

AWS Network Services:

VPC, ELB, Route 53

Hyunchan, Park

<http://oslab.jbnu.ac.kr>

Division of Computer Science and Engineering

Jeonbuk National University

학습 내용

- AWS Network Services
- AWS VPC
- 실습: Rebuild the whole system!



(시작 전에..참고) 실패한 비용 관리

서비스 ▾ 리소스 그룹 ▾ ★

대시보드
청구서
비용 탐색기
예산
보고서
비용 할당 태그
결제 방법
결제 내역
통합 결제
기본 설정
크레딧
세금 설정
DevPay

비용 탐색기

비용 탐색기 시작

소비를 그래프로 그려 시각화하고 분석합니다. 날짜 범위, 서비스, 태그 또는 조합을 지정해 표시되는 내용을 필터링합니다. [자세히 알아보기](#)

미리 구성된 보기

일반적인 소비 질의에 답하기 위해 이미 설정된 보기로 빠르게 시작합니다. 여기에서 보기를 사용자 지정합니다.

[서비스별 월별 소비 보기](#)
지난 3개월 동안의 월별 소비를 AWS 서비스가 그룹화한 것입니다.

[연결된 계정별 월별 소비 보기](#)
지난 3개월 동안의 월별 소비를 연결된 계정이 그룹화한 것입니다. 통합 결제의 지급 계정만 사용할 수 있습니다.

[일별 소비 보기](#)
지난 60일간 일일 소비



(실패한) 비용 관리

NatGateway: 하루 \$1.42 에 세금이 붙어 \$1.56



Cost Explorer > Saved Reports > Daily costs

What's New

2017-08-09: AWS Marketplace cost and usage data is included by default in AWS Cost Explorer. Using the new Billing Entity filtering dimension, you can restrict your data to only AWS Marketplace costs and usage, or dive deeper into a particular product using the Service filtering dimension. [Learn more.](#)

Save as...

Reports ▾

New report

Daily costs

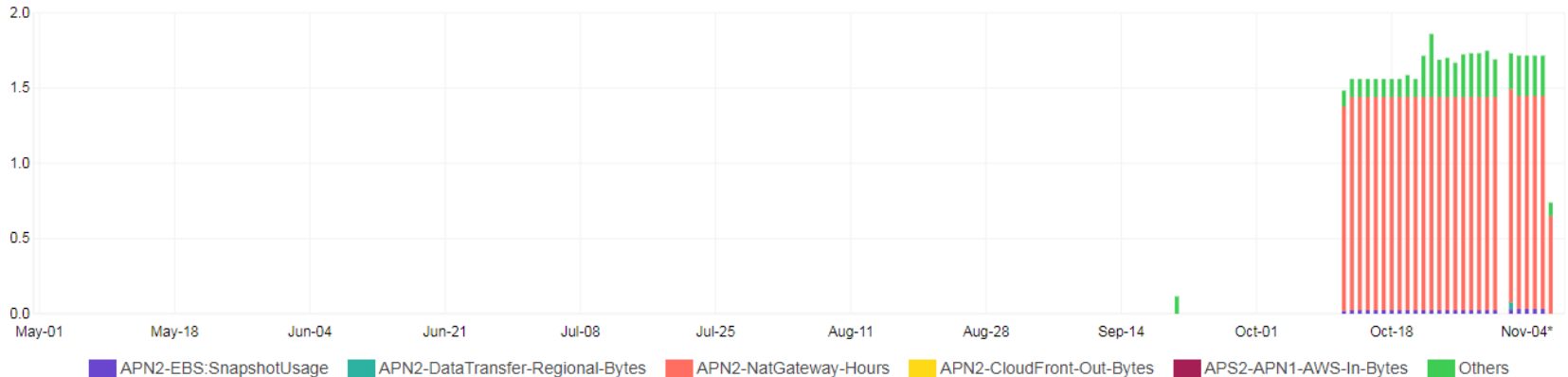
Last 6 Months ▾

Daily ▾

Group by: Usage Type ▾

Stack ▾

Costs (\$)



(실패한) 비용 관리

NatGateway: 윈도우 RDP 때문에 실험하다가 커둔 채로 놔둠

VPC 대시보드

VPC로 필터링:

VPC 선택

가상 프라이빗 클라우드

VPCs

서브넷

라우팅 테이블

인터넷 게이트웨이

외부 전용 인터넷 게이트웨이

DHCP 옵션 세트

탄력적 IP

엔드포인트

NAT 게이트웨이

피어링 연결

NAT 게이트웨이 생성

작업

태그 및 속성별 필터 또는 키워드별 검색

	Name	NAT 게이트웨이 ID	상태	상태 메시지	탄력적 IP 주소	프라이빗 IP 주소	네트워크 인터페이스
		nat-02ac7607d0f5...	사용 가능	-	13.124.184.0	172.31.12.138	eni-57b6a40b



(실패한) 비용 관리

NAT 게이트웨이 요금

VPC에 NAT 게이트웨이를 생성하는 경우, 프로비저닝되고 사용 가능한 NAT에 대해 "NAT 게이트웨이 시간"당 요금이 청구됩니다. 데이터 처리 요금은 트래픽 소스나 대상과 관계없이 NAT 게이트웨이를 통해 처리된 각 기가바이트에 적용됩니다. 1시간 미만의 각 NAT 게이트웨이 사용 시간은 1시간으로 청구됩니다. 또한 NAT 게이트웨이를 통해 전송된 모든 데이터에 대한 표준 AWS 데이터 전송 요금도 발생합니다. NAT 게이트웨이에 대한 요금이 청구되지 않도록 하려면 AWS Management Console, 명령줄 인터페이스 또는 API를 사용하여 NAT 게이트웨이를 삭제하면 됩니다.

리전	NAT 게이트웨이당 요금(USD/시간)	처리된 데이터 GB당 요금(USD)
미국 동부(버지니아 북부)	0.045	0.045
미국 동부(오하이오)	0.045	0.045
미국 서부(오레곤)	0.045	0.045
미국 서부(캘리포니아 북부)	0.048	0.048
캐나다(중부)	0.050	0.050
EU(아일랜드)	0.048	0.048
EU(런던)	0.050	0.050
EU(프랑크푸르트)	0.052	0.052
아시아 태평양(싱가포르)	0.059	0.059
아시아 태평양(도쿄)	0.062	0.062
아시아 태평양(서울)	0.059	0.059
아시아 태평양(시드니)	0.059	0.059
아시아 태평양(뭄바이)	0.056	0.056
남아메리카(상파울루)	0.093	0.093



(실패한) 비용 관리

- EIP, EBS 등등 이제까지 돈 많이 냈습니다!
- 실제로 AWS 등 클라우드 서비스를 이용할 때는 비용 관리가 대단히 큰 비중을 차지함
- 가격 정책 등을 철저히 숙지하고,
- 전체 현황을 관리할 수 있는 시스템을 구축해놓고 진행해야 함



AWS Network Services



AWS Network services

Amazon VPC

Virtual Private Cloud

자체 프라이빗 가상 네트워크를 통해 클라우드 리소스를 격리

Elastic Load Balancing

Load Balancing

클라우드에서 여러 Amazon EC2 인스턴스 전체에 애플리케이션 트래픽을 자동으로 분산

Amazon Route 53

Domain Name Service(DNS)

사용자 요청을 AWS 리소스로 연결할 수 있는 가용성과 확장성이 뛰어난 클라우드 DNS

AWS Direct Connect

AWS로의 전용 네트워크 연결

사용자 네트워크와 Amazon VPC 간의 전용 네트워크 연결



AWS Direct Connect

- 사용자 서버에서 AWS로 전용 네트워크 연결을 설정
 - AWS와 사용자의 데이터 센터, 사무실, 또는 코로케이션 환경 사이에 프라이빗 연결을 설정
 - 인터넷 연결이 아님
 - 네트워크 비용을 줄이고, 대역폭 처리량을 향상하며, 인터넷 기반 연결보다 일관된 네트워크 경험을 제공
- 사용자 서버에서 AWS 프라이빗 리소스에 액세스 가능
 - 예: 프라이빗 IP 공간을 사용하는 Amazon Virtual Private Cloud(VPC)에서 실행되고 있는 Amazon EC2 인스턴스



AWS Direct Connect: Pricing

- 포트 요금 + 데이터 송신 요금

용량	포트-시간 요금(일본을 제외한 모든 AWS Direct Connect 로케이션)	포트-시간 요금(일본)
50M	시간당 0.03 USD	시간당 0.029 USD
100M	시간당 0.06 USD	시간당 0.057 USD
200M	시간당 0.08 USD	시간당 0.076 USD
300M	시간당 0.12 USD	시간당 0.114 USD
400M	시간당 0.16 USD	시간당 0.152 USD
500M	시간당 0.20 USD	시간당 0.190 USD
1G*	시간당 0.33 USD	시간당 0.314 USD
2G*	시간당 0.66 USD	시간당 0.627 USD
5G*	시간당 1.65 USD	시간당 1.568 USD
10G*	시간당 2.48 USD	시간당 2.361 USD

KINX 서울과 아시아 태평양(서울) 리전 간

데이터 송신 – 로컬 리전 GB당 0.041 USD

데이터 송신 – 원격 리전 해당 사항 없음

LG U+ Pyeong-Chon Mega Center, Seoul과 아시아 태평양(서울) 리전 간

데이터 송신 – 로컬 리전 GB당 0.041 USD

데이터 송신 – 원격 리전 해당 사항 없음



참고 자료

- AWS VPC 소개
 - <https://aws.amazon.com/ko/vpc/?hp=tile&so-exp=below>
- AWS VPC 시작하기
 - <https://aws.amazon.com/ko/vpc/?hp=tile&so-exp=below>
- VPC Deep Dive (김상필 AWS solutions architect)
 - https://www.slideshare.net/awskorea/vpc-deep-dive?from_action=save



AWS VPC (Virtual Private Cloud)



Network

- Cloud network service
 - 사용자의 가상 컴퓨팅 자원 간의 가상 네트워크를 구성하는 서비스
 - 기본: IP 주소 범위, 서브넷, 라우팅, 게이트웨이 구성 등
 - 확장: VPN, NAT 등
- AWS Network
 - Private: AWS 내부에서만 사용 가능한 주소
 - 집 공유기에 연결된 내 노트북 IP (192.168.0.22)
 - Public: AWS 외부에서 연결 가능한 주소
 - 내 노트북으로 port forwarding 을 설정해 외부에서 접속하도록 한 경우
 - 외부 -> 공유기 (114.72.x.x / 192.168.0.1) -> 노트북 (114.72.x.x / 192.168.0.22)

AWS VPC (Virtual Private Cloud)

- VPC 서비스
 - Amazon Web Services(AWS) 클라우드에 논리적으로 격리된 가상 네트워크를 정의하고, 그 내부에 AWS 리소스를 배치, 사용할 수 있음
 - (Virtual IDC: Internet Data Center 라고 생각할 수 있음)
- 기능
 - IP 주소 범위 선택, 서브넷 생성, 라우팅 테이블 및 네트워크 게이트웨이 구성 등 가상 네트워킹 환경을 제어
 - IPv4, v6 지원
 - 보안 기능 제공 (filtering, access control, h/w isolation)
- 비용: 무료
 - VPN, NAT 서비스 유료
 - <https://aws.amazon.com/ko/vpc/pricing/>

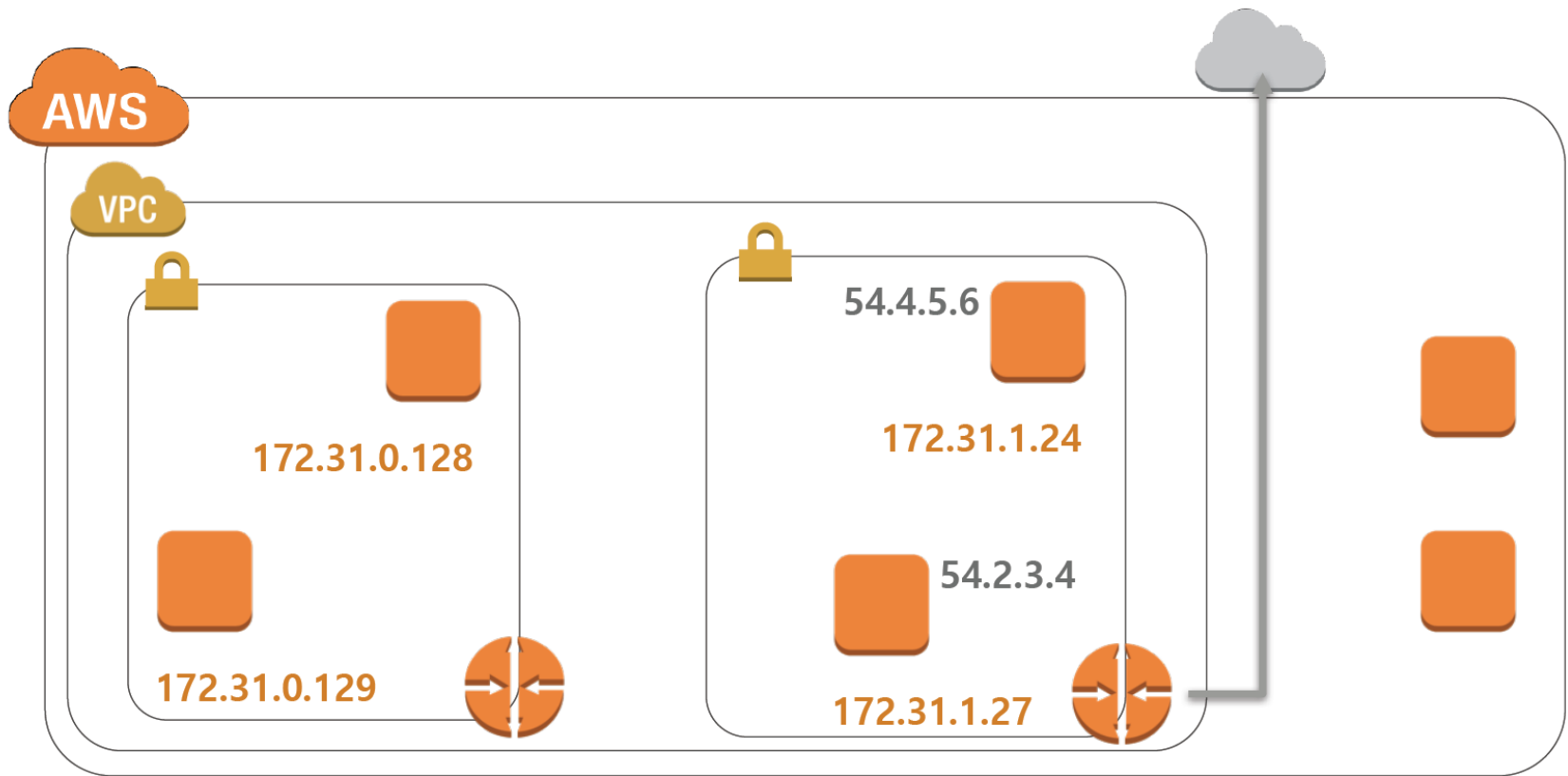


EC2 Instance



Webinars





VPC(Virtual Private Cloud)



Webinars



VPC를 이용한 네트워크 구성 예

- 간단한 공용 웹 사이트 호스팅
 - 블로그 또는 간단한 웹 사이트와 같은 기본 웹 애플리케이션을 VPC에 호스팅
 - 웹 서버가 인터넷의 인바운드 HTTP 및 SSL 요청에 응답하도록 허용
 - 동시에 웹 서버가 인터넷에 대한 아웃바운드 연결을 시작하지 못하도록 하는 보안 그룹 규칙을 만들어 웹 사이트를 보호
 - 타 서버로 능동적으로 접근하지 못하게 하여 DDoS 등에 좀비 PC로 이용되는 것을 방지함

VPC를 이용한 네트워크 구성 예

- 다중 계층 웹 애플리케이션 호스팅
 - 웹 서버, 애플리케이션 서버 및 데이터베이스 간에 액세스 및 보안 제한을 엄격하게 적용
 - 2개의 서브넷: 공개적으로 액세스할 수 있는 서브넷과 비공개로 액세스할 수 있는 서브넷
 - Public subnet: 웹 서버
 - Private subnet: 어플리케이션 서버, DB
 - Outbound access: NAT 게이트웨이 사용 (management console, update 등)
 - 서버와 서브넷 사이의 액세스를 제어
 - 웹 서버가 (혹은 웹 서버만) App 서버 및 DB를 정상적으로 사용하도록,
 - 네트워크 액세스 제어 목록과 보안 그룹에서 제공하는 인바운드 및 아웃바운드 패킷 필터링을 사용

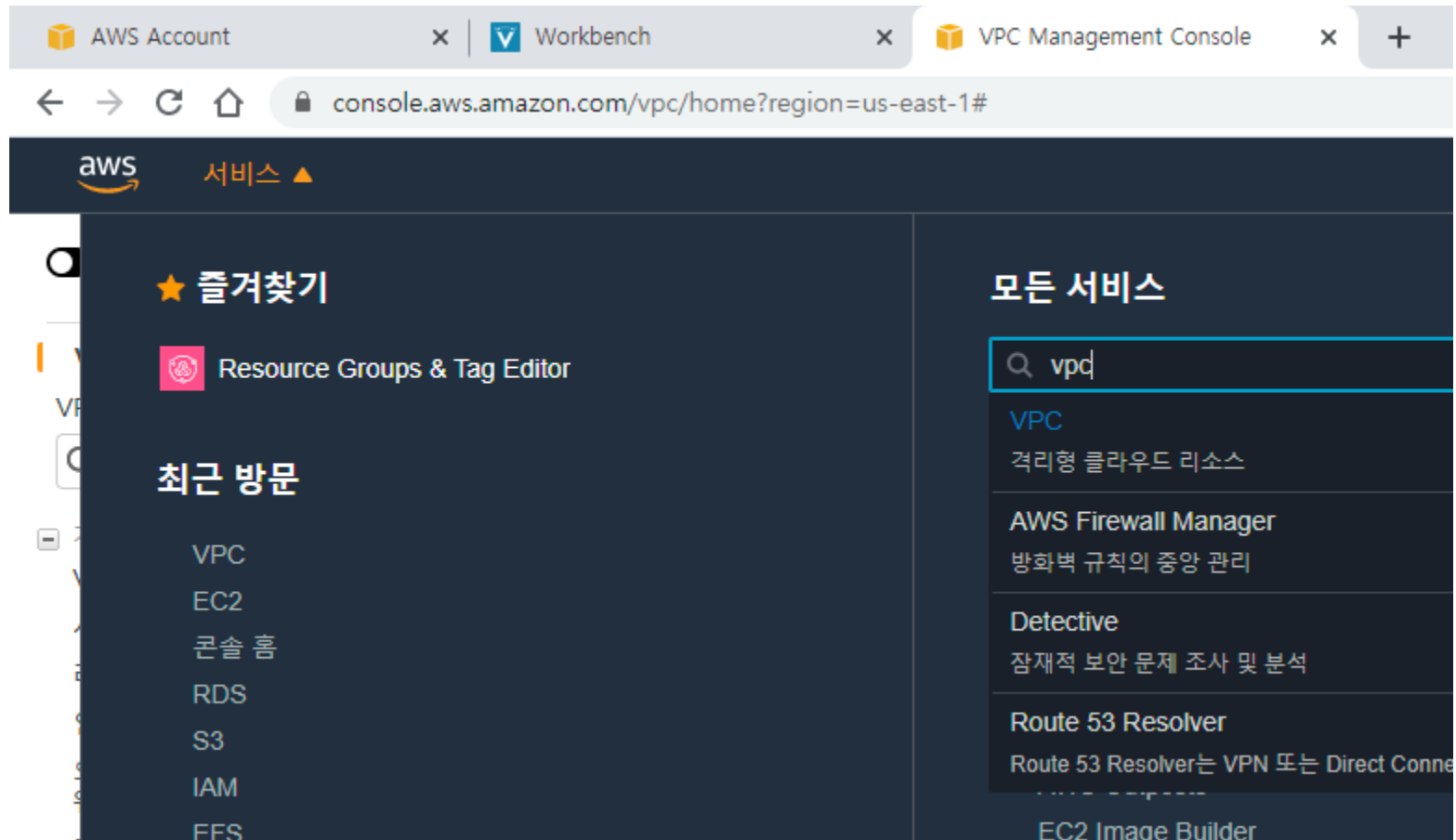
실습: Rebuild the whole system!



진행 내용: 10단계

- 앞의 “다중 계층” 구성에 따라 새롭게 VPC를 생성하고 기존 자원들 정리
 - 웹서버 서브넷과 DB 및 App 서버용 서브넷 분리
 - 총 6개: 가용영역마다 따로 생성 (가용영역 3개: 1a, 1b, 1c)
 - 보안그룹 설정
 - Private and public 을 구분하고, 정책에 맞도록 소스 설정
 - 총 4개 인스턴스: 웹서버 3개 (가용영역 3개에 각각 배치), DB 서버
 - 그 외 불필요한 VPC, 보안그룹 모두 제거
- 과제 별도 없음
 - 다음 과제에서 함께 체크
- 시작 전에...
 - Wordpress 인스턴스 및 DB 인스턴스 start

1. VPC 생성



1. VPC 생성

The screenshot shows the AWS Management Console interface for the VPC console. The left sidebar contains the navigation menu, with 'VPC' highlighted. The main content area displays a summary of VPC resources in the us-east-1 region.

Navigation Menu (Left Sidebar):

- New VPC Experience (Learn more)
- VPC 대시보드
- VPC로 필터링: Q VPC 선택
- 가상 프라이빗 클라우드
 - VPC**
 - 서브넷
 - 라우팅 테이블
 - 인터넷 게이트웨이
 - 외부 전용 인터넷 게이트웨이
 - 캐리어 게이트웨이
 - DHCP 옵션 세트
 - 탄력적 IP
 - 관리형 접두사 목록
 - 엔드포인트
 - 엔드포인트 서비스
 - NAT 게이트웨이
 - 피어링 연결
- 보안
 - 네트워크 ACL
 - 보안 그룹
- VPN(가상 프라이빗 네트워크)
 - 고객 게이트웨이
 - 가상 프라이빗 게이트웨이
 - 사이트 간 VPN 연결
 - 클라이언트 VPN 엔드포인트
- TRANSIT GATEWAY

Main Content Area:

VPC 마법사 시작 **EC2 인스턴스 시작**

참고: 인스턴스는 미국 동부(버지니아 북부) 리전에서 시작됩니다.

리전별 리소스 리소스 새로 고침

다음 Amazon VPC 리소스를 사용하고 있습니다.

리소스	버지니아 북부
VPC 모든 리전 보기 ▼	1
서브넷 모든 리전 보기 ▼	6
라우팅 테이블 모든 리전 보기 ▼	1
인터넷 게이트웨이 모든 리전 보기 ▼	1
외부 전용 인터넷 게이트웨이 모든 리전 보기 ▼	0
DHCP 옵션 세트 모든 리전 보기 ▼	1
탄력적 IP 모든 리전 보기 ▼	0
엔드포인트 모든 리전 보기 ▼	0
엔드포인트 서비스 모든 리전 보기 ▼	0
NAT 게이트웨이 모든 리전 보기 ▼	0
VPC 피어링 연결 모든 리전 보기 ▼	0
네트워크 ACL 모든 리전 보기 ▼	1
보안 그룹 모든 리전 보기 ▼	27
고객 게이트웨이 모든 리전 보기 ▼	0
가상 프라이빗 게이트웨이 모든 리전 보기 ▼	0
사이트 간 VPN 연결 모든 리전 보기 ▼	0
실행 중인 인스턴스 모든 리전 보기 ▼	0



1. VPC 생성

The screenshot shows the AWS Management Console interface for VPC management. The top navigation bar includes the AWS logo, '서비스' (Services), and user information. The left sidebar lists various services, with 'VPC' highlighted under the '가상 프라이빗 클라우드' (Virtual Private Cloud) category. The main content area displays 'VPC (1) 정보' (VPC (1) Information). A search bar labeled 'VPC 필터링' (VPC Filtering) is present. Below it, a table lists VPCs:

Name	VPC ID	상태	IPv4 CIDR	IPv6 CIDR(Network Border Group)	IPv6 풀
-	vpc-375ea64a	Available	172.31.0.0/16	-	-

The 'VPC 생성' (Create VPC) button is highlighted with a red box. At the bottom of the console, there are icons for '위에서 VPC 선택' (Select VPC from above), 'VPC 생성' (Create VPC), and 'VPC 삭제' (Delete VPC).

1. VPC 생성

VPC > VPC > VPC 생성

VPC 생성 정보

VPC는 AWS 클라우드의 격리된 부분으로서, Amazon EC2 인스턴스와 같은 AWS 객체로 채워집니다.

VPC 설정

이름 태그 - 선택 사항
'Name' 키와 사용자가 지정하는 값을 포함하는 태그를 생성합니다.

WP-VPC

IPv4 CIDR 블록 정보
10.0.0/16

IPv6 CIDR 블록 정보

☒ IPv6 CIDR 블록 없음
☐ Amazon에서 IPv6 CIDR 블록을 제공함
☐ 내가 소유한 IPv6 CIDR

테넌시 정보
기본값 ▼

태그

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 선택적 값으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

키 선택 사항

Q Name X

값 선택 사항

Q WP-VPC X

제거

새 태그 추가

49글(음) 태그 개 더 추가할 수 있습니다.

취소 **VPC 생성**



1. VPC 생성 완료

vpc-0b6e7a53b2ce6eb0f / WP-VPC 생성됨

VPC > VPC > vpc-0b6e7a53b2ce6eb0f

vpc-0b6e7a53b2ce6eb0f / WP-VPC 작업 ▼

세부 정보 정보

VPC ID vpc-0b6e7a53b2ce6eb0f	상태 Available	DNS 호스트 이름 비활성화됨	DNS 확인 활성화됨
테넌시 Default	DHCP 옵션 세트 dopt-fbe08581	라우팅 테이블 rtb-0fe48b6c76f4941ce	네트워크 ACL acl-0377bed9a0efc1892
기본 VPC 아니요	IPv4 CIDR 10.0.0.0/16	IPv6 풀 -	IPv6 CIDR(Network Border Group) -
Owner ID 851837490366			

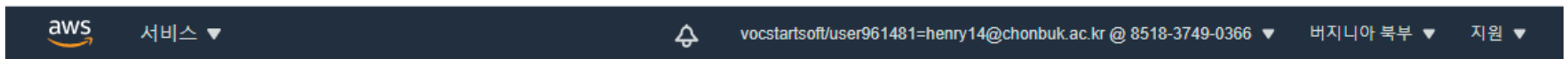
CIDR 블록 | 플로우 로그 | 태그

IPv4 CIDR 블록 정보

CIDR	상태
10.0.0.0/16	Associated

2. 서브넷 생성

- 총 6개 서브넷
 - 웹서버, DB 서브넷에 대해
 - 각각 가용 영역 3개 (1a, 1b, 1c) 마다 생성



서브넷 > 서브넷 생성

서브넷 생성

CIDR 형식에서 서브넷의 IP 주소 블록(예: 10.0.0.0/24)을 지정합니다. IPv4 블록 크기는 /16 ~ /28 넷마스크이어야 하며, VPC와 동일한 크기일 수 있습니다. IPv6 CIDR 블록은 /64 CIDR 블록이어야 합니다.

이름 태그

WebServerNet-Public-1a

i

VPC*

vpc-0b6e7a53b2ce6eb0f

i

가용 영역

us-east-1a

i

VPC CIDR

CIDR	Status	Status Reason
10.0.0.0/16	associated	

IPv4 CIDR 블록*

10.0.0.0/24

i

* 필수 사항

취소 생성



3. VPC 에 인터넷 게이트웨이 연결

- 인터넷 게이트웨이 생성 후, 새로 만든 VPC에 연결
 - 인터넷 게이트웨이가 없으면 외부로 연결 불가

New VPC Experience
Learn more

VPC 대시보드

VPC로 필터링:

VPC 선택

가상 프라이빗 클라우드

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

외부 전용 인터넷 게이트웨이

캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

엔드포인트

엔드포인트 서비스

NAT 게이트웨이

피어링 연결

보안

인터넷 게이트웨이 (1/1) 정보

인터넷 게이트웨이 필터링

작업

인터넷 게이트웨이 생성

<input checked="" type="checkbox"/>	Name	인터넷 게이트웨이 ID	상태	VPC ID	소유자
<input checked="" type="checkbox"/>	-	igw-63a28d18	Attached	vpc-375ea64a	8518374

3. VPC 에 인터넷 게이트웨이 연결

인터넷 게이트웨이 생성 정보

인터넷 게이트웨이는 VPC를 인터넷과 연결하는 가상 라우터입니다. 새 인터넷 게이트웨이를 생성하려면 아래에서 게이트웨이 이름을 지정해야 합니다.

인터넷 게이트웨이 설정

이름 태그

'Name' 키와 사용자가 지정하는 값을 포함하는 태그를 생성합니다.

태그 - 선택 사항

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 선택적 값으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

키



값 - 선택 사항



49을(를) 태그.개 더 추가할 수 있습니다.



3. VPC 에 인터넷 게이트웨이 연결

🕒 igw-0f3d55908a2e77e14 의 인터넷 게이트웨이가 생성되었습니다. 이제 VPC에 연결하여 VPC가 인터넷과 통신하도록 할 수 있습니다.

VPC에 연결



VPC > 인터넷 게이트웨이 > igw-0f3d55908a2e77e14

igw-0f3d55908a2e77e14 / WP-gateway

작업 ▼

세부 정보 정보

인터넷 게이트웨이 ID

📄 igw-0f3d55908a2e77e14

상태

⊖ Detached

VPC ID

-

소유자

📄 851837490366

태그

태그 관리

🔍 태그 검색

< 1 > ⚙️

Key

Value

Name

WP-gateway



3. VPC 에 인터넷 게이트웨이 연결 완료

☑ 인터넷 게이트웨이 igw-0f3d55908a2e77e14이(가) vpc-0b6e7a53b2ce6eb0f에 연결되었습니다.

VPC > 인터넷 게이트웨이 > igw-0f3d55908a2e77e14

igw-0f3d55908a2e77e14 / WP-gateway

작업 ▼

세부 정보 정보

인터넷 게이트웨이 ID

igw-0f3d55908a2e77e14

상태

Attached

VPC ID

vpc-0b6e7a53b2ce6eb0f | WP-VPC

소유자

851837490366

태그

태그 관리

태그 검색

< 1 > ⚙

Key

Value

Name

WP-gateway



4. VPC 라우팅 테이블 변경

- 외부 인터넷 연결을 새로 생성된 인터넷 게이트웨이로 전달

New VPC Experience
Learn more

VPC 대시보드

VPC로 필터링:
VPC 선택

가상 프라이빗 클라우드

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

외부 전용 인터넷 게이트웨이

캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

엔드포인트

엔드포인트 서비스

NAT 게이트웨이

피어링 연결

보안

네트워크 ACL

보안 그룹

라우팅 테이블 생성작업

태그 및 속성별 필터 또는 키워드별 검색

	Name	라우팅 테이블 ID	명시적으로 다음과 연결	Edge associations	기본	VPC ID
<input checked="" type="checkbox"/>		rtb-0fe48b6c76f4941ce	-	-	예	vpc-0b6e7a53b2ce6eb0f [...]
<input type="checkbox"/>		rtb-4eecab30	-	-	예	vpc-375ea64a

라우팅 테이블: rtb-0fe48b6c76f4941ce

요약라우팅서브넷 연결Edge Associations라우팅 전파태그

라우팅 편집

보기모든 라우팅

대상	대상	상태	전파됨
10.0.0.0/16	local	active	아니요



4. VPC 라우팅 테이블 변경

라우팅 테이블 > 라우팅 편집

라우팅 편집

대상	대상	상태	전파됨
10.0.0.0/16	local	active	아니요
0.0.0.0/0	igw-0f3d55908a2e77e14		아니요

라우팅 추가

* 필수 사항

취소

라우팅 저장



4. VPC 라우팅 테이블 변경 완료

태그 및 속성별 필터 또는 키워드별 검색

Name	라우팅 테이블 ID	명시적으로 다음과 연결	Edge associations	기본	VPC ID
<input checked="" type="checkbox"/>	rtb-0fe48b6c76f4941ce	-	-	예	vpc-0b6e7a53b
<input type="checkbox"/>	rtb-4eecab30	-	-	예	vpc-375ea64a

라우팅 테이블: rtb-0fe48b6c76f4941ce

요약 라우팅 서브넷 연결 Edge Associations 라우팅 전파 태그

라우팅 편집

보기 모든 라우팅

대상	대상	상태	전파됨
10.0.0.0/16	local	active	아니요
0.0.0.0/0	igw-0f3d55908a2e77e14	active	아니요

5. 보안그룹 생성

- 웹서버
 - 인바운드: HTTP, HTTPS, SSH
 - SSH의 소스는 관리자의 IP 주소만 오픈하는 것이 안전함
 - 아웃바운드: MYSQL/Aurora (3306), HTTP, HTTPS (wordpress 관리 등을 위함)
 - 소스는 DB 보안그룹을 생성한 이후, 해당 보안그룹 ID로 설정
- DB
 - 인바운드: MYSQL/Aurora (3306)
 - 소스는 웹서버 보안그룹으로 설정
 - 아웃바운드: none

The screenshot shows the '보안 그룹 생성' (Create Security Group) form in the AWS Management Console. The form is titled '보안 그룹 생성' and has a close button 'X' in the top right corner. It contains the following fields:

- 보안 그룹 이름** (Security Group Name): WP-DatabaseSG
- 설명** (Description): WP-DatabaseSG
- VPC**: vpc-e7c6698f | WP-VPC

Below these fields is a section for '보안 그룹 규칙' (Security Group Rules). It has two tabs: '인바운드' (Inbound) and '아웃바운드' (Outbound). The '인바운드' tab is selected. The table below shows the rule configuration:

유형	프로토콜	포트 범위	소스	설명
MYSQL/Aurora	TCP	3306	사용자 지정 sg-83d50ee8	예: 관리자 데스크톱용 SSH

At the bottom of the rule configuration section is a button labeled '규칙 추가' (Add Rule).

5. 보안그룹 생성

- 웹서버 보안 그룹

인바운드 규칙 정보

유형 정보	프로토콜 정보	포트 범위 정보	소스 정보	설명 - 선택 사항 정보
SSH	TCP	22	사용자 지정 Q 0.0.0.0/0 X	<div></div> <div>삭제</div>
HTTP	TCP	80	사용자 지정 Q 0.0.0.0/0 X	<div></div> <div>삭제</div>
HTTPS	TCP	443	사용자 지정 Q 0.0.0.0/0 X	<div></div> <div>삭제</div>

규칙 추가

아웃바운드 규칙 정보

유형 정보	프로토콜 정보	포트 범위 정보	대상 정보	설명 - 선택 사항 정보
MYSQL/Aurora	TCP	3306	사용자 지정 Q sg-077d971c005948662 X	<div></div> <div>삭제</div>
HTTP	TCP	80	사용자 지정 Q 0.0.0.0/0 X	<div></div> <div>삭제</div>
HTTPS	TCP	443	사용자 지정 Q 0.0.0.0/0 X	<div></div> <div>삭제</div>

규칙 추가

DB 보안 그룹을 지정



5. 보안그룹 생성

- DB 보안 그룹의 인바운드 규칙 수정
 - 소스를 웹서버 보안그룹으로 지정
 - 해당 보안 그룹을 사용하는 인스턴스만 3306 포트로 접근 가능
 - 아웃바운드에는 아무 내용 없음
 - DB 인스턴스는 외부로 접속 불가. 실제 사용 시, 업데이트에 문제가 있을 수 있으니 확인할 것

VPC > 보안 그룹 > sg-077d971c005948662 - WP-Database-SG > 인바운드 규칙 편집

인바운드 규칙 편집 정보

인바운드 규칙은 인스턴스에 도달하도록 허용된 수신 트래픽을 제어합니다.

인바운드 규칙 정보

유형 정보

MYSQL/Aurora ▼

프로토콜 정보

TCP

포트 범위 정보

3306

소스 정보

사용자 지정 ▼

Q

sg-016725a400dbffc2f X

규칙 추가

⚠ 참고: 기존 규칙을 편집하면 편집된 규칙이 삭제되고 새 세부 정보로 새 규칙이 생성됩니다. 이렇게 하면 새 규칙이 생성될 때까지 해당 규칙에 의존하는 트래픽이 잠시 중단될 수 있습니다.



5. 보안그룹 생성 완료 및 정리

- 기존 웹서버들의 보안그룹을 default 로 변경한 후,
- 불필요한 기존 보안그룹 모두 정리 (default 는 남겨둘 것)

태그 및 속성별 필터 또는 키워드별 검색

<input type="checkbox"/>	Name ▾	그룹 ID ▾	그룹 이름 ▲	VPC ID ▾	설명 ▾
<input type="checkbox"/>		sg-1ab26971	default	vpc-e7c6698f	default VPC security group
<input type="checkbox"/>		sg-6e865b06	default	vpc-76d28f1f	default VPC security group
<input type="checkbox"/>		sg-d57cb7be	load-balancer-wizard-1	vpc-76d28f1f	load-balancer-wizard-1 created
<input type="checkbox"/>	WP-DatabaseSG	sg-0213c969	WP-DatabaseSG	vpc-e7c6698f	WP-DatabaseSG
<input type="checkbox"/>	WP-WebserverSG	sg-6810ca03	WP-WebserverSG	vpc-e7c6698f	WP-WebserverSG



(참고) 각 서버넷에 보안 설정을 하고 싶다면?

- 네트워크 ACL 변경
 - VPC 대시보드
 - 참고: [VPC 네트워크 ACL](#)

네트워크 ACL 생성 **삭제**

이름	네트워크 ACL ID	연결 대상	기준값	VPC
	acl-4e62ea26	4 서버넷	예	vpc-e7c6698f WP-VPC
	acl-587e5231	2 서버넷	예	vpc-76d28f1f

acl-587e5231

요약 **인바운드 규칙** **아웃바운드 규칙** **서버넷 연결** **태그**

인바운드 트래픽을 허용합니다. 네트워크 ACL이 상태 비저장이므로 인바운드 및 아웃바운드 규칙을 생성해야 합니다.

편집

보기:: **모든 규칙**

규칙 #	유형	프로토콜	포트 범위	소스	허용/거부
100	모든 트래픽	모두	모두	0.0.0.0/0	허용
*	모든 트래픽	모두	모두	0.0.0.0/0	거부



6. AMI 를 이용해 새로운 VPC에 인스턴스 복제

- 기존 인스턴스의 VPC를 변경하는 것은 불가능
 - 따라서 새롭게 인스턴스를 만들어야 함.
- 기존 인스턴스를 기반으로 이미지 생성 후, 해당 이미지로 다시 생성
 - 워드프레스 관련 데이터는 모두 remote DB에 적재되어 있는 상태
 - Local DB가 시작되지 않도록 수정
 - 서버의 설정파일, 워드프레스 소스, 실행파일, 플러그인 등은 로컬 FS 에 적재
- 이미지 생성 이전에 VPC, 서브넷, 보안그룹을 모두 정리해둘 것



6. AMI 를 이용해 새로운 VPC에 인스턴스 복제

- 이미지 생성 전, 서비스 설정 수정
 - `$ sudo vi /etc/init.d/bitnami`
 - `/etc/rc.d` 에서 분석을 해보면, 위 파일의 스크립트로 여러 서비스를 부팅 시에 수행함을 확인할 수 있음
 - 본래 3개 서비스를 모두 start 하게 되어있지만, 아래와 같이 apache 와 php-fpm 만 시작하도록 수정 (mysql 제외)

```
skip_bitnami_start_check && exit 0
$script 2>&1 || true
done
) | tee /opt/bitnami/var/log/pre-start.log
chmod 0600 /opt/bitnami/var/log/pre-start.log

skip_bitnami_start_check && exit 0
/opt/bitnami/ctlscript.sh start
RESULT=$?

# Initialization after services are started
(
for script in `find /opt/bitnami/var/init/post-start -type l -executable | sort`; do
    $script 2>&1 || true
done
) | tee /opt/bitnami/var/log/post-start.log
chmod 0600 /opt/bitnami/var/log/post-start.log
;;
*)
    exec /opt/bitnami/ctlscript.sh "$@"
;;
esac

exit $RESULT
```

→

```
#!/opt/bitnami/ctlscript.sh start
/opt/bitnami/ctlscript.sh start php-fpm
/opt/bitnami/ctlscript.sh start apache
```

6. AMI 를 이용해 새로운 VPC에 인스턴스 복제

- 사용자 데이터의 스크립트 동작 확인
 - `$ sudo reboot`
- 인스턴스 재부팅이 완료된 다음,
 - `$ sudo /opt/bitnami/ctlscript.sh status`

```
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 3.13.0-116-generic x86_64)
```

$$\begin{array}{ccccccc} \overline{|-|} & \overline{|-|}) & \overline{|-|} & \overline{|-|} & \overline{|-|} & \overline{|-|} & (\overline{|-|}) \\ | & - & \backslash & | & - & \backslash & | \\ | & - & \backslash & | & - & \backslash & | \\ | & - & / & - & \backslash & | & - & \backslash & | & - & \backslash & | \end{array}$$

```
*** Welcome to the Bitnami WordPress 4.7.4.php56-0 ***
```

*** Documentation: <https://docs.bitnami.com/aws/apps/wordpress/> ***

```
*** https://docs.bitnami.com/aws/ ***
```

*** Bitnami Forums: <https://community.bitnami.com/> ***

Last login: Tue Nov 3 04:43:11 2020 from 114.70.193.40

```
bitnami@ip-172-31-19-145:~$ sudo /opt/bitnami/ctlscript.sh status
```

php-fpm already running

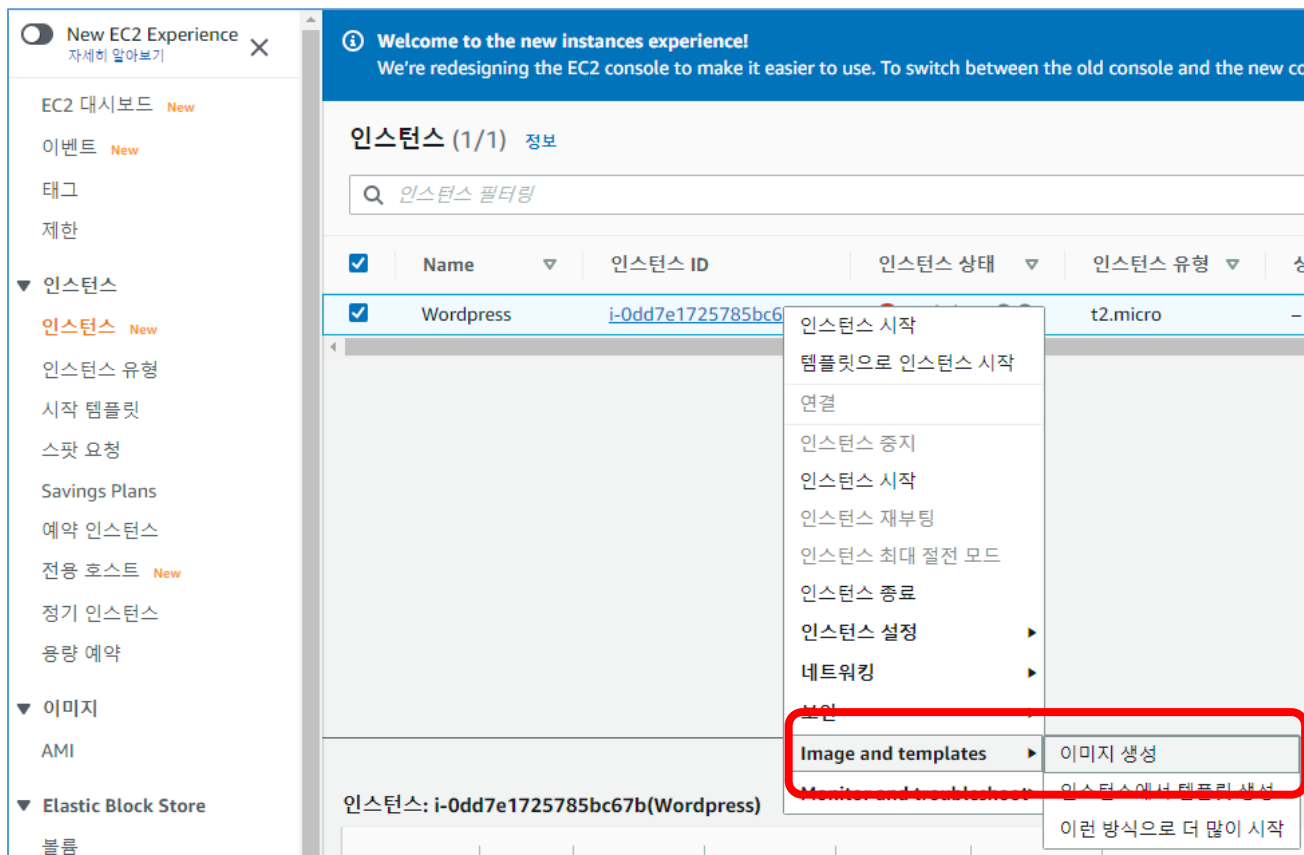
apache already running

mysql not running

```
bitnami@ip-172-31-19-145:~$
```

6. AMI 를 이용해 새로운 VPC에 인스턴스 복제

- AMI 이미지 생성
- 앞의 내용을 모두 수행 후, 인스턴스 종료하고 이미지 생성
 - `$ sudo shutdown -h now`
- 완료 후, AMI 에서 확인 (시간이 오래 걸릴 수 있음)



6. AMI 를 이용해 새로운 VPC에 인스턴스 복제

EC2 > 인스턴스 > i-Odd7e1725785bc67b > 이미지 생성

이미지 생성 정보

이미지(AMI라고도 함)는 EC2 인스턴스를 시작할 때 적용되는 프로그램 및 설정을 정의합니다. 기존 인스턴스의 구성에서 이미지를 생성할 수 있습니다.

인스턴스 ID

 i-Odd7e1725785bc67b (Wordpress)

이미지 이름

WP-base-image

최대 127자. 생성 후에는 수정할 수 없습니다.

이미지 설명 - 선택 사항

Image description

최대 255자

재부팅 안 함

☐ 활성화

인스턴스 볼륨

볼륨 유형

디바이스

스냅샷

크기

볼륨 유형

IOPS

종료 시 삭제

암호화됨

EBS ▼

/dev/sda1 ▼

Create new snapshot fr... ▼

10


EBS 범용 SSD - gp2 ▼

100

☒ 활성화

☐ 활성화

볼륨 추가

 이미지 생성 프로세스 중에 Amazon EC2는 위의 각 볼륨의 스냅샷을 생성합니다.

취소

이미지 생성



7. 이미지를 이용해 웹서버 인스턴스 시작

- 새로 생성한 VPC, 서브넷, 보안그룹 등으로 설정
- 나머지는 앞서 진행했던 설정과 동일하게. (instance type, IAM Role, storage 등)

The screenshot shows the AWS Management Console interface for the EC2 Image Builder service. On the left-hand navigation pane, the 'AMI' option under the 'Image' category is highlighted with a red box. The main content area displays a table of AMIs. The first row shows an AMI named 'WP-base-image' with ID 'ami-07deb5efba2dda268'. The 'Start' button and the 'available' status for this AMI are both highlighted with red boxes. A context menu is open over the 'Start' button, listing various actions such as 'Start', 'Cancel', 'New AMI', 'AMI Copy', 'Image Permissions', 'Tag Add/Edit', 'Boot Volume Settings', and 'EC2 Image Builder'.

Name	AMI 이름	AMI ID	소스	소유자	표시 여부	상태
<input type="checkbox"/>	WP-base-image	ami-07deb5efba2dda268	851837490366/...		이벳	available

(AMI 선택 화면에서 선택해도 됨)

1. AMI 선택

2. 인스턴스 유형 선택

3. 인스턴스 구성

4. 스토리지 추가

5. 태그 추가

6. 보안 그룹 구성

7. 검토

단계 1: Amazon Machine Image(AMI) 선택

[취소 및 종료](#)

AMI는 인스턴스를 시작하는 데 필요한 소프트웨어 구성(운영 체제, 애플리케이션 서버, 애플리케이션)이 포함된 템플릿입니다. AWS, 사용자 커뮤니티 또는 AWS Marketplace에서 제공하는 AMI를 선택하거나, 자체 AMI 중 하나를 선택할 수도 있습니다.

[SSM 파라미터로 검색](#)

빠른 시작

나의 AMI

AWS Marketplace


커뮤니티 AMI

▼ 소유권

- ☒ 사용자 소유
- ☐ 나와 공유됨

▼ 아키텍처

- ☐ 32비트(x86)



WP-base-image - ami-07deb5efba2dda268

선택

루트 디바이스 유형: **ebs**

가상화 유형: **hvm**

소유자: 851837490366

ENA 활성화: **64비트(x86)**

아니요



7. 이미지를 이용해 웹서버 인스턴스 시작

1. AMI 선택

2. 인스턴스 유형 선택

3. 인스턴스 구성

4. 스토리지 추가

5. 태그 추가

6. 보안 그룹 구성

7. 검토

단계 3: 인스턴스 세부 정보 구성

요구 사항에 적합하게 인스턴스를 구성합니다. 동일한 AMI의 여러 인스턴스를 시작하고 스팟 인스턴스를 요청하여 보다 저렴한 요금을 활용

인스턴스 개수 ⓘ

1

[Auto Scaling 그룹 시작 ⓘ](#)

구매 옵션 ⓘ

☐ 스팟 인스턴스 요청

네트워크 ⓘ

vpc-0b6e7a53b2ce6eb0f | WP-VPC

[새 VPC 생성](#)

서브넷 ⓘ

subnet-0aa136b565d0eb1e6 | WebSubnet-Public-1a

[새 서브넷 생성](#)

251개 IP 주소 사용 가능

퍼블릭 IP 자동 할당 ⓘ

서브넷 사용 설정(비활성화)

배치 그룹 ⓘ

☐ 배치 그룹에 인스턴스 추가

용량 예약 ⓘ

열기

도메인 조인 디렉터리 ⓘ

디렉터리 없음

[새 디렉터리 생성](#)

IAM 역할 ⓘ

iam-wpoffload

[새 IAM 역할 생성](#)



7. 이미지를 이용해 웹서버 인스턴스 시작

1. AMI 선택 2. 인스턴스 유형 선택 3. 인스턴스 구성 4. 스토리지 추가 5. 태그 추가 6. 보안 그룹 구성 7. 검토

단계 6: 보안 그룹 구성

보안 그룹은 인스턴스에 대한 트래픽을 제어하는 방화벽 규칙 세트입니다. 이 페이지에서는 특정 트래픽을 인스턴스에 도달하도록 허용할 규칙을 추가할 수 있습니다. 예를 들면 웹 서버를 설정하여 인터넷 트래픽을 인스턴스에 도달하도록 허용하려는 경우 HTTP 및 HTTPS 트래픽에 대한 무제한 액세스를 허용하는 규칙을 추가합니다. 새 보안 그룹을 생성하거나 아래에 나와 있는 기존 보안 그룹 중에서 선택할 수 있습니다. Amazon EC2 보안 그룹에 대해 자세히 알아보기.

보안 그룹 할당: ☐ 새 보안 그룹 생성
☒ 기존 보안 그룹 선택

보안 그룹 ID	이름	설명	작업
----------	----	----	----

sg-016725a400dbffc2f에 대한 인바운드 규칙 (선택한 보안 그룹: sg-016725a400dbffc2f)

웹서버 보안 그룹을 지정



유형 ⓘ	프로토콜 ⓘ	포트 범위 ⓘ	소스 ⓘ	설명 ⓘ
HTTP	TCP	80	0.0.0.0/0	
SSH	TCP	22	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	

취소 이전 검토 및 시작



7. 이미지를 이용해 웹서버 인스턴스 시작

- 인스턴스 정리
- 각 가용 영역마다 총 3개 인스턴스를 생성하고, 불필요한 인스턴스 삭제
 - 각각 서로 다른 서브넷 지정을 통해,
 - 인스턴스들을 각각 분리된 가용영역에 지정함으로써,
 - 고가용성 (HA) 구조로 구성할 준비 완료



8. 각 인스턴스에 Elastic IP 할당

- Elastic IP (탄력적 IP 주소)
 - AWS의 고정 public IPv4 주소 서비스
 - EC2의 IP 주소는 계속 변경되므로, public 으로 사용할 EIP 를 할당받고, 이를 VPC 내의 EC2 instance에 매핑하여 사용함
 - http://docs.aws.amazon.com/ko_kr/AmazonVPC/latest/UserGuide/vpc-eips.html
 - 요금: 활성화된 인스턴스에 연결해 사용 중일 때는 부과되지 않음
 - 불필요하게 EIP 만 할당해놓고 사용하지 않는 경우, \$0.005/hour (\$3.6/month)
 - 이번 실습 종료 후, 반드시 제거할 것! 학기 종료 후에도 확인
 - <https://aws.amazon.com/ko/premiumsupport/knowledge-center/elastic-ip-charges/>
 - 참고: VPC의 IP주소 지정
 - http://docs.aws.amazon.com/ko_kr/AmazonVPC/latest/UserGuide/vpc-ip-addressing.html#vpc-eips



8. 각 인스턴스에 Elastic IP 할당

자세히 알아보기

EC2 대시보드 **New**

이벤트 **New**

태그

제한

▼ 인스턴스

인스턴스 **New**

인스턴스 유형

시작 템플릿

스팟 요청

Savings Plans

예약 인스턴스

전용 호스트 **New**

정기 인스턴스

용량 예약

▼ 이미지

AMI

▼ Elastic Block Store

볼륨

스냅샷

수명 주기 관리자

▼ 네트워크 및 보안

보안 그룹 **New**

탄력적 IP **New**

탄력적 IP 주소

작업 ▼

탄력적 IP 주소 할당

Q 탄력적 IP 주소 필터링

< 1 > ⚙

	Name	할당된 IPv4 주소	유형
--	------	-------------	----



8. 각 인스턴스에 Elastic IP 할당

EC2 > 탄력적 IP 주소 > 탄력적 IP 주소 할당

탄력적 IP 주소 할당

할당받을 퍼블릭 IP 주소가 포함된 퍼블릭 IPv4 주소 풀을 선택하여 탄력적 IP 주소를 할당합니다. 실행 중인 인스턴스와 연결된 탄력적 IP(EIP) 주소 하나를 무료로 사용할 수 있습니다. 추가 EIP를 해당 인스턴스와 연결할 경우 해당 인스턴스에 연결된 각 추가 EIP에 대해 비례 할당으로 요금이 청구됩니다. 추가 EIP는 Amazon VPC에서만 사용할 수 있습니다. 탄력적 IP 주소의 효율적인 사용을 위해 이러한 IP 주소가 실행 중인 인스턴스와 연결되어 있지 않거나 중지된 인스턴스 또는 연결되지 않은 네트워크 인터페이스와 연결되어 있는 경우 소액의 시간당 요금이 부과됩니다. [자세히 알아보기](#)

탄력적 IP 주소 설정

네트워크 경계 그룹

네트워크 경계 그룹은 퍼블릭 IPv4 주소가 보급되는 영역의 논리적 그룹입니다. IPv4 주소를 네트워크 경계 그룹의 영역으로 제한하려면 이 파라미터를 설정합니다.

us-east-1

퍼블릭 IPv4 주소 풀

퍼블릭 IP 주소는 Amazon의 퍼블릭 IP 주소 풀, 사용자가 소유하여 계정으로 가져오는 풀 또는 사용자가 소유하고 계속 광고하는 풀에서 할당됩니다..

☒ Amazon의 IPv4 주소 풀

☐ AWS 계정으로 가져오는 퍼블릭 IPv4 주소(풀을 찾을 수 없으므로 옵션이 비활성화됨) [자세히 알아보기](#)

☐ IPv4 주소의 고객 소유 풀(고객 소유 풀을 찾을 수 없기 때문에 옵션이 비활성화됨) [자세히 알아보기](#)

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [자세히 알아보기](#)

Create accelerator

취소

할당



8. 각 인스턴스에 Elastic IP 할당

☑ 탄력적 IP 주소가 할당되었습니다.
탄력적 IP 주소 50.19.191.223

이 탄력적 IP 주소 연결

탄력적 IP 주소 (1/1)

🔄

작업 ▲

탄력적 IP 주소 할당

🔍 탄력적 IP 주소 필터링

퍼블릭 IPv4 주소: 50.19.191.223 ✕

필터 지우기

- 세부 정보 보기
- 탄력적 IP 주소 릴리스
- 탄력적 IP 주소 연결
- 탄력적 IP 주소 연결 해제

<input checked="" type="checkbox"/>	Name	할당된 IPv4 주소	유형
<input checked="" type="checkbox"/>	-	50.19.191.223	퍼블릭 IP



8. 각 인스턴스에 Elastic IP 할당

EC2 > 탄력적 IP 주소 > 탄력적 IP 주소 연결

탄력적 IP 주소 연결

이 탄력적 IP 주소에 연결할 인스턴스 또는 네트워크 인터페이스를 선택합니다. (50.19.191.223)

탄력적 IP 주소: 50.19.191.223

리소스 유형

탄력적 IP 주소를 연결할 리소스의 유형을 선택합니다.

☒ 인스턴스

☐ 네트워크 인터페이스

⚠ 탄력적 IP 주소가 이미 연결되어 있는 인스턴스에 탄력적 IP 주소를 연결하면 이전에 연결된 탄력적 IP 주소가 연결 해제되지만 계정에는 계속 할당된 상태로 남아 있습니다. [자세히 알아보기](#)

인스턴스

Q i-0044f17f8a067bb7b

X

↺

프라이빗 IP 주소

탄력적 IP 주소를 연결할 프라이빗 IP 주소입니다.

Q 프라이빗 IP 주소 선택

재연결

이미 리소스에 연결되어 있는 탄력적 IP 주소를 다른 리소스에 재연결할 수 있는지 여부를 지정합니다.

☐ 이 탄력적 IP 주소를 재연결하도록 허용

취소

연결



8. 각 인스턴스에 Elastic IP 할당

- 아래와 같이 3개 인스턴스에 대해 각각 EIP 할당

✓ 탄력적 IP 주소가 연결되었습니다.
탄력적 IP 주소 54.221.34.128이(가) 인스턴스에 연결되었습니다.i-0bf2b8f5d5a03109a

탄력적 IP 주소 (3)

🔄

작업 ▼

탄력적 IP 주소 할당

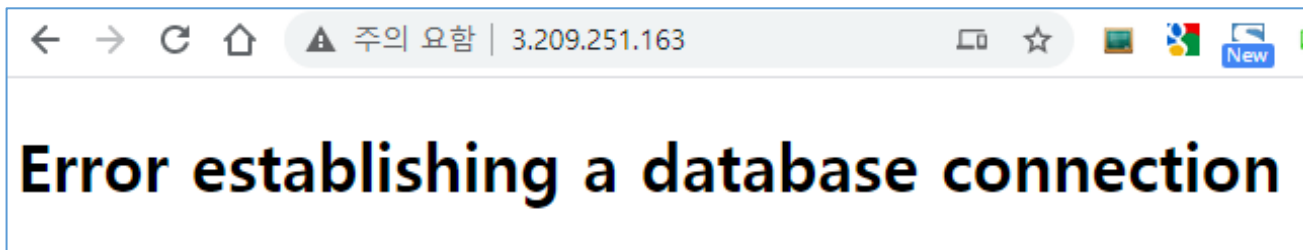
< 1 >

⚙️

▼	할당 ID	▼	연결된 인스턴스 ID	▼	프라이빗 IP 주소
	eipalloc-0cbfb027898067715		i-05f16b9ca57e0632b 🔗		10.0.0.237
	eipalloc-0c0f30475e02ad227		i-0044f17f8a067bb7b 🔗		10.0.2.103
	eipalloc-04b6a777026671ae1		i-0bf2b8f5d5a03109a 🔗		10.0.1.180

8. 각 인스턴스에 Elastic IP 할당

- Public IP 주소로 HTTP 접속해보기
 - 오류: DB 인스턴스가 연결이 되지 않기 때문
 - SSH 로 접속해서 동작 확인
- EIP 동작 확인: Instance를 stop 했다가, 다시 start
 - Private IP 주소가 변경되었는지 확인
 - 재부팅 때마다 각 서브넷의 DHCP 에서 새롭게 IP를 할당해줌
 - 기존과 동일한 IP가 부여될 수도 있음
 - 다시 Public IP 주소로 접근하기
 - EIP 는 변경되지 않으므로,
인스턴스 restart 와 무관하게 동일한 IP로 접속 가능



9. DB 인스턴스의 VPC, 서브넷 이동

- DB 인스턴스는 **DB 서브넷 그룹**에만 속할 수 있음
 - DB 서브넷 그룹은 RDS 콘솔에서 생성 및 수정 가능함
 - 서브넷 자체는 VPC 콘솔에서 미리 생성
 - 제약 사항: 지정된 리전에서 두 개 이상의 가용 영역에 서브넷이 있어야 함
 - 여러 가용 영역에 DB 서비스를 제공하기 위함
 - DB 가 기존에 위치하고 있던 가용 영역이 포함되어야 함
 - 필요한 경우, DB 서브넷을 하나 더 생성하여 사용
- 참고: [VPC에서 Amazon RDS DB 인스턴스를 사용한 작업](#)



9. DB 인스턴스의 VPC, 서브넷 이동

- DB 인스턴스의 Subnet group 생성

Amazon RDS

×

Dashboard

데이터베이스

Query Editor

성능 개선 도우미

스냅샷

Automated backups

예약 인스턴스

Proxies

서브넷 그룹

파라미터 그룹

옵션 그룹

Custom Availability Zones

이벤트

이벤트 구독

Recommendations

RDS > 서브넷 그룹 > Create DB subnet group

DB 서브넷 그룹 생성

새 서브넷 그룹을 생성하려면 이름과 설명을 입력하고 기존 VPC를 선택합니다. 그러면 해당 VPC와 관련된 서브넷을 추가할 수 있습니다.

서브넷 그룹 세부 정보

이름

서브넷 그룹이 생성된 후에는 이름을 수정할 수 없습니다.

WP-DB-subnet-group

1~255자로 구성되어야 합니다. 영숫자, 공백, 하이픈, 밑줄 및 마침표를 사용할 수 있습니다.

설명

For WP DB

VPC

DB 서브넷 그룹에 사용할 서브넷에 해당하는 VPC 식별자를 선택합니다. 서브넷 그룹이 생성된 후에는 다른 VPC 식별자를 선택할 수 없습니다.

WP-VPC (vpc-0b6e7a53b2ce6eb0f)



9. DB 인스턴스의 VPC, 서브넷 이동

서브넷 추가

DB 인스턴스가 기존 동작하던 가용 영역이 포함되어야 함
(다음 슬라이드 참조)

가용 영역

추가할 서브넷이 포함된 가용 영역을 선택합니다.

가용 영역 선택

us-east-1a X

us-east-1b X

us-east-1c X

서브넷

추가할 서브넷을 선택합니다. 목록에는 선택한 가용 영역의 서브넷이 포함됩니다.

서브넷 선택

subnet-010f6bc17fd75aaf0 (10.0.100.0/24) X

subnet-0d8b9d2f33ad354be (10.0.102.0/24) X

subnet-0f7de0c435098ec1e (10.0.101.0/24) X

서브넷이 선택됨 (3)

가용 영역	서브넷 ID	CIDR 블록
us-east-1a	subnet-010f6bc17fd75aaf0	10.0.100.0/24
us-east-1c	subnet-0d8b9d2f33ad354be	10.0.102.0/24
us-east-1b	subnet-0f7de0c435098ec1e	10.0.101.0/24

취소

생성



(DB 서브넷 추가)

- 새로운 DB 서브넷 그룹에는
 - 기존 DB 인스턴스가 위치한 AZ를 포함한 서브넷이 반드시 들어가야 함
 - 이를 위해 새로 해당 가용영역을 기반한 DB 서브넷을 생성하고,
 - 해당 DB 서브넷도 포함하도록 설정. 총 4개가 되어도 무방함

database-1

수정작업

요약

DB 식별자

database-1

CPU

3.05%

정보

사용 가능

클래스

db.t2.small

역할

인스턴스

현재 활동

0 연결

엔진

MySQL Community

리전 및 AZ

us-east-1f

<input checked="" type="checkbox"/>	DBSubnet-Private-1f	subnet-0d68727631019a6bb	available	vpc-0b6e7a53b2ce6eb0f ...	10.0.4.0/24	251
<input type="checkbox"/>	WebSubnet-Public-1a	subnet-0aa136b565d0eb1e6	available	vpc-0b6e7a53b2ce6eb0f ...	10.0.0.0/24	250

서브넷: subnet-0d68727631019a6bb

설명

플로우 로그

라우팅 테이블

네트워크 ACL

태그

공유 중

서브넷 ID	subnet-0d68727631019a6bb	상태	available
VPC	vpc-0b6e7a53b2ce6eb0f WP-VPC	IPv4 CIDR	10.0.4.0/24
사용 가능한 IPv4 주소	251	IPv6 CIDR	-
가용 영역	us-east-1f (use1-az5)	Network Border Group	us-east-1

9. DB 인스턴스의 VPC, 서브넷 이동

- DB instance 수정
 - “사용 가능” 상태에서만 “수정” 가능

RDS > 데이터베이스 > database-1


database-1

수정 작업 ▼

요약

DB 식별자 database-1	CPU <div><div></div>3.05%</div>	정보 ✔ 사용 가능	클래스 db.t2.small
역할 인스턴스	현재 활동 <div><div></div>0 연결</div>	엔진 MySQL Community	리전 및 AZ us-east-1f

9. DB 인스턴스의 VPC, 서브넷 이동

연결 

서브넷 그룹
wp-db-subnet-group ▼

보안 그룹
이 DB 인스턴스와 연결할 DB 보안 그룹 목록입니다.
보안 그룹 선택 ▼

default ✕ 보안 그룹은 나중에 변경

인증 기관
rds-ca-2019 ▼

▶ 추가 연결 구성

취소

계속



9. DB 인스턴스의 VPC, 서브넷 이동

RDS > 데이터베이스 > Modify DB instance: database-1

DB 인스턴스 수정: database-1

수정 사항 요약

You are about to submit the following modifications. Only values that will change are displayed. Carefully verify your changes and click Modify DB Instance.


속성	현재 값	새 값
서브넷 그룹	default-vpc-375ea64a	wp-db-subnet-group

수정 예약

수정 사항을 적용할 시간

☐ 예약된 다음 유지 관리 기간 중에
현재 유지 관리 기간: wed:09:23-wed:09:53

☒ 즉시
이 업그레이드와 보류 중인 수정 사항은 이 데이터베이스 인스턴스의 유지 관리 기간에 관계없이 가능한 빨리 비동기식으로 적용됩니다.

 예기치 않은 잠재적 가동 중단 시간

변경 사항을 즉시 적용하려는 경우 보류 중인 수정 사항 대기열에 있는 모든 변경 사항도 적용됩니다. 보류 중인 수정 사항에 가동 중지가 필요한 경우 이 옵션을 선택하면 예기치 못한 가동 중지가 발생할 수 있습니다.

취소

뒤로

DB 인스턴스 수정



9. DB 인스턴스의 VPC, 서브넷 이동

- DB 인스턴스 상태가 “moving-to-vpc” 로 바뀌면서 수정 진행
- “사용 가능” 상태가 될 때까지 대기
 - 거의 10분 이상 걸림 (적절한 유튜브 콘텐츠 감상...)
- 다시 “수정” 을 눌러, 보안 그룹 수정
 - Default 보안 그룹 제거, DB 보안그룹 지정
 - “수정 예약” 은 다시 “즉시” 로 설정
- 이번에는 즉각 “사용 가능”

9. DB 인스턴스의 VPC, 서브넷 이동

- DB 인스턴스 최종 상태 확인

연결 & 보안모니터링로그 및 이벤트구성유지 관리 및 백업태그

연결 & 보안

엔드포인트 및 포트

엔드포인트
database-1.cpyyj6u4joee.us-east-1.rds.amazonaws.com

포트
3306

네트워킹

가용 영역
us-east-1f

VPC
WP-VPC (vpc-0b6e7a53b2ce6eb0f)

서브넷 그룹
wp-db-subnet-group

서브넷
subnet-0d68727631019a6bb
subnet-0f7de0c435098ec1e
subnet-010f6bc17fd75aaf0
subnet-0d8b9d2f33ad354be

보안

VPC 보안 그룹
WP-Database-SG (sg-077d971c005948662)
(활성)

퍼블릭 액세스 가능성
아니요

인증 기관
rds-ca-2019

인증 기관 날짜
Aug 23rd, 2024

보안 그룹 규칙 (1)

Q 보안 그룹 규칙 필터

< 1 >

⚙

보안 그룹

▲

유형

▼

규칙

▼

WP-Database-SG (sg-077d971c005948662)

EC2 Security Group - Inbound

sg-016725a400dbffc2f

10. 전체 최종 상태 확인

- 각 인스턴스의 EIP 로 HTTP 접속하여 웹페이지 확인
 - 잘 나오면, 잘 설정된 것
- 각 인스턴스에 SSH로 접속하여 service status 확인
 - `$ sudo /opt/bitnami/ctlscript.sh status`
- 문제가 있다면?
 - VPC, 서브넷, DB 서브넷 그룹, 보안그룹 등 앞서 설정한 내용들을 모두 천천히 확인할 것
 - 내용이 많으니 차근 차근 진행할 것

10. 전체 최종 상태 확인

- 완료 후, 리소스 중지 및 EIP 해제
 - 인스턴스들 3개 모두 중지
 - 연결된 EIP 3개 삭제
 - DB 인스턴스 1개 중지
- 현재 남아있는 유료 서비스
 - EBS: Wordpress AMI
 - DB 인스턴스: DB 인스턴스의 저장소 및 스냅샷
 - 모두 학기 종료 후, 최종 성적 공지 이후 삭제

(참고) wordpress 유저 암호 업데이트 방법

- Wordpress 관련 데이터의 저장 장소
 - Local FS: 소스 및 실행 파일, 미디어파일, 플러그인
 - 현재 미디어파일은 S3로 offload 함
 - DB: 유저 정보, 게시물
 - Remote DB로 offload함
 - 새로운 인스턴스를 생성하더라도, wordpress user 암호는 remote DB에 기록된 내용을 사용함

- 만약 DB의 user 암호가 유실된 경우, 아래 명령으로 update

```
USE bitnami_wordpress;  
UPDATE wp_users  
SET user_pass = MD5('NEW_PASSWORD')  
WHERE user_login = 'user'  
LIMIT 1
```