AWS 기술 에센셜

실습 안내서

버전 4.0

100-ESS-40-KO-LG

목차

실습 1
VPC 구축 및 웹 서버 배포

개요

본 실습 섹션에서는 Amazon Virtual Private Cloud(VPC)를 사용하여 자체 VPC를 생성하고, VPC에 구성 요소를 추가하여 사용자 정의된 네트워크를 구성합니다. EC2 인스턴스에 대한 보안 그룹을 생성합니다. 웹 서버를 실행하고 이를 VPC에서 시작하도록 EC2 인스턴스를 구성 및 사용자 정의합니다.

목표

본 실습을 마친 후 다음을 할 수 있게 됩니다.

- VPC 생성
- 서브넷 생성
- 보안 그룹 구성
- VPC에서 EC2 인스턴스 시작

사전 조건

본 실습을 위해서는 다음이 필요합니다.

- Microsoft Windows, Mac OS X 또는 Linux(Ubuntu, SuSE, Red Hat)가 실행되며 Wi-Fi가 되는 컴퓨터 사용
- iPad나 태블릿 디바이스로는 qwikLABS 실습 환경에는 액세스가 안되지만, 수강생 안내서는 볼 수 있습니다.
- Chrome, Firefox 또는 IE9 이상 버전과 같은 인터넷 브라우저(IE9 이전 버전은 지원 안 됨)

기간

본 실습에는 약 45분 정도가 소요됩니다.

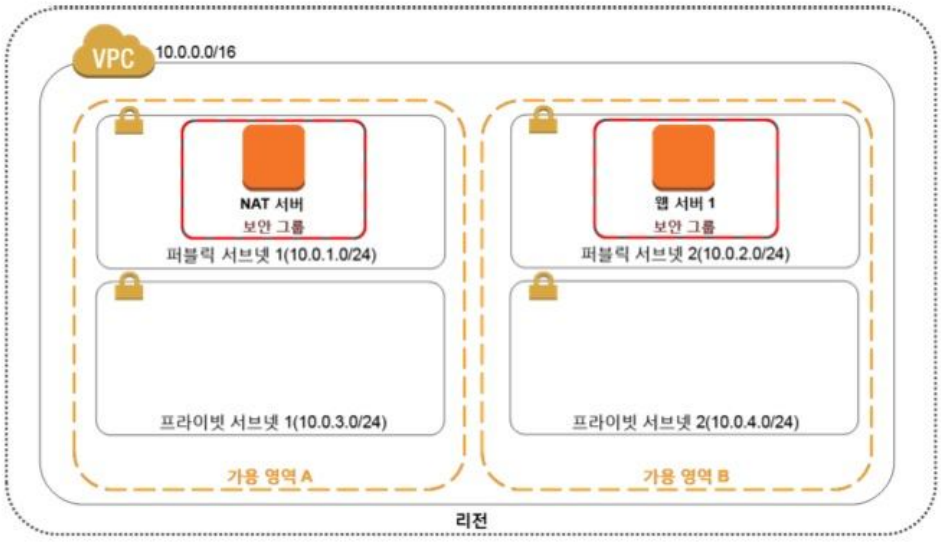
Task 1: VPC 생성

개요

이 섹션에서는 VPC를 생성합니다.

시나리오

본 실습에서는 다음과 같은 인프라를 구축하게 됩니다.



Task 1.1: VPC 생성

이 작업에서는 하나의 가용 영역에서 2개의 서브넷으로 구성된 VPC를 생성합니다.

1.1.1 **AWS Management Console**의 **Services** 메뉴에서 **VPC**를 클릭합니다.

1.1.2 **Start VPC Wizard**를 클릭합니다.

1.1.3 탐색 창에서 **VPC with Public and Private Subnets**를 클릭합니다.

1.1.4 **Select**를 클릭합니다.

- 다음 정보를 입력합니다.
- **IP CIDR block**: **10.0.0.0/16**
- **VPC name**: **My Lab VPC**
- **Public subnet**: **10.0.1.0/24**
- **Availability Zone**: 가용 영역을 클릭
- **Public subnet name**: **Public Subnet 1**
- **Private subnet**: **10.0.3.0/24**
- **Availability Zone**: 퍼블릭 서브넷과 같은 가용 영역을 클릭
- **Private subnet name**: **Private Subnet 1**

1.1.5 **Specify the details of your NAT gateway**에서 화면 오른쪽의 **Use a NAT instance instead**를 클릭합니다.

1.1.6 **Instance type**에 나열된 첫 번째 인스턴스 유형을 선택합니다(예: t2.micro).

1.1.7 **Key pair name**에서 **qwikLABS** 키 페어를 선택합니다.

1.1.8 **Create VPC**를 클릭합니다.

1.1.9 VPC가 생성되면, VPC가 성공적으로 생성되었다는 메시지가 표시된 페이지가 보입니다. **OK**를 클릭합니다.

Task 1.2: 추가 서브넷 생성

본 작업에서는 다른 가용 영역에 서브넷 2개를 추가로 생성하고 기존 라우팅 테이블을 통해 서브넷을 연결합니다.

1.2.1 탐색 창에서 **Subnets**를 클릭합니다.

1.2.2 **Create Subnet**을 클릭합니다.

1.2.3 **Create Subnet** 대화 상자에서 다음 세부 정보를 입력합니다.

- **Name tag**: **Public Subnet 2**
- **VPC**: **My Lab VPC** 클릭
- **Availability Zone**: 앞의 작업에서 프라이빗 서브넷 1과 퍼블릭 서브넷 1용으로 선택한 가용 영역이 아닌 다른 가용 영역을 선택
- **CIDR block**: **10.0.2.0/24**

1.2.4 **Yes, Create**를 클릭합니다.

1.2.5 **Create Subnet**을 클릭합니다.

1.2.6 **Create Subnet** 대화 상자에서 다음 세부 정보를 입력합니다.

- **Name tag**: **Private Subnet 2**
- **VPC**: **My Lab VPC** 클릭
- **Availability Zone:** 퍼블릭 서브넷 2용으로 선택한 것과 같은 가용 영역을 선택
- **CIDR block**: **10.0.4.0/24**

1.2.7 **Yes, Create**를 클릭합니다.

1.2.8 **Public Subnet 2**를 선택하고, 모든 다른 서브넷이 선택 해제되었는지 확인한 다음, 아래쪽 창에 있는 **Route Table**을 클릭합니다. 아래로 스크롤하여 **Destination 0.0.0.0/0**의 **Target**에 접두사 **igw**가 포함되어 있는지 확인합니다. 포함되어 있지 않은 경우, **Edit**를 클릭하고 **Change to:** 목록에 있는 다른 라우팅 테이블을 클릭하여 **Destination 0.0.0.0/0**의 **Target**이 접두사 **igw**를 포함하도록 변경합니다. **Save**를 클릭합니다.

1.2.9 **Private Subnet 2**를 선택하고, 모든 다른 서브넷이 선택 해제되었는지 확인한 다음, 아래쪽 창에 있는 **Route Table**을 클릭합니다. 아래로 스크롤하여 **Destination 0.0.0.0/0**의 **Target**에 접두사 **eni**가 포함되어 있는지 확인합니다. 포함되어 있지 않은 경우, **Edit** 를 클릭하고 **Change to:** 목록에 있는 다른 라우팅 테이블을 클릭하여 **Destination 0.0.0.0/0**의 **Target**이 접두사 **eni**를 포함하도록 변경합니다. **Save**를 클릭합니다.

Task 1.3: VPC 보안 그룹 생성

웹 및 SSH 트래픽에 대한 액세스 권한을 부여하는 VPC 보안 그룹을 생성합니다.

1.3.1 탐색 창에서 **Security Groups**를 클릭합니다.

1.3.2 **Create Security Group**을 클릭합니다.

1.3.3 **Create Security Group** 대화 상자에서 다음 정보를 입력합니다.

- **Name tag**: **WebSecurityGroup**
- **Group name**: **WebSecurityGroup**
- **Description**: **Enable HTTP access**
- **VPC**: 작업 1.1에서 생성한 VPC를 클릭(**My Lab VPC**)

1.3.4 **Yes, Create**를 클릭합니다.

1.3.5 **WebSecurityGroup**을 선택합니다.

1.3.6 **Inbound Rules** 탭을 클릭합니다.

1.3.7 **Edit**를 클릭합니다.

1.3.8 **Type**에서 **HTTP (80)**를 클릭합니다.

1.3.9 **Source** 상자를 클릭하고 **0.0.0.0/0**을 입력합니다.

1.3.10 **Add another rule**을 클릭합니다.

1.3.11 **Type**에서 **SSH (22)**를 클릭합니다.

1.3.12 **Source** 상자를 클릭하고 **0.0.0.0/0**을 입력합니다.

1.3.13 **Save**를 클릭합니다.

Task 2: Web Server 시작

개요

VPC를 생성한 후, 생성한 VPC에서 EC2 인스턴스를 시작하고, 웹 서버의 역할을 하도록 부트스트랩합니다.

명령 참조 파일

본 실습 매뉴얼에 제공된 텍스트를 복사할 때는 명령 참조 파일을 사용합니다. 명령 참조 파일은 qwikLABS 실습에서 [ADDL. INFO] 버튼을 클릭하면 받을 수 있습니다.

매뉴얼의 다양한 서식으로 인해 불필요한 문자가 삽입되어 실습에 오류가 발생할 수 있으므로, 본 실습 매뉴얼에서 직접 명령을 복사해서 붙여 넣어서는 안 됩니다. 대신 명령 참조 파일을 컴퓨터에 다운로드하십시오.

Task 2.1: 첫 번째 웹 서버 인스턴스 시작

본 작업에서는 VPC에서 EC 인스턴스를 시작하는 과정을 살펴봅니다. 이 인스턴스는 웹 서버의 역할을 합니다.

2.1.1 **Services** 메뉴에서 **EC2**를 클릭합니다.

2.1.2 **Launch Instance**를 클릭합니다.

2.1.3 **Amazon Linux AMI** 행에서 **Select**를 클릭합니다.

2.1.4 **Step 2: Choose an Instance Type** 페이지에서 **t2.micro**가 선택되었는지 확인하고 **Next: Configure Instance Details**를 클릭합니다.

2.1.5 **Step 3: Configure Instance Details** 페이지에서 다음 정보를 입력하고 나머지 값은 모두 기본값으로 둡니다.

- **Network**: 작업 1.1에서 생성한 VPC를 클릭(**My Lab VPC**)
- **Subnet**: 작업 1.2에서 생성한 **Public Subnet 2 (10.0.2.0/24)**를 클릭
- **Auto-assign Public IP**: **Enable**을 클릭

2.1.6 아래로 스크롤하여 **Advanced Details** 섹션을 확장합니다.

2.1.7 명령 참조 파일에서 다음 사용자 데이터를 복사하여 **User data** 상자에 붙여 넣고, **As text**가 선택되었는지 확인합니다.

```
#!/bin/bash -ex
yum -y update
yum -y install httpd php mysql php-mysql
chkconfig httpd on
/etc/init.d/httpd start
if [ ! -f /var/www/html/lab2-app.tar.gz ]; then
cd /var/www/html
wget https://us-west-2-aws-staging.s3.amazonaws.com/awsu-ilt/AWS-100-ESS/v4.0/lab-2-configure-website-datastore/scripts/lab2-app.tar.gz
tar xvfz lab2-app.tar.gz
chown apache:root /var/www/html/lab2-app/rds.conf.php
fi
```

2.1.8 **Next: Add Storage**를 클릭합니다.

2.1.9 **Next: Add Tags** 를 클릭합니다.

2.1.10 **Step 5: Add Tags** 페이지에서 다음 정보를 입력합니다.

- **Key**: **Name**
- **Value**: **Web Server 1**

2.1.11 **Next: Configure Security Group**을 클릭합니다.

2.1.12 **Step 6: Configure Security Group** 페이지에서 **Select an existing security group**을 클릭한 후, 작업 1.3에서 생성한 보안 그룹을 선택합니다(**WebSecurityGroup**).

2.1.13 **Review and Launch**를 클릭합니다.

2.1.14 인스턴스 정보를 확인한 후 **Launch**를 클릭합니다.

2.1.15 **Choose an existing key pair**를 클릭하고, **qwikLABS** 키 페어를 클릭하고, 승인 확인란을 선택한 후, **Launch Instances**를 클릭합니다.

2.1.16 아래로 스크롤하여 **View Instances**를 클릭합니다.

2.1.17 2개의 인스턴스(**Web Server 1**과 VPC 마법사에서 시작한 NAT 인스턴스)가 보일 것입니다.

2.1.18 **Web Server 1**의 **Status Checks** 열에 2/2 checks passed가 표시될 때까지 기다립니다. 3~5분 정도 걸립니다. 오른쪽 위에 있는 새로 고침 아이콘을 사용하여 업데이트를 확인합니다.

2.1.19 **Web Server 1**을 선택하고 **Public DNS** 값을 복사합니다.

2.1.20 새 웹 브라우저 창이나 탭에 **Public DNS** 값을 붙여 넣고 [Enter]를 누릅니다. **Amazon Linux AMI Test Page**가 보일 것입니다.

실습 완료

축하합니다! 성공적으로 VPC를 생성하고 생성한 VPC에서 EC2 인스턴스를 시작했습니다.
다음을 수행하여 실습 환경을 정리하십시오.

1. 오른쪽 위 모서리에서 **awsstudent**를 클릭하여 **AWS Management Console**에서 로그아웃하고, **Sign Out**을 클릭합니다.

2. 실습을 시작한 **qwikLABS** 페이지로 돌아가서 **End**를 클릭합니다.

실습 2

웹 사이트를 위한 관계형 데이터 스토어 구성

개요

이 실습은 이전 실습을 기반으로 합니다. Amazon Relational Database Service(RDS) DB 인스턴스를 시작하는 과정을 살펴봅니다. 관계형 데이터베이스 관리 시스템(RDBMS) 요구 사항에 맞게 Amazon RDS를 사용하도록 앞에서 생성한 웹 서버를 구성합니다. 본 실습은 AWS 관리형 데이터베이스 인스턴스를 활용하여 관계형 데이터베이스 요구 사항을 해결하는 개념을 강화하도록 설계되었습니다.

목표

본 실습을 마친 후 다음을 할 수 있게 됩니다.

- 고가용성을 갖춘 Amazon RDS DB 인스턴스를 시작
- 웹 서버로부터의 연결을 허용하도록 DB 인스턴스를 구성
- 웹 애플리케이션을 열고 데이터베이스와 상호 작용

사전 조건

본 실습을 위해서는 다음이 필요합니다.

- Microsoft Windows, Mac OS X 또는 Linux(Ubuntu, SuSE, Red Hat)가 실행되며 Wi-Fi가 되는 컴퓨터 사용
- iPad나 태블릿 디바이스로는 qwikLABS 실습 환경에는 액세스가 안되지만, 수강생 안내서는 볼 수 있습니다.
- Chrome, Firefox 또는 IE9 이상 버전과 같은 인터넷 브라우저(IE9 이전 버전은 지원 안 됨)

기간

본 실습에는 약 45분 정도가 소요됩니다.

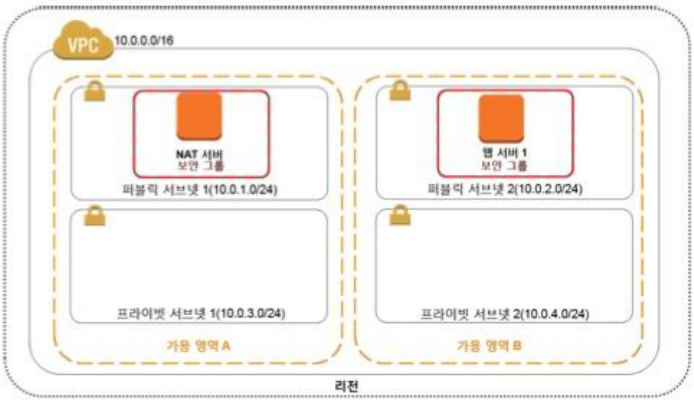
Task 1: Amazon RDS DB 인스턴스 시작

개요

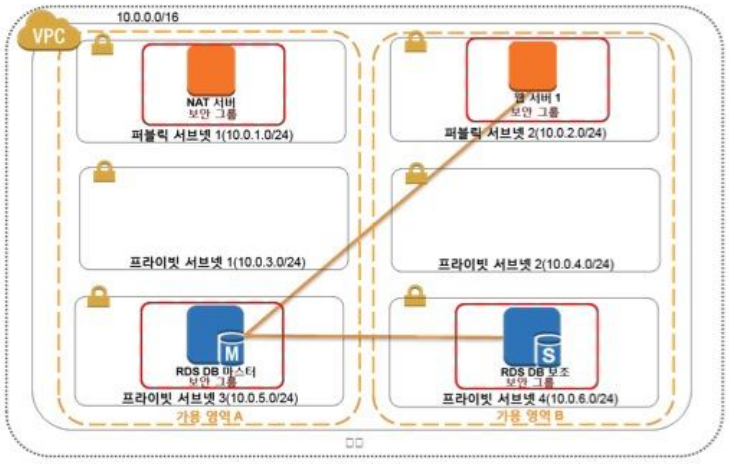
이 작업에서는 MySQL이 지원되는 Amazon RDS DB 인스턴스를 시작합니다.

시나리오

다음 인프라에서 시작합니다.



다음 인프라를 구축합니다.



Task 1.1: RDS DB 인스턴스에 대한 VPC 보안 그룹 생성

이 작업에서는 웹 서버가 RDS DB 인스턴스에 액세스하도록 허용하는 VPC 보안 그룹을 생성합니다.

1.1.1 **AWS Management Console**의 **Services** 메뉴에서 **VPC**를 클릭합니다.

1.1.2 탐색 창에서 **Security Groups**를 클릭합니다.

1.1.3 **Create Security Group**을 클릭합니다.

1.1.4 **Create Security Group** 대화 상자에서 다음 세부 정보를 입력합니다.

- **Name tag**: **DBSecurityGroup**
- **Group name**: **DBSecurityGroup**
- **Description**: **DB Instance Security Group**
- **VPC**: **My Lab VPC** 클릭

1.1.5 **Yes, Create**를 클릭합니다.

1.1.6 방금 생성한 **DBSecurityGroup**을 선택하고, 다른 모든 보안 그룹이 선택 해제되어 있는지 확인합니다.

1.1.7 **Inbound Rules** 탭을 선택하고 **Edit**를 클릭합니다.

1.1.8 다음 세부 정보로 인바운드 규칙을 생성합니다.

- **Type**: **MySQL/Aurora (3306)**
- **Protocol**: **TCP(6)**
- **Source**: **WebSecurityGroup** 클릭

1.1.9 **Save**를 클릭합니다.

Task 1.2: Amazon RDS 인스턴스용 프라이빗 서브넷 생성

이 작업에서는 Amazon RDS 인스턴스용 프라이빗 서브넷을 2개 생성합니다.

1.2.1 탐색 창에서 **Subnets**를 클릭합니다.

1.2.2 **Public Subnet 1**을 선택하고, 모든 다른 서브넷을 선택 해제한 다음, 아래쪽 창에 있는 **Summary** 탭으로 스크롤합니다. 이 서브넷의 **Availability Zone**을 적어둡니다.

1.2.3 **Public Subnet 2**를 선택하고, 모든 다른 서브넷을 선택 해제한 다음, 아래쪽 창에 있는 **Summary** 탭으로 스크롤합니다. 이 서브넷의 **Availability Zone**을 적어둡니다.

1.2.4 **Create Subnet**을 클릭합니다.

1.2.5 **Create Subnet** 대화 상자에서 다음 세부 정보를 입력합니다.

- **Name tag**: **Private Subnet 3**
- **VPC**: **My Lab VPC** 선택
- **Availability Zone:** 앞에서 퍼블릭 서브넷 1용으로 적어둔 가용 영역을 클릭
- **CIDR block**: **10.0.5.0/24**

1.2.6 **Yes, Create**를 클릭합니다.

1.2.7 **Create Subnet**을 클릭합니다.

1.2.8 **Create Subnet** 대화 상자에서 다음 세부 정보를 입력합니다.

- **Name tag**: **Private Subnet 4**
- **VPC**: **My Lab VPC** 클릭
- **Availability Zone:** 앞에서 퍼블릭 서브넷 2용으로 적어둔 가용 영역을 클릭
- **CIDR block**: **10.0.6.0/24**

1.2.9 **Yes, Create**를 클릭합니다.

1.2.10 **Private Subnet 3**를 선택하고, 모든 다른 서브넷이 선택 해제되었는지 확인한 다음, 아래쪽 창에 있는 **Route Table**을 클릭합니다. 아래로 스크롤하여 **Destination 0.0.0.0/0**의 **Target**에 접두사 **eni**가 포함되어 있는지 확인합니다. 포함되어 있지 않거나 **Destination 0.0.0.0/0**이 없는 경우, **Edit**를 클릭하고 **Change to:** 목록에서 **Private Route Table**을 클릭하여 **Destination 0.0.0.0/0**의 **Target**이 접두사 **eni**를 포함하도록 변경합니다. **Save**를 클릭합니다.

1.2.11 **Private Subnet 4**에서 앞에서 수행한 단계를 반복합니다.

Task 1.3: DB 서브넷 그룹 생성

이 작업에서는 DB 서브넷 그룹을 생성합니다. 각 DB 서브넷 그룹은 지정된 리전에서 두 개 이상의 가용 영역에 서브넷이 있어야 합니다.

1.3.1 **Services** 메뉴에서 **RDS**를 클릭합니다.

1.3.2 탐색 창에서 **Subnet Groups**를 클릭합니다.

1.3.3 **Create DB Subnet Group**을 클릭합니다.

1.3.4 **Create DB Subnet Group** 페이지에서 다음 세부 정보를 입력합니다.

- **Name**: **dbsubnetgroup**
- **Description**: **Lab DB Subnet Group**
- **VPC ID**: **My Lab VPC** 클릭

1.3.5 **Availability Zone**의 경우, **Private Subnet 3**용으로 선택한 가용 영역을 클릭합니다.

1.3.6 **Subnet ID**의 경우, **10.0.5.0/24**를 클릭한 다음 **Add**를 클릭합니다.

1.3.7 **Availability Zone**의 경우, **Private Subnet 4**용으로 선택한 가용 영역을 클릭합니다.

1.3.8 **Subnet ID**의 경우, **10.0.6.0/24**를 클릭한 다음 **Add**를 클릭합니다.

1.3.9 **Create**를 클릭합니다.

1.3.10 새 서브넷 그룹이 보이지 않으면, 콘솔의 오른쪽 위 모서리에 있는 새로 고침 아이콘을 클릭합니다.

Task 1.4: RDS DB 인스턴스 생성

이 작업에서는 MySQL 지원 Amazon RDS DB 인스턴스를 구성 및 시작합니다.

1.4.1 **Services** 메뉴에서 **RDS**를 클릭합니다.

1.4.2 **Get Started Now**를 클릭합니다.

1.4.3 **MySQL**을 클릭하고 **Select**를 클릭합니다.

1.4.4 **Production** 아래의 **MySQL**을 클릭합니다.

1.4.5 **Next Step**을 클릭합니다.

1.4.6 **Specify DB Details** 페이지에서 다음 세부 정보를 입력합니다.

- **DB Instance Class**: 목록에 있는 첫 번째 옵션을 클릭
- **Multi-AZ Deployment**: **Yes** 클릭
- **DB Instance Identifier**: **labdbinstance**
- **Master Username**: **labuser**
- **Master Password**: **labpassword**
- **Confirm Password**: **labpassword**

1.4.7 **Next Step**을 클릭합니다.

1.4.8 **Configure Advanced Settings** 페이지에서 다음 정보를 입력하고 나머지 값은 모두 기본값으로 둡니다.

- **VPC**: **My Lab VPC**
- **Subnet Group**: **dbsubnetgroup**
- **Publicly Accessible**: **No**
- **VPC Security Group(s)**: **DBSecurityGroup (VPC)**
- **Database Name**: **sampledb**

다음으로 Monitoring 항목에서 Enable Enhanced Monitoring : No 를 설정합니다.

1.4.9 **Launch DB Instance**를 클릭합니다.

1.4.10 **View Your DB Instances**를 클릭합니다.

1.4.11 **labdbinstance**를 선택하고, **Endpoint**가 available 또는 modifying 으로 변할 때까지 기다립니다. 최대 10분 정도 걸릴 수 있습니다. 오른쪽 위에 있는 새로 고침 아이콘을 사용하여 업데이트를 확인합니다.

1.4.12 **Endpoint**를 복사하여 저장합니다. 3306을 복사하지 않도록 주의합니다. **Endpoint**는 qr7g2qco3oeq5h.cze6p5rivinc.us-west-2.rds.amazon.com과 비슷한 형태입니다.

Task 2: 데이터베이스와 상호 작용

개요

이 작업에서는 이전 실습에서 생성한 웹 서버에 배포된 PHP 웹 애플리케이션을 통해 데이터베이스와 상호 작용합니다.

Task 2.1: 데이터베이스 웹 애플리케이션에 액세스

웹 서버에서 실행되는 웹 애플리케이션을 엽니다.

2.1.1 **Services** 메뉴에서 **EC2**를 클릭합니다.

2.1.2 탐색 창에서 **Instances**를 클릭합니다.

2.1.3 **Web Server 1**을 선택하고, 모든 다른 인스턴스가 선택 해제되었는지 확인한 후, 아래쪽 창에 있는 **Description** 탭까지 아래로 스크롤합니다.

2.1.4 **Web Server 1**의 **Public IP** 주소를 복사합니다.

2.1.5 IP 주소를 새 브라우저 탭 또는 창에 붙여 넣습니다. 웹 애플리케이션이 웹 서버의 인스턴스 메타데이터와 함께 표시됩니다.

2.1.6 AWS 로고 오른쪽 옆에 있는 **RDS** 링크를 클릭합니다.

2.1.7 다음 정보를 입력합니다.

- **Endpoint**: 앞에서 복사한 엔드포인트를 붙여 넣습니다. 3306이 생략되어 있는지 확인합니다.
- **Database**: **sampledb**
- **Username**: **labuser**
- **Password**: **labpassword**

2.1.8 **Submit**를 클릭합니다. 연결 문자열이 표시된 후, 페이지가 리디렉션됩니다. 2개의 새로운 레코드가 주소 테이블에 추가되어 표시됩니다.

2.1.9 또 다른 담당자를 추가하려면 **Add Contact**을 클릭하고 **Name**, **Phone** 및 **Email**을 입력한 후, **Submit**를 클릭합니다.

2.1.10 담당자를 수정하려면, **Edit**를 클릭하고, 원하는 필드를 수정한 다음, **Submit**를 클릭합니다.

2.1.11 레코드를 삭제하려면, **Remove**를 클릭합니다.

2.1.12 이제 이 브라우저 탭이나 창을 닫아도 됩니다.

실습 완료

축하합니다! 웹 사이트를 위한 관계형 데이터 스토어 구성을 성공적으로 완료했습니다. 다음을 수행하여 실습 환경을 정리하십시오.

1. 오른쪽 위 모서리에서 **awsstudent**를 클릭하여 **AWS Management Console**에서 로그아웃하고, **Sign Out**을 클릭합니다.

2. 실습을 시작한 **qwikLABS** 페이지로 돌아가서 **End**를 클릭합니다.

실습 3
인프라 관리

개요

본 실습은 이전 실습을 기반으로 하며, Elastic Load Balancing(ELB)과 Auto Scaling 서비스를 사용하여 인프라를 로드 밸런싱하고 자동 조정하는 과정을 살펴봅니다.

목표

본 실습을 마친 후 다음을 할 수 있게 됩니다.

- 실행 중인 인스턴스에서 Amazon 머신 이미지(AMI)를 생성
- 로드 밸런서 추가
- 시작 구성 생성
- Auto Scaling 그룹 생성
- 프라이빗 서브넷 내에서 새 인스턴스를 자동 조정
- Amazon CloudWatch 경보 생성
- 인프라의 성능 모니터링

사전 조건

본 실습을 위해서는 다음이 필요합니다.

- Microsoft Windows, Mac OS X 또는 Linux(Ubuntu, SuSE, Red Hat)가 실행되며 Wi-Fi 가 되는 컴퓨터 사용
- iPad 나 태블릿 디바이스로는 qwikLABS 실습 환경에는 액세스가 안되지만, 수강생 안내서는 볼 수 있습니다.
- Chrome, Firefox 또는 IE9 이상 버전과 같은 인터넷 브라우저(IE9 이전 버전은 지원 안 됨)

기간

본 실습에는 약 45 분 정도가 소요됩니다.

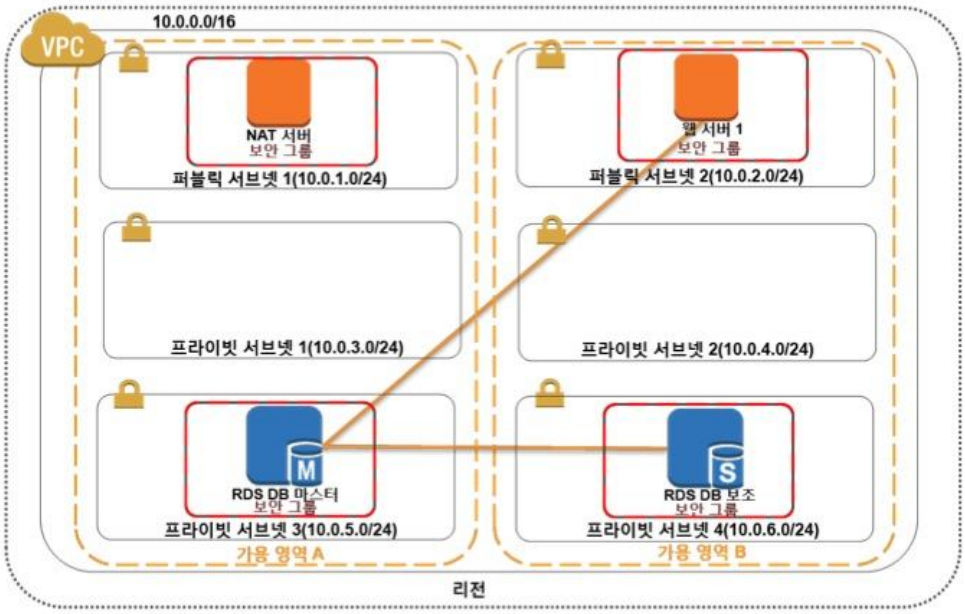
Task 1: Auto Scaling

개요

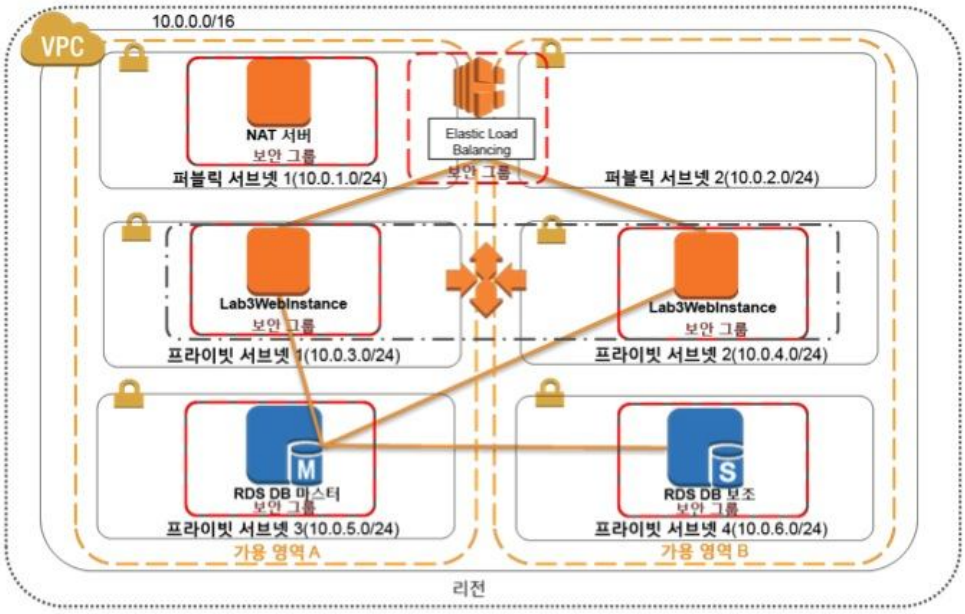
이 작업에서는 인프라를 생성하고 자동 조정합니다.

시나리오

다음 인프라에서 시작합니다.



다음 인프라를 구축합니다.



Task 1.1: Auto Scaling 용 AMI 생성

이 작업에서는 Auto Scaling 에서 사용할 새로운 인스턴스를 시작하는 출발점으로 AMI 를 생성합니다.

1.1.1 **AWS Management Console** 의 **Services** 메뉴에서 **EC2** 를 클릭합니다.

1.1.2 탐색 창에서 **Instances** 를 클릭합니다.

1.1.3 **Web Server 1** 의 **Status Checks** 가 2/2 checks passed 로 표시되어 있는지 확인합니다. 아닌 경우, 변경될 때까지 기다렸다가 다음 단계로 진행합니다. 오른쪽 위에 있는 새로 고침 버튼을 사용하여 업데이트를 확인합니다.

1.1.4 **Web Server 1** 을 오른쪽 마우스 클릭하고, **Image** 를 클릭한 후, **Create Image** 를 클릭합니다.

1.1.5 다음 정보를 입력하고, 나머지 값은 그대로 기본값으로 둡니다.

- **Image name**: **Web Server AMI**
- **Image description**: **Lab 3 AMI for Web Server**

1.1.6 **Create Image** 를 클릭합니다.

1.1.7 확인 화면에 새로운 AMI 용 **AMI ID** 가 표시됩니다.

1.1.8 **Close** 를 클릭합니다.

Task 1.2: 로드 밸런서 추가

이 작업에서는 로드 밸런서를 생성하여 2 개의 가용 영역에서 여러 EC 인스턴스에 걸쳐 트래픽을 로드 밸런싱합니다.

1.2.1 탐색 창에서 **Load Balancers** 를 클릭합니다.

1.2.2 **Create Load Balancer** 를 클릭한 후 다음 화면에서 Classic Load Balancer를 선택합니다.

1.2.3 다음 정보를 입력하고, 나머지 값은 그대로 기본값으로 둡니다.

- **Load Balancer name**: **Lab3ELB**
- **Create LB inside**: **My Lab VPC** 선택
- **Select Subnets**: [+]를 클릭하여 **Public Subnet 1** 및 **Public Subnet 2** 를 선택

1.2.4 **Next: Assign Security Groups** 를 클릭합니다.

1.2.5 **default** 보안 그룹을 선택 해제하고, 이름에 **WebSecurityGroup** 이 포함되고 **Enable HTTP access** 라는 **Description** 이 있는 보안 그룹을 선택합니다.

1.2.6 **Next: Configure Security Settings** 를 클릭합니다.

1.2.7 본 실습에서는 보안 리스너는 구성하지 않으므로, **Next: Configure Health Check** 를 클릭합니다.

1.2.8 다음 정보를 입력하고, 나머지 값은 그대로 기본값으로 둡니다.

- **Ping Path**: **/index.php** (기본값과 다른 값입니다)
- **Interval**: **6**
- **Healthy Threshold**: **2** 를 선택

1.2.9 **Next: Add EC2 Instances** 를 클릭합니다.

1.2.10 다음 작업에서 로드 밸런서에 EC2 인스턴스를 추가합니다. **Next: Add Tags** 를 클릭합니다.

1.2.11 **Review and Create** 를 클릭합니다.

1.2.12 로드 밸런서의 구성을 확인하고 **Create** 를 클릭합니다.

1.2.13 **Close** 를 클릭합니다.

1.2.14 **Lab3ELB** 를 선택하고, 아래쪽 창의 **Description** 에서 로드 밸런서의 **DNS Name** 을 적어둡니다. 이때 (A Record)는 생략합니다.

Task 1.3: 시작 구성 및 Auto Scaling 그룹 생성

이 작업에서는 Auto Scaling 그룹에 대한 시작 구성을 생성합니다.

1.3.1 탐색 창에서 **Launch Configurations** 를 클릭합니다.

1.3.2 **Create Auto Scaling group** 과 **Create launch configuration** 을 클릭합니다.

1.3.3 탐색 창에서 **My AMIs** 를 클릭합니다.

1.3.4 앞에서 생성한 **Web Server AMI** 를 선택하기 위해 **Select** 를 클릭합니다.

1.3.5 **t2.micro** 선택을 수락하려면 **Next: Configure details** 를 클릭합니다.

1.3.6 다음 정보를 입력하고, 나머지 값은 그대로 기본값으로 둡니다.

- **Name**: **Lab3Config**
- **Monitoring**: **Enable CloudWatch detailed monitoring** 선택

1.3.7 **Next: Add Storage** 를 클릭합니다.

1.3.8 **Next: Configure Security Group** 을 클릭합니다.

1.3.9 **Select an existing security group** 을 클릭하고, 이름에 **WebSecurityGroup** 이 포함되고 **Enable HTTP access** 라는 **Description** 이 있는 보안 그룹을 선택합니다.

1.3.10 **Review** 를 클릭합니다.

1.3.11 시작 구성의 세부 정보를 확인하고, **Create launch configuration** 을 클릭합니다.

1.3.12 **Choose an existing key pair** 를 클릭하고, **qwikLABS key pair** 를 선택하고, 승인 확인란을 선택한 후, **Create launch configuration** 을 클릭합니다.

1.3.13 Auto Scaling 그룹에 대한 다음 정보를 입력하고, 나머지 값은 그대로 기본값으로 둡니다.

- **Group name**: **Lab3ASGroup**
- **Group size**: **2** 개의 인스턴스로 시작
- **Network**: **My Lab VPC** 선택
- **Subnet**: **Private Subnet 1 (10.0.3.0/24)** 및 **Private Subnet 2 (10.0.4.0/24)** 선택

1.3.14 아래로 스크롤하여 **Advanced Details** 를 확장하고 **Receive traffic from one or more load balancers** 를 선택합니다.

1.3.15 **Classic Load Balancers** 텍스트 상자를 클릭한 다음, **Lab3ELB** 를 클릭합니다.

1.3.16 다음 정보를 입력하고, 나머지 값은 그대로 기본값으로 둡니다.

- **Health Check Type**: **ELB** 선택
- **Monitoring**: **Enable CloudWatch detailed monitoring** 선택

1.3.17 **Next: Configure scaling policies** 를 클릭합니다.

1.3.18 **Use scaling policies to adjust the capacity of this group** 을 선택합니다.

1.3.19 **2** 개와 **6** 개의 인스턴스 범위 내에서 조정할 수 있도록 **Scale between** 텍스트 상자를 수정합니다.

1.3.20 **Increase Group Size** 에서 **Execute policy when** 에 대해 **Add New Alarm** 을 클릭합니다.

1.3.21 **Send a notification to:**가 선택되어 있는지 확인한 후, **create topic** 을 클릭합니다(이메일 알림을 생성하는 것은 선택 사항이며, 나머지 실습에서 [*]로 표시된 관련 단계를 건너뛰어도 좋습니다. 이메일 알림 을 받지 않으려면, **Send a notification to:** 을 선택 해제해야 합니다).

1.3.22 다음 정보를 입력하고, 나머지 값은 그대로 기본값으로 둡니다.

- ***Send a notification to**: **ASTopic**
- ***With these recipients**: 액세스 권한이 있는 이메일 주소를 입력
- **Whenever**: **Average of CPU Utilization**
- **Is >= 65 Percent**
- **For at least**: **1** consecutive period(s) of **1 minute**
- **Name of alarm**: **HighCPUUtilization**

1.3.23 **Create Alarm** 을 클릭합니다.

1.3.24 **Increase Group Size** 의 나머지 부분에 다음 정보를 입력합니다.

- **Take the action**: **Add** 선택, **1** 입력, **instances** 선택, **65** 입력
- **Instances need**: 각 단계 후 준비에 **60** 초

1.3.25 **Decrease Group Size** 에서 **Execute policy when** 에 대해 **Add New Alarm** 을 클릭합니다.

1.3.26 ***Send a notification to:**가 선택되어 있는지 확인하고, **ASTopic (<your email address>)**을 선택합니다. 이메일 알림을 받지 않으려면 이 항목을 선택 해제합니다.

1.3.27 다음 정보를 입력하고, 나머지 값은 그대로 기본값으로 둡니다.

- **Whenever**: **Average of CPU Utilization**

- **Is <= 20 Percent**
- **For at least**: **1** consecutive period(s) of **1 minute**
- **Name of alarm**: **LowCPUUtilization**

1.3.28 **Create Alarm** 을 클릭합니다.

1.3.29 **Decrease Group Size** 의 나머지 부분에 다음 정보를 입력합니다.

- **Take the action**: **Remove** 선택, **1** 입력, **instances** 선택, **20** 입력

1.3.30 **Next: Configure Notifications** 를 클릭합니다.

1.3.31 **Next: Configure Tags** 를 클릭합니다.

1.3.32 다음 정보를 입력하고, 나머지 값은 그대로 기본값으로 둡니다.

- **Key**: **Name**
- **Value**: **Lab3WebInstance**

1.3.33 **Review** 를 클릭합니다.

1.3.34 Auto Scaling 그룹의 세부 정보를 확인한 다음, **Create Auto Scaling group** 을 클릭합니다.

1.3.35 Auto Scaling 그룹이 생성되면 **Close** 를 클릭합니다.

1.3.36 * Auto Scaling 그룹에 대한 알림 구독을 확인하는 이메일을 받게 됩니다. 이메일을 열고 **Confirm subscription link** 를 클릭합니다.

Task 1.4: Auto Scaling 이 작동하는지 확인하고 인스턴스를 로드 밸런서에 추가

이 작업에서는 Auto Scaling 이 올바르게 작동하고 있는지 확인합니다.

1.4.1 탐색 창에서 **Instances** 를 클릭합니다.

1.4.2 4 개의 인스턴스(**Web Server 1**, **NAT Server**, 그리고 **Lab3WebInstance** 라는 이름의 새로운 인스턴스 2 개)가 보일 것입니다.

1.4.3 탐색 창에서 **Load Balancers** 를 클릭합니다.

1.4.4 **Lab3ELB** 를 선택하고, 아래로 스크롤하여 **Instances** 탭을 클릭합니다. 이 로드 밸런서 목록에 **Lab3WebInstance** 가 나열된 것이 보일 것입니다.

1.4.5 **Lab3ELB** 의 **Instances** 탭에서 이 인스턴스의 **Status** 가 InService 로 바뀔 때까지 기다립니다. 오른쪽 위에 있는 새로 고침 버튼을 사용하여 업데이트를 확인합니다.

1.4.6 로드 밸런서가 인스턴스가 실행되고 있는 가용 영역의 **Healthy?** 필드 아래에 **Yes** 를 표시합니다.

Task 2: 인프라 모니터링

개요

인스턴스가 최소 2 개, 최대 6 개인 Auto Scaling 그룹을 생성했습니다. Auto Scaling 그룹을 한번에 인스턴스 하나씩 증가하거나 축소하는 Auto Scaling 정책을 생성했습니다. 그룹의 전체 평균 CPU 사용률이 >= 65%와 <= 20%일 때 각각 해당 정책을 트리거하는 Amazon CloudWatch 경보를 생성했습니다. 최소 크기는 2 이고 부하가 전혀 없으므로 현재 2 개의 인스턴스가 실행 중입니다. 생성한 CloudWatch 경보를 사용하여 이제 인프라를 모니터링할 수 있습니다.

Task 2.1: Auto Scaling 테스트

이 작업에서는 앞에서 구현한 Auto Scaling 구성을 테스트합니다.

2.1.1 **Services** 메뉴에서 **CloudWatch** 를 클릭합니다.

2.1.2 탐색 창에서 **Alarms** 를 클릭합니다(**ALARM** 이 아님).

2.1.3 **HighCPUUtilization** 과 **LowCPUUtilization** 이라는 2 개의 경보가 보입니다. **LowCPUUtilization** 은 **State** 가 **Alarm** 이어야 하고, **HighCPUUtilization** 은 **State** 가 **OK** 여야 합니다. 이는 현재 그룹 CPU 사용률이 20% 미만이기 때문입니다. 그룹 크기가 현재 최소 크기인 (2)이므로, Auto Scaling 은 어떠한 인스턴스도 제거하지 않습니다.

2.1.4 단계 1.2.13 에서 복사한 로드 밸런서의 DNS 이름을 새 브라우저 창 또는 탭에 복사합니다.

2.1.5 AWS 로고 오른쪽 옆에 있는 **LOAD TEST** 를 클릭합니다. 애플리케이션이 인스턴스에 대한 부하 테스트를 수행하고 5 초 간격으로 자동 새로 고침합니다. [Current CPU Load] 가 100%로 상승한 것을 볼 수 있습니다. **Load Test** 링크는 간단한 백그라운드 프로세스를 트리거합니다.

2.1.6 **Services** 메뉴에서 **CloudWatch** 를 클릭합니다.

5 분 이내에 **Low CPU** 경보 상태가 **OK** 로 변경되고 **High CPU** 경보 상태가 **ALARM** 으로 변경되는 것을 확인할 수 있습니다.

2.1.7 **Services** 메뉴에서 **EC2** 를 클릭합니다.

2.1.8 탐색 창에서 **Instances** 를 클릭합니다.

2.1.9 이제 **Lab3WebInstance** 라는 이름의 인스턴스가 2 개 이상 실행되는 것을 볼 수 있습니다.

2.1.10 단계 2.1.3 에서 연 브라우저 탭 또는 창을 닫습니다.

Task 2.2: 선택 사항: 웹 서버 1 종료

이 작업에서는 퍼블릭 서브넷 2 의 웹 서버 1 을 종료합니다. Auto Scaling 그룹이 프라이빗 서브넷에서 인스턴스를 시작했으므로, 공개적으로 액세스 가능한 원래 웹 서버는 더 이상 필요 없습니다.

2.2.1 **Services** 메뉴에서 **EC2** 를 클릭합니다.

2.2.2 탐색 창에서 **Instances** 를 클릭합니다.

2.2.3 **Web Server 1** 을 마우스 오른쪽 버튼으로 클릭하고 **Instance State** 와 **Terminate** 를 각각클릭합니다.

실습 완료

축하합니다! Auto Scaling 과 Elastic Load Balancing 을 사용하여 인프라를 관리하는 작업을 성공적으로 완료했습니다. 다음을 수행하여 실습 환경을 정리하십시오.

1. 오른쪽 위 모서리에서 **awsstudent** 를 클릭하여 **AWS Management Console** 에서 로그아웃하고, **Sign Out** 을 클릭합니다.

2. 실습을 시작한 **qwikLABS** 페이지로 돌아가서 **End** 를 클릭합니다.

부록 A

AWS Management Console 로그인하기

소개

이 부록에서는 본 과정의 일환으로 생성된 수강생 계정에 로그인하는 방법을 학습합니다.

수강생 계정

본 과정의 각 실습에는 qwikLABS 페이지에서 시작되는 실습 환경이 있습니다. (강사가 이미 qwikLABS 계정을 만드는 방법을 설명했을 것입니다.) 새 실습을 시작할 때마다 qwikLABS 환경이 수강생을 위해 새로운 AWS 계정을 생성합니다. 이 AWS 계정에서 **awsstudent**라는 이름의 IAM 사용자가 생성됩니다. 수강생이 실습을 종료하면 이 계정은 재활용되고 이와 관련된 모든 리소스가 종료됩니다.

본 과정에서 새 실습을 시작할 때마다 사용자 **awsstudent**로 새 실습 환경에 로그인해야 합니다. 이때 각 실습을 위한 qwikLABS 페이지에서 자동으로 생성된 암호를 사용합니다.

Task 1.1: 로그인하기

다음 지침은 AWS Management Console에 로그인하는 방법을 안내합니다.

1.1.1 qwikLABS의 **Class Details** 페이지에서 현재 실습을 검색하여 **Select**를 클릭합니다.

1.1.2 **Start Lab**을 클릭합니다.

1.1.3 실습 페이지에서, Create in Progress... 텍스트가 화면에서 사라질 때까지 기다립니다. 일부 실습에서는 이 과정이 즉시 이루어지지만, 다른 실습에서는 초기화가 5~10분이 걸릴 수도 있습니다.

참고: 실습 생성 프로세스가 완료된 후에 다음 단계로 이동하십시오.

1.1.4 **AWS Management Console** 아래에 **User Name** 및 **Password** 필드가 있습니다. 이것이 AWS 계정 자격 증명입니다. **Password** 필드를 선택하여 복사합니다.

1.1.5 **Open Console**을 클릭합니다. qwikLABS가 생성한 AWS 계정 ID가 미리 입력된 상태로 AWS Management Console이 열립니다.

참고: 이 버튼을 마우스 오른쪽 버튼으로 클릭하고 웹 브라우저의 "새 탭에서 열기" 기능을 사용하면 이 페이지가 새 창에서 열리지 않도록 할 수 있습니다.

1.1.6 AWS Management Console이 열려 있는 새 창 또는 탭에서 계정 ID가 이미 입력되어 있는 것이 보일 것입니다. Username 필드에 **awsstudent**를 입력합니다. Password 필드에 3단계에서 복사한 암호를 붙여 넣습니다. 마지막으로 **Sign In** 버튼을 클릭합니다.

참고: 드물게 로그인 페이지에서 계정 ID가 비어 있을 수 있습니다. qwikLABS 계정 ID를 찾는 방법은 강사에게 문의하십시오.