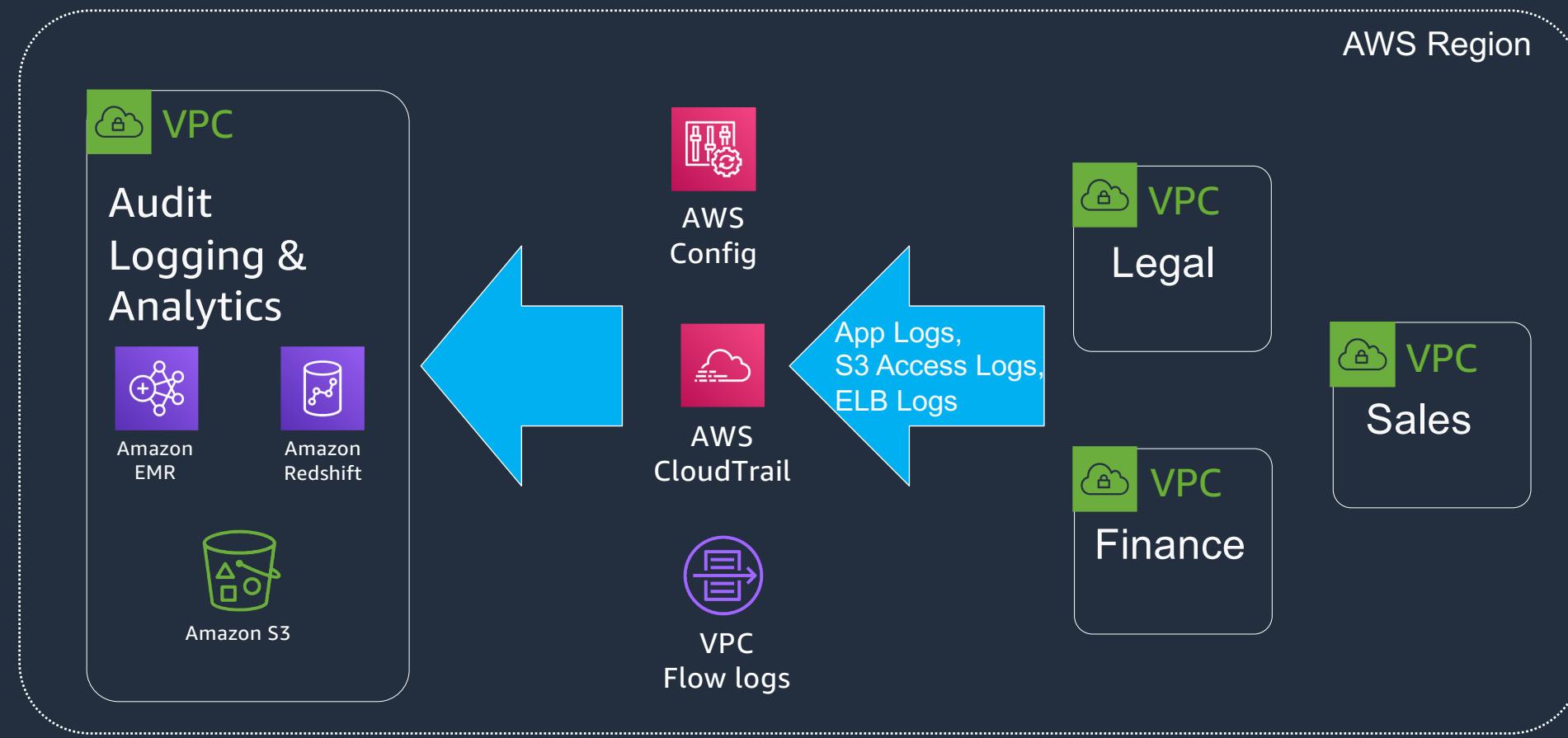
Larger VPCs or accounts

- Less accounts and networks to setup
- Tighter control within the account or VPC
 - Identity and Access Management (IAM)
 - Strict security groups and routing
 - Identifying resources with tags
- Billing and ownership complexity
- Larger account or VPC blast radius
 - User privileges, AWS limits

Smaller VPCs or accounts

- More accounts and infrastructure to setup
- Tighter control of provisioning and standards
 - Automation of infrastructure
 - AWS Direct Connect and VPN standards
 - Subnet and routing standards
- Simpler billing
- Smaller blast radius for users and networks
 - Larger blast radius for shared infrastructure and services

Considerations for One or Many VPCs



AWS Transit Gateway

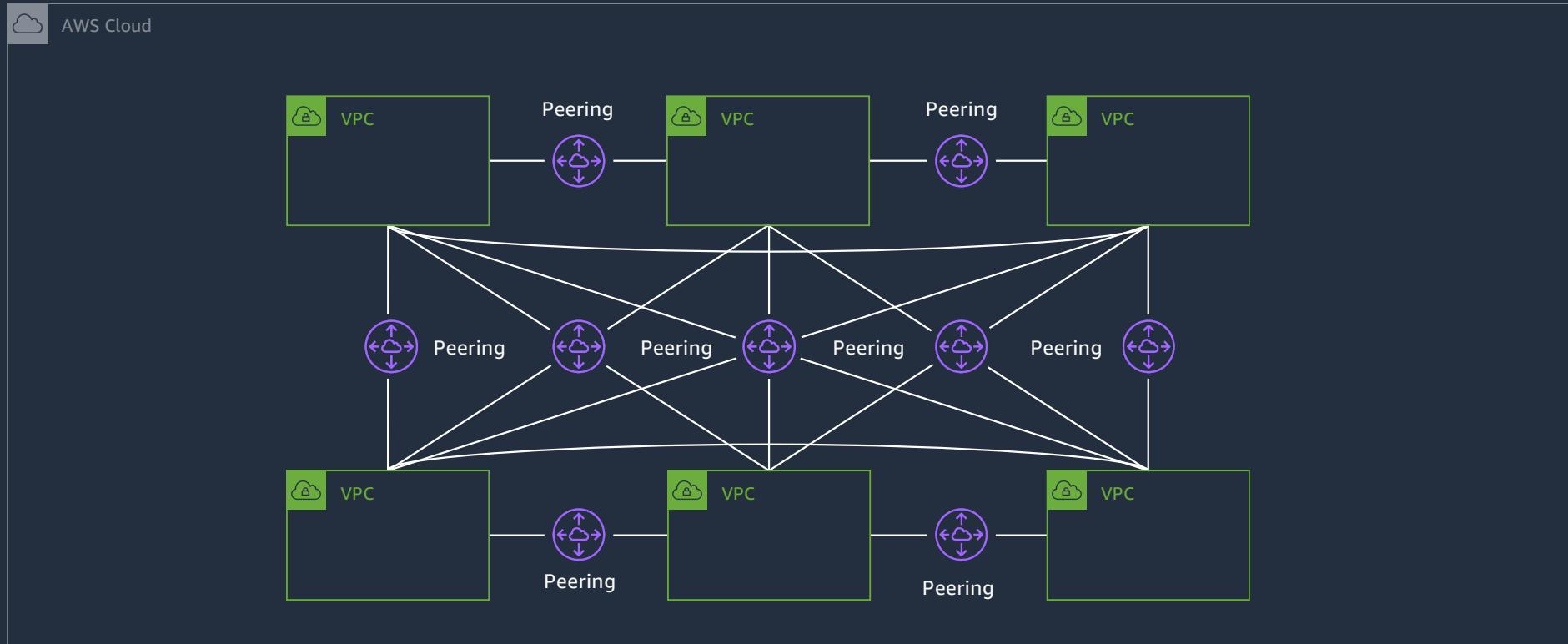
© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



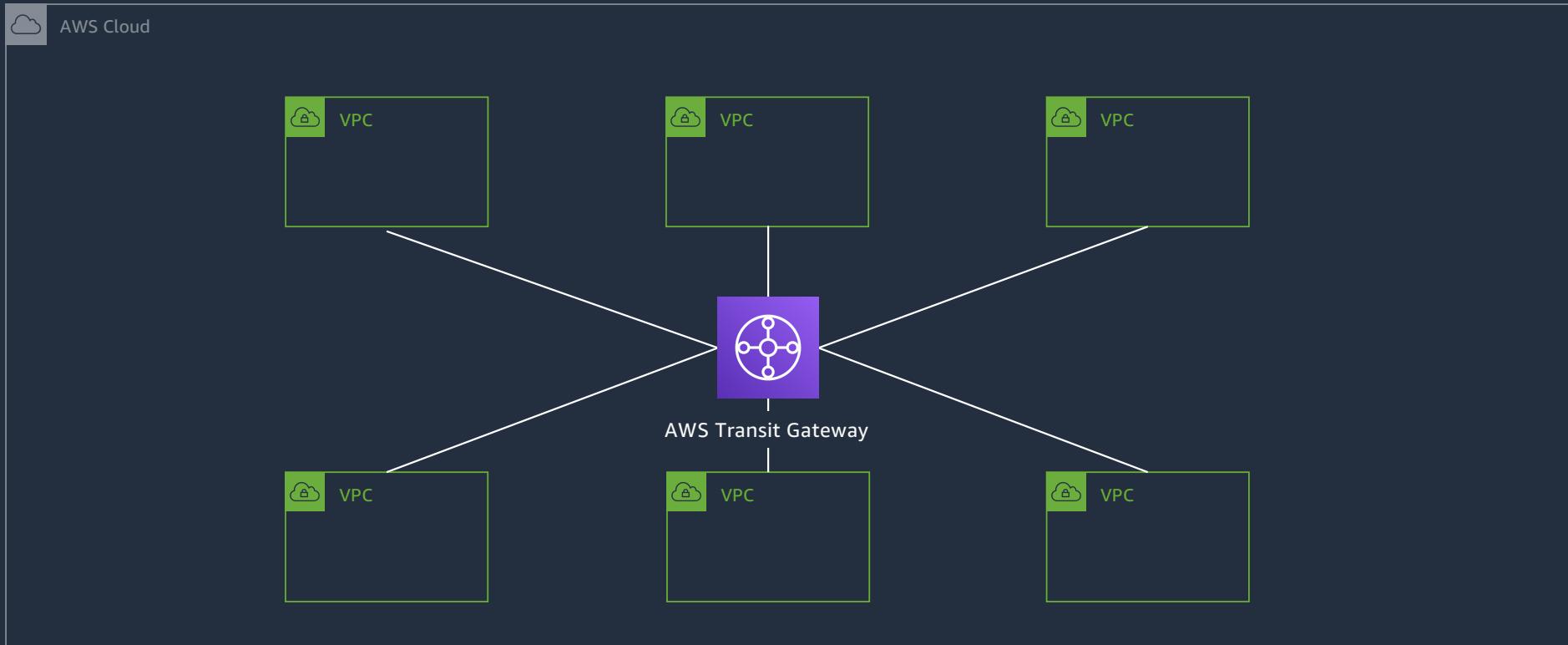
AWS Transit Gateway

- AWS Transit Gateway (TGW) acts as a Regional virtual router for traffic flowing between attachments.
- A TGW scales elastically based on the volume of network traffic
- Simplifies connectivity with many
 - Amazon VPCs
 - On-premises data centers
 - Remote offices

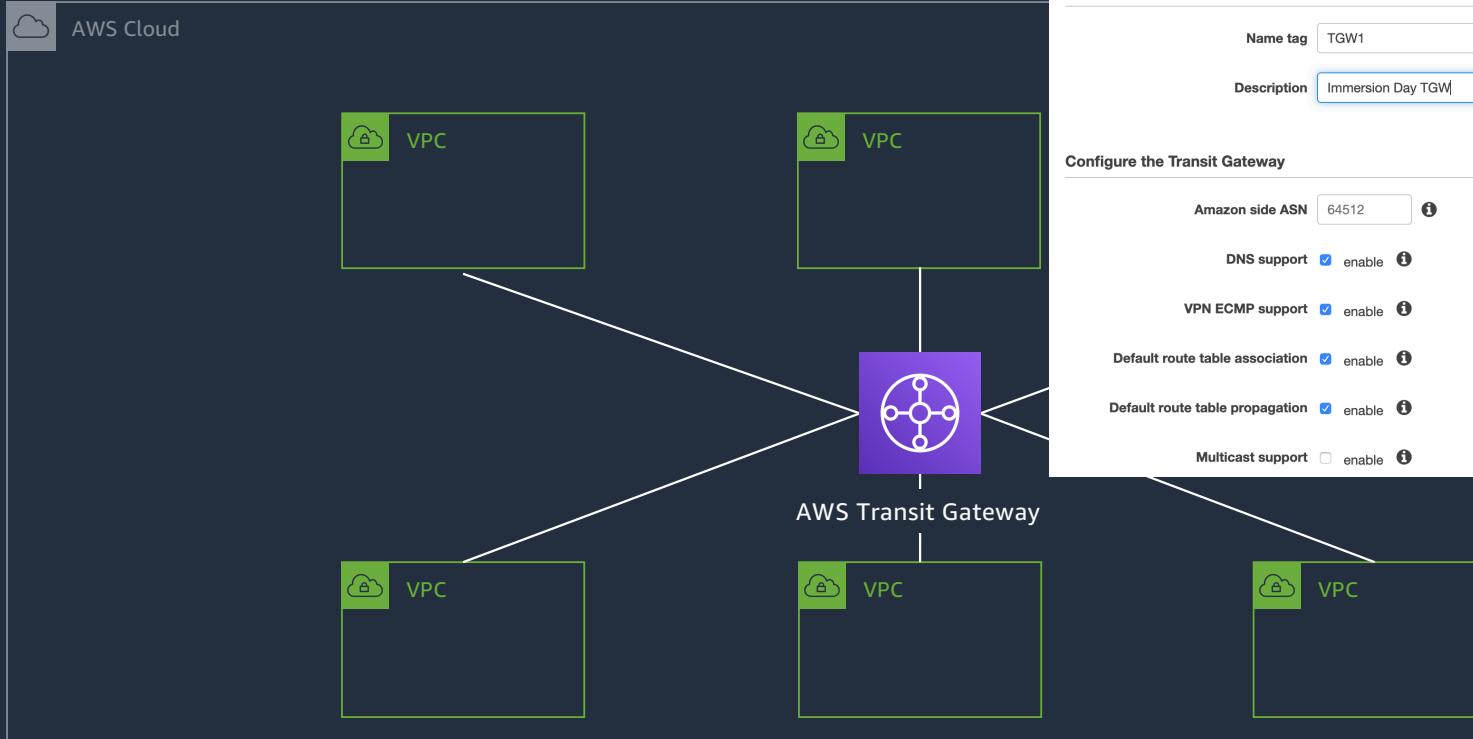
Interconnecting many VPCs



AWS Transit Gateway



Creating AWS Transit Gateway



Transit Gateways > Create Transit Gateway

Create Transit Gateway

A Transit Gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same account or across accounts.

Name tag: TGW1 i

Description: Immersion Day TGW i

Configure the Transit Gateway

Amazon side ASN: 64512 i

DNS support: enable i

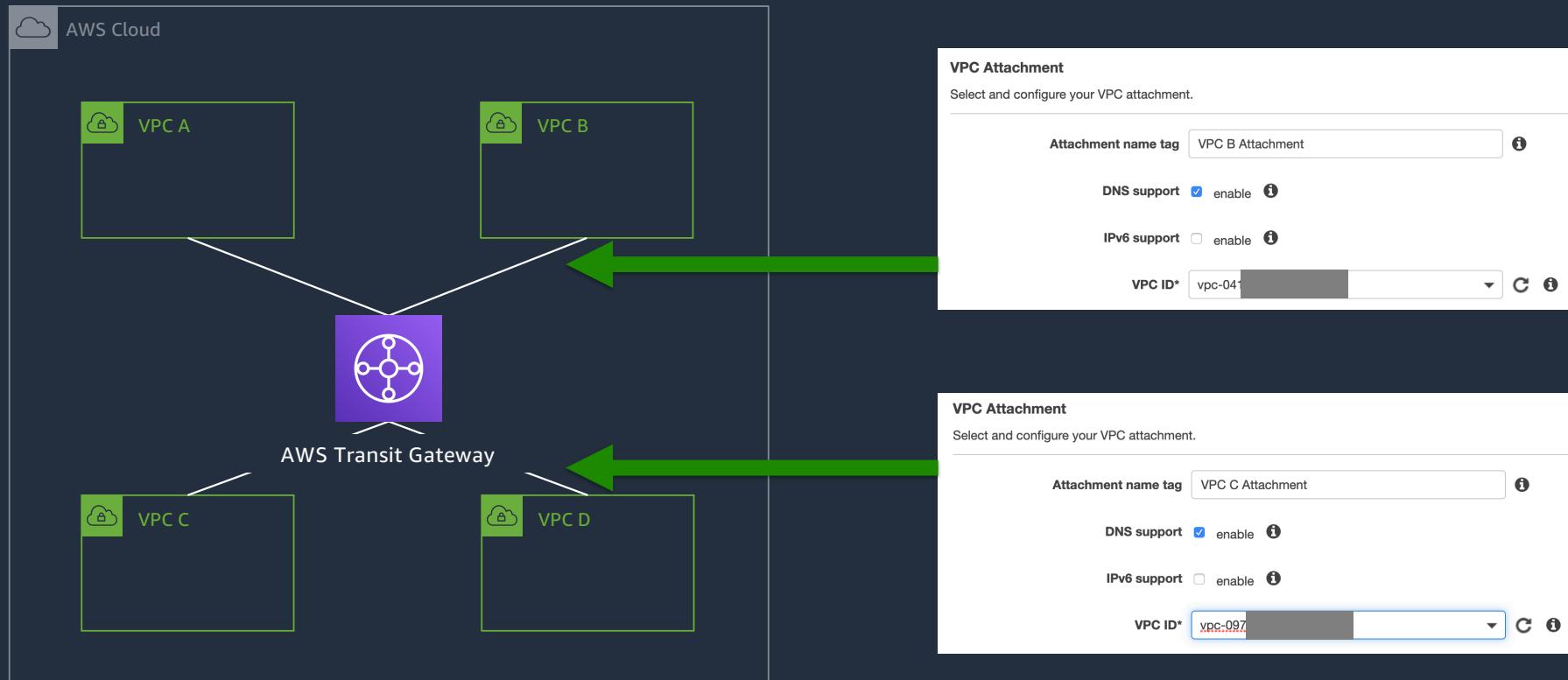
VPN ECMP support: enable i

Default route table association: enable i

Default route table propagation: enable i

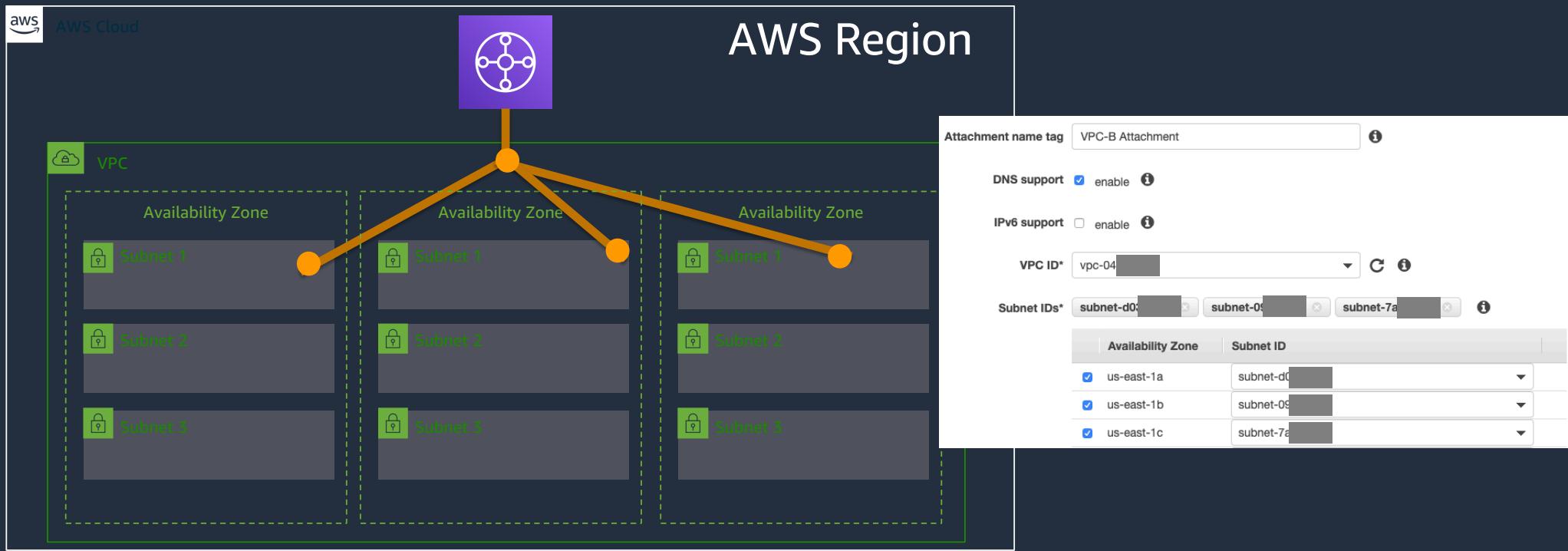
Multicast support: enable i

Configuring AWS Transit Gateway attachments



TGW attachment

Single attachment can span multiple Availability Zones



*The best practice is to have an attachment in every AZ
Dedicate subnets for the VPC attachment*

© 2021, Amazon Web Services, Inc. or its Affiliates.



AWS Transit Gateway attachments

You can attach the following resources to your transit gateway:

- One or more VPCs
- One or more VPN connections
- One or more AWS Direct Connect gateways
- One or more transit gateway peering connections

Note: If you attach a transit gateway peering connection, the transit gateway must be in a different Region.

AWS Transit Gateway associations

- Associating an attachment to a route table
- Allows traffic to be sent from the attachment to the target route table
- An attachment can only be associated to one route table.

Transit Gateway ID tgw-03a [REDACTED]

Transit Gateway route table ID tgw-rtb-02 [REDACTED] 1

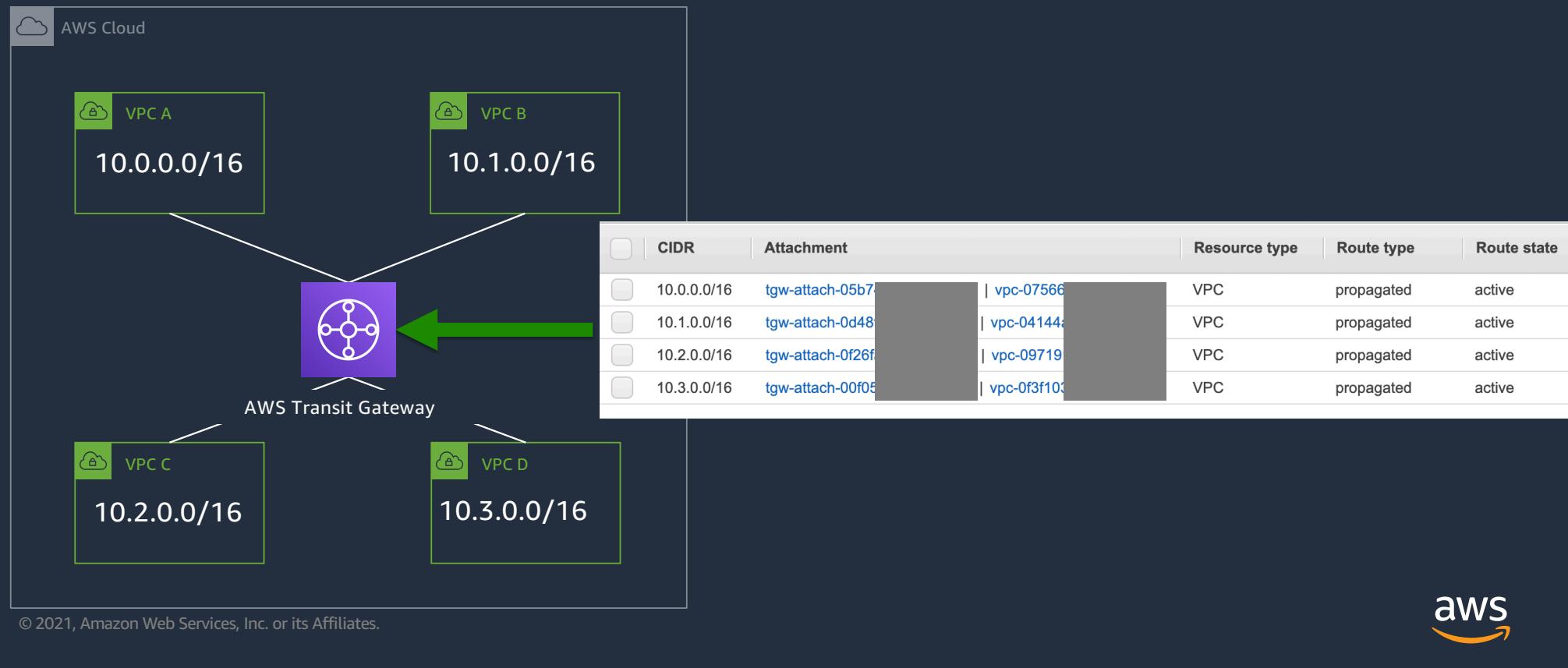
Choose attachment to associate* | C

* Required

Attachment ID	Name tag	Resource ID	Resource owner ID	Association route table
tgw-attach-01	vpc-0c	53	tgw-rtb-02	
tgw-attach-09	vpc-04	53	tgw-rtb-02	

AWS Transit Gateway route tables

Required to configure routing for your TGW attachments
Ingress packets are routed by matching the destination IP address



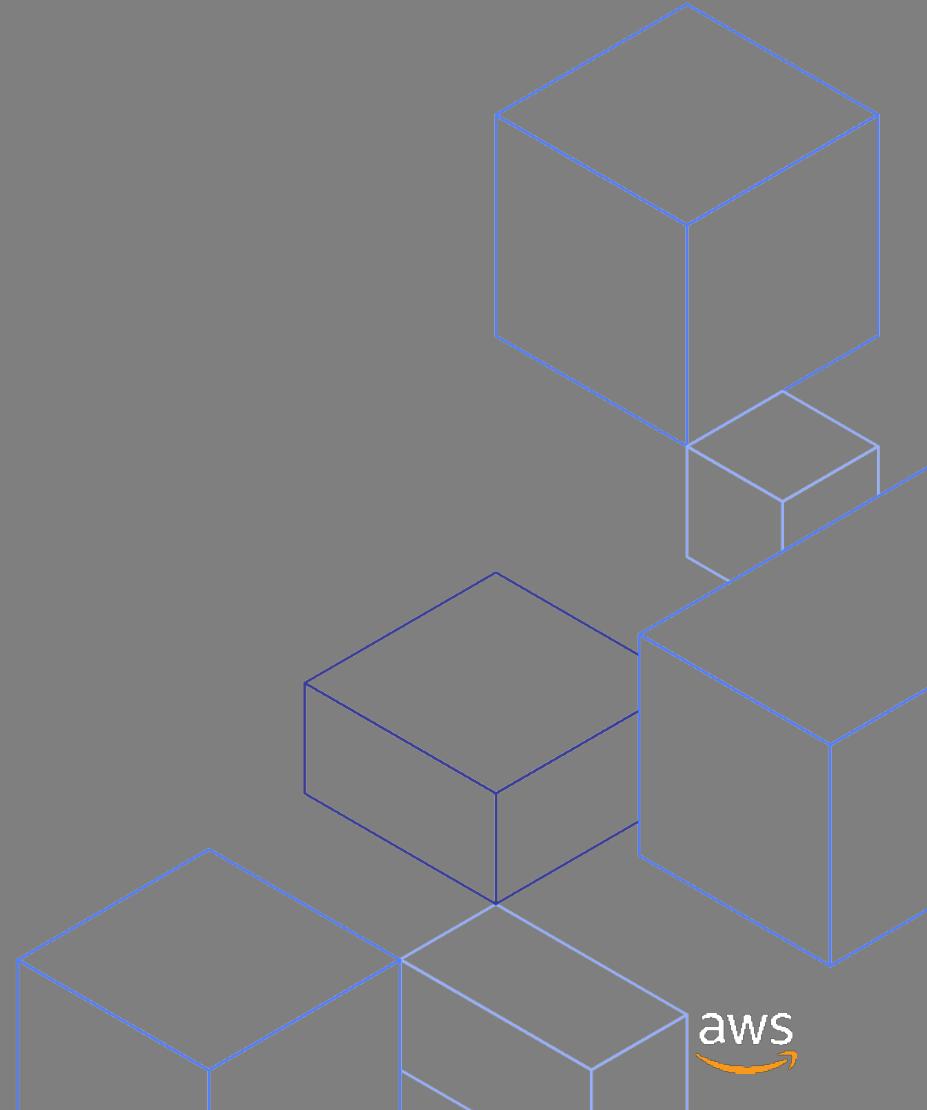
AWS Transit Gateway - Performance and limits

Limit	Default
Number of AWS Transit Gateway attachments	5,000
Maximum bandwidth per VPN tunnel (can bundle multiple VPN tunnels using ECMP)	1.25 Gbps
Maximum bandwidth (burst) per VPC, Direct Connect gateway, or peered Transit Gateway connection	50 Gbps
Number of AWS Transit Gateways per account	5
Number of AWS Transit Gateway attachments per VPC	5
Number of routes	10,000
Number of Direct Connect gateways per AWS Transit Gateway	20

Additional Information: <https://aws.amazon.com/transit-gateway/faqs/>

TGW Route Tables

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



TGW Route Tables

- TGW can have many Route Tables
- Similar to virtual routing and forwarding (VRFs)
- Can build complex network topologies, e.g. Hub & Spoke
- Route distribution between tables can be controlled via Propagations
- Can define static and blackhole routes

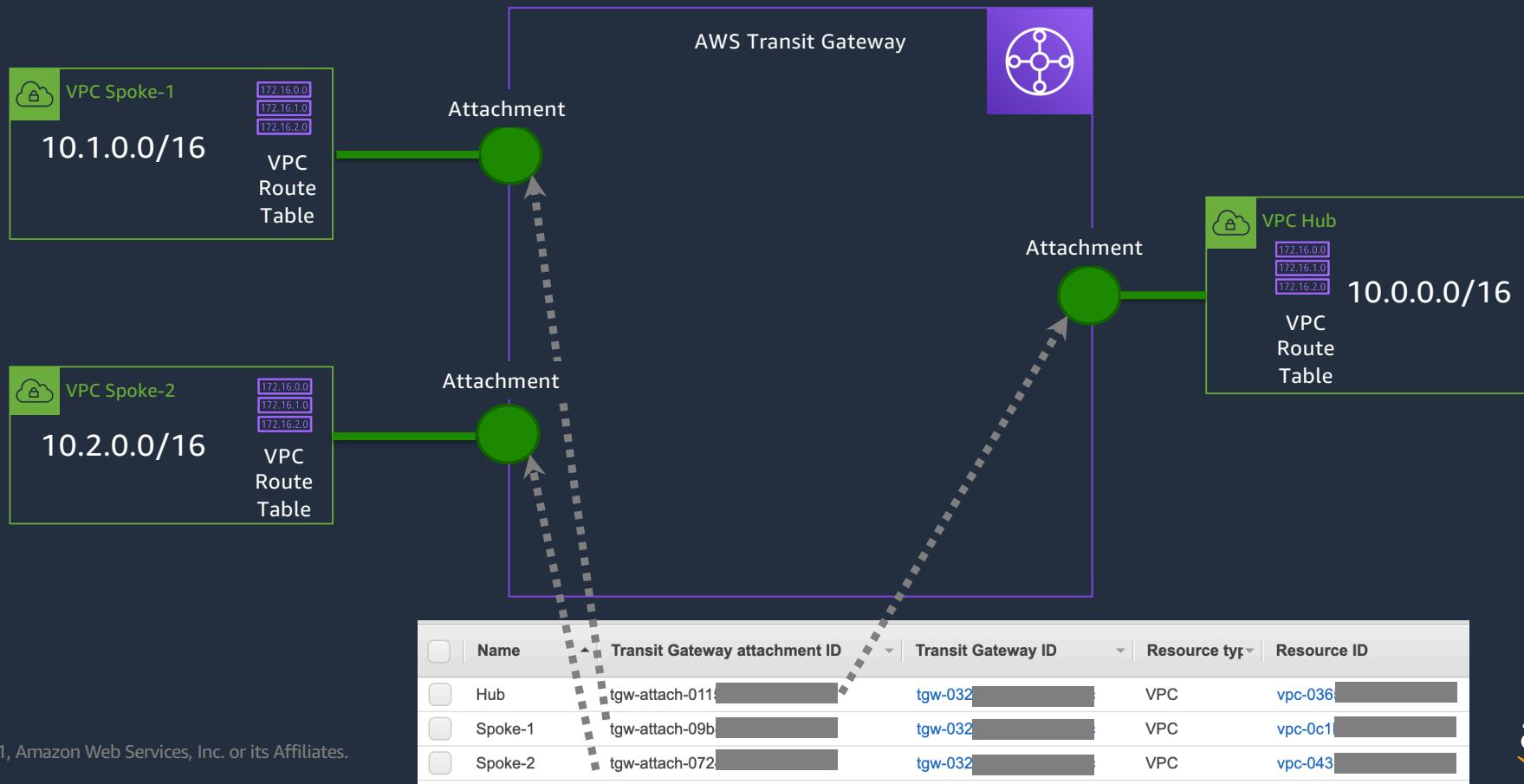
TGW Route Tables

Hub and Spoke Topology



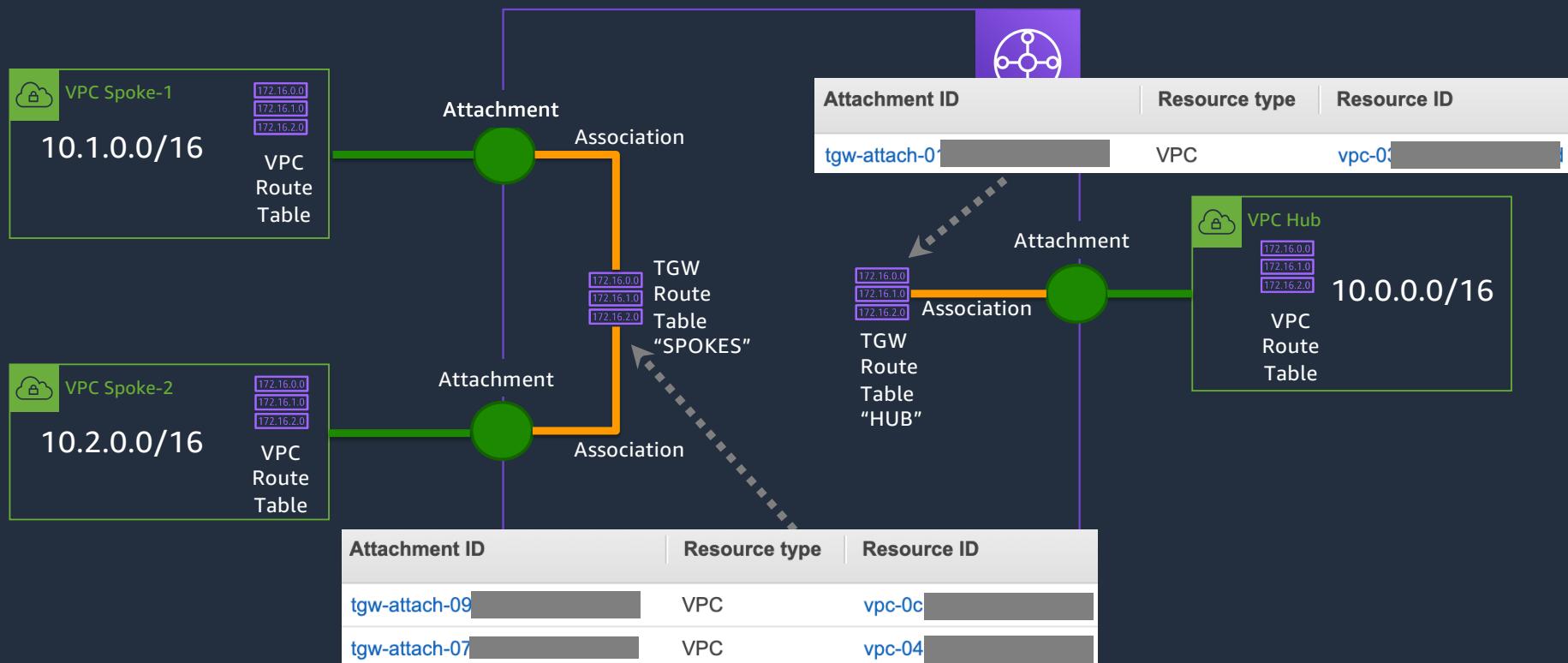
TGW Route Tables

Attaching VPCs to AWS Transit Gateway



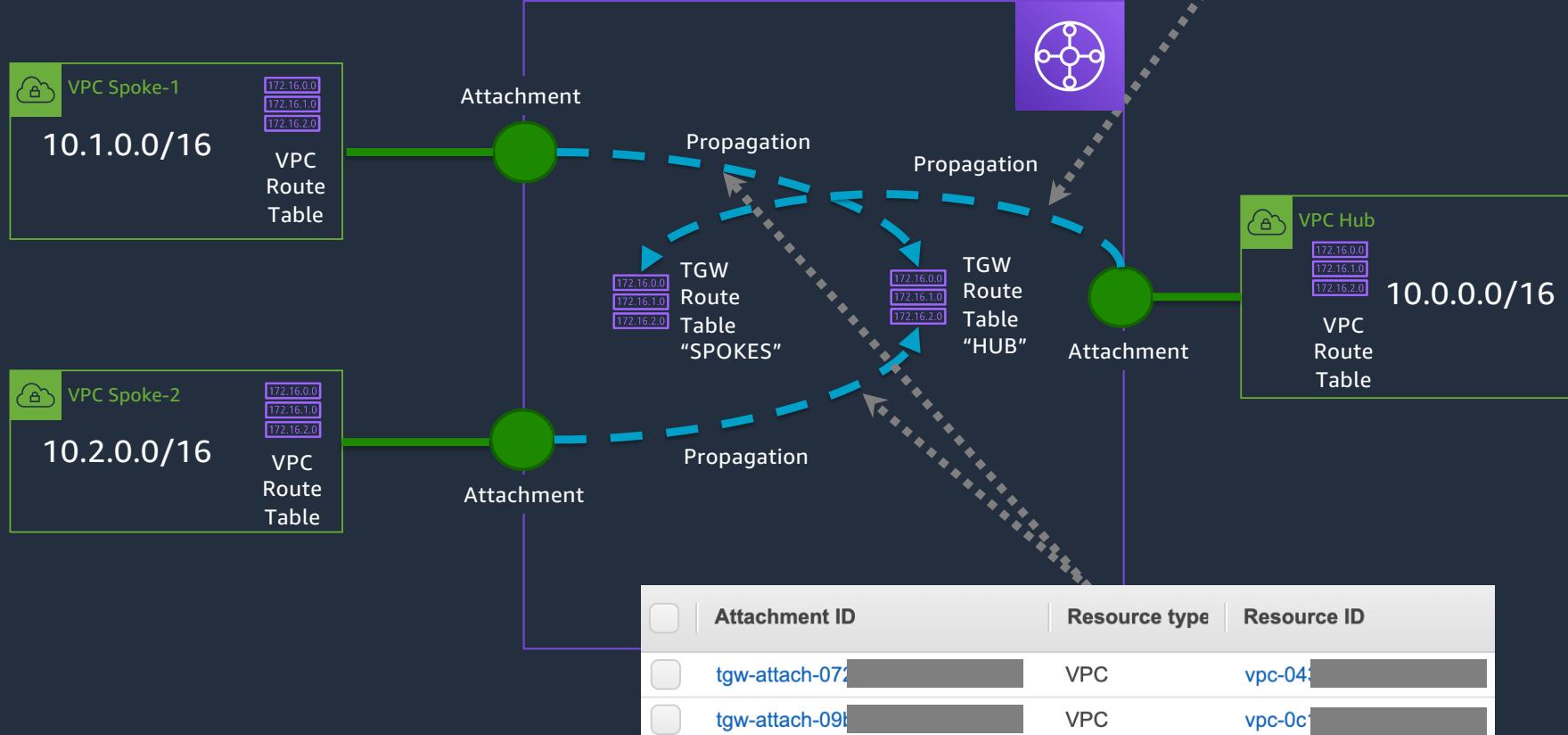
TGW Route Tables

Associating Attachments to Route Tables



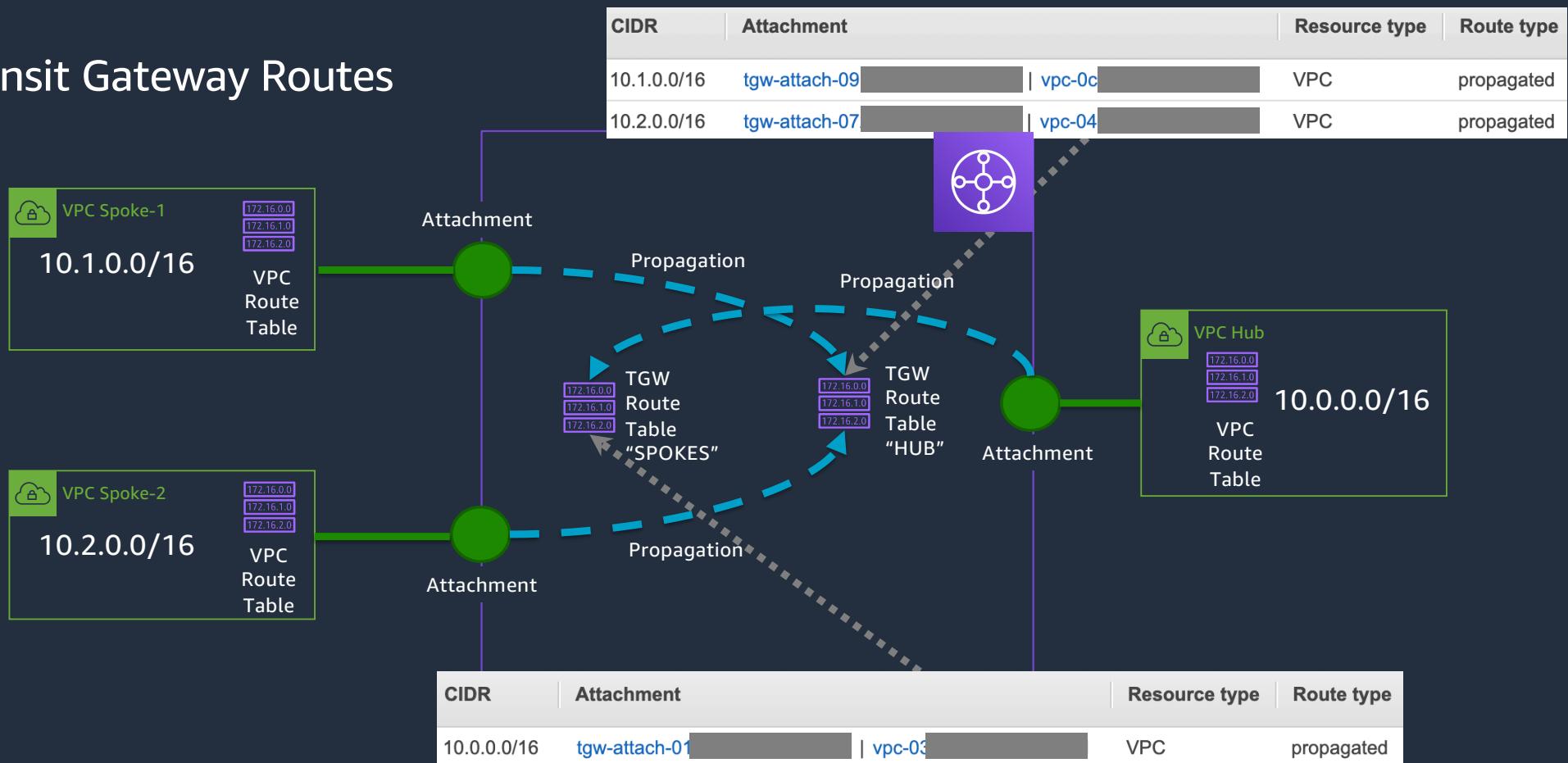
TGW Route Tables

Transit Gateway Propagations



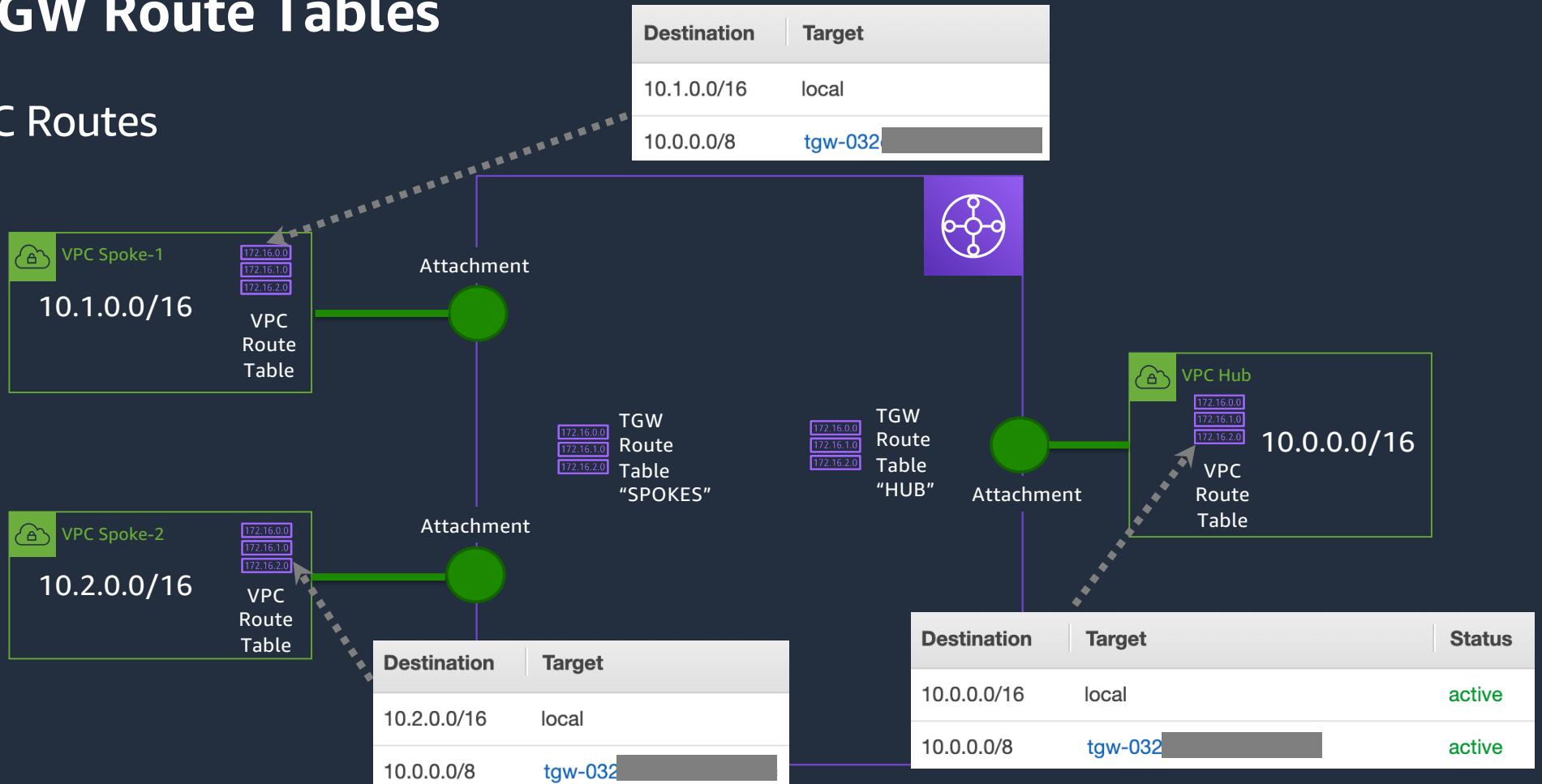
TGW Route Tables

Transit Gateway Routes



TGW Route Tables

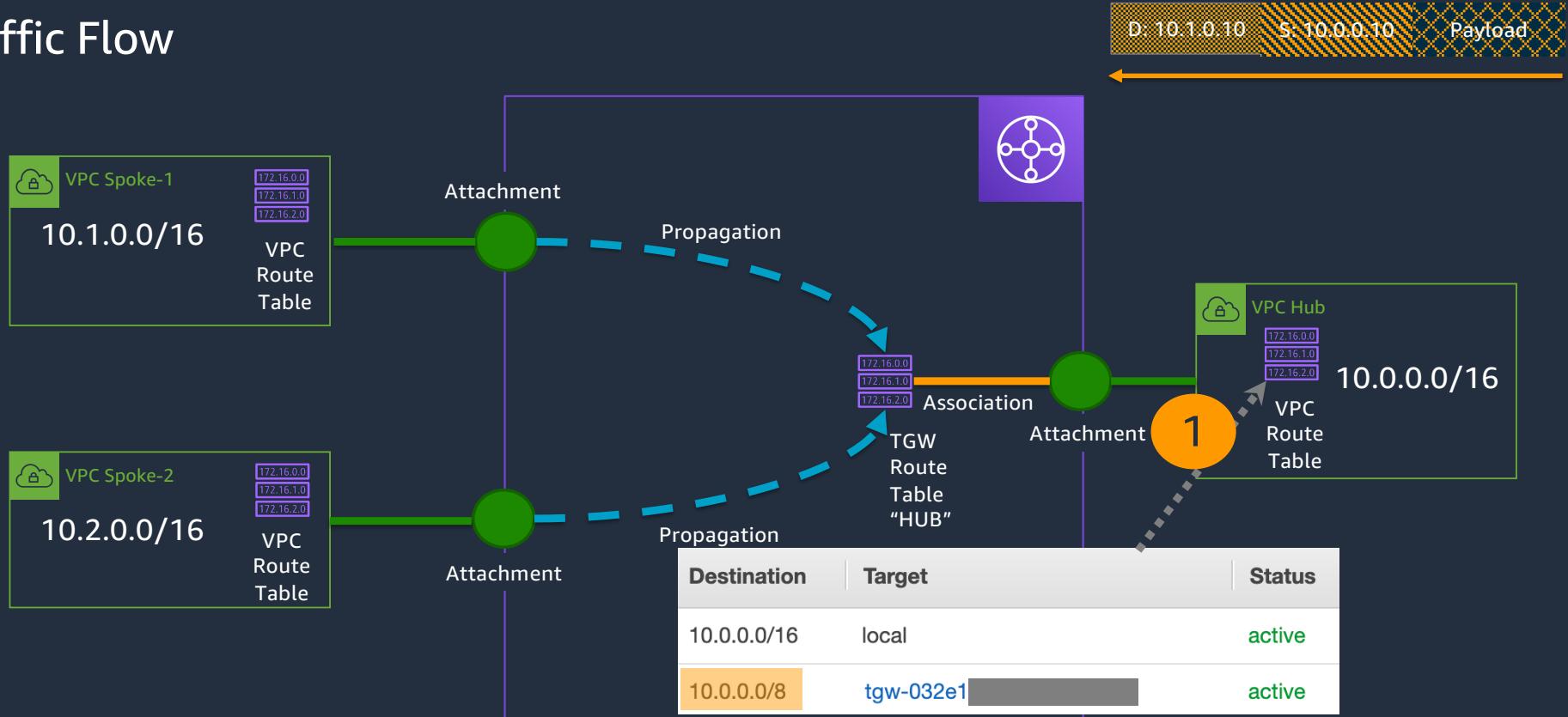
VPC Routes



Note: 10.0.0.0/8 route was manually added to VPC route-tables

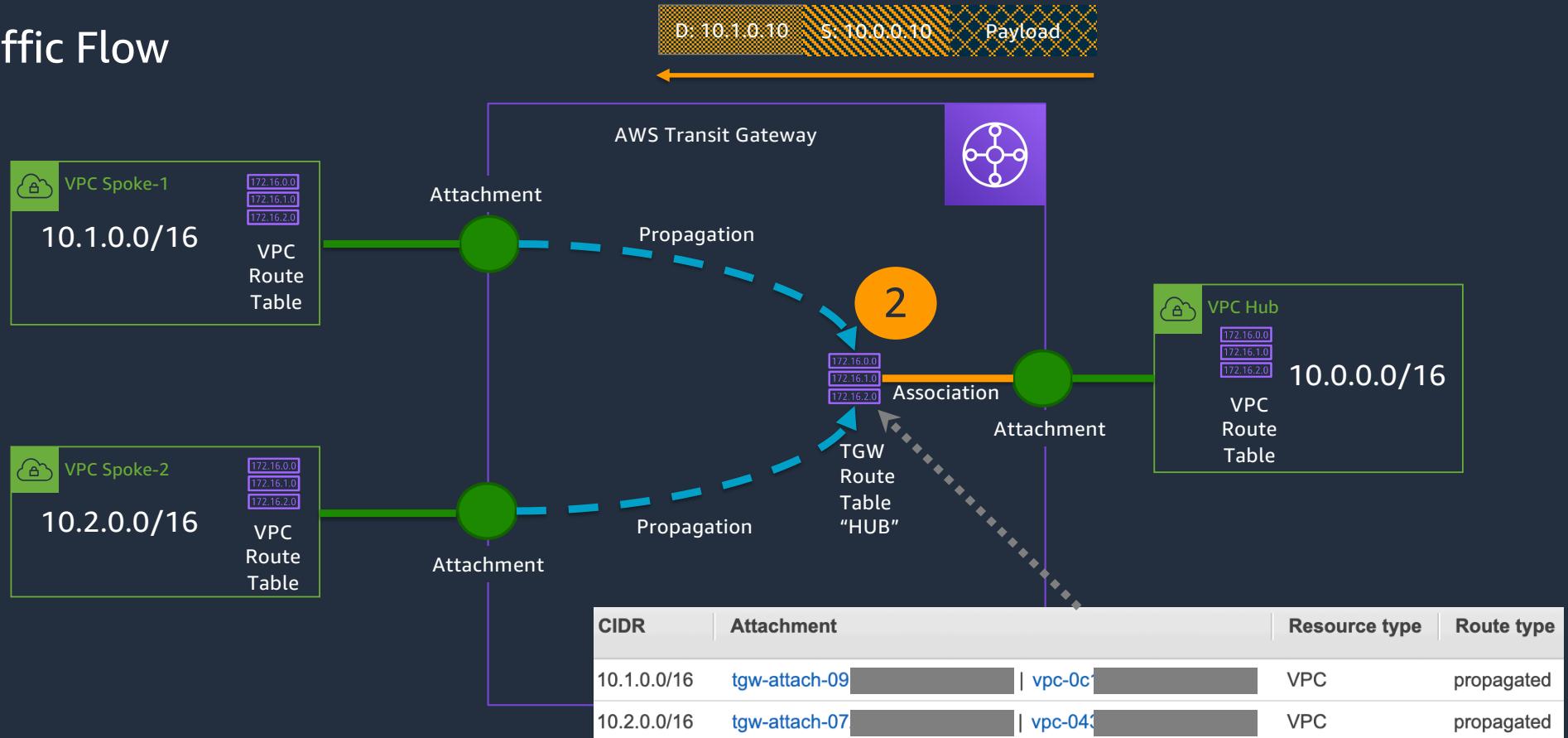
TGW Route Tables

Traffic Flow



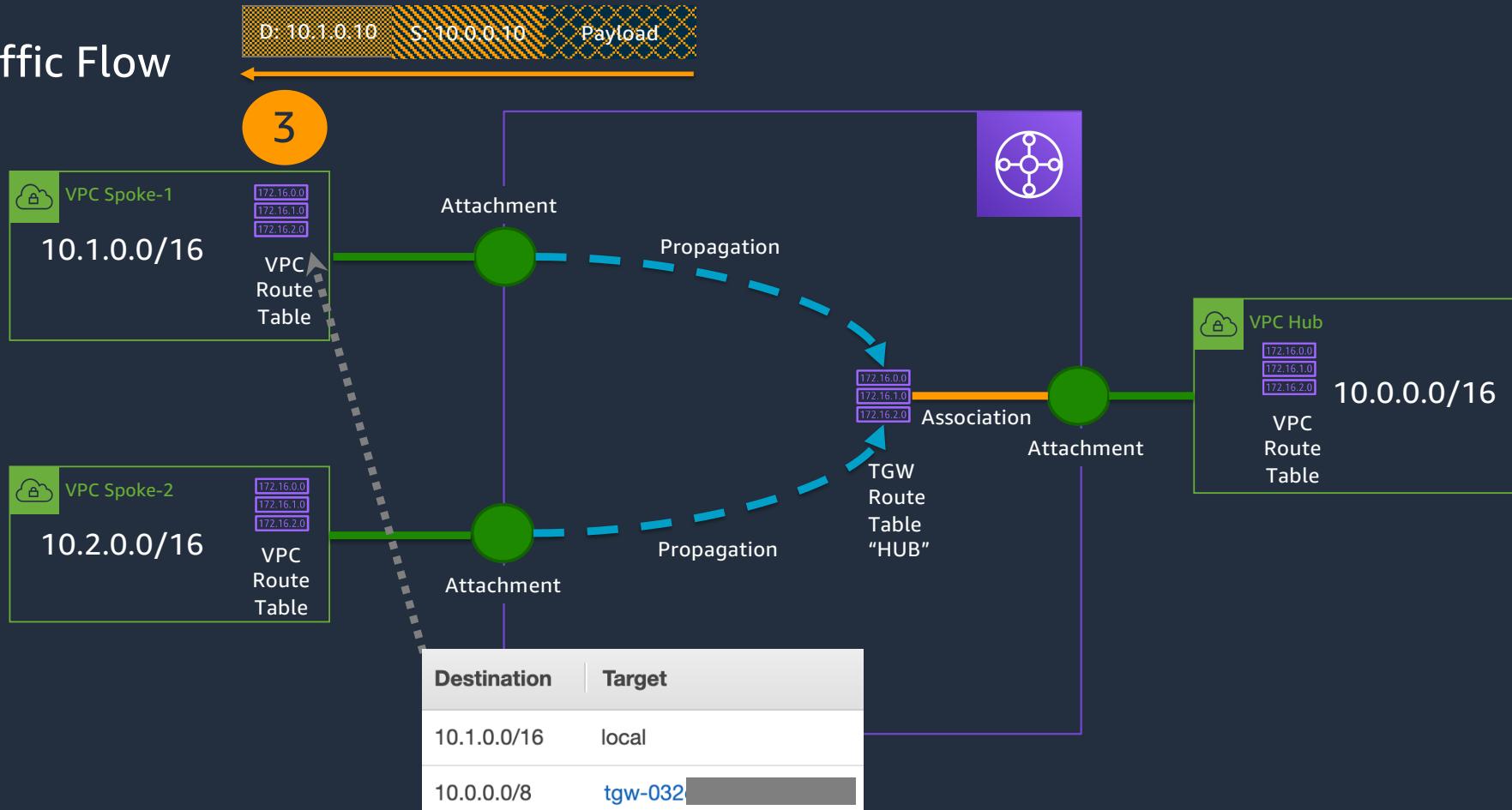
TGW Route Tables

Traffic Flow



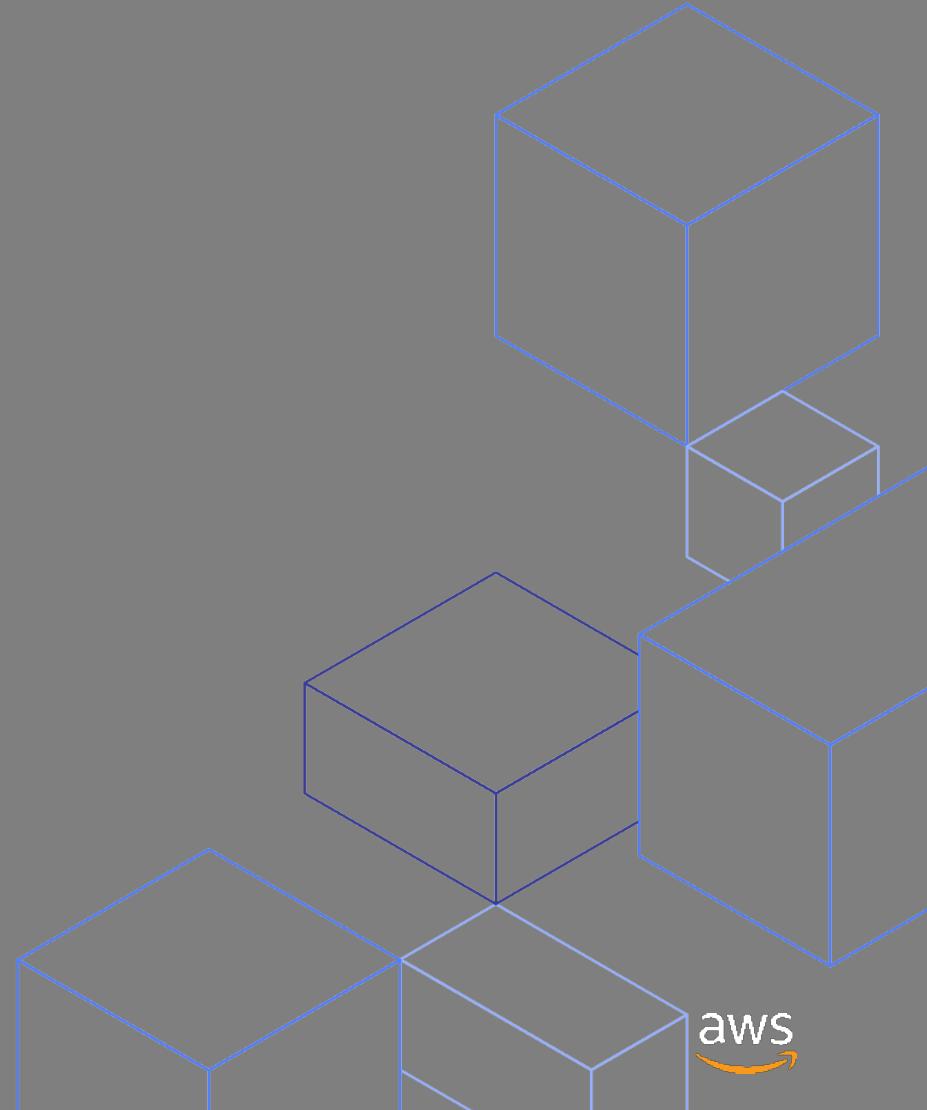
TGW Route Tables

Traffic Flow



Shared VPC

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



VPC sharing



VPC sharing

Allows for a VPC to be shared by multiple AWS accounts within an AWS Organization



Network Engineers

Central oversight and control for network engineers



Developers

No network management for application developers



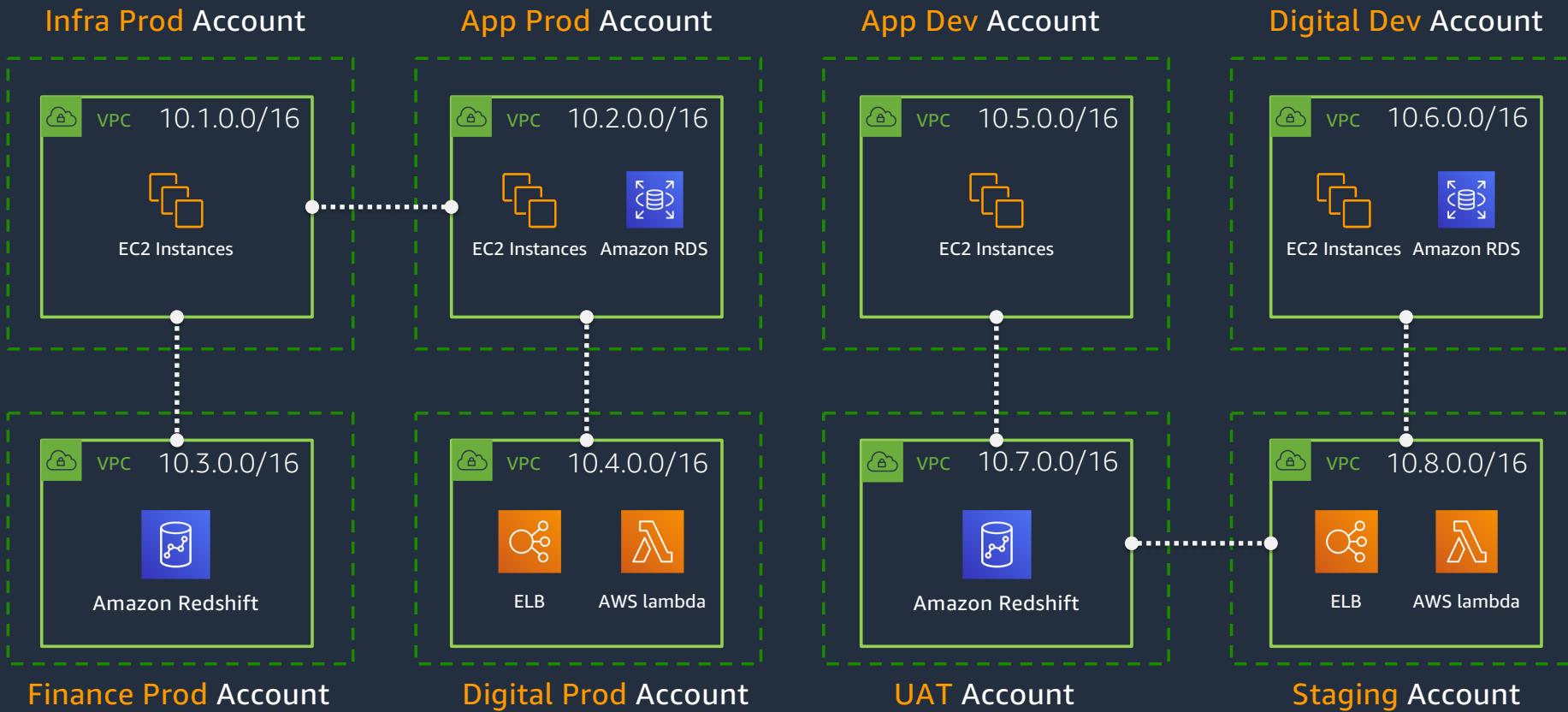
Edge Connectivity

Centralizes VPN and Direct Connect connections

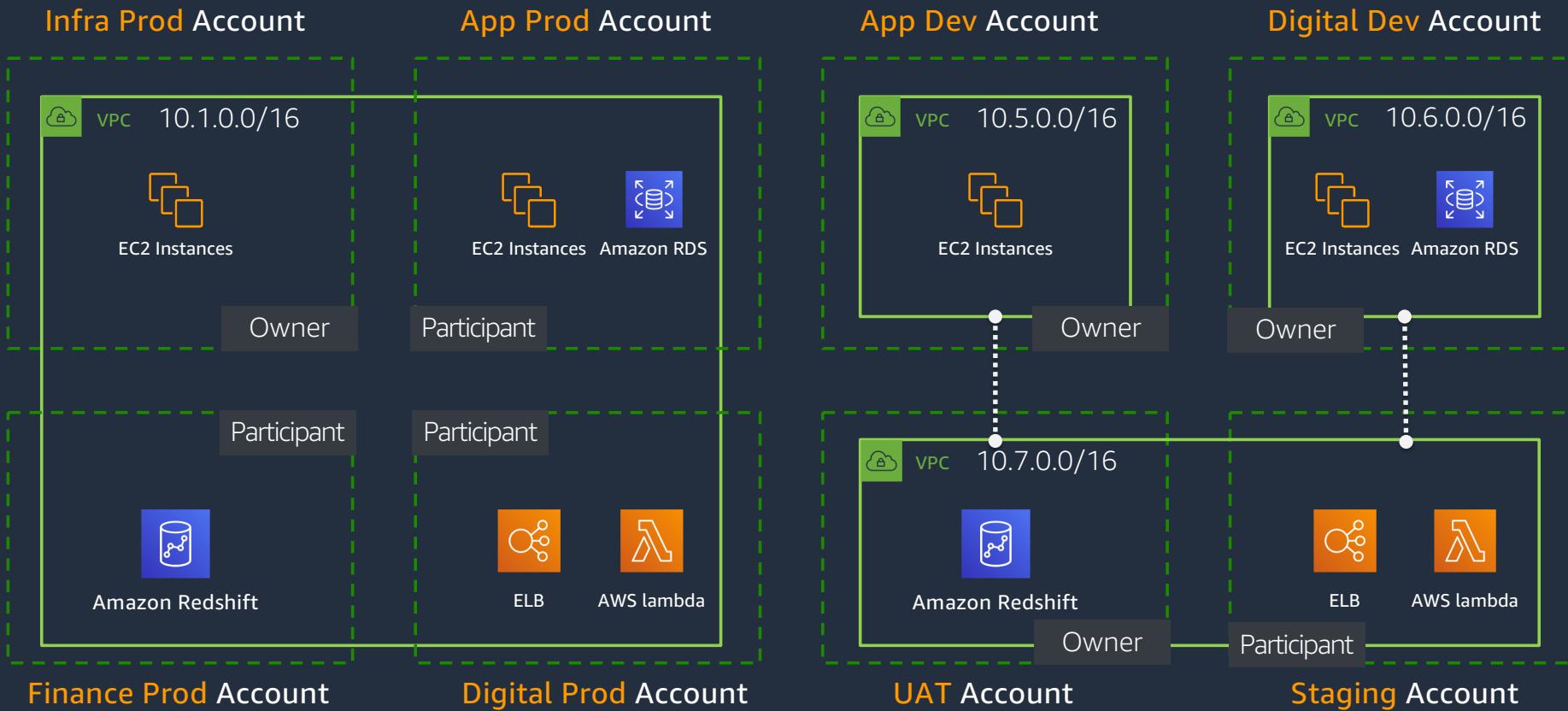


Avoid creating a single large VPC and sharing it with an entire organization. Instead, use VPC sharing together with AWS Transit Gateway and AWS PrivateLink

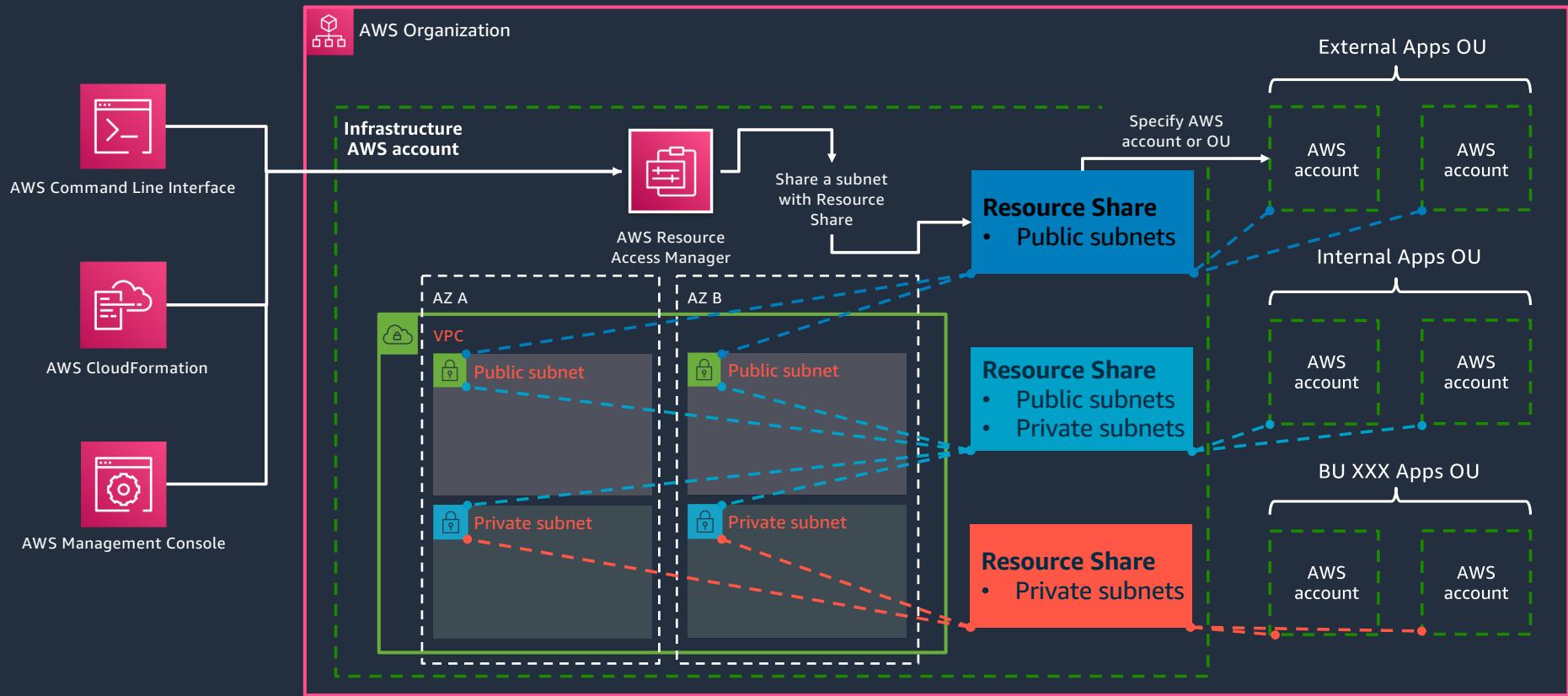
Before VPC sharing



After VPC sharing

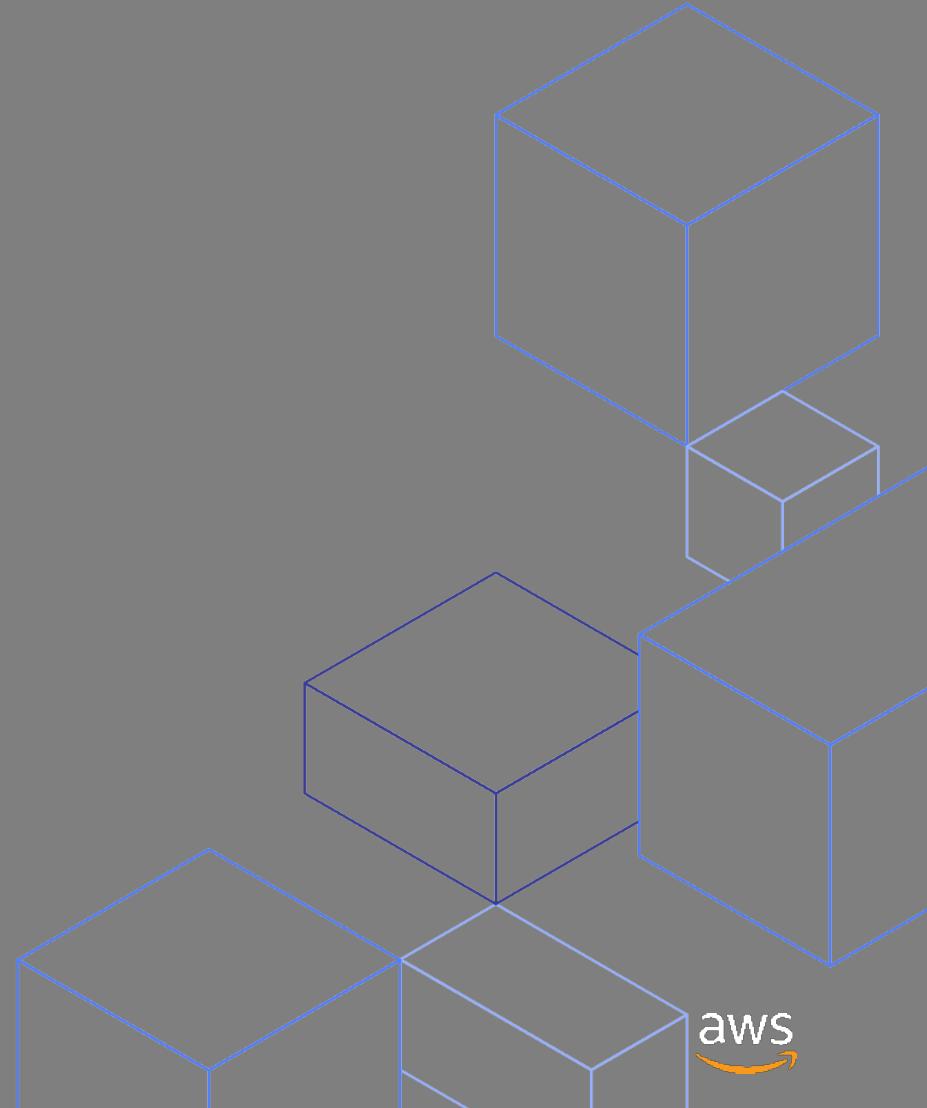


How does it actually work?



VPC Endpoints

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



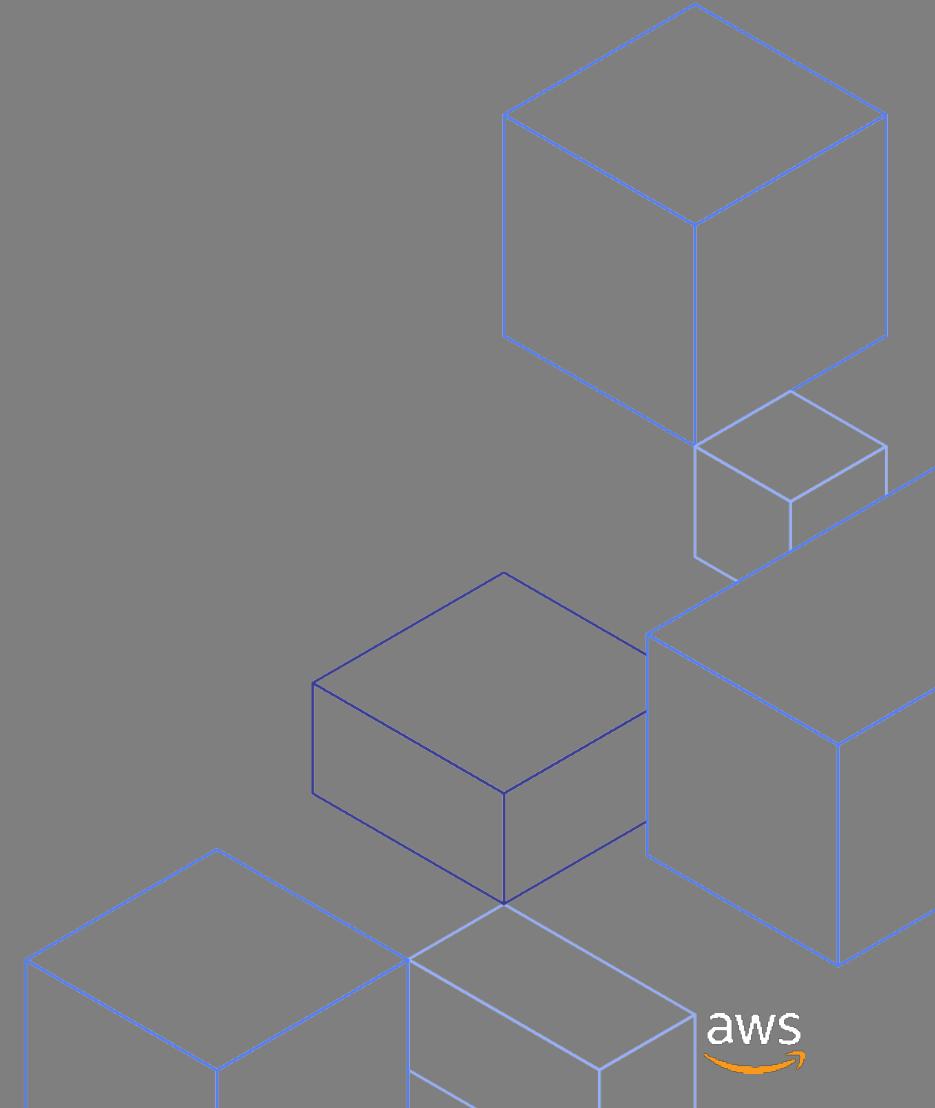
VPC Endpoints

- Privately connect your VPC to supported services
- Endpoints are virtual devices
 - Horizontally scaled
 - Redundant
 - Highly available
- Two types of VPC endpoints:
 - ❖ *Gateway Endpoints*
 - ❖ *Interface Endpoints*

VPC Endpoints

Gateway Endpoints

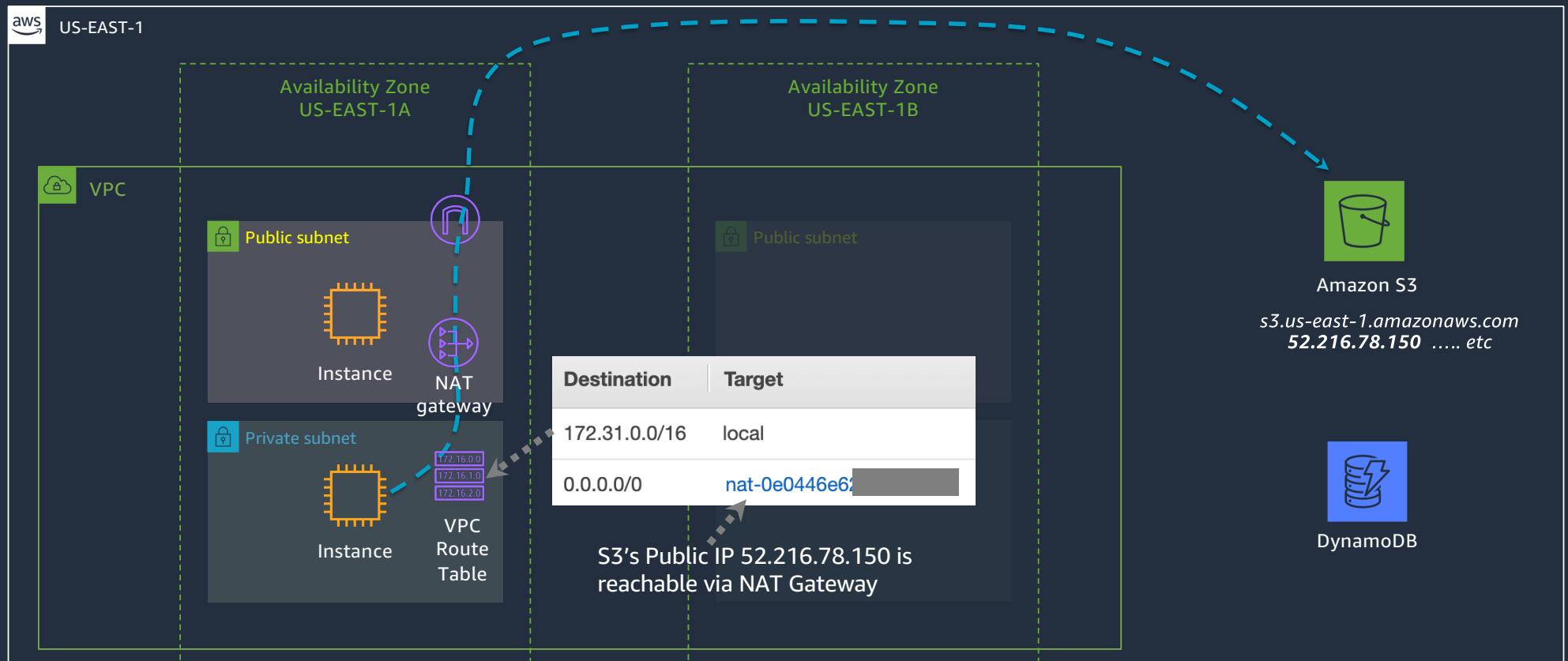
© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



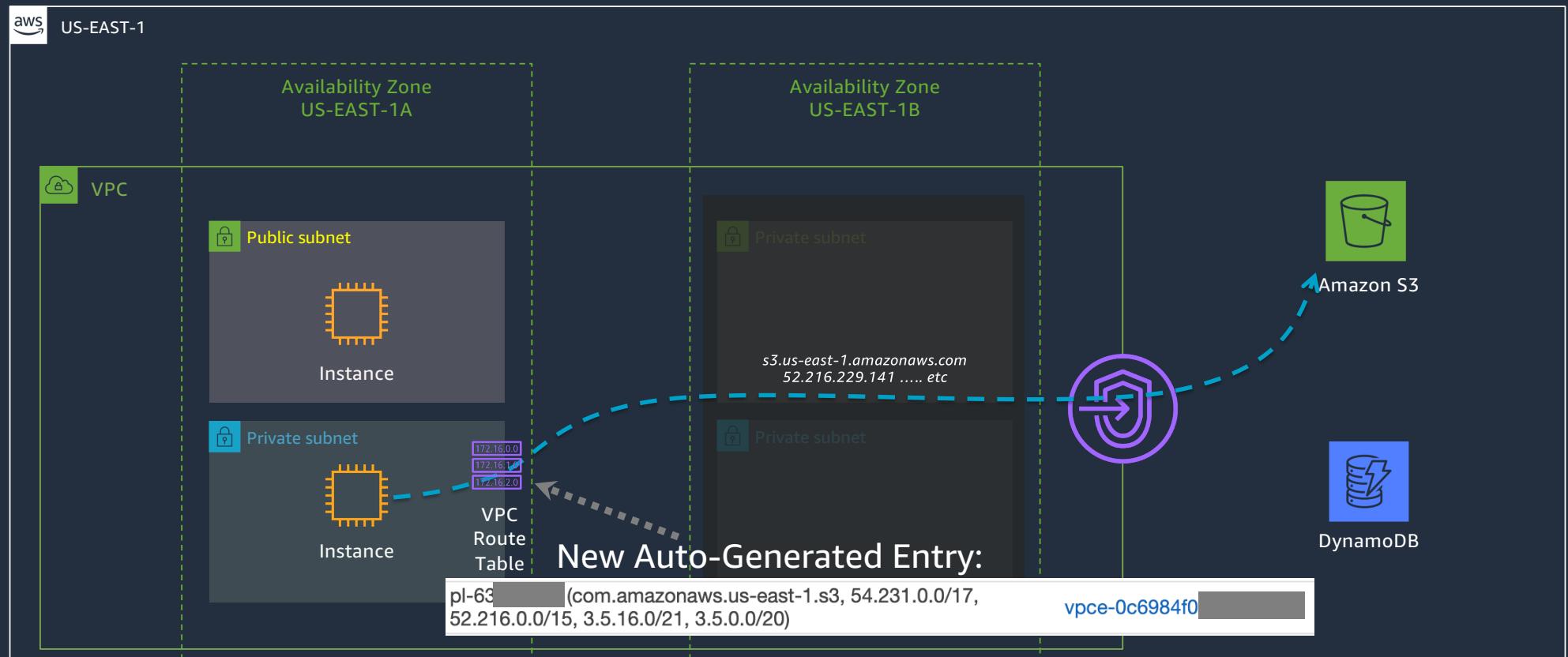
Gateway Endpoints

- Target for traffic destined to a supported AWS service
- Requires VPC route table entry with VPC endpoint being the next-hop
- Service prefix list is the destination CIDR
- Supported Services:
 - Amazon S3
 - DynamoDB

Accessing S3 and DynamoDB Without VPC Gateway Endpoint

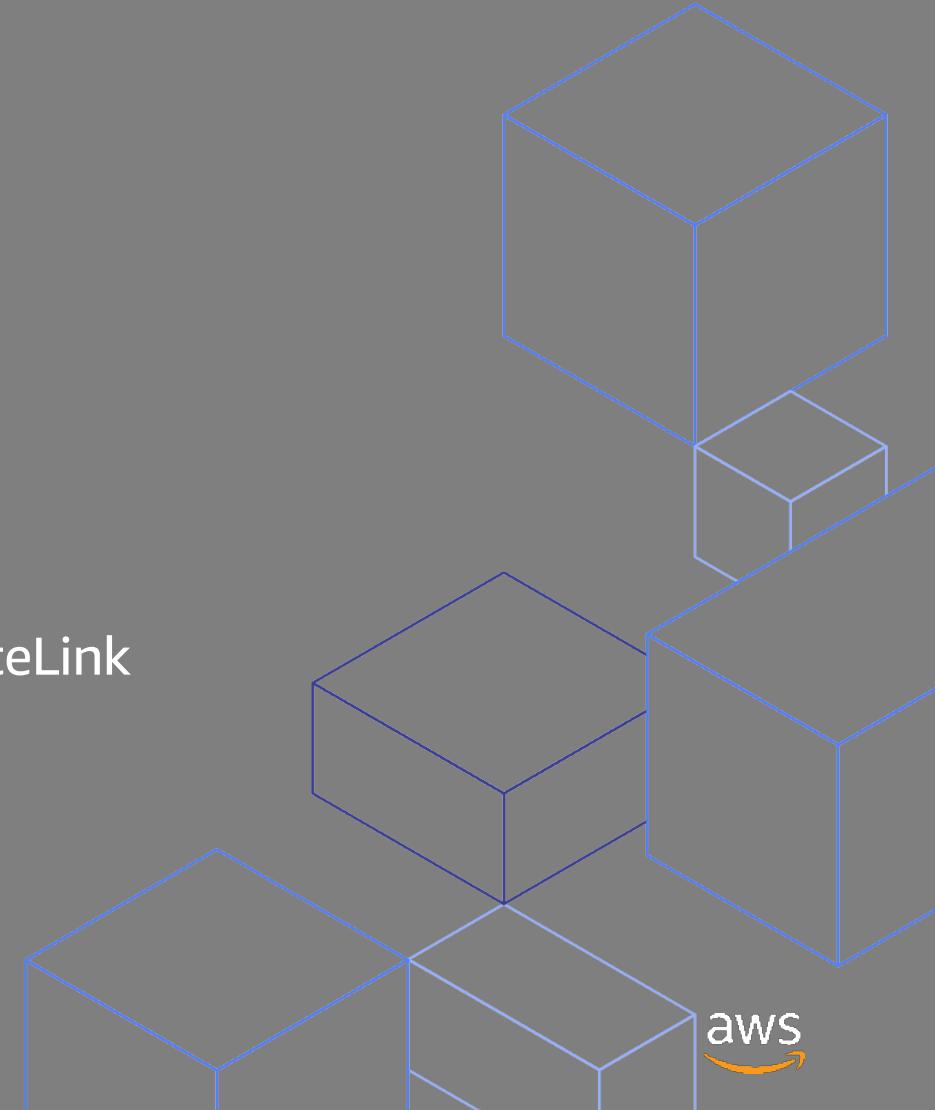


Accessing S3 via Gateway VPC Endpoints



VPC Endpoints

Interface Endpoints, powered by AWS PrivateLink



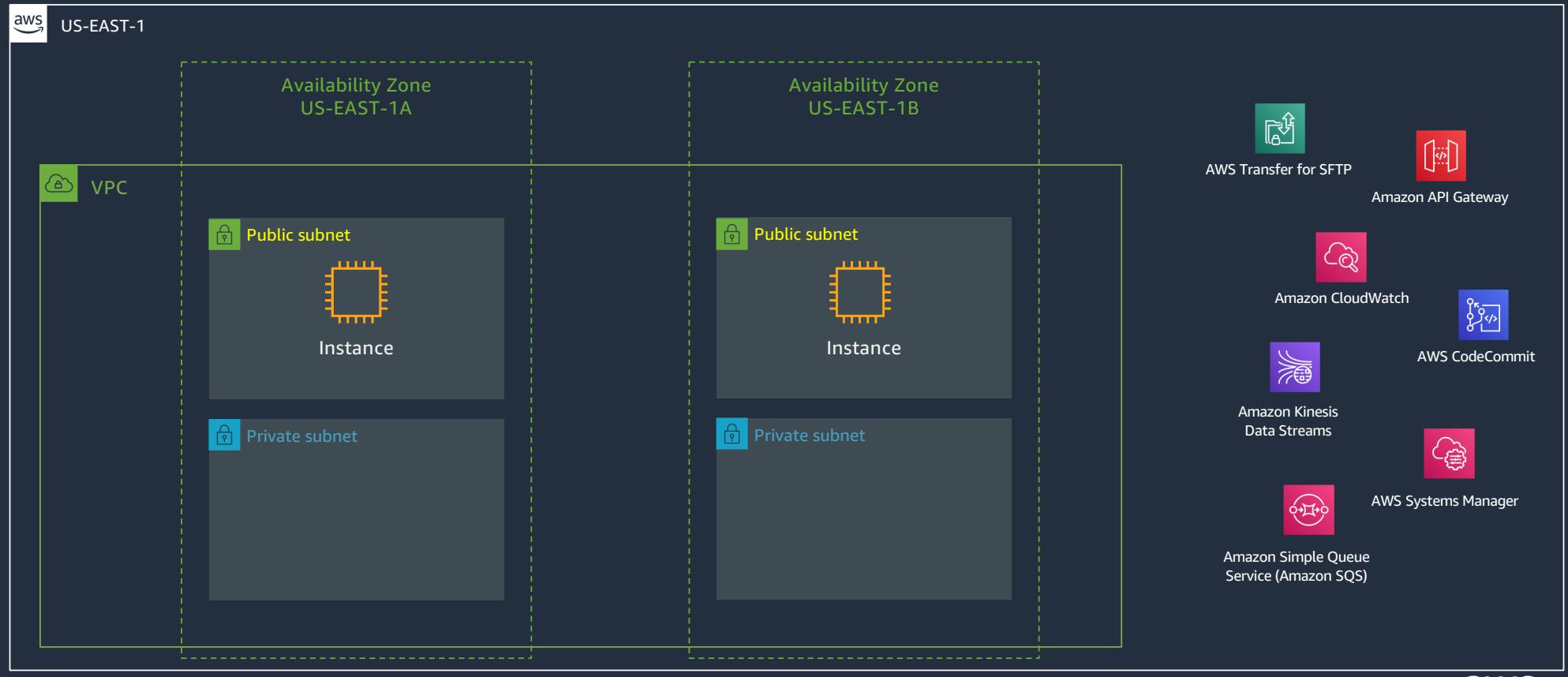
Interface Endpoints

- Elastic network interface with a private IP created in a VPC within a subnet
- Multiple services are supported:
 - Amazon API Gateway
 - Amazon AppStream 2.0
 - AWS App Mesh
 - Application Auto Scaling
 - Amazon Athena
 - <MANY MORE>

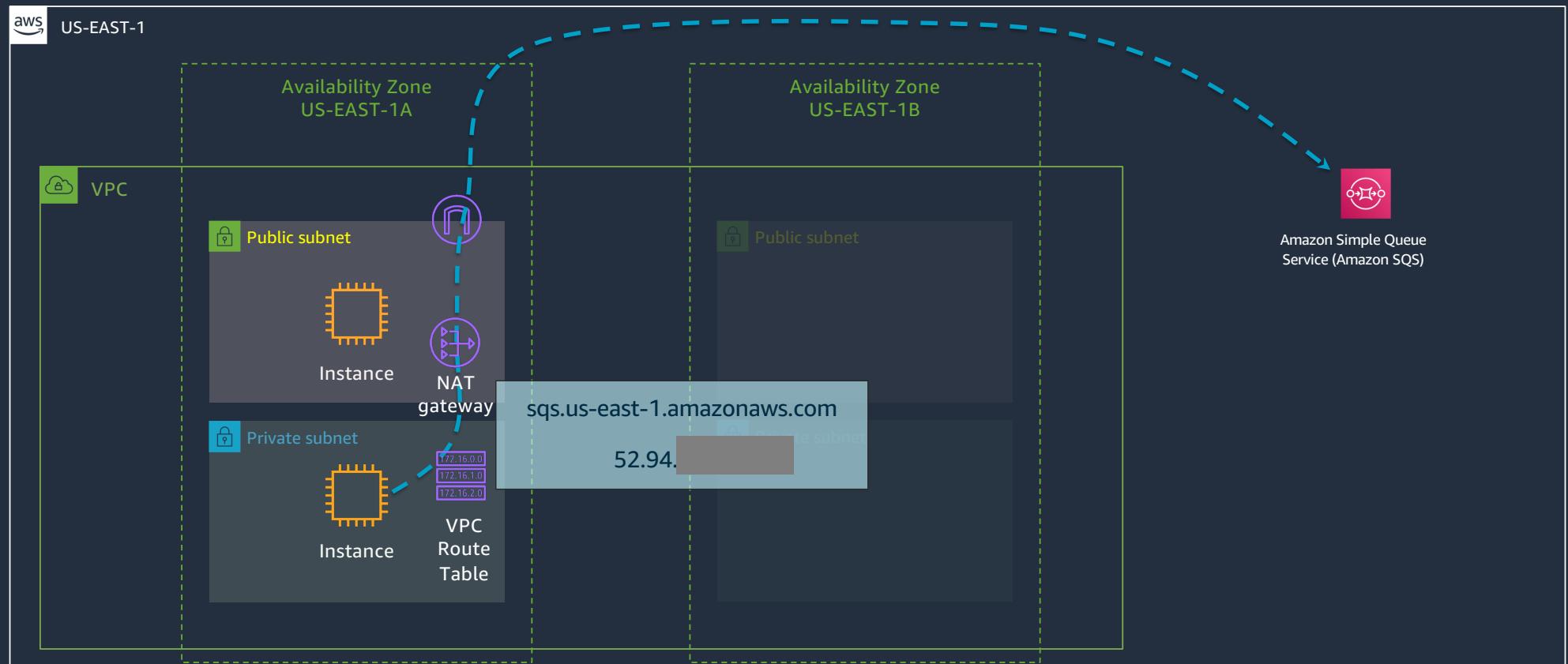
List of supported services:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html> 

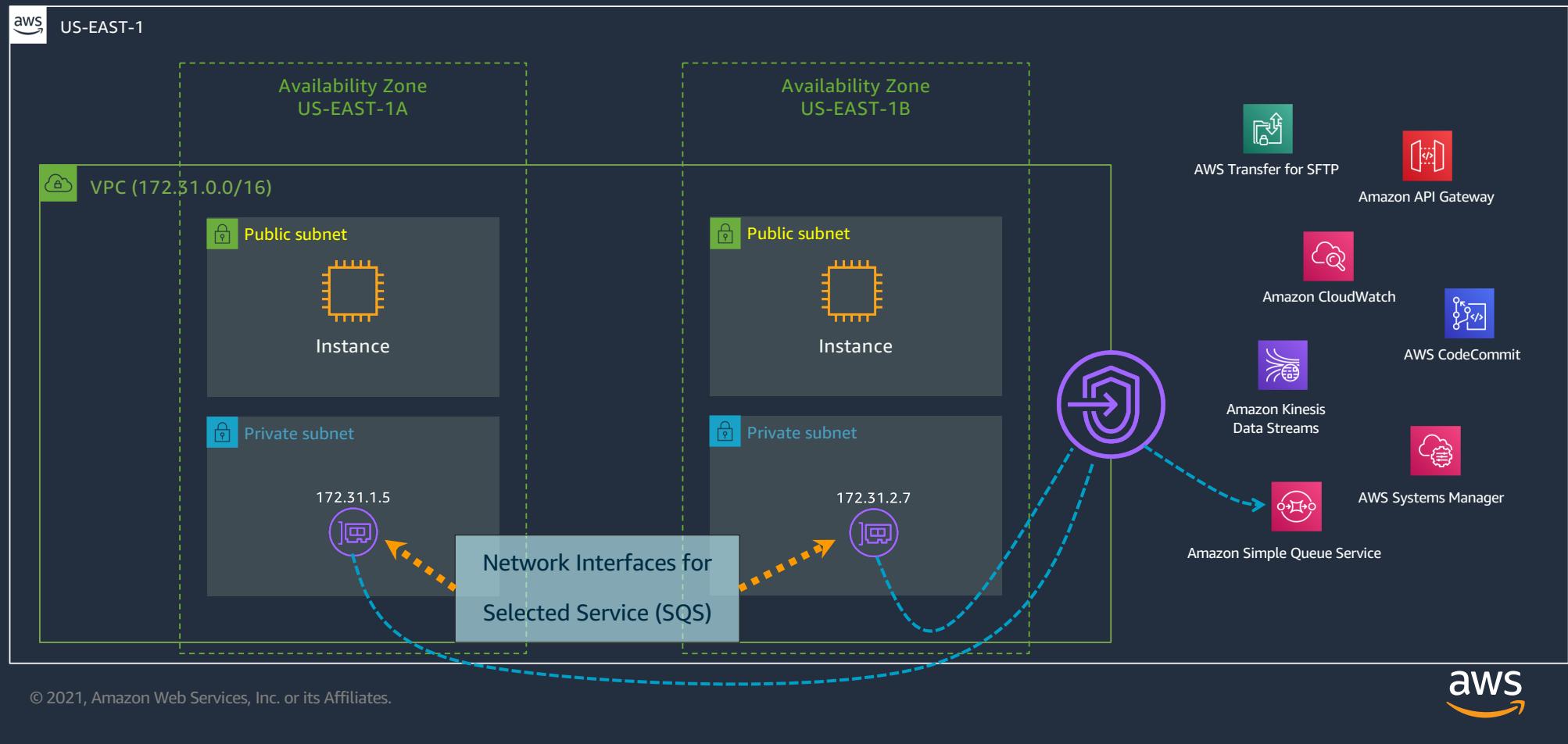
Interface VPC endpoints (AWS PrivateLink)



Accessing SQS Without Interface Endpoint



Interface VPC endpoints (AWS PrivateLink)



AWS SSO

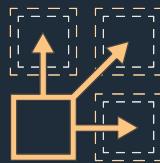
AWS Managed Microsoft AD

© 2021, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Introducing AWS Single Sign-On (SSO)

Cloud single sign-on (SSO) service that helps centrally manage SSO access to AWS accounts and business applications.



Centrally manage access to multiple AWS accounts.



Use your existing corporate identities.



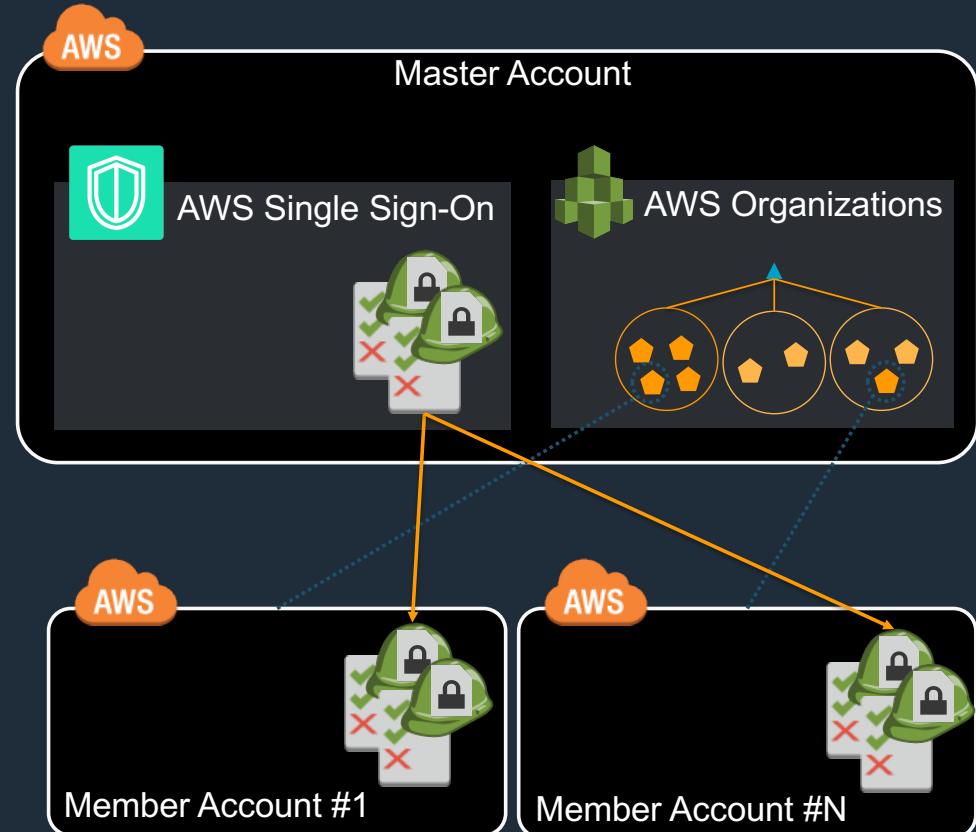
Easy to enable and use.



SSO access to business applications.



Define and Manage Permissions



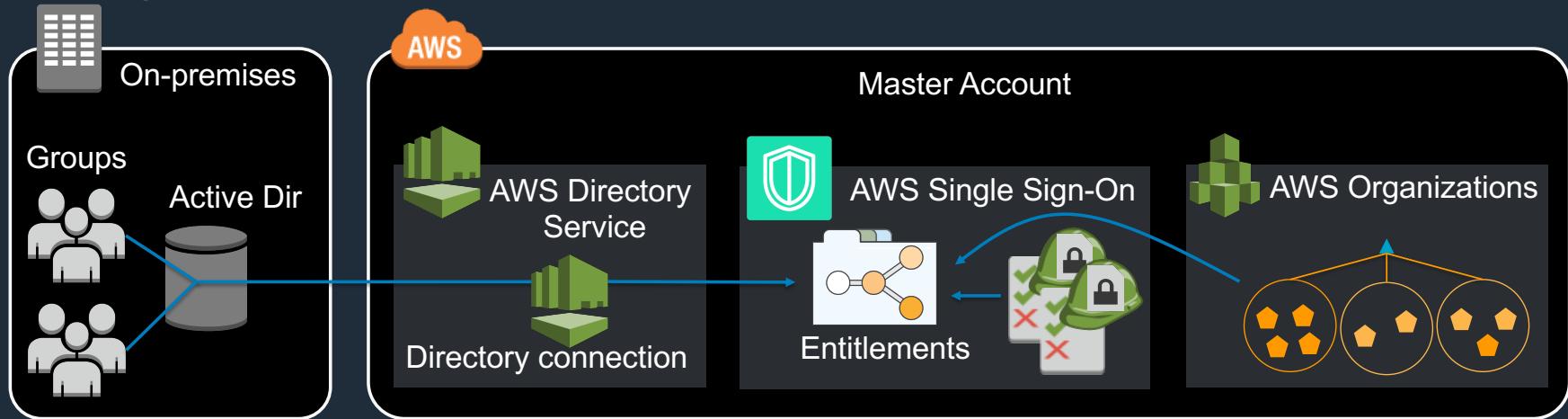
Uses **AWS Organizations** to retrieve your list and **structure of accounts**.

Define **permissions** using standard syntax and tools.

Definitions and policies automatically deployed and maintained in member accounts.



Assign AWS accounts to users



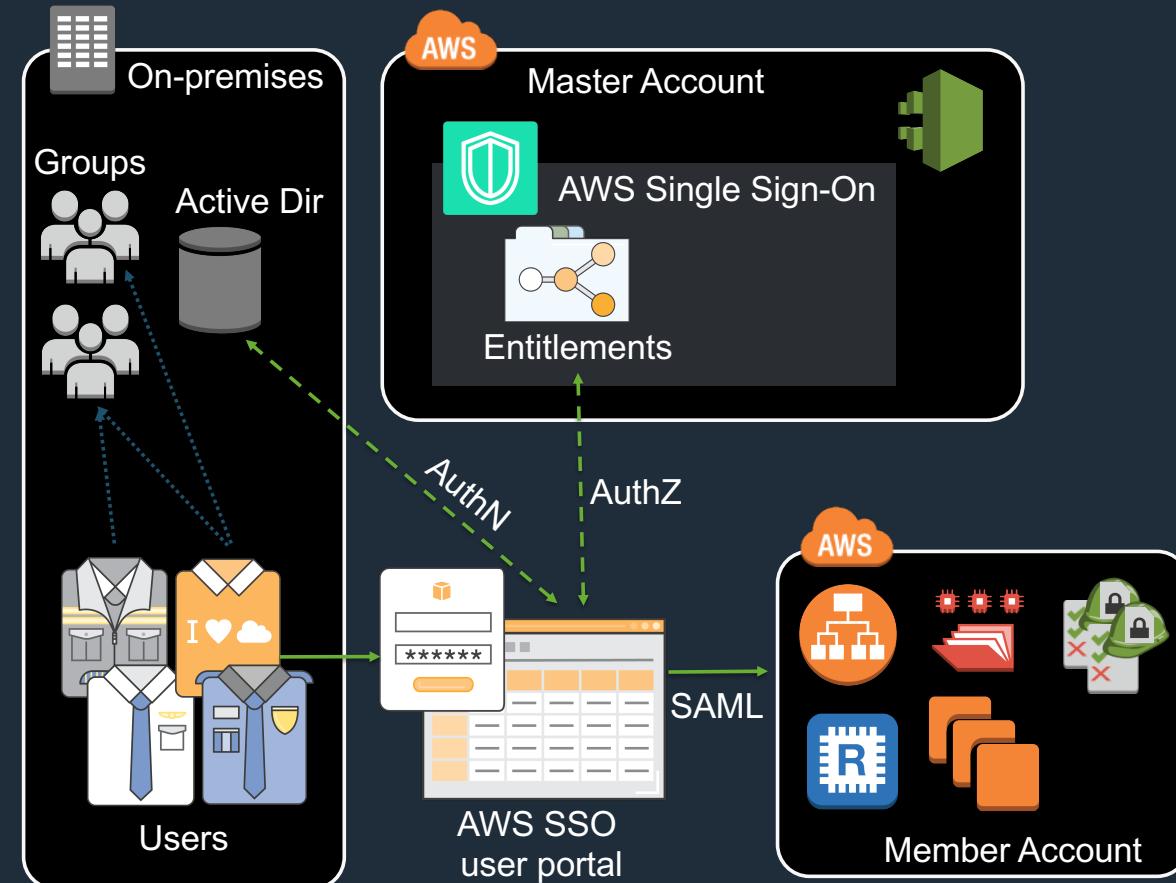
Uses AWS Directory Service to connect to on-premises AD

Map AD groups to defined permissions

Grant access to one AWS account, an OU, or the entire Organization.



Login Flow (AWS Accounts)



Users browse to the AWS SSO user portal and are authenticated using their corporate credentials.

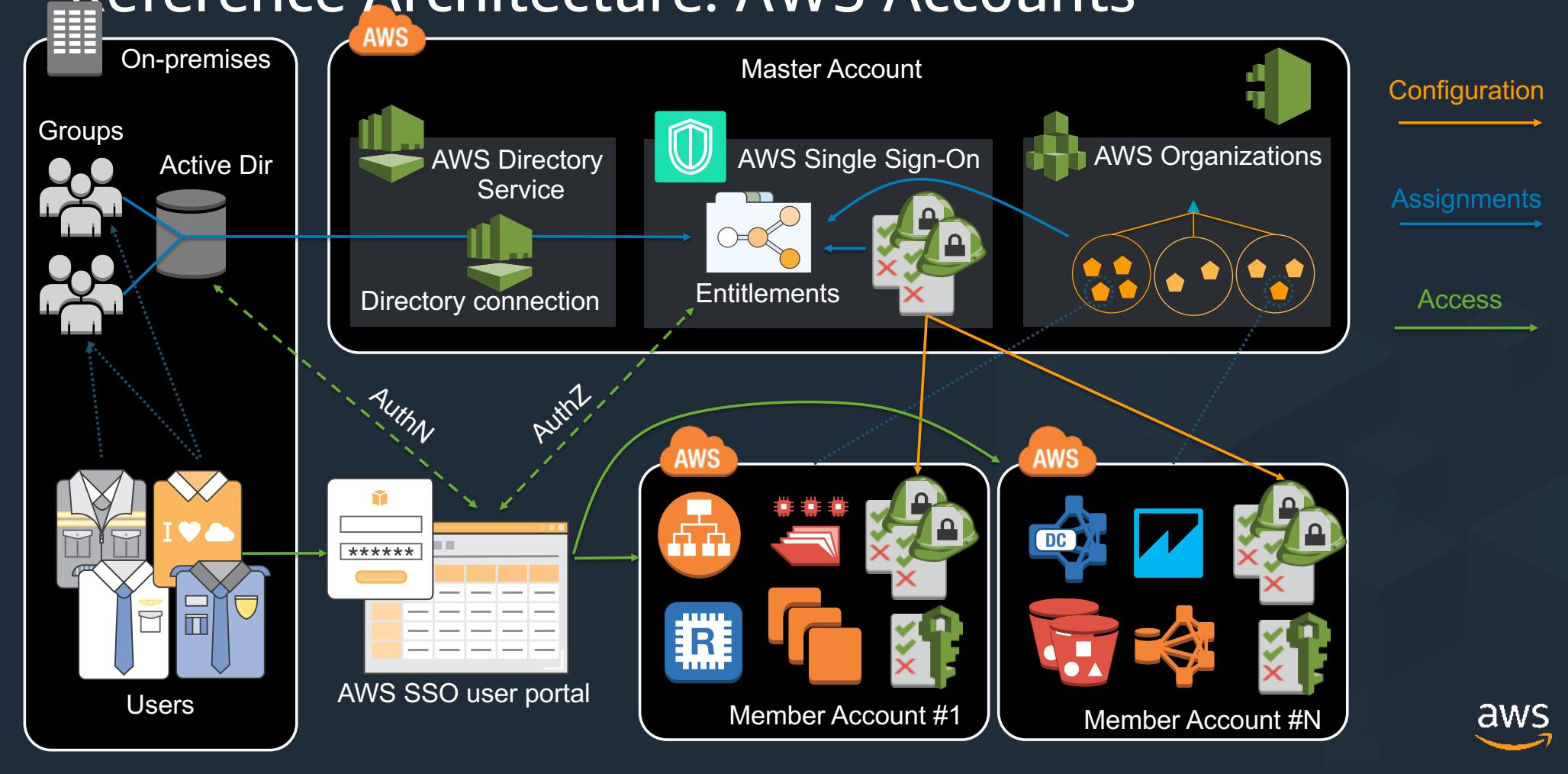
AWS SSO authorizes the user based on their entitlements.

Users are federated into an IAM role in member account.

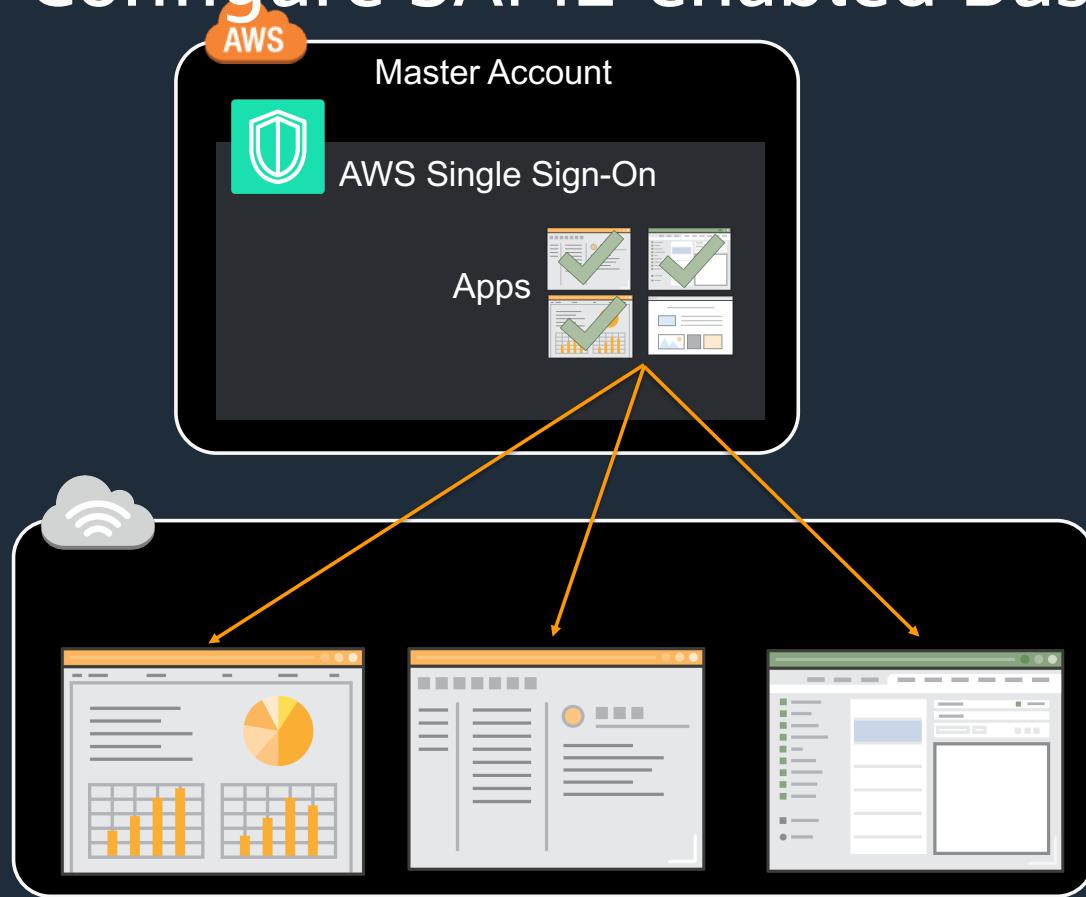
Actions and resource access are governed by Organizations SCPs and IAM policies as usual.

Monitor and audit via CloudTrail.

Reference Architecture: AWS Accounts



Configure SAML-enabled Business Apps



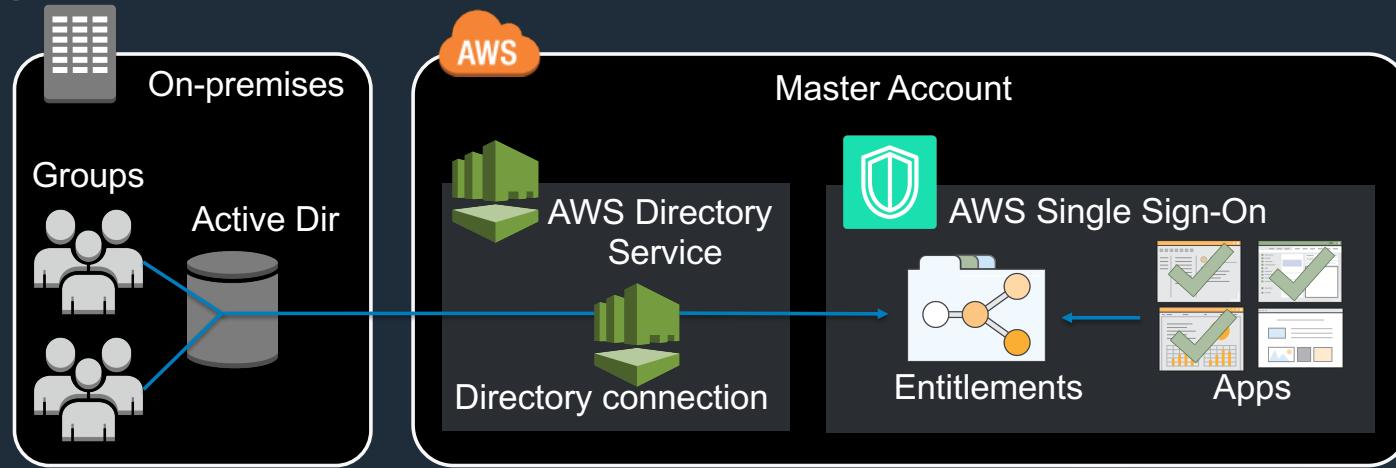
Add any **SAML-enabled application** via application configuration wizard.

Select the **preintegrated cloud business apps** used by your enterprise.

AWS configures **SSO access** and monitors **SSO integration** for changes.



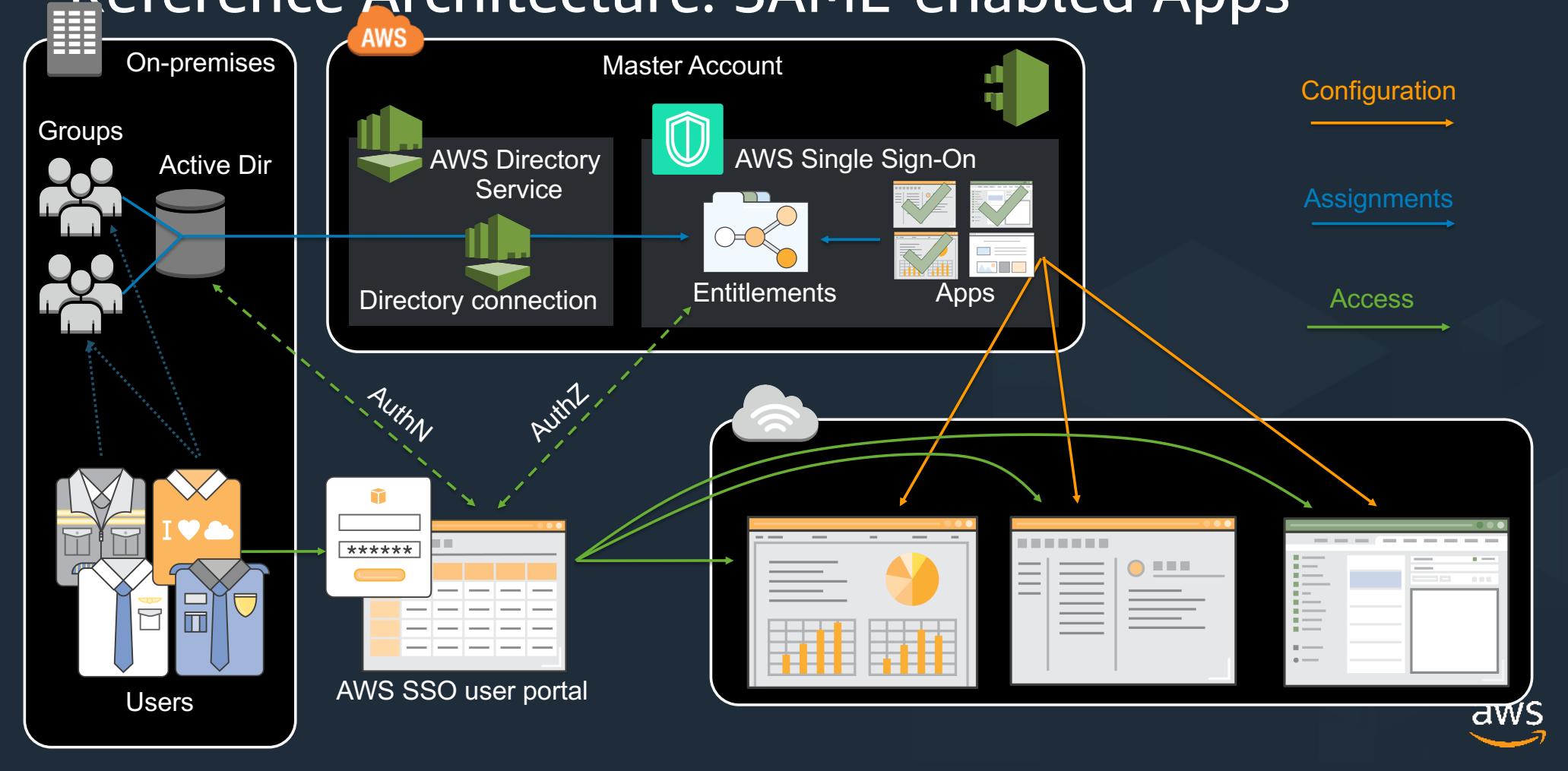
Assign business apps to AD users



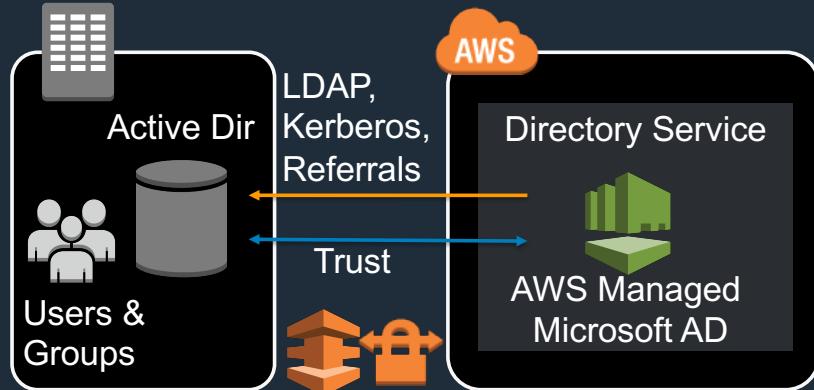
Grant users access to applications by mapping AD groups.



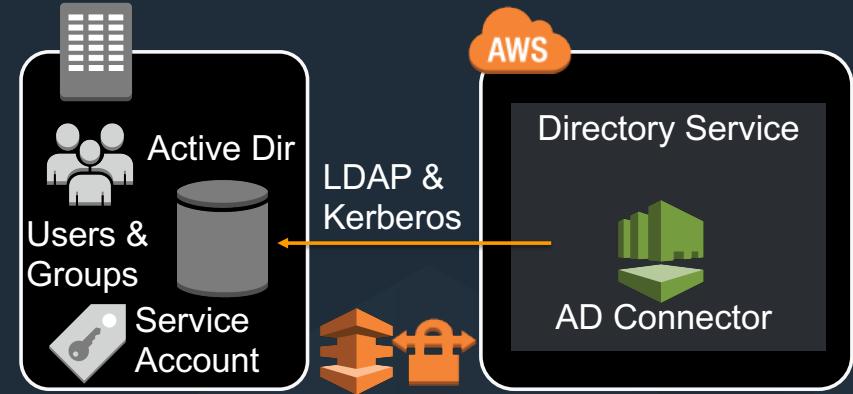
Reference Architecture: SAML-enabled Apps



Integrating with AWS Directory Services



Option 1: AWS Managed Microsoft AD with Trust



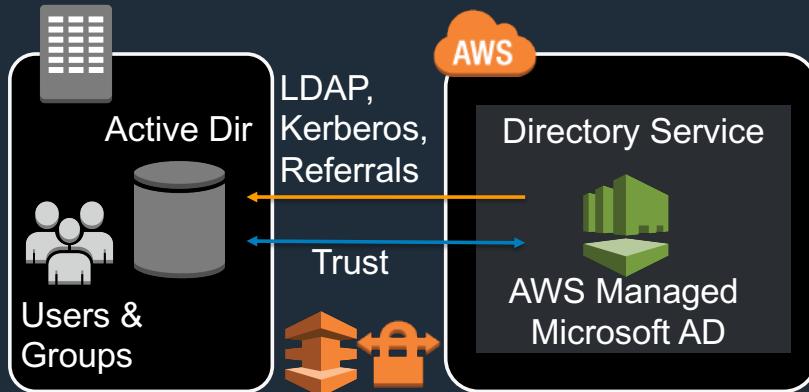
Option 2: AD Connector



Option 3: Stand alone AWS Managed Microsoft AD



Option 1: AWS Managed Microsoft AD with Trust



Option 1: AWS Managed Microsoft AD with Trust

Use when: Preferred option for connecting to on-premises directory.

Trust established between AWS Managed Microsoft AD and on-premises directory.

Performs LDAP operations, Kerberos authentication, and AD referrals to on-premises directory.

Connection established using Direct Connect and/or VPN.

Option 2: AD Connector



Option 2: AD Connector

Service Account created in on-premises directory, then configured in AD Connector.

Proxies LDAP operations and Kerberos authentication to on-premises directory.

Connection established using Direct Connect and/or VPN.

Use when: Policies or other challenges prevent the use of Active Directory trusts.



Option 3: Stand alone AWS Managed Microsoft AD



AWS Managed Microsoft AD instance created in AWS.

Create users and groups in the directory in a stand-alone fashion.

Option 3: Stand alone AWS Managed AD

Use when: You want to use a managed AD service.



AWS Managed Microsoft AD use cases

