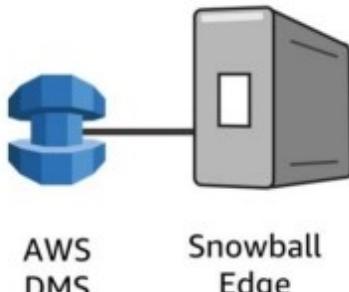


AWS Snowball Edge 및 AWS DMS를 사용



The diagram illustrates the integration between AWS DMS and AWS Snowball Edge. On the left, a blue hexagonal icon represents AWS DMS, connected by a line to a grey rectangular icon representing the Snowball Edge device. Below the icons, the text 'AWS DMS' and 'Snowball Edge' is written respectively.

AWS DMS에는 Snowball Edge 통합 포인트가 있습니다.

Snowball Edge 디바이스를 사용하여 하나 이상의 데이터베이스를 마이그레이션할 수 있습니다.

- 멀티 테라바이트 스토리지
- 인터넷 또는 DX 대역폭을 사용하지 않음

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

외부에서 포트를 여는 것이 아니라 데이터 센터 내부에서 직접 안전하고 견고한 디바이스를 물리적으로 연결할 수 있습니다.

이제 매우 큰 데이터베이스를 온프레미스에서 AWS 클라우드로 이전할 수 있습니다.

이 통합은 "pull" 모델이 아니라 "push" 모델을 통한 데이터베이스를 마이그레이션합니다.

네트워크 인프라를 업그레이드하고 전용 대역폭을 사용할 필요 없이 동일한 AWS Snowball Edge 디바이스를 사용하여 하나 이상의 데이터베이스를 마이그레이션할 수 있습니다.

이러한 멀티 테라바이트 또는 멀티 페타바이트 데이터베이스를 AWS로 마이그레이션하는 동안 온프레미스 데이터베이스가 온라인 상태로 유지됩니다. AWS Snowball Edge 어플라이언스가 AWS로 반송되어 자동으로 대상 Amazon RDS 또는 Amazon EC2 기반 데이터베이스로 로드되면 온프레미스 데이터베이스를 폐기할 수 있습니다.

기존 데이터를 마이그레이션하거나(일회성) 선택적으로 대상 데이터베이스로 지속적 데이터 복제를 수행할 수 있습니다.

AWS Snowball Edge 및 AWS DMS 작업에 대한 몇 가지 참고 사항:

- AWS DMS를 통합하는 데 필요한 AWS Snowball의 버전은 [AWS Snowball Edge](#)입니다.
- 현재, AWS DMS Snowball 에이전트를 실행하려면 Linux 호스트가 필요합니다.
- AWS Snowball Edge가 원본 데이터베이스와 동일한 네트워크에 있어야 합니다.

DO NOT COPY
zlagusdbs@gmail.com

AWS Schema Conversion Tool

aws training and certification

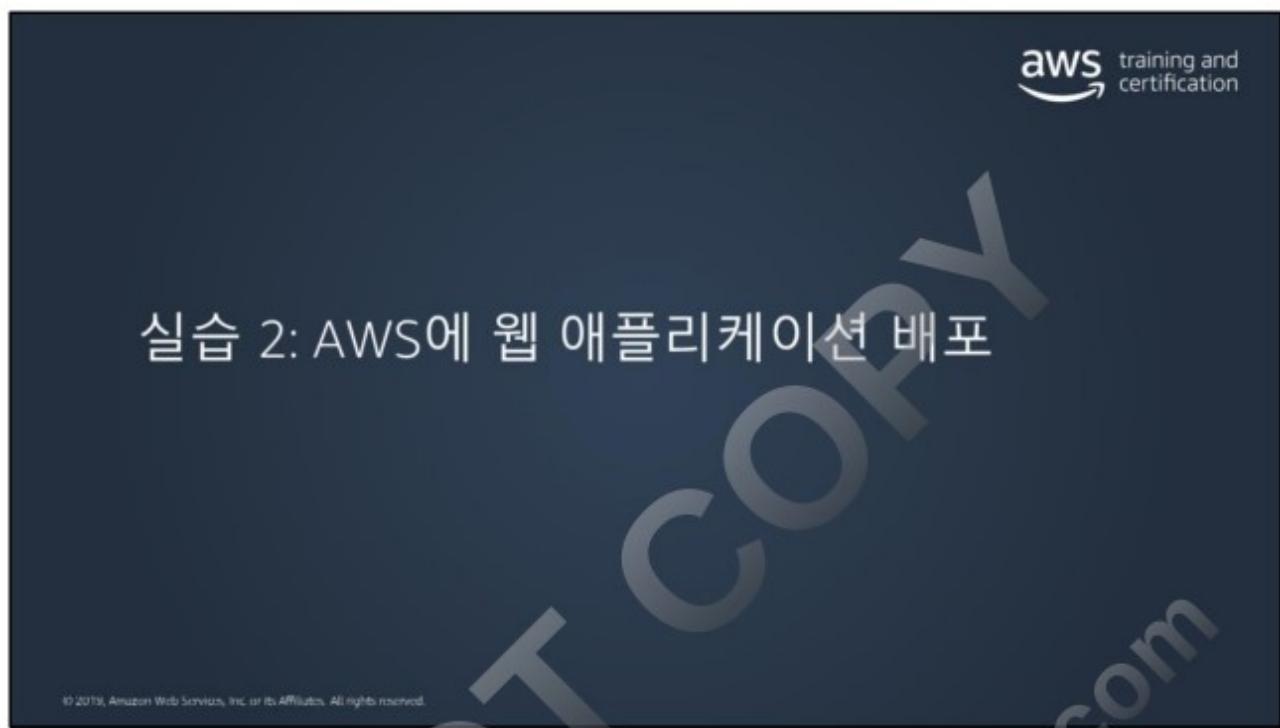
사용자가 기존 데이터베이스 스키마를 한 데이터베이스 엔진에서 다른 데이터베이스 엔진으로 변환하도록 해주는 독립형 애플리케이션입니다.

원본 데이터베이스	대상 데이터베이스
Microsoft SQL Server	Amazon Aurora, MySQL, PostgreSQL
MySQL	PostgreSQL
Oracle	Amazon Aurora, MySQL, PostgreSQL
Oracle 데이터 웨어하우스	Amazon Redshift
PostgreSQL	Amazon Aurora, MySQL
Teradata	Amazon Redshift

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Schema Conversion Tool에 대한 자세한 내용은

<http://docs.aws.amazon.com/SchemaConversionTool/latest/userguide/Welcome.html>
을 참조하십시오.



실습 2: AWS에 웹 애플리케이션 배포



"웹 애플리케이션과 데이터베이스를 호스팅하려고 합니다."

사용된 기술:

- Amazon EC2
- Amazon RDS
- 보안 그룹

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

실습 2: AWS에 웹 애플리케이션 배포

aws training and certification

실습 시작 시 제공됨:

- 2개의 가용영역에 걸친 VPC
- 2개의 퍼블릭 서브넷
- 2개의 프라이빗 서브넷

The diagram illustrates a Lab VPC structure. At the top, a cloud icon labeled "VPC" contains two separate sections, each representing an "Availability Zone". Each zone contains a "Public Subnet" (10.0.0.0/24) and a "Private Subnet" (10.0.2.0/23 and 10.0.4.0/23). Each subnet is enclosed in a dashed orange border and features a small padlock icon at the bottom right corner, indicating it is locked or private. The entire VPC is labeled "Lab VPC" at the bottom center.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

실습 2: AWS에 웹 애플리케이션 배포



보안 구성

- 앱 보안 그룹: 인터넷에서 액세스하도록 허용
- DB 보안 그룹: 앱 보안 그룹에서 액세스하도록 허용



"울타리를 치고 리소스를 그 안에 배치합니다."

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

실습 2: AWS에 웹 애플리케이션 배포

aws training and certification

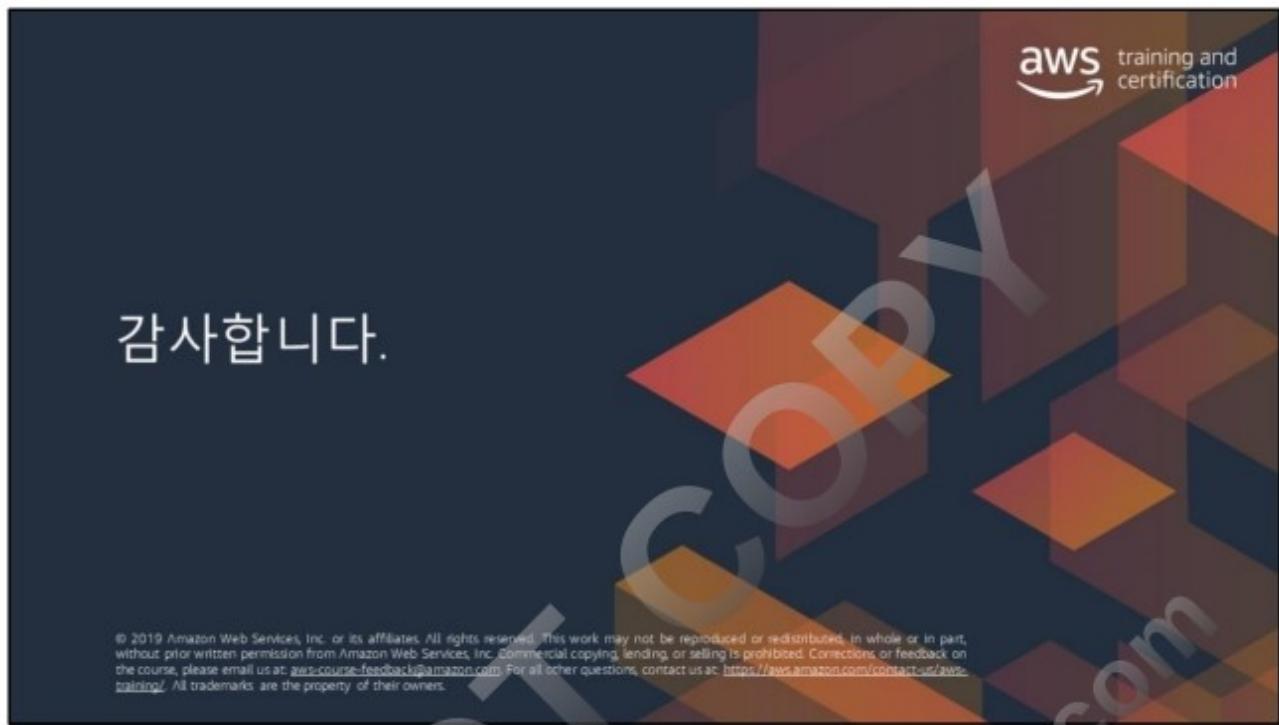
이 실습에서는

- 데이터베이스 서버를 배포합니다.
- 애플리케이션 서버를 배포합니다.
- 애플리케이션을 테스트합니다.

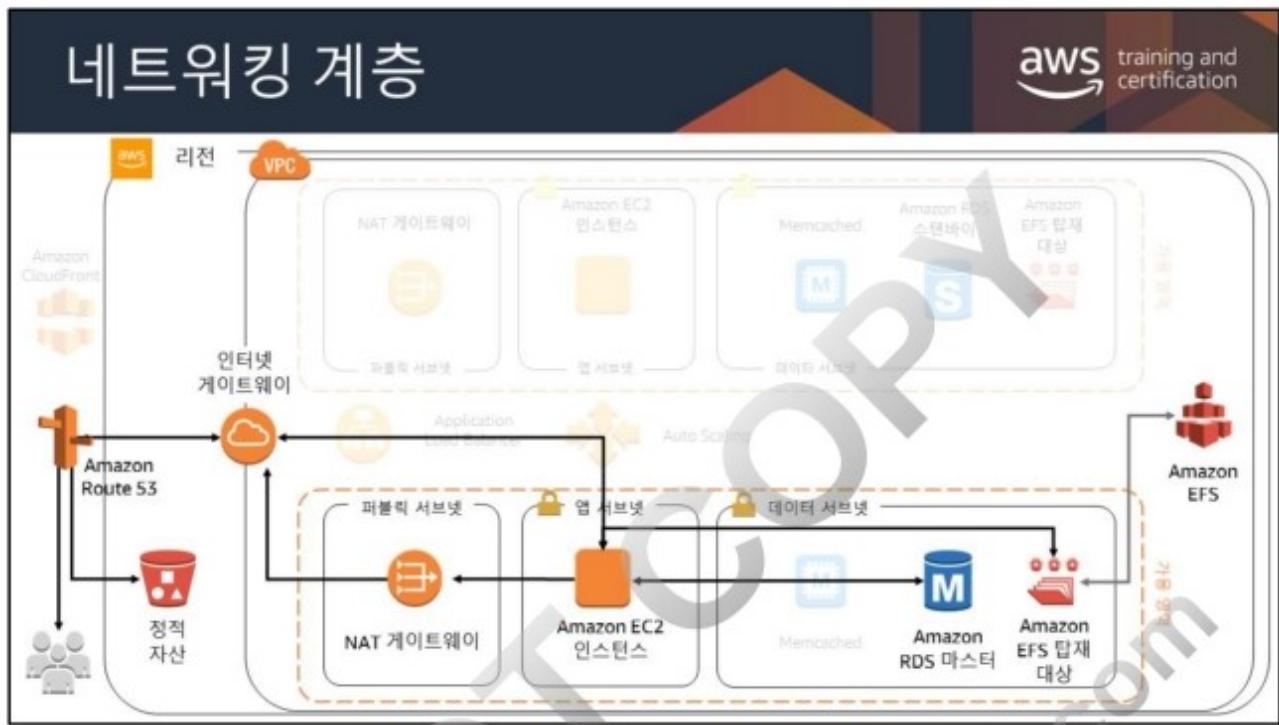
시간: 30분

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

The diagram illustrates a VPC (Virtual Private Cloud) network structure. At the top, a cloud icon labeled "VPC" contains two separate sections, each represented by a dashed-line box. The left section, labeled "Lab VPC", contains two subnets: "퍼블릭 서브넷 1" (IP range 10.0.0.0/24) and "퍼블릭 서브넷 2" (IP range 10.0.1.0/24). The right section contains two subnets: "프라이빗 서브넷 1" (IP range 10.0.2.0/23) and "프라이빗 서브넷 2" (IP range 10.0.4.0/23). Within these subnets, there are various AWS services and instances: an "App Server" (orange square icon), an "Amazon RDS DB Instance" (MySQL icon), and two "MySQL" databases. Each service is accompanied by its specific IP range and subnet name. Below the subnets, the text "가용 영역" (Available Region) is repeated twice.







수업이 끝나면 이 아키텍처 디어그램의 모든 구성 요소를 이해할 수 있습니다.
또한 마찬가지로 규모가 크고 강력한 자체 아키텍처 솔루션을 구축할 수 있습니다.

모듈 5



아키텍처 측면에서의 필요성

워크로드 격리를 제공하는 네트워크 환경에서 AWS 리소스를 배포하고 관리해야 합니다.

모듈 개요

- Amazon Virtual Private Cloud (VPC)
- 서브넷
- 게이트웨이
- 네트워크 보안

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



VPC란 무엇입니까?

VPC

AWS Cloud의 프라이빗 네트워크 공간

개발 테스트

워크로드에 대한 논리적 격리를 제공합니다.

리소스에 대한 사용자 지정 액세스 제어 및 보안 설정을 허용합니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

An infographic titled "VPC란 무엇입니까?" (What is VPC?). It features a large orange cloud icon labeled "VPC". Below it, text reads "AWS Cloud의 프라이빗 네트워크 공간" (Private network space in the AWS Cloud). To the right, two boxes labeled "개발" (Development) and "테스트" (Testing) are shown above the text "워크로드에 대한 논리적 격리를 제공합니다." (Provides logical separation for workloads). Further to the right, a user icon is connected to a shield icon, with the text "리소스에 대한 사용자 지정 액세스 제어 및 보안 설정을 허용합니다." (Allows custom access control and security settings for resources). The AWS logo and "training and certification" text are in the top right corner.

Amazon VPC 세부 사항

VPC는 AWS 계정 전용 가상 네트워크입니다.

IPv4 또는 IPv6 주소 범위에 존재합니다.

점유 리소스에 대한 특정 CIDR 범위를 생성할 수 있습니다.

인바운드 및 아웃바운드 트래픽에 대한 엄격한 액세스 규칙을 제공합니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon VPC (Amazon Virtual Private Cloud)는 클라우드의 네트워크 환경입니다. Amazon VPC는 AWS 리소스를 사용자가 정의한 가상 네트워크안에서 시작할 수 있게 합니다.

Amazon VPC는 사용자 본인의 IP 주소 범위 선택, 서브넷 작성, 라우팅 테이블 및 네트워크 게이트웨이 구성을 포함해 사용자의 환경과 리소스를 상호 격리할 때 이를 보다 효과적으로 제어할 수 있도록 설계되었습니다. VPC에서 IPv4와 IPv6을 모두 사용하여 리소스와 애플리케이션을 안전하고 쉽게 액세스할 수 있습니다. Virtual Private Cloud (VPC)는 사용자의 AWS 계정 전용 가상 네트워크입니다.

참고: 기본적으로 Amazon EC2와 Amazon VPC는 IPv4 주소 지정 프로토콜을 사용합니다. 인터넷을 통해 프라이빗 IPv4 주소에 연결할 수는 없지만, 전역적으로 고유한 퍼블릭 IPv4 주소를 인스턴스에 할당할 수는 있습니다. IPv6 CIDR 블록을 VPC와 서브넷에 연결하고 해당 블록의 IPv6 주소를 VPC의 리소스에 할당할 수도 있습니다. IPv6 주소는 퍼블릭이며 인터넷을 통해 연결할 수 있습니다.

VPC에서의 IP 주소 지정에 대한 자세한 내용은

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-ip-addressing.html>을

참조하십시오.

DO NOT COPY
zlagusdbs@gmail.com

VPC 배포

VPC는 22개의 AWS 리전 중 1개 리전에 배포됩니다.

VPC 리전 내 모든 가용 영역의 리소스를 호스팅할 수 있습니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

하나의 VPC 사용

aws training and certification

하나의 VPC가 적절한 사용 사례는 **제한적입니다**.

- 한 명 또는 매우 작은 팀이 관리하는 소규모 단일 애플리케이션
- 고성능 컴퓨팅
- 자격 증명 관리

대부분의 사용 사례에서는 인프라를 구성하는 데 2개의 기본 패턴을 사용합니다.

다중 VPC 및 복수 계정

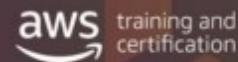
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

단일 VPC 환경이 여러 VPC에 걸쳐 분산된 환경보다 자연 시간이 짧으므로 고성능 컴퓨팅 환경(예: 물리 시뮬레이션)은 단일 VPC 내에서 가장 잘 작동할 수 있습니다.

자격 증명 관리 환경은 최적의 보안을 위해 하나의 VPC로 제한되는 것이 좋을 수 있습니다.

작은 팀이 지원하는 소규모 애플리케이션은 하나의 VPC를 사용하는 것이 가장 간편할 수 있습니다.

다중 VPC 패턴

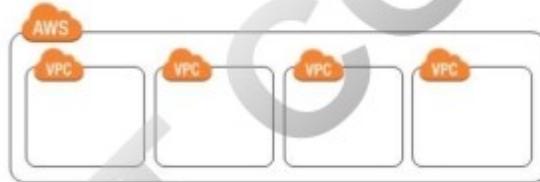


다음에 가장 적합:

- 단일 팀 또는 단일 조직(예: 관리형 서비스 공급자)
- 더 쉽게 표준 상태를 유지하고 액세스를 관리할 수 있는 제한된 팀

예외:

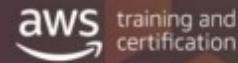
- 거버넌스 및 규정 준수 표준은 조직의 복잡성과 관계없이 워크로드 격리를 요구할 수 있습니다.



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

다중 VPC 패턴은 각 애플리케이션 환경의 모든 리소스 프로비저닝 및 관리를 완전히 제어하는 단일 팀 또는 조직에 적합합니다. 예를 들어, 대규모 전자 상거래 애플리케이션을 개발하는 단일 팀은 개발자가 개발/프로덕션 환경에 대한 전체 액세스 권한이 있을 때 이 패턴을 사용할 수 있습니다. 또한 테스트/프로덕션의 모든 리소스를 관리하는 관리형 서비스 공급자(MSP)의 경우, 이 패턴이 매우 일반적입니다.

복수 계정 패턴

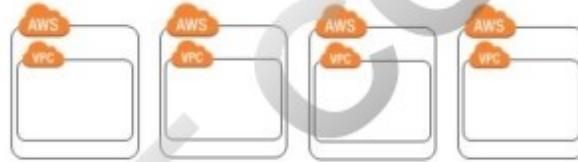


다음에 가장 적합:

- 대규모 조직 및 여러 IT 팀이 있는 조직
- 빠른 성장이 예상되는 중간 규모의 조직

그 이유는 무엇일까요?

- 액세스 및 표준 관리는 조직이 복잡할수록 더 어려울 수 있습니다.



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

다중 계정 패턴은 여러 팀에서 관리하는 애플리케이션을 배포하는 엔터프라이즈 고객 또는 조직에 가장 적합합니다. 예를 들어, 2개 이상의 팀을 지원하는 조직은 이 패턴을 사용하여, 개발 환경 리소스에는 전체 액세스 권한이 있지만, 프로덕션 환경 리소스에는 제한된 액세스 또는 전혀 액세스 권한이 없는 개발자를 지원할 수 있습니다.

VPC 제한

동일한 리전 또는 다른 리전에 여러 VPC를 보유할 수 있습니다.

The diagram illustrates VPC limits across two regions: eu-west-1 and us-east-2. In the eu-west-1 region, there are five VPC icons represented by orange clouds with the word 'VPC' inside. In the us-east-2 region, there are two VPC icons. A large watermark reading 'DO NOT COPY' diagonally across the slide also contains the URL 'zlagusdbs@gmail.com'.

eu-west-1

us-east-2

서비스 제한: 계정당 리전당 VPC 5개

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

동일한 리전 또는 다른 리전, 동일한 계정 또는 다른 계정에서 여러 VPC를 생성할 수 있습니다. 계정당 지원 가능한 VPC의 수는 한도가 있으므로 VPC의 서비스 제한을 숙지해야 합니다.

VPC 및 IP 주소 지정



- 각 VPC는 사용자가 지정하는 프라이빗 IP 주소의 범위를 예약합니다.
- 이러한 프라이빗 IP 주소는 해당 VPC에 배포된 리소스에서 사용할 수 있습니다.
- IP 범위는 CIDR (Classless Inter-Domain Routing) 표기법을 사용하여 정의됩니다.
- 고유 IP 주소 가져오기(BYOLP-Bring Your Own IP) 접두사 지원

예: 10.0.0.0/16 = 10.0.0.0에서 10.0.255.255까지의 모든 IP

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon VPC는 AWS 클라우드 내의 분리된 안전한 사설 공간입니다. 사용자는 자신이 정의한 이 가상 네트워크 공간안에서 AWS 리소스들을 시작할 수 있습니다. VPC를 생성하면 사용자는 VPC의 인스턴스가 사용할 사설 IP 주소를 직접 제공할 수 있습니다.

VPC는 듀얼 스택 모드로 작동할 수 있습니다 : 리소스는 IPv4, IPv6 또는 이들 두 가지 IP 모두를 통해 통신할 수 있습니다. IPv4 주소와 IPv6 주소는 서로 독립적입니다. VPC에서는 IPv4와 IPv6에 대해 별도로 라우팅 및 보안을 구성해야 합니다.

Amazon Virtual Private Cloud(VPC)에서는 고객이 자신의 퍼블릭 IP 주소 접두사를 AWS로 가져와서 사용할 수 있습니다. 고객 IP를 탄력적 IP 주소로 가져온 다음 동일한 방식으로 사용할 수 있습니다. 예를 들어 고객 IP를 Amazon EC2 인스턴스, 네트워크 로드 밸런서 및 NAT 게이트웨이에 연결할 수 있습니다. AWS를 통해 IP 주소 범위를 알리면 서비스의 다운타임을 최소화할 수 있으므로, 이는 특히 마이그레이션에 유용합니다.

또한 개별 IP 주소 또는 접두사를 화이트리스트에 추가할 필요가 있는 파트너와 고객이 사용하는 신뢰할 수 있는 IP 주소를 유지하는 데에도 유용합니다. 예를 들어 상업용 이메일은 IP 주소 평판에 의존합니다. BYOIP(Bring Your Own IP)를 사용하면 고객은 이미 신뢰할 수 있는 이메일 애플리케이션을 기준 전송 평판을 잃지 않고 AWS로 마이그레이션할 수 있습니다.

BYOIP 사용은 무료입니다. 탄력적 IP 주소와 달리 고객은 BYOIP로 가져온 연결되지 않은 IP 주소에 비용을 지불할 필요가 없습니다. BYOIP에 대한 자세한 내용은 다음을 참조하십시오. <https://aws.amazon.com/about-aws/whats-new/2018/10/announcing-the-general-availability-of-bring-your-own-ip-for-amazon-virtual-private-cloud/>.

CIDR 예

CIDR	총 IP
/28	16
...	...
/20	4,096
/19	8,192
/18	16,384
/17	32,768
/16	65,536

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

이 주소 집합을 CIDR (Classless Inter-Domain Routing) 블록 형태로 지정합니다(예. 10.0.0.0/16). 이것은 VPC의 기본 CIDR 블록입니다. 또한, /28 (16 IP 주소)과 /16 (65,536 IP 주소) 사이에서 네트워크의 블록 크기를 지정할 수도 있습니다.

Amazon VPC는 IPv4 및 IPv6 주소 지정을 지원하며, 이들 IP에 대해 상이한 CIDR 블록 크기 제한이 있습니다. 기본적으로 모든 VPC와 서브넷에는 IPv4 CIDR 블록이 있어야 합니다. 이러한 동작은 변경할 수 없습니다. IPv6 CIDR 블록을 VPC에 선택적으로 연결할 수 있습니다.

서브넷을 사용하여 VPC 분리

aws training and certification

서브넷은 리소스 그룹을 격리할 수 있는 VPC IP 주소 범위의 세그먼트 또는 파티션입니다.

예:

CIDR /22인 VPC는 총 1,024개의 IP를 포함합니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

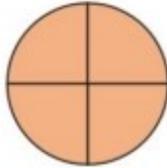
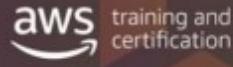
Amazon VPC를 사용하면 고객들이 가상 네트워크를 생성하고 이를 서브넷으로 분할할 수 있습니다. VPC 서브넷은 특정 가용 영역에 매핑됩니다. 따라서 서브넷 배치는 EC2 인스턴스를 여러 위치에 올바르게 분산할 수 있도록 보장하는 하나의 메커니즘입니다.

서브넷을 생성할 때는 VPC CIDR 블록의 하위 집합에 속하는 CIDR 블록을 해당 서브넷에 대해 지정합니다. 각 서브넷은 하나의 가용 영역 내에 모두 상주해야 하며, 다른 영역으로 확장할 수 없습니다.

이전에 설명한 대로 IPv6 CIDR 블록을 VPC에 할당하고 IPv6 CIDR 블록을 서브넷에 할당할 수도 있습니다.

VPC에서 IP 주소 지정에 관한 자세한 내용은 아래의 사이트를 각각 참조하십시오.
<https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html>
https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#vpc-sizing-ipv6

서브넷: 키 속성



- 서브넷은 VPC CIDR 블록의 하위 집합입니다.
- 서브넷 CIDR 블록은 중첩될 수 없습니다.
- 각 서브넷은 하나의 가용 영역 내에서만 존재합니다
- 가용 영역에 서브넷이 여러 개 포함될 수 있습니다.

AWS는 각 서브넷에서 5개의 IP 주소를 예약합니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS는 각 서브넷의 CIDR 블록에서 첫 IP 주소 4개와 마지막 IP 주소를 예약합니다.

AWS 설명서에서:

예를 들어, CIDR 블록이 10.0.0.0/24인 서브넷에서는 다음과 같은 5개의 IP 주소가 예약되어 있습니다.

- 10.0.0.0: 네트워크 주소
- 10.0.0.1: AWS에서 VPC 라우터용으로 예약
- 10.0.0.2: AWS에 의해 예약됨. DNS 서버의 IP 주소는 항상 VPC 네트워크 범위 +2에 위치합니다. 다만 우리는 각 서브넷 범위 +2의 위치도 예약합니다. 여러 개의 CIDR 블록이 있는 VPC의 경우, DNS 서버의 IP 주소는 기본 CIDR에 위치합니다. 자세한 내용은

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html#AmazonDNS를 참조하십시오.

- 10.0.0.3: 차후 사용을 위해 AWS에서 예약
- 10.0.0.255: 네트워크 브로드캐스트 주소. AWS는 VPC에서 브로드캐스트를 지원하지 않으므로 이 주소를 예약합니다.

라우팅 테이블: VPC 리소스 간에 트래픽 보내기

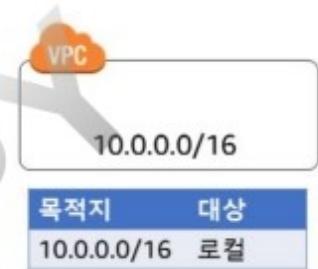
aws training and certification

라우팅 테이블:

- VPC 리소스 간에 트래픽을 연결하는 데 필요합니다.
- 각 VPC에는 주요(기본) 라우팅 테이블이 있습니다.
- 사용자 지정 라우팅 테이블을 생성할 수 있습니다.
- 모든 서브넷에는 연결된 라우팅 테이블이 있어야 합니다.

모범 사례: 각 서브넷에 대해 사용자 지정 라우팅 테이블 사용

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



라우팅 테이블은 네트워크 트래픽이 향하는 방향을 결정하는 데 사용되는 경로라고 부르는 규칙 세트를 포함합니다.

VPC를 생성하면, 자동으로 기본 라우팅 테이블이 생성됩니다. 처음에는 기본 라우팅 테이블(및 VPC의 모든 라우팅 테이블)에 단일 경로 즉, VPC 내 모든 리소스에 대하여 통신을 허용하는 로컬 경로만 포함되어 있습니다. 라우팅 테이블의 로컬 경로는 수정할 수 없습니다. VPC에서 인스턴스를 시작할 때마다 로컬 경로는 해당 인스턴스에 자동으로 적용됩니다. 라우팅 테이블에 새 인스턴스를 추가할 필요가 없습니다. VPC에 대한 사용자 정의 라우팅 테이블을 추가로 생성할 수 있습니다.

VPC에 있는 각 서브넷은 라우팅 테이블에 연결되어 있어야 합니다. 이 테이블이 서브넷에 대한 라우팅을 제어합니다. 서브넷을 특정 라우팅 테이블과 명시적으로 연결하지 않는 경우, 서브넷은 암시적으로 기본 라우팅 테이블과 연결되어 이를 사용합니다. 서브넷은 한 번에 하나의 라우팅 테이블에만 연결할 수 있지만, 여러 서브넷을 같은 라우팅 테이블에 연결할 수 있습니다.

각 서브넷에 대한 사용자 지정 라우팅 테이블을 사용하여 대상에 대해 세부적인 라우팅을 활성화합니다.

서브넷을 통해 허용되는 다양한 수준의 네트워크 격리

aws training and certification

퍼블릭 서브넷

서브넷을 사용하여 인터넷 액세스 접근성을 정의합니다.

퍼블릭 서브넷

- 퍼블릭 인터넷에 대한 인바운드/아웃바운드 액세스를 지원하도록 인터넷 게이트웨이에 대한 라우팅 테이블 항목을 포함합니다.

프라이빗 서브넷

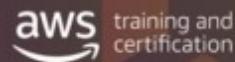
- 인터넷 게이트웨이에 대한 라우팅 테이블 항목이 없습니다.
- 퍼블릭 인터넷에서 직접 액세스할 수 없습니다.
- 일반적으로 제한된 아웃 바운드 퍼블릭 인터넷 액세스를 지원하기 위해 NAT 게이트웨이를 사용합니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

애플리케이션 또는 기능 티어(웹/앱/데이터 등)를 기준으로 서브넷을 정의하기보다는, 인터넷 접근성을 기준으로 서브넷을 구성해야 합니다. 이를 통해 퍼블릭 리소스와 프라이빗 리소스 간에 명확한 서브넷 수준의 격리를 정의할 수 있습니다.

참고: PCI 규정 준수 등 특정 상황에서 매우 민감한 데이터는 인터넷에 직접 또는 간접적으로 연결될 수 없는 경우, 이러한 서브넷을 "보호된" 서브넷이라고 부릅니다.

퍼블릭 서브넷에 인터넷 연결



인터넷 게이트웨이

- VPC의 인스턴스와 인터넷 간에 통신을 허용합니다.
- 기본적으로 가용성이 뛰어나고, 중복적이며, 수평적으로 확장됩니다.
- 인터넷으로 라우팅 가능한 트래픽에 대한 서브넷 라우팅 테이블에 대상을 제공합니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

인터넷 게이트웨이는 수평적 확장으로 이중화를 지원하는 고가용성 VPC 구성 요소로서 VPC의 인스턴스와 인터넷 간 통신이 가능한 이유도 인터넷 게이트웨이가 있기 때문입니다. 따라서 네트워크 트래픽에 가용성 위험이나 대역폭 제약이 발생하지 않습니다.

인터넷 게이트웨이를 사용하는 2가지 목적은 인터넷 라우팅 트래픽에 대한 VPC 라우팅 테이블의 대상을 제공하고 퍼블릭 IPv4 주소가 할당된 인스턴스에 대해 네트워크 주소 변환(NAT)을 수행하는 데 있습니다.

인터넷 게이트웨이는 IPv4 및 IPv6 트래픽을 지원합니다.

퍼블릭 서브넷에 인터넷 연결

인터넷 게이트웨이

- VPC의 인스턴스와 인터넷 간에 통신을 허용합니다.
- 기본적으로 가용성이 뛰어나고, 중복적이며, 수평적으로 확장됩니다.
- 인터넷으로 라우팅 가능한 트래픽에 대한 서브넷 라우팅 테이블에 대상을 제공합니다.

인터넷 게이트웨이

VPC 10.0.0.0/16

인터넷 게이트웨이

사용자

인터넷 게이트웨이

10.0.0.0/16

퍼블릭 라우팅 테이블

목적지	대상
10.0.0.0/16	로컬
0.0.0.0/0	<igw-id>

인스턴스 A
(퍼블릭 IP 보유)
10.0.10.0/24
퍼블릭 서브넷

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

프라이빗 서브넷에 인터넷 연결



NAT 게이트웨이

- 프라이빗 서브넷의 인스턴스가 인터넷 또는 다른 AWS 서비스로의 아웃바운드 트래픽을 시작하도록 활성화합니다.
- 프라이빗 인스턴스가 인터넷에서 인바운드 트래픽을 수신하는 것을 차단합니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

프라이빗 서브넷에 인터넷 연결

NAT 게이트웨이

- 프라이빗 서브넷의 인스턴스가 인터넷 또는 다른 AWS 서비스로의 아웃바운드 트래픽을 시작하도록 활성화합니다.
- 프라이빗 인스턴스가 인터넷에서 인바운드 트래픽을 수신하는 것을 차단합니다.

퍼블릭 라우팅 테이블

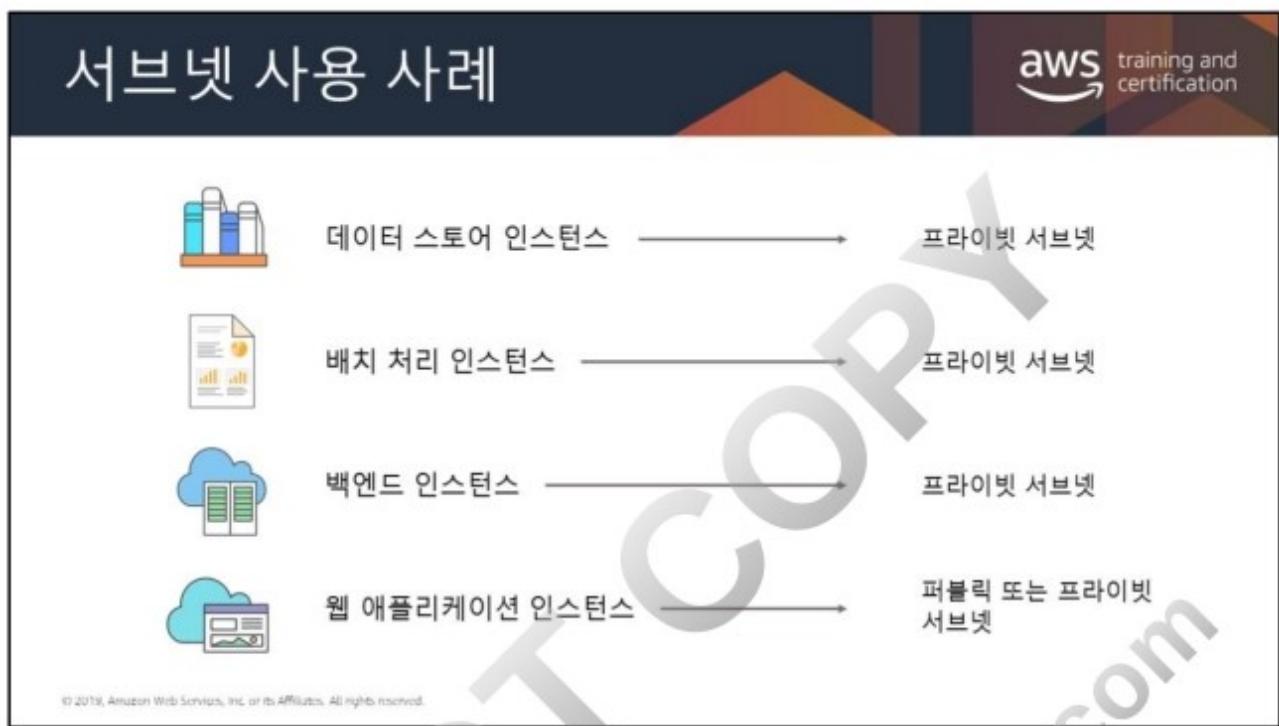
목적지	대상
10.0.0.0/16	로컬
0.0.0.0/0	<igw-id>

프라이빗 라우팅 테이블

목적지	대상
10.0.0.0/16	로컬
0.0.0.0/0	<nat-id>

VPC 사용자 인터넷 게이트웨이 10.0.0.0/16 VPC NAT 게이트웨이 10.0.10.0/24 사용자 프라이빗 인스턴스 (프라이빗 IP 보유) 10.0.20.0/24 프라이빗 서브넷

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



웹 티어 인스턴스를 퍼블릭 서브넷에 넣을 수 있지만 AWS는 퍼블릭 서브넷에 배치된 로드 밸런서 뒷쪽의 프라이빗 서브넷 내부에 이 인스턴스를 배치할 것을 권장합니다. 일부 환경에서는 웹 애플리케이션 인스턴스를 탄력적 IP에 직접 연결해야 하며(탄력적 IP를 로드 밸런서에 연결할 수 있더라도), 그런 경우 웹 애플리케이션 인스턴스는 퍼블릭 서브넷에 있어야 합니다. 로드 밸런서는 이후 모듈에서 자세히 다루기로 하겠습니다.

서브넷 권장 사항

작은 크기보다는 더 큰 크기의 서브넷을 고려합니다(/24 이상).

워크로드 배치 간소화:

- 워크로드를 10개의 작은 서브넷 중 어디에 배치할지 선택하는 것이 1개의 큰 서브넷보다 더 복잡합니다.

IP를 낭비하거나 IP가 부족할 확률이 낮음:

- 서브넷에서 사용 가능한 IP가 부족한 경우, 해당 서브넷에 IP를 추가할 수 없습니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

기본 서브넷 구성

aws training and certification

서브넷을 설정하기 위한 가장 좋은 방법을 잘 모르는 경우:

가용 영역당 1개의 퍼블릭 서브넷과 1개의 프라이빗 서브넷으로 시작합니다.

VPC 10.0.0.0/21 (10.0.0.0-10.0.7.255)

퍼블릭 서브넷
퍼블릭 서브넷
프라이빗 서브넷
프라이빗 서브넷
가용 영역 A
가용 영역 B

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Auto Scaling 시 충분한 IP 주소 용량을 제공하기 위해 가용 영역당 퍼블릭 서브넷과 프라이빗 서브넷을 하나씩 사용할 것을 고려하십시오.

서브넷은 인터넷 접근성을 정의하는 데 사용되어야 하므로 가용 영역당 1개의 퍼블릭 서브넷과 1개의 프라이빗 서브넷보다 더 많은 서브넷을 구성할 이유는 없습니다. 이러한 환경에서는 인터넷에 직접 액세스해야 하는 모든 리소스(퍼블릭 로드 밸런서, NAT 인스턴스, 배스천 호스트 등)는 퍼블릭 서브넷으로 가고, 모든 다른 인스턴스는 프라이빗 서브넷으로 갑니다(예외: 직접적 또는 간접적으로 인터넷에 대한 액세스가 전혀 필요 없는 리소스는 별도의 프라이빗 서브넷으로 갑니다).

일부 환경에서는 리소스 "티어" 간에 분리 계층을 생성하는데 서브넷을 사용하려고 시도합니다(예: 백엔드 애플리케이션 인스턴스와 데이터 소스를 개별 프라이빗 서브넷에 추가). 이러한 사례에서는 각 서브넷에 필요한 호스트 수를 좀 더 정확히 예측해야 하므로, IP가 빠르게 고갈되거나, 다른데 사용할 수 있었을 미사용 IP가 너무 많이 남을 가능성이 높습니다.

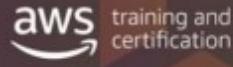
서브넷은 네트워크 ACL 규칙을 사용하여 리소스 간에 매우 기본적인 분리 요소를 제공할 수 있습니다. 반면에 보안 그룹은 인프라를 너무 복잡하게 만들고, IP를 낭비하거나 IP가 부족할 위험 없이 리소스 간에 좀 더 정교한 수준의 트래픽 제어를 제공할 수 있습니다. 이 접근 방식에서는 VPC에서 필요한 퍼블릭 IP와 프라이빗 IP 수만 예측하고 서브넷 내 리소스 간에 분리는 다른 리소스를 사용하여 생성하면 됩니다.

DO NOT COPY
zlagusdbs@gmail.com



AWS의 리소스 대부분은 프라이빗 서브넷에서 호스팅할 수 있으며, 필요에 따라 인터넷에 대한 제어된 액세스를 위해 퍼블릭 서브넷을 사용할 수 있습니다. 때문에 퍼블릭 서브넷과 비교하여 프라이빗 서브넷에 훨씬 더 많은 IP를 제공하도록 서브넷을 계획해야 합니다. 아키텍처를 계획할 때, VPC에서 필요한 호스트 수가 몇 개인지와 그중 몇 개를 프라이빗 서브넷에 배치할 수 있는지를 예측하는 것이 중요합니다. 프라이빗 서브넷에 퍼블릭 리소스를 배치하는 데 대한 전략을 뒤에서 좀 더 상세히 다루기로 하겠습니다.

탄력적 네트워크 인터페이스



**탄력적 네트워크 인터페이스는
가상 네트워크 인터페이스입니다.**
동일한 가용영역 안에서 EC2 인스턴스
간에 이동할 수 있습니다.

새 인스턴스로 이동하면 네트워크 인터페이스는
다음을 유지합니다.

- 프라이빗 IP 주소
- 탄력적 IP 주소
- MAC 주소

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

탄력적 네트워크 인터페이스는 VPC에서 인스턴스에 장착할 수 있는 가상 네트워크 인터페이스입니다. 네트워크 인터페이스를 만들고 인스턴스에 연결하는 것은 물론, 인스턴스에서 분리한 후 다른 인스턴스에 연결할 수도 있습니다. 프라이빗 IP 주소, 탄력적 IP 주소 및 MAC 주소를 포함한 네트워크 인터페이스의 속성은 네트워크 인터페이스를 따르는데, 그 이유는 이 인터페이스가 인스턴스에 연결되거나 혹은 인스턴스에서 분리되었다가 다른 인스턴스에 다시 연결되기 때문입니다. 네트워크 인터페이스를 인스턴스 간에 이동하면 네트워크 트래픽이 새 인스턴스로 리디렉션됩니다. VPC의 각 인스턴스에는 사용자 VPC의 IP 주소 범위에서 프라이빗 IP 주소가 할당된 기본 네트워크 인터페이스(primary network interface)가 있습니다. 인스턴스의 기본 네트워크 인터페이스는 분리할 수 없습니다. 추가 네트워크 인터페이스를 생성하고 연결할 수는 있습니다.

다음 작업을 수행하려는 경우, 여러 네트워크 인터페이스를 하나의 인스턴스에 연결하면 유용합니다.

- 관리 네트워크 생성
- VPC에서 네트워크 및 보안 어플라이언스 사용
- 별도의 서브넷에 있는 워크로드/역할로 이중 홈 인스턴스 생성
- 저예산 고가용성 솔루션 생성

한 서브넷의 네트워크 인터페이스를 동일 VPC에 있는 다른 서브넷의 인스턴스에 연결할 수 있지만, 네트워크 인터페이스와 인스턴스가 둘 다 동일 가용 영역 안에 상주해야 합니다. 이는 트래픽을 다른 가용 영역으로 리디렉션하려는 일부 DR 시나리오에서 사용이 제한됩니다. 그래도 이것은 동일한 서브넷 또는 가용 영역의 대기 VM으로 장애 조치를 수행할 필요가 있는 비교적 덜 파국적인 시나리오에서 유용합니다.

DO NOT COPY
zlagusdbs@gmail.com

탄력적 네트워크 인터페이스

aws training and certification

인스턴스에 네트워크 인터페이스가 두 개 이상 있는 이유는 무엇입니까?

요구 사항:

- 관리 네트워크 생성
- VPC에서 네트워크 및 보안 어플라이언스 사용
- 별도의 서브넷에 있는 워크로드/역할로 이중 홈 인스턴스 생성

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

다음 작업을 수행하려는 경우, 여러 네트워크 인터페이스를 하나의 인스턴스에 연결하면 유용합니다.

- 관리 네트워크 생성
- VPC에서 네트워크 및 보안 어플라이언스 사용
- 별도의 서브넷에 있는 워크로드/역할로 이중 홈 인스턴스 생성
- 저예산 고가용성 솔루션 생성



네트워크 인터페이스를 사용하여 관리 네트워크를 생성할 수 있습니다. 이 시나리오에서는 인스턴스의 기본 네트워크 인터페이스(eth0)가 퍼블릭 트래픽을 처리하고, 보조 네트워크 인터페이스(eth1)는 백엔드 관리 트래픽을 처리하며 VPC에서 액세스 제어가 더욱 제한되는 별도의 서브넷에 연결됩니다.

로드 밸런서 뒤에 있거나 없을 수 있는 퍼블릭 인터페이스에는 인터넷에서 서버에 액세스할 수 있도록 허용(예: 0.0.0.0/0 또는 로드 밸런서에서 TCP 포트 80 및 443을 허용)하는 보안 그룹이 연결되어 있는 반면, 프라이빗 인터페이스에는 VPC 내 또는 인터넷에서 허용된 IP 주소 범위, VPC 내 프라이빗 서브넷 또는 가상 프라이빗 게이트웨이에서만 SSH 액세스를 허용하는 보안 그룹이 연결되어 있습니다.

탄력적 IP 주소



- 인스턴스 또는 네트워크 인터페이스에 연결할 수 있습니다.
- 즉시 트래픽을 재연결하고 전송할 수 있습니다.
- AWS 리전당 5개가 허용됩니다.
- BYOIP (Bring Your Own IP) 주소를 생성할 수 있습니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

탄력적 IP 주소(EIP)는 동적 클라우드 컴퓨팅을 위해 설계된 고정 퍼블릭 IPv4 주소입니다. 계정의 어떤 VPC에 대해서든 탄력적 IP 주소를 인스턴스 또는 네트워크 인터페이스와 연결할 수 있습니다. 탄력적 IP 주소로 주소를 VPC의 다른 인스턴스에 신속하게 다시 매핑하여 인스턴스의 장애를 숨길 수 있습니다. 탄력적 IP 주소를 인스턴스와 직접 연결하는 대신 네트워크 인터페이스에 연결하면 네트워크 인터페이스의 모든 속성을 한 번에 한 인스턴스에서 다른 인스턴스로 이동할 수 있다는 이점이 있습니다.

하나의 인스턴스에서 다른 인스턴스로 탄력적 IP 주소를 이동할 수 있습니다. 인스턴스는 동일한 VPC 또는 다른 VPC에 위치할 수 있습니다. 탄력적 IP 주소는 VPC의 인터넷 게이트웨이를 통해 액세스할 수 있습니다. VPC와 네트워크 간에 VPN 연결을 설정한 경우, VPN 트래픽은 인터넷 게이트웨이가 아닌 가상 프라이빗 게이트웨이를 통과하기 때문에 탄력적 IP 주소에 액세스할 수 없습니다.

탄력적 IP 주소는 5개로 제한되며, 이를 절약하기 위해 NAT 디바이스를 사용할 수 있습니다. 인스턴스 장애 시, 주소를 다른 인스턴스로 매핑하고 다른 모든 노드와의 통신에서 DNS 호스트 이름을 사용하려면 기본적으로 탄력적 IP 주소를 사용할 것을 적극 권장합니다.

BYOIP (Bring Your Own IP) 주소 접두사에서 탄력적 IP 주소를 생성하여 EC2 인스턴스, Network Load Balancer 및 NAT Gateway와 같은 AWS 리소스에 사용할 수 있습니다. BYOIP 주소 접두사에서 생성하는 탄력적 IP 주소는 Amazon에서 가져오는 탄력적 IP 주소와 정확히 동일하게 작동합니다.

인스턴스를 중지해도 탄력적 IP 주소는 인스턴스와 연결된 상태를 유지합니다. IPv6에 대한 탄력적 IP 주소는 현재 지원되지 않습니다.

DO NOT COPY
zlagusdbs@gmail.com

탄력적 IP 주소

aws training and certification



- 인스턴스 또는 네트워크 인터페이스에 연결할 수 있습니다.
- 즉시 트래픽을 재연결하고 전송할 수 있습니다.
- AWS 리전당 5개가 허용됩니다.



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



DO NOT COPY
zlagusdbs@gmail.com

보안 그룹



- AWS 리소스에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 **가상 방화벽**
- 트래픽은 모든 IP 프로토콜, 포트 또는 IP 주소로 **제한**될 수 있습니다.
- 규칙은 **상태 저장**입니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Amazon VPC는 인스턴스의 송수신 트래픽을 모두 필터링할 수 있는 완전한 방화벽 솔루션을 지원합니다. 기본 그룹은 동일한 그룹 내의 다른 구성원으로부터의 인바운드 통신과 모든 대상에 대한 아웃바운드 통신을 허용합니다. 트래픽은 모든 IP 프로토콜, 서비스 포트, 원본/대상 IP 주소(개별 IP 또는 Classless Inter-Domain Routing (CIDR) 블록)에 의해 제한될 수 있습니다.

상태 저장 규칙 관련: 예를 들어 집 컴퓨터에서 인스턴스에 대한 ICMP 펑 명령을 시작하고, 인바운드 보안 그룹 규칙이 ICMP 트래픽을 허용한 경우, 연결에 대한 정보(포트 정보 포함)가 추적됩니다. 펑 명령에 대한 인스턴스의 응답 트래픽은 새로운 요청으로 추적되지 않고 대신 설정된 연결로 처리되므로 아웃바운드 보안 그룹 규칙이 아웃바운드 ICMP 트래픽을 제한하는 경우에도 인스턴스 외부로의 트래픽 흐름이 허용됩니다.

모든 트래픽 흐름이 추적되지는 않습니다. 보안 그룹 규칙이 모든 트래픽(0.0.0.0/0)에 대한 TCP 또는 UDP 흐름을 허용하고, 반대 방향에 이에 상응하는 규칙이 응답 트래픽을 허용하는 경우, 해당 트래픽 흐름은 추적되지 않습니다. 따라서 응답 트래픽은 응답 트래픽을 허용하는 인바운드 또는 아웃바운드 규칙을 기준으로 흐름이 허용되며, 추적 정보에 포함되지 않습니다.

보안 그룹: 기본 설정

aws training and certification

새 보안 그룹:

모든 인바운드
트래픽 차단

모든 아웃바운드
트래픽 허용

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

기본적으로 보안 그룹은 모든 아웃바운드 트래픽을 허용하는 아웃바운드 규칙을 포함합니다. 규칙을 제거하고 특정 아웃바운드 트래픽만 허용하는 아웃바운드 규칙을 추가할 수 있습니다. 보안 그룹에 아웃바운드 규칙이 없는 경우, 인스턴스에서 시작하는 아웃바운드 트래픽은 허용되지 않습니다.

트래픽은 프로토콜, 서비스 포트 및 소스 IP 주소(개별 IP 또는 CIDR 블록) 또는 보안 그룹에 의해 제한 될 수 있습니다.

보안 그룹은 다른 클래스의 인스턴스에 대해 서로 다른 규칙을 설정하도록 구성할 수 있습니다. 기존의 3계층 웹 애플리케이션을 예로 들어 보겠습니다. 웹 서버 그룹에는 인터넷에 개방된 80번 포트(HTTP) 및/또는 443번 포트(HTTPS)가 있을 수 있습니다. 애플리케이션 서버 그룹에는 웹 서버 그룹에만 액세스할 수 있는 8000번 포트(애플리케이션별)가 있을 수 있습니다. 데이터베이스 서버 그룹에는 애플리케이션 서버 그룹에만 개방된 3306번 포트(MySQL)가 있을 수 있습니다. 세 그룹 모두 포트 22 (SSH)에 대한 관리 액세스는 허용되나, 고객의 기업 네트워크에서만 가능합니다. 이 메커니즘을 이용하면 매우 안전한 애플리케이션을 배포할 수 있습니다.

보안 그룹: 트래픽 제어

aws training and certification

대부분 조직은 각 기능 티어에 대한 인바운드 규칙으로 보안 그룹을 생성합니다.

The diagram illustrates a security group rule within a private subnet. It shows two orange boxes labeled '앱' (App) connected by a blue line, representing an Application Layer security group. Below them is a blue box labeled '데이터' (Data) with an 'M' icon, representing a Web Layer security group. A red line connects the bottom of the App group to the top of the Data group. To the right, two arrows point from the groups to text labels: '앱 티어 보안 그룹' (Application Layer security group) and '웹 티어 보안 그룹' (Web Layer security group). The entire setup is enclosed in a box labeled '프라이빗 서브넷' (Private Subnet) with a lock icon at the top left.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



이 슬라이드는 보안 그룹 체인의 예입니다. 트래픽이 상위 티어에서 하위 티어로만 흐른 후 다시 반대로 흐르도록 인바운드와 아웃바운드 규칙이 설정됩니다. 보안 그룹은 한 티어에서 발생한 보안 위반으로 손상된 클라이언트에 서브넷 전체의 모든 리소스에 대한 액세스가 자동으로 제공되는 것을 방지하는 방화벽 역할을 합니다.

네트워크 ACL(액세스 제어 목록)

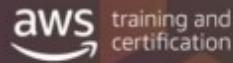


- 서브넷 경계의 방화벽
- 기본적으로 모든 인바운드 및 아웃바운드 트래픽을 허용합니다.
- 상태 비저장으로 인바운드 및 아웃바운드 트래픽 모두에 대한 명시적인 규칙이 필요합니다.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

DO NOT COPY
zlagusdbs@gmail.com

네트워크 ACL(액세스 제어 목록)



특정 네트워크 보안
요구 사항에서 권장됩니다.

- 서브넷 경계의 방화벽
- 모든 인바운드 및 아웃바운드 트래픽을 허용합니다 (VPC의 기본 NACL)
- 상태 비저장이므로 인바운드 및 아웃바운드 트래픽 모두에 대한 명시적인 규칙이 필요합니다.



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

사용자 지정 네트워크 ACL을 생성하여 서브넷과 연결할 수 있습니다. 기본적으로 각 사용자 지정 네트워크 ACL은 규칙을 추가하기 전에는 모든 인바운드 및 아웃바운드 트래픽을 거부합니다.