****

**EC2 Basic Session**

**Hands-On Lab (EC2 Linux)**

**Aug, 2018**

**Amazon Web Services**

**Table of Contents**

[Overview 3](#_Toc520987552)

[1. 새로운 키 쌍(Key Pair) 생성 4](#_Toc520987554)

[2. EC2 인스턴스 생성 6](#_Toc520987555)

[3. EC2의 웹 서버 접속 테스트 방법 11](#_Toc520987556)

[4. SSH로 EC2 접속 12](#_Toc520987557)

## Overview

Amazon Elastic Compute Cloud(Amazon EC2)는 클라우드상에서 손쉽게 용량 변경이 가능한 웹 기반 서비스입니다. Amazon EC2의 단순한 웹 서비스 기반 인터페이스를 통하여 사용자는 손쉽게 용량을 확보 할 수 있습니다. Amazon EC2는 사용자의 요구에 따라 빠르게 용량을 조정(Scale-Up 및 Scale-Down)할 수 있고 수분 이내에 컴퓨팅 자원(인스턴스)을 확보하고 시작 시킬 수 있습니다. Amazon EC2는 사용자가 실제로 사용한 컴퓨팅 용량과 시간만큼 비용을 지불합니다.

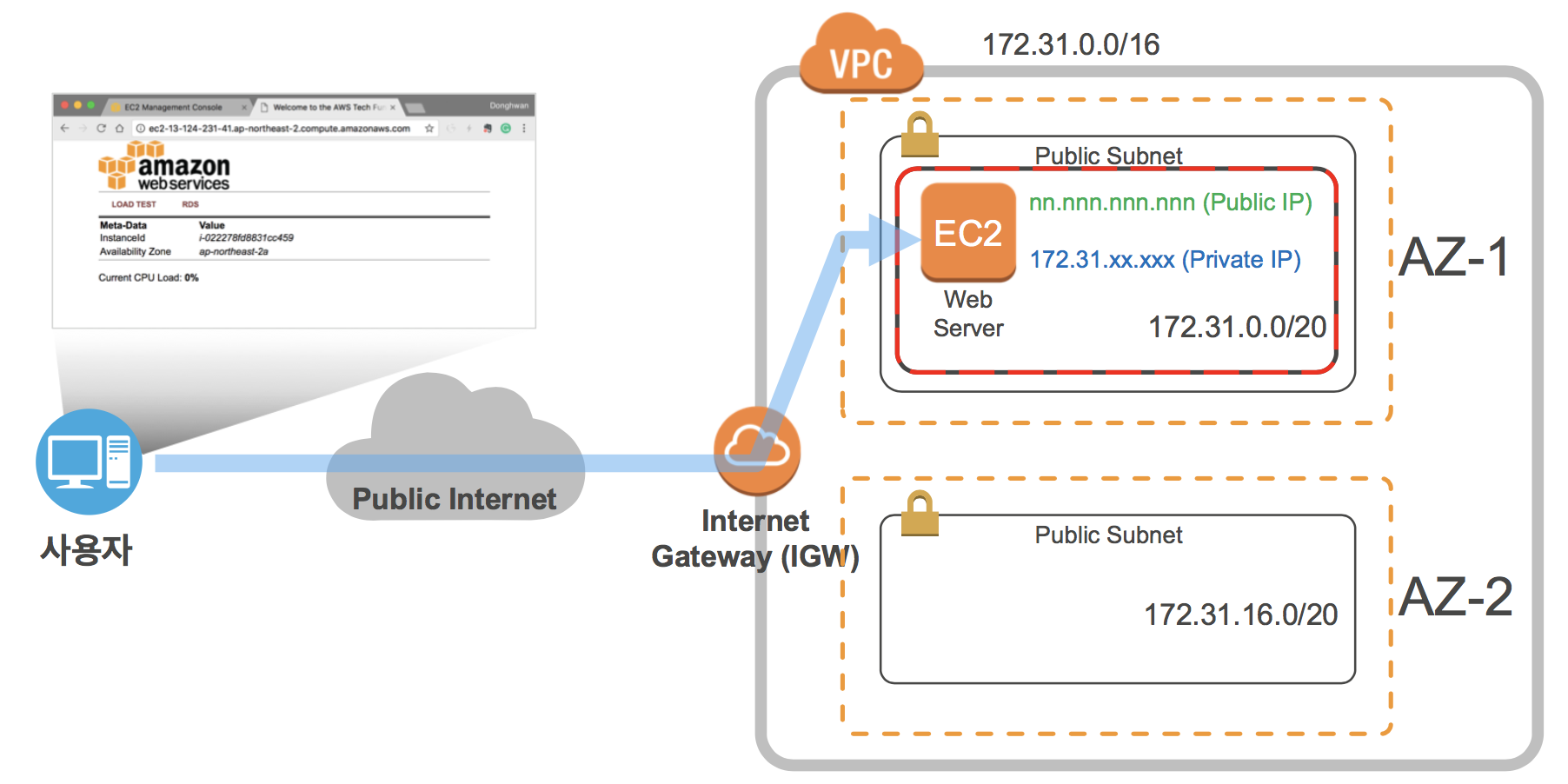
본 Lab은 웹 서비스를 수행하기 위한 EC2 가상머신(인스턴스)을 시작(Launching)하고 사용자의 요구에 맞게 구성하는 과정을 설명합니다. 이를 통하여 사용자는 AWS Management Console을 통하여 EC2 인스턴스를 프로비저닝하고 시작하는 과정을 익히게 됩니다.

본 Lab은 아래의 내용을 포함하고 있습니다.

* 키 페어 생성
* EC2 인스턴스 시작(Launching) 및 사용자 지정 데이터(User Data)의 실행
* 보안 그룹(Security Group)의 설정
* 고정 IP(Elastic IP)의 할당
* 인스턴스로 접속

### 목표 구성도

본 EC2 Lab은 Default VPC내에 EC2 Linux 인스턴스를 배포하고 Web Service를 구성하여 외부 사용자가 Web Browser를 통하여 Sample Web Page에 접근할 수 있도록 구성합니다.



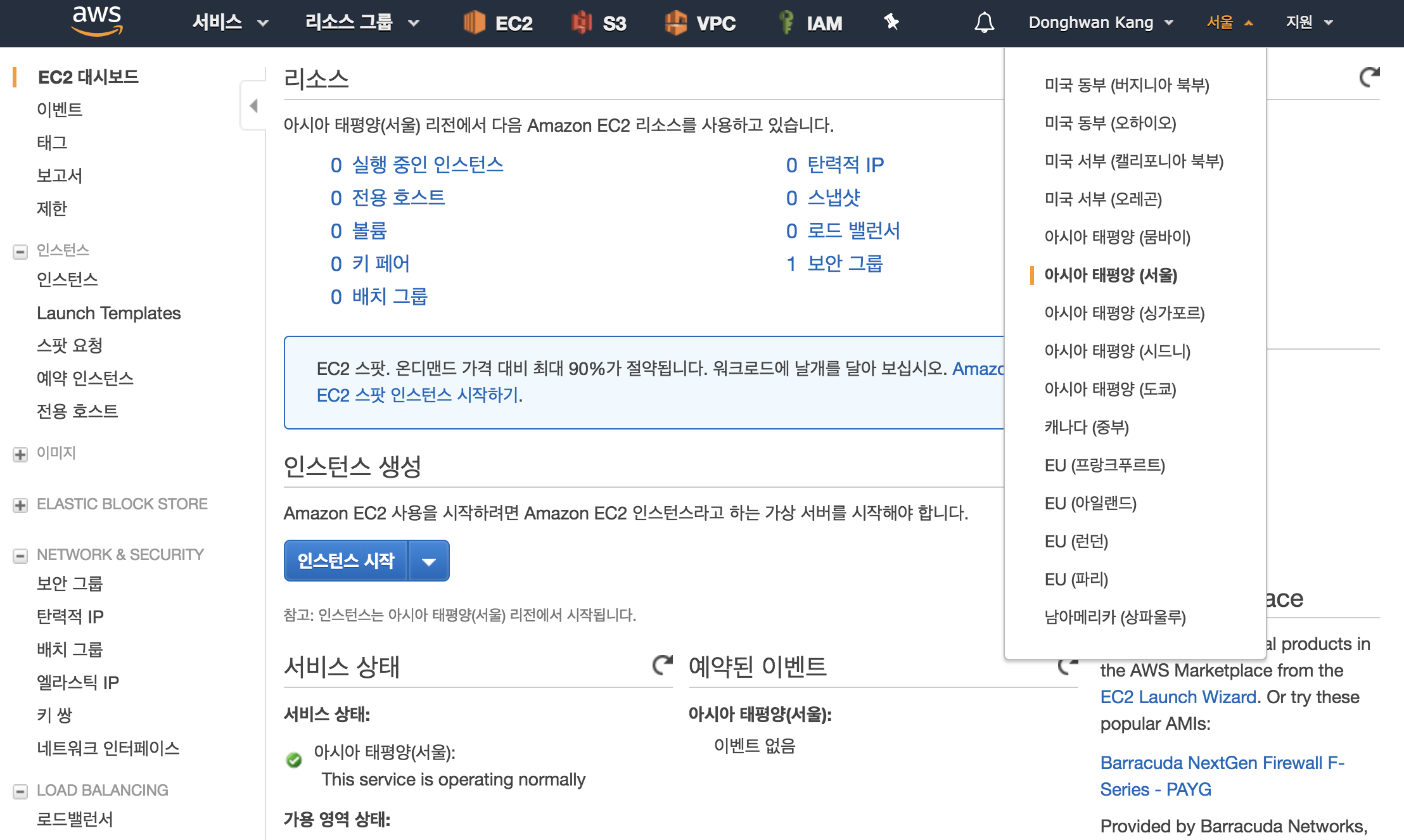
## 새로운 키 쌍(Key Pair) 생성

본 Lab의 수행을 위하여 사용자는 SSH Key Pair를 사용하는 EC2 인스턴스를 생성해야 합니다. 다음의 과정은 Lab 수행에 필요한 별도의 SSH Key Pair를 생성하는 과정을 설명합니다.

**icons_07_bw.eps**

키 쌍(Key Pairs)는 각 리전(Region)별로 독립적으로 관리됩니다.

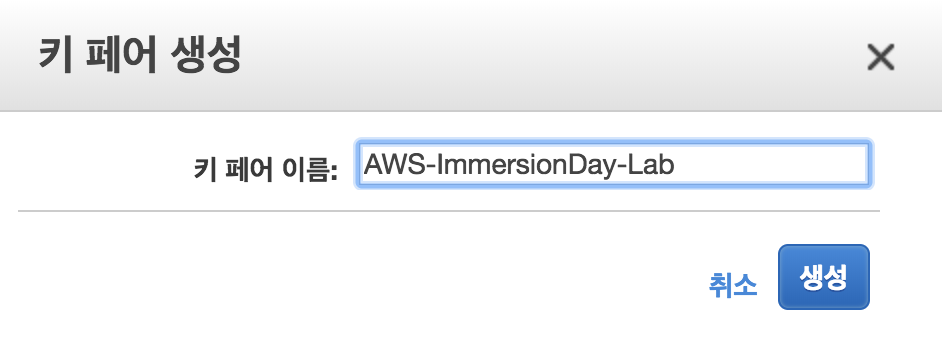
1. AWS Management Console에 로그인하고, Amazon EC2 Console을 여십시오. (<https://console.aws.amazon.com/ec2)>
2. AWS Management Console 화면 우측 상단의 사용 리전이 여러분이 사용 하고자 의도한 리전이 맞는지 확인하십시오.



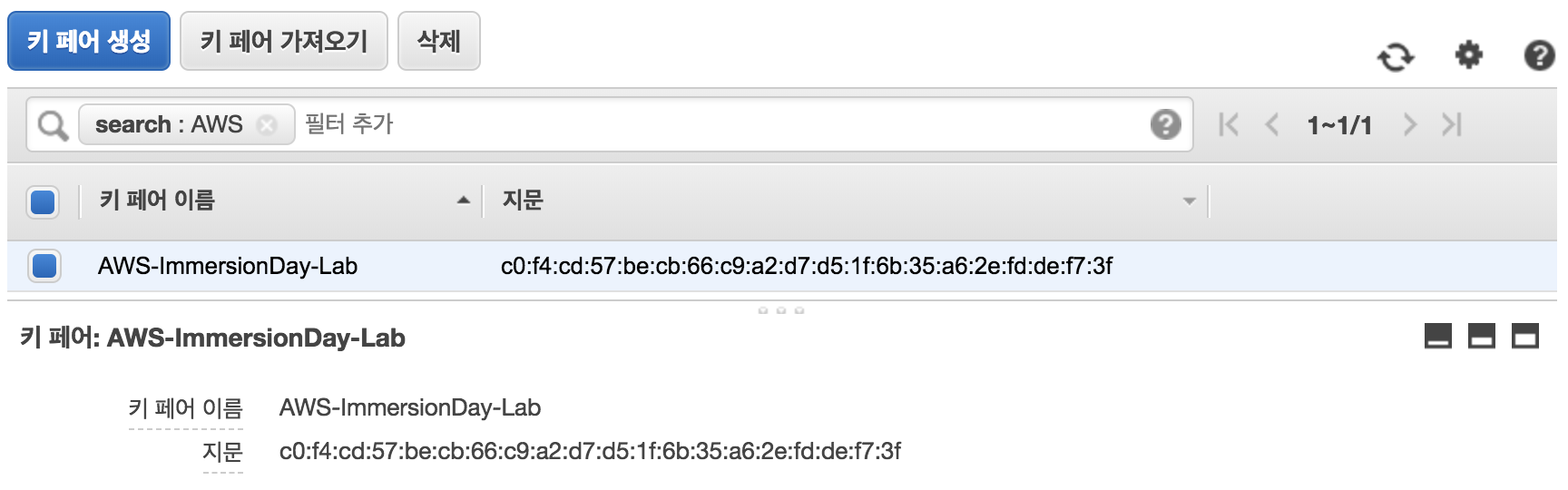
1. NETWORK & SECURITY 항목에 있는 **“키 쌍(Key Pairs)”**을 선택하십시오. SSH Key Pair를 관리할 수 있는 페이지가 보여지게 됩니다.
2. 새로운 SSH Key Pair를 생성하기 위하여 화면 상단 또는 화면 중간(키 페어가 없는 경우)의 **“키 페어 생성”** 버튼을 클릭 하십시오.



1. 키 페어 생성 윈도우에서, ***AWS-ImmersionDay-Lab*** 형식으로 키 페어 이름을 지정하고 **“생성”**을 클릭 하십시오. 키페어의 이름은 사용자가 식별하기 쉽도록 목적과 용도에 따라 지정이 가능합니다.



1. 새로운 키 페어가 생성되고, 최초 1회에 한하여 사용자의 PC로 다운로드 됩니다. 파일이름은 ***AWS-ImmersionDay-Lab.pem*** 입니다.



1. 다운로드된 키 페어 파일을 안전한 위치에 보관하시기 바랍니다.

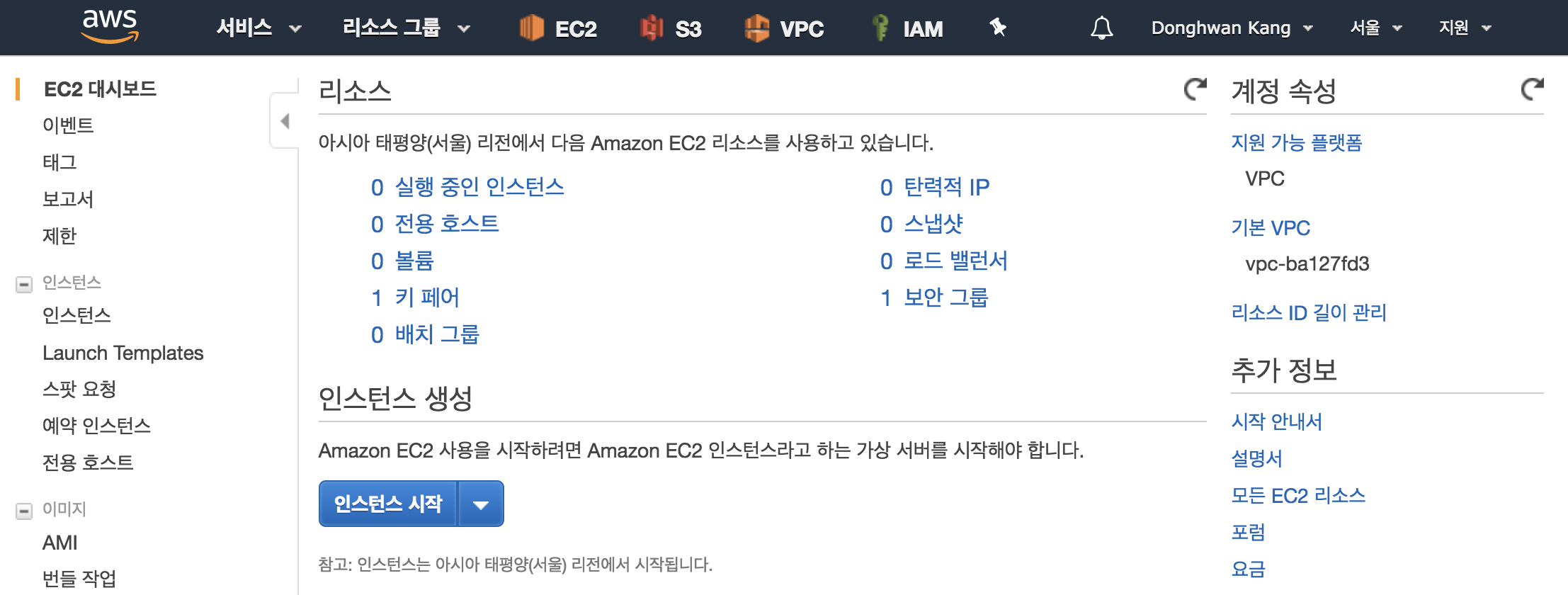
**icons_07_bw.eps**

다운로드된 키 페어 파일은 이후 Lab과정에서 생성하는 EC2 인스턴스에 지정하는데 사용됩니다. 또한, 이후 EC2 인스턴스에 로그인하기 위해서도 반드시 필요합니다.

## EC2 인스턴스 생성

이 과정에서는 기본 Amazon Linux 인스턴스를 시작하고, 초기화 과정에서 Apache/PHP Web Server를 자동으로 구성하도록 합니다.

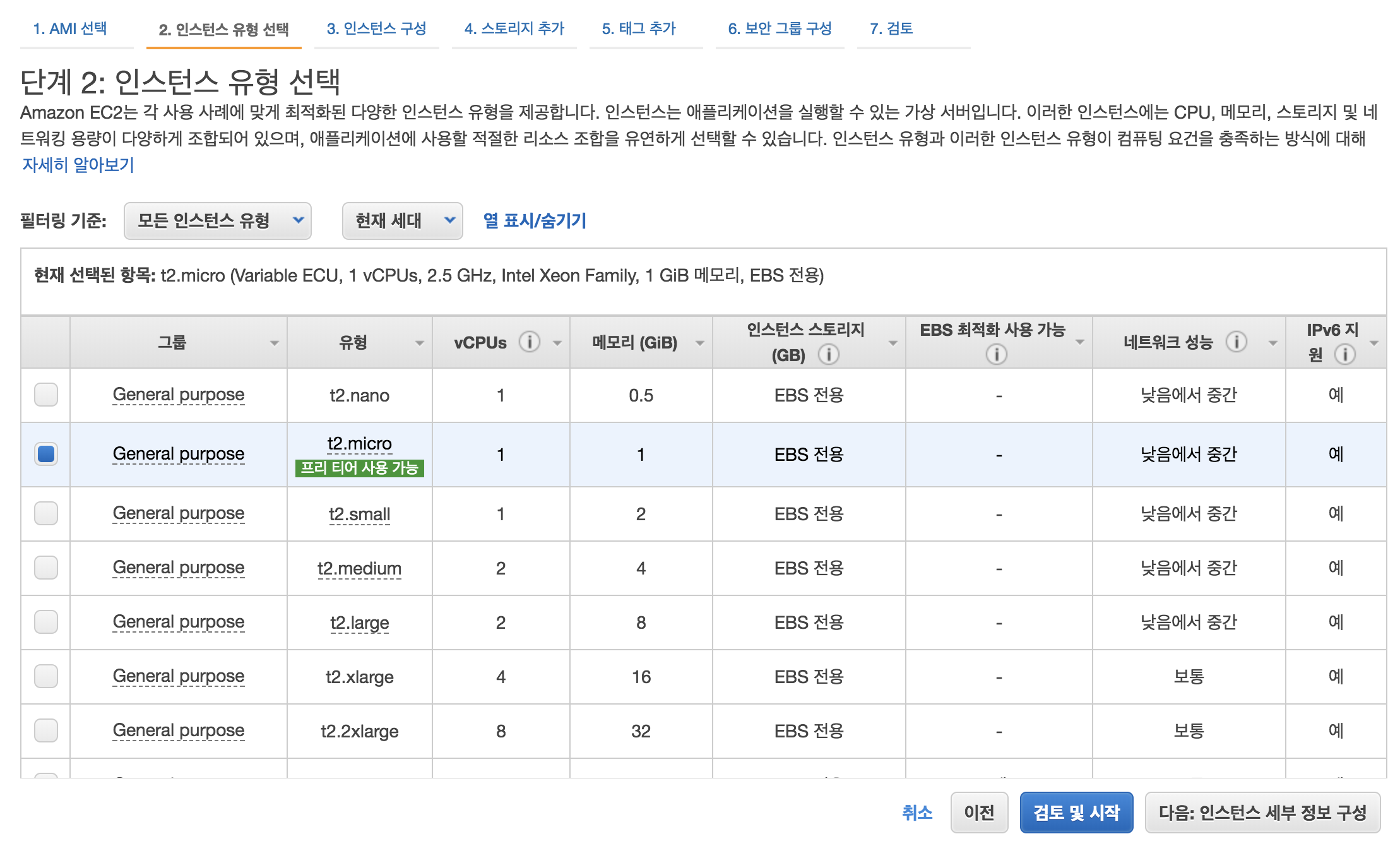
1. 좌측 메뉴 상단의 **“EC2 대시보드”**를 클릭합니다.
2. **“인스턴스 시작**”을 선택합니다.



1. [빠른 시작]에서 가장 상위에 있는 Amazon Linux AMI를 선택하십시오.



1. [단계 2:인스턴스 유형 선택]에서 ***t2.micro***를 선택하고 **“다음: 인스턴스 세부 정보 구성”**을 클릭 하십시오.



1. [단계 3:인스턴스 세부 정보 구성]에서 나머지 모든 값들은 기본값을 사용하고, 화면 하단의 **“어드밴스 세부 정보”**를 클릭하여 확장하십시오. “사용자 데이터” 입력란에 아래의 내용을 입력 하시오. 사용자 데이터(User Data)는 최초 인스턴스 생성시 실행되는 사용자 정의 초기화 스크립트 입니다.

|  |
| --- |
| #include <https://awstechbootcamp.s3.amazonaws.com/bootstrap.sh> |

[ 참고 ]지정된 User Data의 상세 내용은 아래와 같습니다. (bootstrap.sh)

#!/bin/sh

yum -y install httpd php mysql php-mysql

chkconfig httpd on

/etc/init.d/httpd start

if [ ! -f /var/www/html/bootcamp-app.tar.gz ]; then

cd /var/www/html

wget <https://s3.amazonaws.com/awstechbootcamp/GettingStarted/bootcamp-app.tar.gz>

tar xvfz bootcamp-app.tar.gz

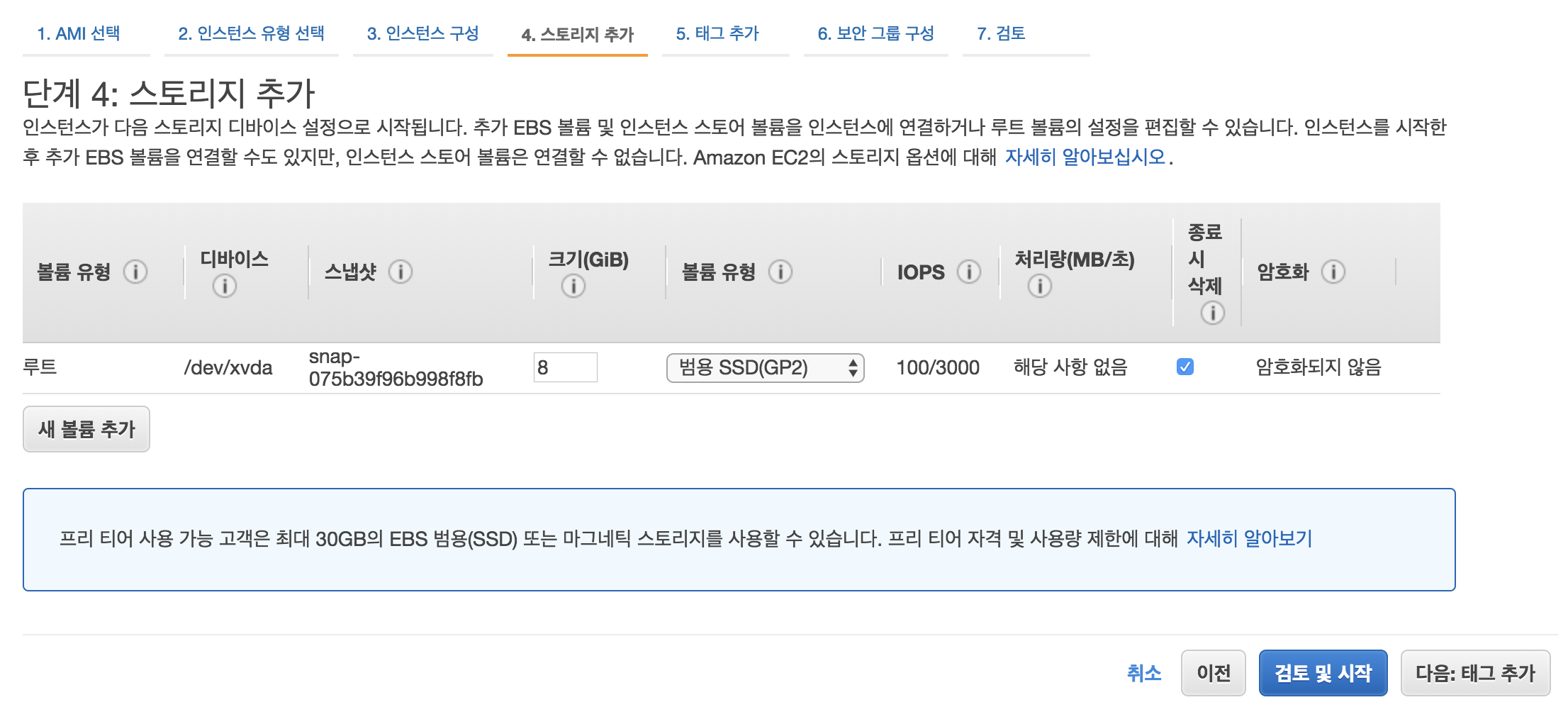
chown apache:root /var/www/html/rds.conf.php

fi

yum -y update



1. 사용자 데이터 입력 후, **“다음: 스토리지 추가”**를 선택 하십시오. 인스턴스에 할당하는 OS Volume(EBS Volume)을 정의합니다. 기본 값인 8GB(SSD Type)를 그대로 사용합니다. **“다음: 태그 추가”**를 클릭하여 다음 단계로 진행합니다.



1. [단계 5: 태그 추가]에서는 인스턴스를 식별할 수 있는 다양한 정보를 추가할 수 있습니다. 태그 정보를 통하여 사용자는 인스턴스의 용도, 목적, 비용관련 정보등을 손쉽게 확인 할 수 있습니다. **“태그 추가”**를 클릭하고, 키와 값을 아래와 같이 입력하고 **“다음: 보안 그룹 구성”**을 클릭하십시오.

키 : ***Name***

값 : ***Immersion Day – Web Server***



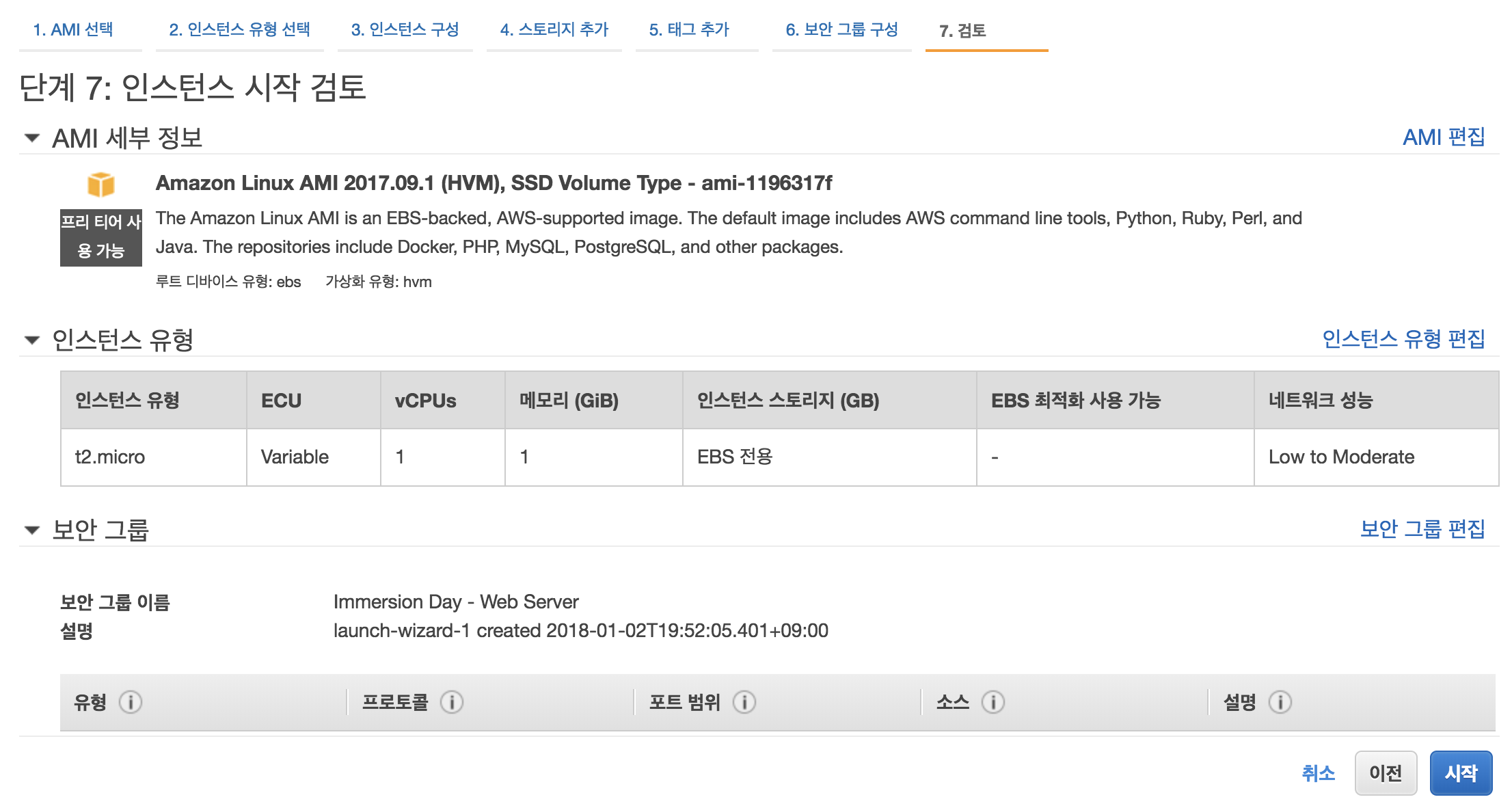
1. [단계 6: 보안 그룹 구성]에서는 새로운 보안 그룹을 만들거나 기존에 만들어진 보안 그룹을 선택 할 수 있습니다. 보안 그룹은 방화벽 정책으로 허용하고자 하는 프로토콜과 주소를 지정하게 됩니다. Lab을 위하여 새로운 보안 그룹을 생성하고 이름을 지정합니다.

기본 설정된 관리용 SSH(TCP/22)외에 **“규칙 추가”**를 선택하여 Web Service를 위한 TCP/80도 함께 허용합니다. 소스 주소의 **0.0.0.0/0**은 모든 네트워크에서의 접근을 의미합니다.



**“검토 및 시작”**을 클릭하여 전체 구성을 확인합니다.

1. 앞서 구성한 정보를 확인하고 **“시작”**을 선택하여 인스턴스를 시작하십시오.

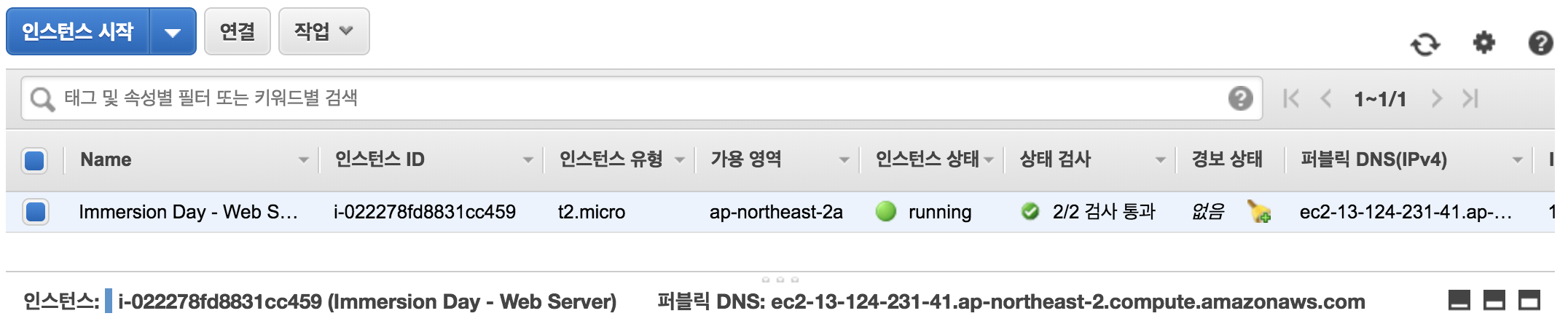


1. 키 페어 생성 과정에서 생성한 키 페어를 선택하고, 체크박스도 선택하십시오. 이 과정을 통하여 지정된 키 페어 중 Public Key 가 초기화 과정에서EC2 인스턴스에 설치됩니다. 이 후, 사용자가 다운로드한 키 페어 중 개인키(Private Key) 를 사용하여 EC2 인스턴스에 접속 할 수 있습니다. **“인스턴스 시작”**을 클릭하십시오.
2. 화면 하단의 **“인스턴스 보기”**를 선택하여 EC2인스턴스의 목록을 확인 할 수 있습니다. 인스턴스의 시작이 완료되면 인스턴스가 구동되고 있는 가용 영역, 외부에서 접근 가능한 IP 및 DNS 정보를 확인 할 수 있습니다.

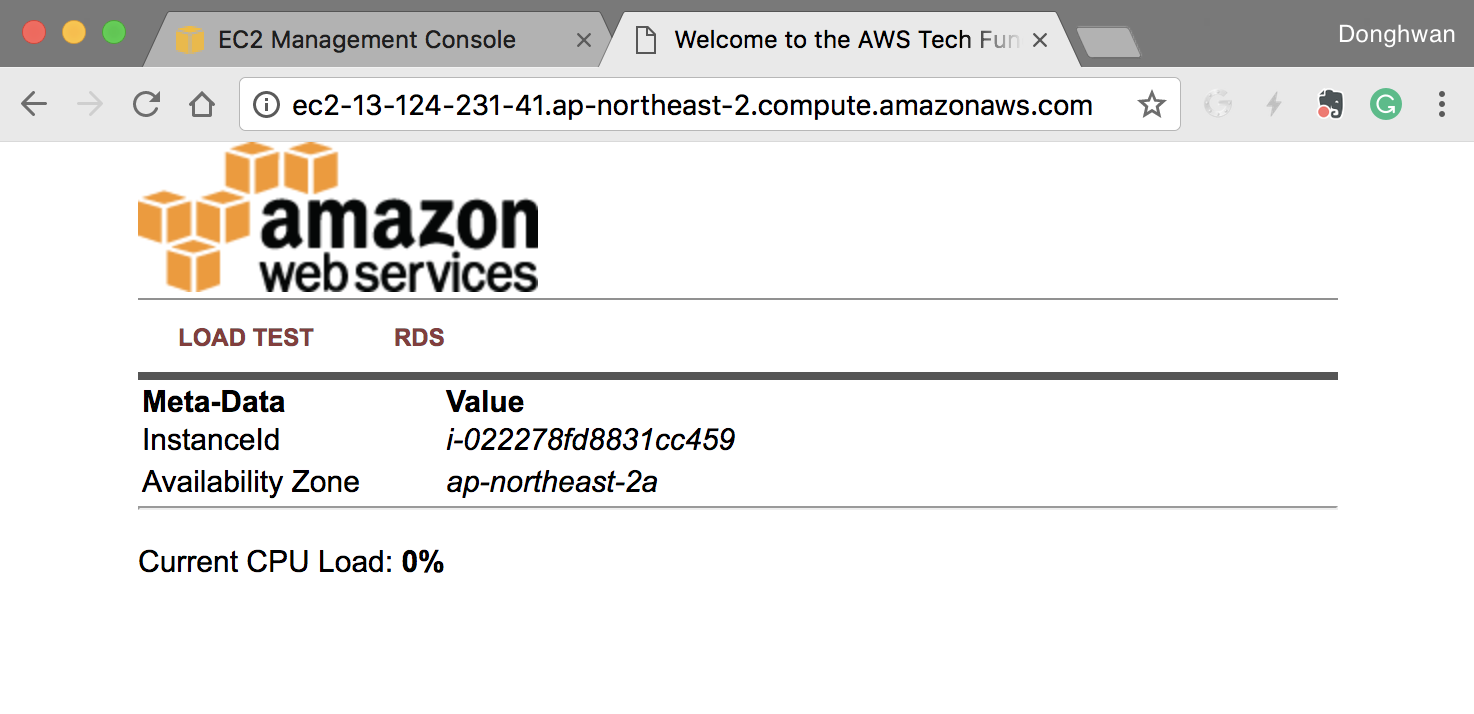


## EC2 인스턴스의 웹 서버 접속 확인 (OPTIONAL)

1. 인스턴스의 **“상태 검사”** 결과가 **“2/2 검사 통과”**가 될 때 까지 대기 하십시오. 초기화가 완료되면 **“2/2 검사 통과”**로 변경됩니다.



1. 새로운 웹 브라우저 탭을 열고, EC2 인스턴스의 퍼블릭 DNS 또는 Ipv4 퍼블릭 IP를 입력하십시오. 아래와 같이 페이지가 보여지면 웹 서버 인스턴스가 정상적으로 구성된 것입니다.



정상적으로 생성된 EC2 Web Server는 이후 ELB Lab에서 사용됩니다.

## SSH로 EC2 접속

사용자의 Private Key는 Key Pair 생성과정에서 최초 1회에 한하여 사용자가 Download 할 수 있으며, 배포과정에서 EC2 Linux 인스턴스에는 지정된 Key Pair에 해당하는 Public Key가 설치됩니다. 이후 사용자는 자신만의 Private Key를 이용하여 EC2 Linux 인스턴스에 SSH 인증 및 접속이 가능하게 됩니다.

접속하는 사용자가 사용하는 운영체제 및 SSH Client Tool의 종류에 따라 사전 준비 작업이 필요할 수 있습니다. 사용자의 단말 운영체제가 Windows기반이고, 사용하는 SSH Client Tool 이 “putty”인 경우에만 사전 인증서의 변환 작업이 필요합니다. Linux, Mac 사용자의 경우에는 추가적인 인증서 변경 작업이 필요하지 않습니다.

**Mac사용자용**

|  |
| --- |
| ssh -I *[path]/[key-pair]*.pem *ec2-user*@*[Public\_IP]* |

* 콘솔에서 Public\_IP 확인 방법



**Window 사용자용**

### Windows Laptop 사용자를 위한 PuTTY 인증서 변환

AWS는 표준 인증서 포맷인 PEM(Privacy-enhanced Electronic Mail)형식으로 제공되나, Windows Laptop 사용자들이 주로 사용하는 대표적인 Freeware SSH Client인 PuTTY는 PEM 형식을 인증서를 직접 지원하지 않고 있습니다.(그 외 대부분의 SSH Client들은 PEM인증서를 기본적으로 지원합니다.)

따라서, 사용자가 Windows Laptop기반에서 PuTTY를 사용하는 경우, EC2 인스턴스에 SSH 연결을 위하여 추가적으로 표준 PEM(.pem) 형식의 Private Key를 PuTTY가 지원하는 PPK(.ppk, PuTTY Private Key Files) 파일로 변환하는 과정이 필요합니다. 아래의 절차를 통하여 Download하신 PEM 형식의 Private Key를 PuTTY용 PPK파일로 변환 하시기 바랍니다.



**PuTTY Package Installer (putty.org)**

32-bit : <https://the.earth.li/~sgtatham/putty/latest/w32/putty-0.70-installer.msi>

64-bit : <https://the.earth.li/~sgtatham/putty/latest/w64/putty-64bit-0.70-installer.msi>

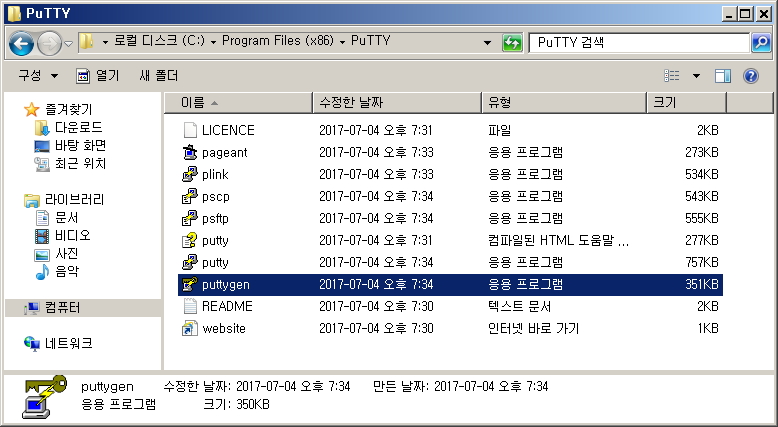
표준 Installer에는 PuTTY를 비롯하여 인증서 변환에 필요한 PuTTYgen이 포함되어 있습니다. 만일 표준 Installer가 아닌 단독으로 실행 가능한 PuTTY Binary만 설치하신 경우에는 PuTTYgen을 별도로 Download 하여야 합니다.

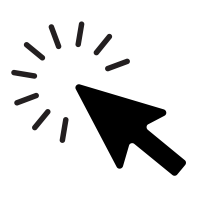
**puttygen.exe**

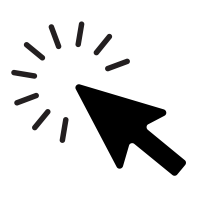
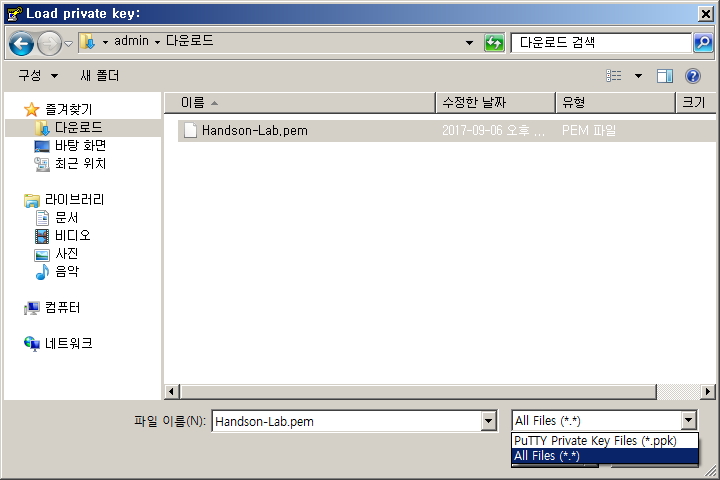
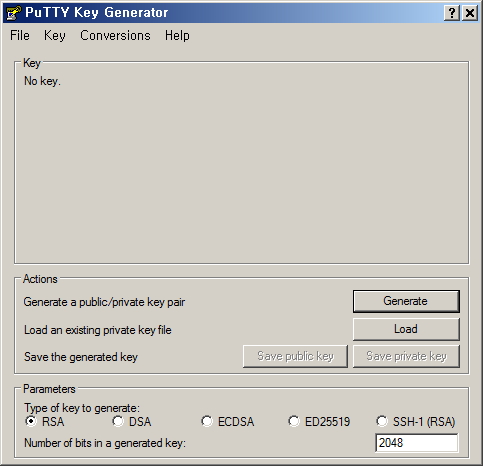
32-bit : <https://the.earth.li/~sgtatham/putty/latest/w32/puttygen.exe>

64-bit : <https://the.earth.li/~sgtatham/putty/latest/w64/puttygen.exe>

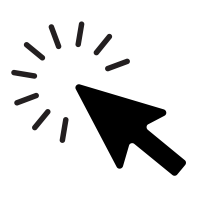
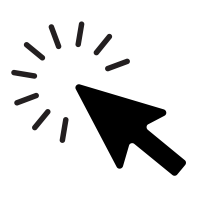
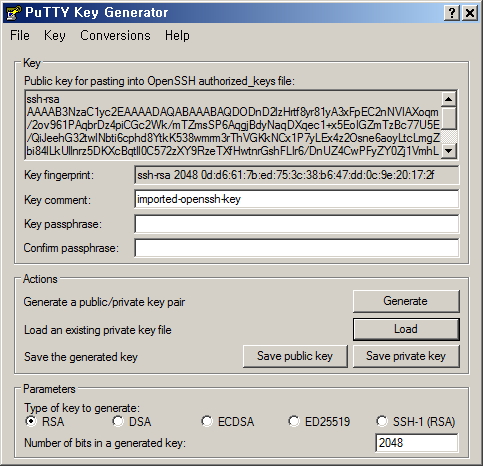
Key 형식 변환을 위하여 PuTTYgen을 실행 하십시오. (프로그램>PuTTY>PuTTYgen)



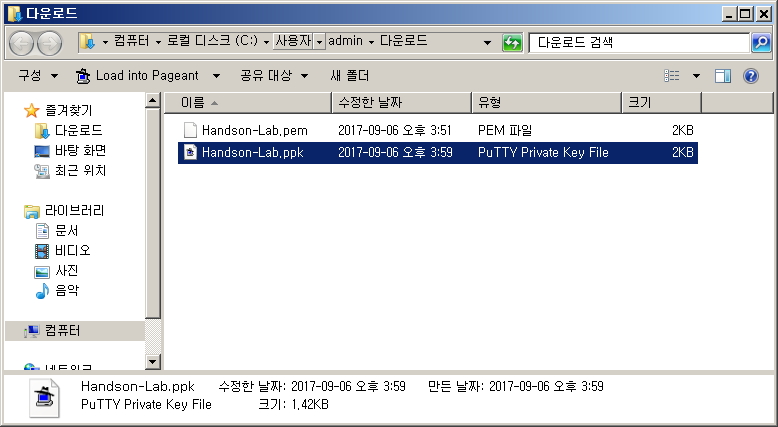
PuTTYgen 실행 후, **“Load”**를 선택하여 저장한 키페어 생성시 다운로드한 PEM 형식의 Private Key를 불러 옵니다. ***(AWS-ImmersionDay-Lab.pem)***



PEM 형식의 Private Key를 PPK형식의 Private Key로 저장하기 위하여 **“Save private key”**를 클릭하십시오. 별도의 Pass-Phrase는 지정하지 않습니다.



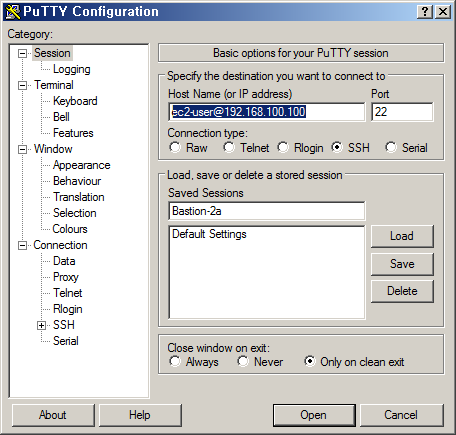
PuTTY가 지원하는PPK형식의 Private Key파일이 추가적으로 생성되었습니다.



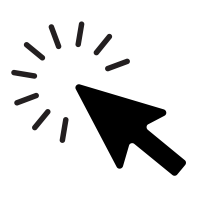
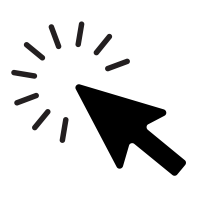
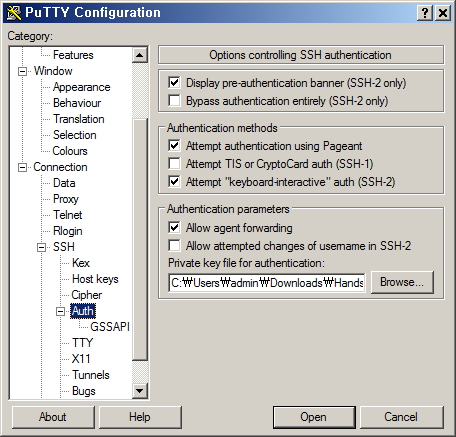
### 

### PuTTY에서 PPK 인증서를 지정하고 연결하기

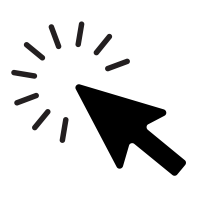
PuTTY를 실행하고, 연결할 Host에 ***ec2-user@EC2\_PUBLIC\_IP\_ADDRESS/FQDN*** 의 형식으로 지정합니다.

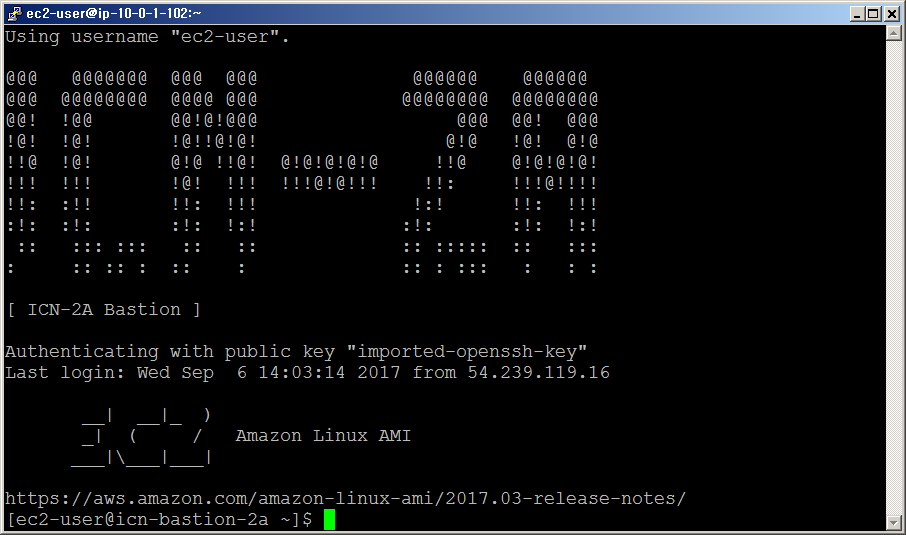


**Connection > SSH > Auth** 메뉴의 **“Private key file for authentication:”** 항목의 **“Browse”**를 선택하여 PPK형식으로 변환한 인증서(Private Key)를 지정 하십시오. 향후, 접속한 EC2 인스턴스에서 VPC내부의 다른 EC2 인스턴스로 SSH연결을 할 경우, **“Allow agent forwarding”** 기능을 선택하십시오.



**“Open”**을 선택하면, 인증서 Cache여부에 대한 질문 후 SSH Session이 연결 됩니다.





이제 개인용 인증서(Private Key)를 지정하여 SSH연결이 가능합니다. 기본적인 Linux 명령을 이용하여 OS의 구성등을 확인하십시오.