

> K PaaS-TA

사용자 가이드

IaaS 사용 가이드



# IaaS 사용 가이드

1. 키페어 생성	01p
2. 보안정책 생성	05p
3. 인스턴스 생성	11p
4. 공인 IP 생성	16p
5. 인스턴스와 공인 IP 연결	19p
6. 인스턴스 ssh 접속	25p
7. 인스턴스 apache 서비스	29p



## IaaS 사용자 가이드 개요

**IaaS(Infrastructure as a Service)**는 클라우드 환경에서 가상 서버, 네트워크, 스토리지를 사용자가 정의하고 사용할 수 있도록 제공하는 서비스입니다.

서버 운영에 필요한 서버 자원, 네트워크, 스토리지 등 다양한 인프라 서비스를 제공합니다.

사용자는 인프라 구축을 신경 쓰지 않고 클라우드 환경에서 필요한 만큼의 인프라를 제공 받아 운영체제를 설치하고, 어플리케이션을 배포하여 사용자가 원하는 대로 서비스 운영이 가능합니다.

본 사용자 가이드는

먼저 가상 서버와 연결할 수 있도록 키페어 생성과 보안정책을 설정 한 후에 가상 서버를 생성하고, 공인 IP를 통해 외부에서 접속이 가능하도록 연결, 가상 서버와 키페어를 통한 SSH 접속, 웹 서버를 운영하기 위한 apache 서비스 설치 후 접속 절차를 소개합니다.



## IaaS 사용자 가이드 안내

### 1장, 2장, 3장

가상 서버를 생성하기 위한 키페어, 보안정책 생성에 대하여 소개하고 있습니다.

또한 키페어와 보안정책 생성 후 인스턴스를 생성하는 방법에 대해서 소개하고 있습니다.

### 4장, 5장

생성한 인스턴스를 외부에서 접속이 가능하도록 공인 IP 할당과 인스턴스와 공인 IP를 연결하는 방법에 대해서 소개하고 있습니다.

### 6장, 7장

생성한 인스턴스에 접속하기 위한 SSH 접속 방법과 웹 서버 구축을 위한 인스턴스에 apache 서비스 배포하는 방법에 대해서 소개하고 있습니다.

# 1. 키페어 생성

01

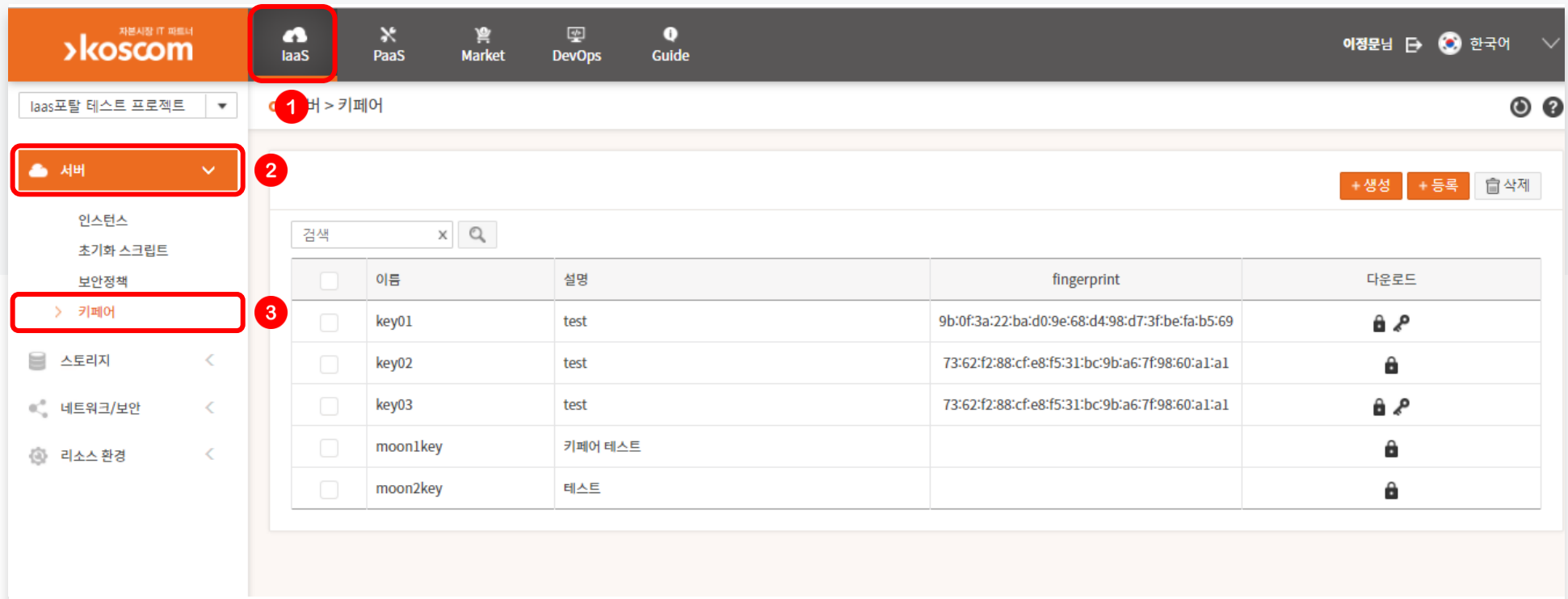


K PaaS-TA 메인 페이지

## 1) Console 페이지 이동

- ① K PaaS-TA에 로그인을 합니다.
- ② K PaaS-TA 페이지 우측 상단에 있는 ① [Console] 버튼을 클릭합니다.

# 1. 키페어 생성



IaaS의 키페어 페이지

## 2) IaaS의 키페어 페이지 이동

- ① Console 페이지 상단에 위치한 ① [IaaS] 버튼을 클릭하여 IaaS 페이지로 이동합니다.
- ② IaaS 페이지 좌측에 위치한 ② [서버] 을 클릭하여 하단메뉴에 위치한 ③ [키페어] 메뉴를 클릭하면 위 이미지와 같은 키페어 페이지로 이동합니다.

# 1. 키페어 생성

The screenshot displays the KMS interface. At the top right, there are buttons for '+ 생성' (Create), '+ 등록' (Register), and '삭제' (Delete). A red circle with the number '1' highlights the '+ 생성' button. Below this is a table with columns: '이름' (Name), '설명' (Description), 'fingerprint', and '다운로드' (Download). The table contains six rows of keys. Below the table, a modal window titled '키페어 생성' (Key Creation) is shown. It has two input fields: '이름' (Name) and '설명' (Description). A red circle with the number '2' highlights the '이름' field. At the bottom of the modal, there are two buttons: '확인' (Confirm) and '취소' (Cancel). A red circle with the number '3' highlights the '확인' button.

<input type="checkbox"/>	이름	설명	fingerprint	다운로드
<input type="checkbox"/>	key01	test	9b:0f:3a:22:ba:d0:9e:68:d4:98:d7:3f:be:fa:b5:69	
<input type="checkbox"/>	key02	test	73:62:f2:88:cf:e8:f5:31:bc:9b:a6:7f:98:60:a1:a1	
<input type="checkbox"/>	key03	test	73:62:f2:88:cf:e8:f5:31:bc:9b:a6:7f:98:60:a1:a1	
<input type="checkbox"/>	moon1key	키페어 테스트		
<input type="checkbox"/>	moon2key	테스트		

IaaS의 키페어 생성

## 3) 키페어 생성

- ① 키페어 생성 페이지 우측 상단에 위치한 ① [+생성] 버튼을 클릭하여 키페어 설정 팝업을 생성합니다.
- ② 키페어 설정 팝업에서 ② [키페어 이름, 설명] 에 알맞은 정보를 입력 후 ③ [확인] 버튼을 클릭하여 생성을 완료 합니다.

# 1. 키페어 생성

laas포탈 테스트 프로젝트

laaS PaaS Market DevOps Guide

이정문님 한국어

laaS > 키페어

+ 생성 + 등록 삭제

검색 x

<input type="checkbox"/>	이름	설명	fingerprint	다운로드
<input type="checkbox"/>	key01	test	9b:0f:3a:22:ba:d0:9e:68:d4:98:d7:3f:be:fa:b5:69	
<input type="checkbox"/>	key02	test	73:62:f2:88:cf:e8:f5:31:bc:9b:a6:7f:98:60:a1:a1	
<input type="checkbox"/>	key03	test	73:62:f2:88:cf:e8:f5:31:bc:9b:a6:7f:98:60:a1:a1	
<b>1</b>	Key_test_1	test_1	48:d5:44:3a:2d:ed:b3:c4:c6:ca:c0:4d:84:ff:91:84	
<input type="checkbox"/>	moon1key	키페어 테스트		
<input type="checkbox"/>	moon2key	테스트		

laaS의 키페어 페이지

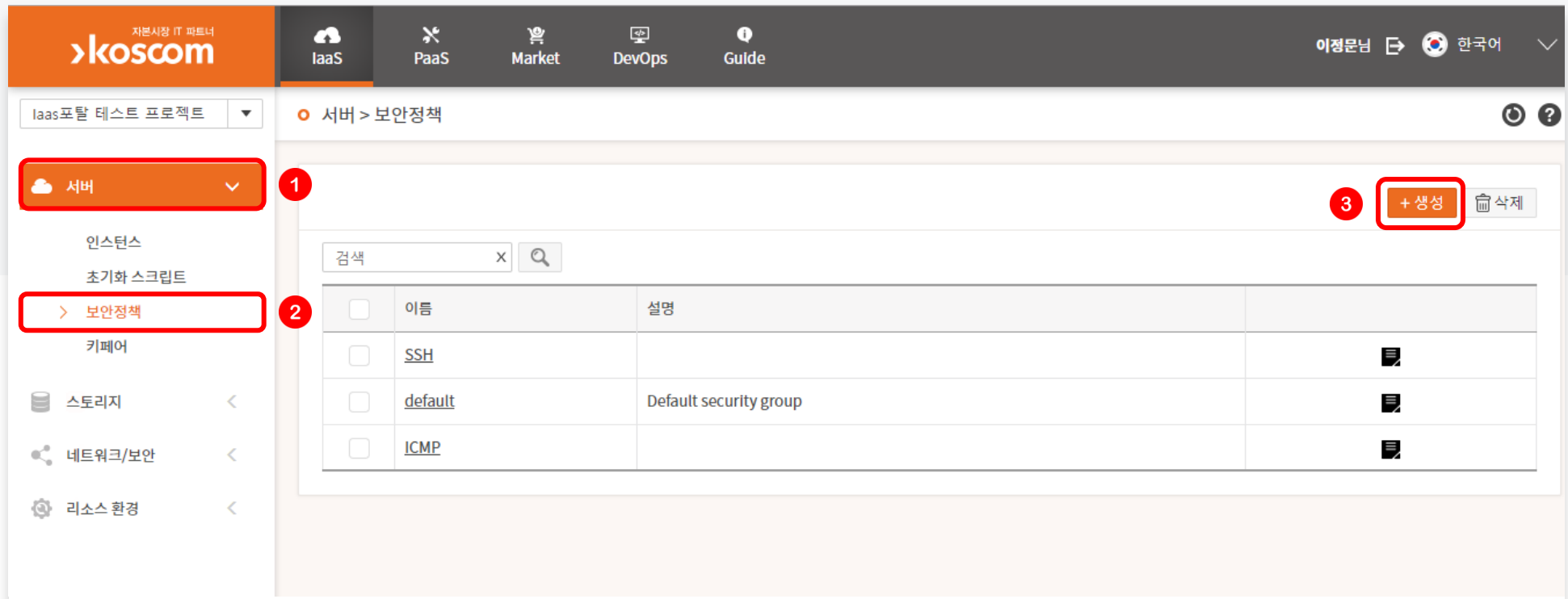
## 4) 키페어 생성 완료

- ① 키페어 생성을 완료하면 ①번과 같이 키페어가 새로 생성 된 것을 확인 할 수 있습니다.



## 2. 보안정책 생성

05



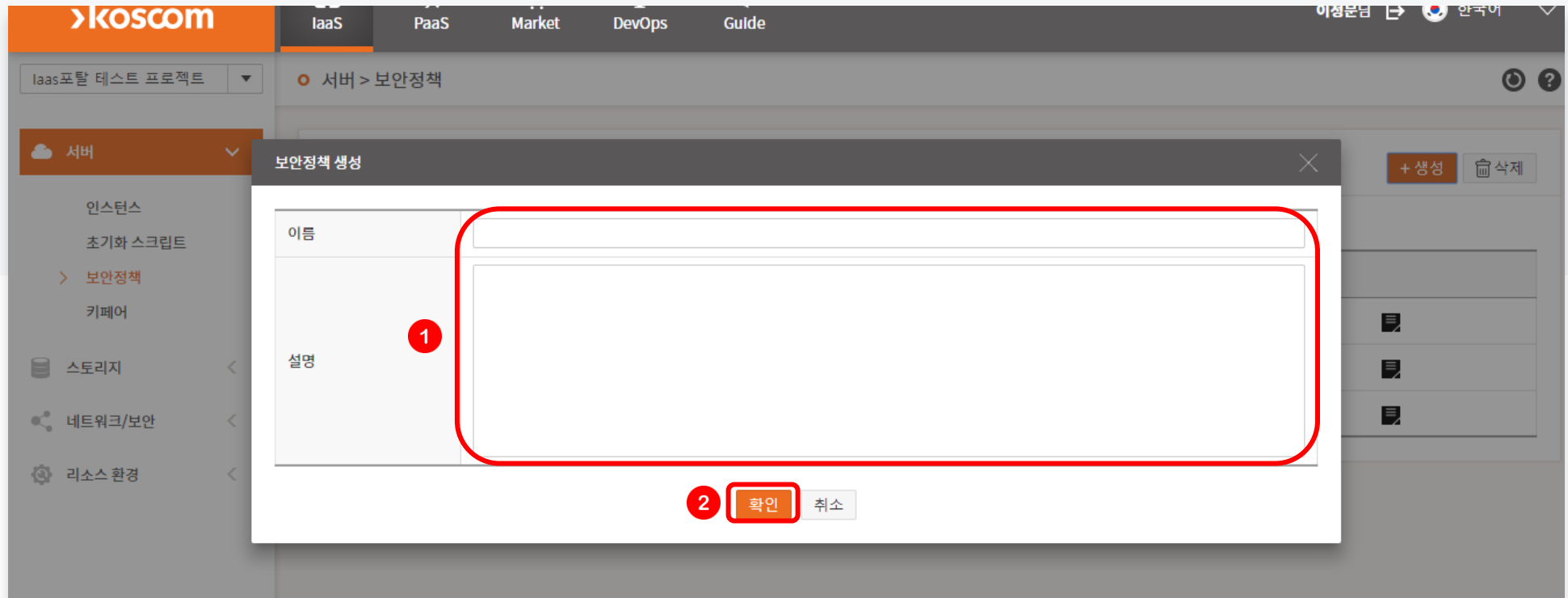
IaaS의 보안정책 페이지

### 1) IaaS의 보안정책 페이지 이동

- ① IaaS 페이지 좌측에 위치한 ① [서버] 을 클릭하여 하단메뉴에 위치한 ② [보안정책] 메뉴를 클릭하면 위 이미지와 같은 키페어 페이지로 이동합니다.
- ② 보안 정책 페이지 우측 상단 위에 위치한 ㉠ [+생성] 버튼을 클릭하여 보안 정책 생성 팝업을 생성합니다.

## 2. 보안정책 생성

06



보안정책 팝업 페이지

### 2) 보안정책 생성

- ① 보안 정책 생성 팝업 페이지에서 ❶ 번에 사용자가 생성할 보안정책의 이름과 설명을 입력하세요.
- ② 보안 정책 생성 팝업 페이지 하단에 위치한 ❷ [확인] 버튼을 클릭하여 보안정책을 생성하세요.

## 2. 보안정책 생성

07

자본시장 IT 파트너  
koscom

이정문님 한국어

laaS PaaS Market DevOps Guide

laas포탈 테스트 프로젝트

서버

인스턴스  
초기화 스크립트  
> 보안정책  
키페어  
스토리지  
네트워크/보안  
리소스 환경

서버 > 보안정책

+ 생성 삭제

검색 x

<input type="checkbox"/>	이름	설명	
<input type="checkbox"/>	SSH		
<input type="checkbox"/>	default	Default security group	
<input type="checkbox"/>	ICMP		
1	test	test	2

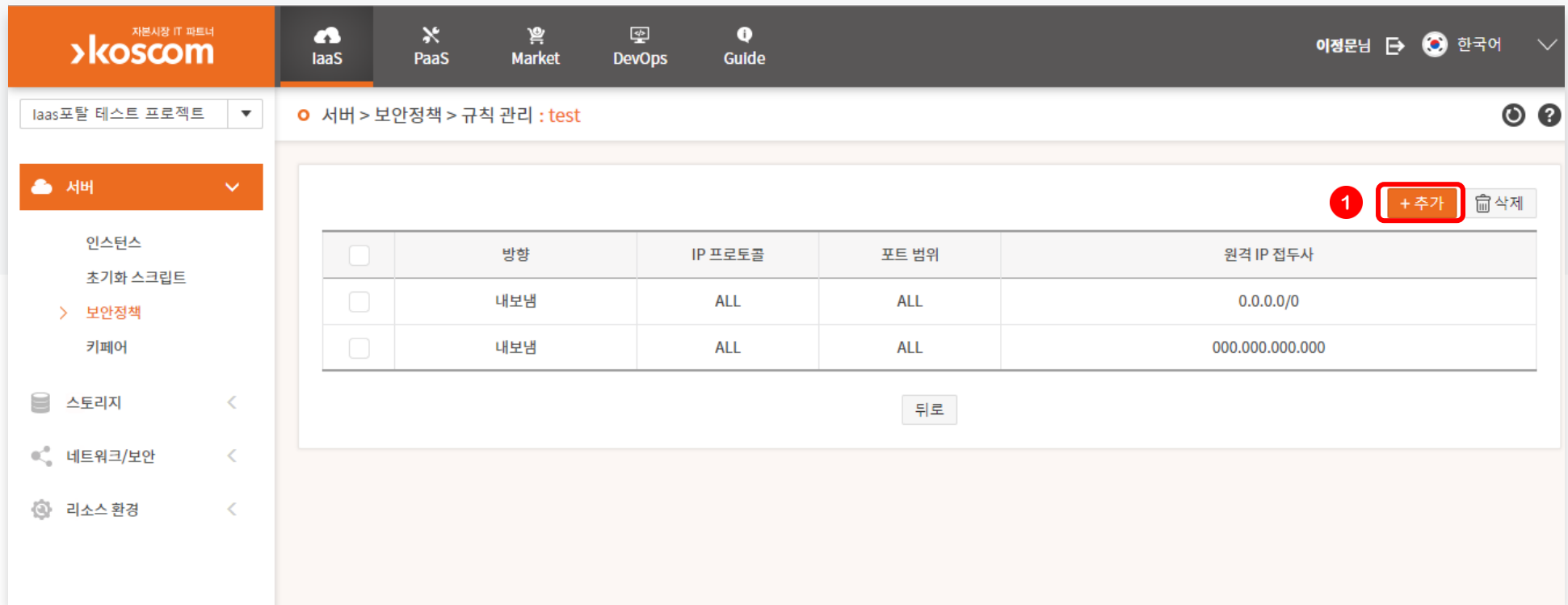
보안정책 팝업 페이지

### 3) 보안정책 설정

- ① 1번과 같이 보안 정책이 성공적으로 생성 된 것을 확인 할 수 있습니다.
- ② 생성한 보안 정책 우측에 2번을 클릭하여 보안정책 설정으로 이동합니다.

## 2. 보안정책 생성

08



laas포탈 테스트 프로젝트

laaS PaaS Market DevOps Guide

이정문님 한국어

laas포탈 테스트 프로젝트

서버

- 인스턴스
- 초기화 스크립트
- > 보안정책
- 키페어
- 스토리지
- 네트워크/보안
- 리소스 환경

서버 > 보안정책 > 규칙 관리 : test

1 + 추가 삭제

<input type="checkbox"/>	방향	IP 프로토콜	포트 범위	원격 IP 접두사
<input type="checkbox"/>	내보냄	ALL	ALL	0.0.0.0/0
<input type="checkbox"/>	내보냄	ALL	ALL	000.000.000.000

뒤로

보안정책 팝업 페이지

### 4) 보안정책 설정 추가

- ① 보안 정책 설정 페이지 우측 상단에 위치하고 있는 ① [+추가] 를 클릭하여 보안정책 설정 규칙 추가 팝업을 생성합니다.

## 2. 보안정책 생성

09

The screenshot displays the KOSCOM PaaS console interface. A modal window titled '규칙추가' (Add Rule) is open, showing the process of adding a new security rule. The rule is named '사용자정의 TCP 규칙' (User-defined TCP Rule). The direction is set to '들어옴' (Incoming). The scope is defined as '포트' (Port). The port number is currently empty. The CIDR is set to '0.0.0.0/0'. The '확인' (Confirm) button is highlighted with a red circle and the number 4.

보안정책 팝업 페이지

### 5) 보안정책 설정 규칙 추가

- ① 보안정책 설정 규칙 추가 팝업에 정보들을 순서에 맞게 알맞게 입력합니다.  
① 규칙 선택 ② 범위 정의 선택 ③ 포트 입력 순서로 입력
- ② 보안정책 설정 규칙 추가 팝업 하단에 위치한 ④ [확인] 버튼을 클릭하여 규칙을 추가합니다.

## 2. 보안정책 생성

10

laas포탈 테스트 프로젝트

laaS PaaS Market DevOps Guide

이정문님 한국어

laaS포탈 테스트 프로젝트

서버

인스턴스  
초기화 스크립트  
> 보안정책  
키페어  
스토리지  
네트워크/보안  
리소스 환경

서버 > 보안정책 > 규칙 관리 : test

+ 추가 삭제

	방향	IP 프로토콜	포트 범위	원격 IP 접두사
1	들어옴	TCP	80/80	0.0.0.0/0
	내보냄	ALL	ALL	0.0.0.0/0
	내보냄	ALL	ALL	000.000.000.000

뒤로

보안정책 팝업 페이지

### 6) 보안정책 설정 규칙 추가

- ① 보안 정책 설정 페이지에 ① 번과 같이 규칙이 추가 된 것을 확인 할 수 있습니다.

### 3. 인스턴스 생성

11

	이름	이미지	용도	상태	작업상태	키페어	내부IP	공인IP	
<input type="checkbox"/>	testing	ubuntu-16.04-1	WAS	active		key01	192.168.211.12	211.239.163.243	상세관리
<input type="checkbox"/>	snap_test			active			192.168.211.21		상세관리
<input type="checkbox"/>	test_2	ubuntu-16.04-1	WEB	active		moon1key	192.168.211.11		상세관리
<input type="checkbox"/>	test	ubuntu-16.04-1	WEB	active		moon1key	192.168.211.10		상세관리
<input type="checkbox"/>	test1	ubuntu 16.04-cloud	WAS	active		moon1key	192.168.211.7	211.239.163.229	상세관리
<input type="checkbox"/>	vw	cirros-0.3.4	WAS	active		moon1key	192.168.211.9		상세관리
<input type="checkbox"/>	vm_test_1_1	cirros-0.3.4	WAS	active		moon1key	10.10.10.4		상세관리
<input type="checkbox"/>	vm_test_1	cirros-0.3.4	WAS	active		moon1key	192.168.211.8		상세관리
<input type="checkbox"/>	testum	cirros	WAS	active		moon1key	192.168.211.6		상세관리

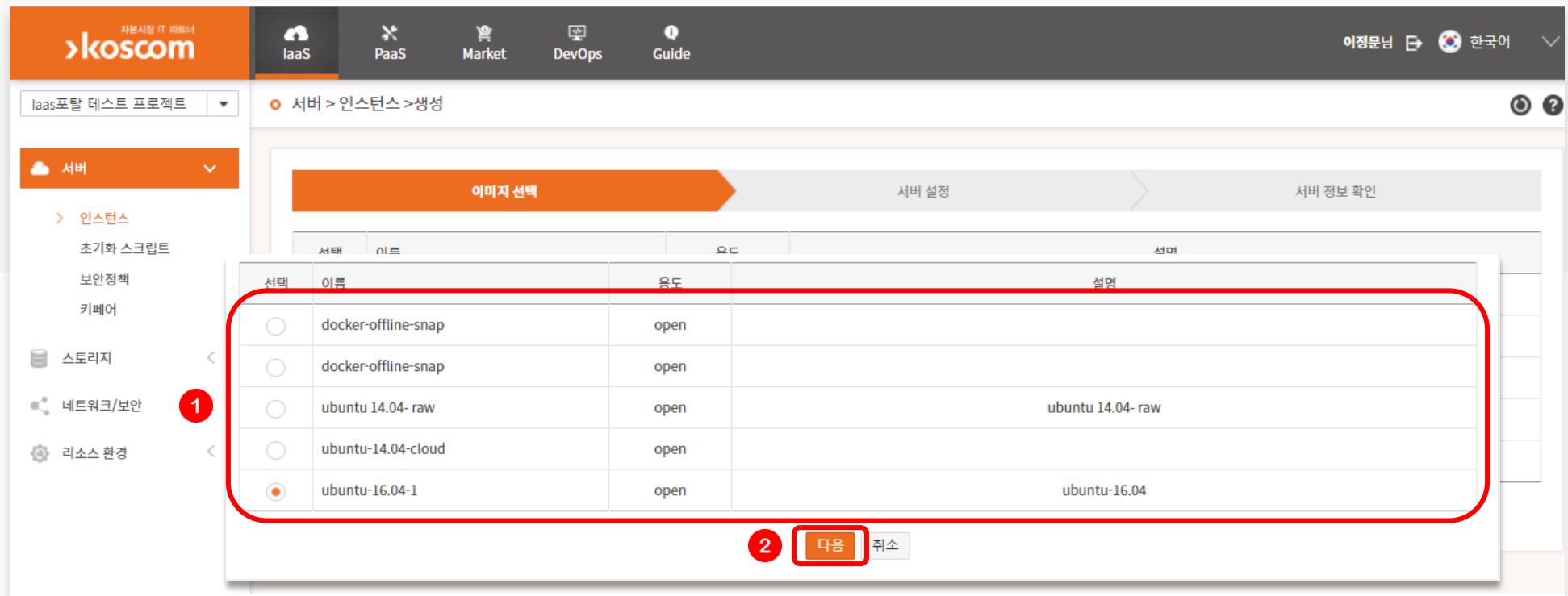
IaaS의 인스턴스 페이지

#### 1) IaaS의 인스턴스 생성 페이지 이동

- ① IaaS 페이지 좌측에 위치한 ① [서버] 을 클릭하여 하단메뉴에 위치한 ② [인스턴스] 메뉴를 클릭하면 위 이미지와 같은 인스턴스 페이지로 이동합니다.
- ② 인스턴스 페이지의 우측 상단에 위치한 ③ [+생성] 버튼을 클릭하여 인스턴스 생성 페이지로 이동합니다.

### 3. 인스턴스 생성

12



IaaS의 인스턴스 생성 페이지

#### 2) 인스턴스 생성에 필요한 이미지 선택

- ① 인스턴스 생성에 필요한 ① [이미지] 를 선택 후, 하단에 위치한 ② [다음] 버튼을 클릭하여 다음 페이지로 넘어 갑니다.



### 3. 인스턴스 생성

13

자본시장 IT 파트너  
koscom

laas포탈 테스트 프로젝트

서버

> 인스턴스

초기화 스크립트

보안정책

키페어

스토리지

네트워크/보안

리소스 환경

조직명 laas포탈 테스트 프로젝트 이미지 ubuntu-16.04-1

★이름 1

★용도 2 사용자정의

★스펙 3 선택

★키페어 4 선택

초기화 스크립트 선택 사용

초기화 스크립트 내용

리소스

vCPU 29개 / 200개 14 %

메모리 23.5 GB / 40 GB 59 %

디스크 153GB / 1,000GB 15 %

5 다음 취소

IaaS의 인스턴스 생성 페이지

#### 3) 인스턴스 생성에 필요한 서버 설정

- ① 인스턴스 1 [이름] 을 설정 합니다.
- ② 인스턴스 2 [사용 용도] 를 설정 합니다.
- ③ 인스턴스 3 [스펙] 을 설정 합니다.
- ④ 인스턴스에서 사용할 4 [키페어] 를 설정합니다.
- ⑤ 인스턴스에 대한 설정이 완료 되면 하단에 있는 5 [다음] 버튼을 클릭하여 다음 페이지로 넘어 갑니다.

### 3. 인스턴스 생성

14

이미지 선택		서버 설정		서버 정보 확인	
조직명	laas포탈 테스트 프로젝트	이름	test_11		
용도	WAS	이미지	ubuntu-16.04-1		
★스펙	[default.server.spec] cpu 1개, ram 2048 MB, disk 20 GB	네트워크	기본 네트워크		
		내부IP	자동할당 192.168.211.XXX		
보안정책		★키페어	key01		
초기화 스크립트 내용	<div></div>				

1 서버 생성 취소

IaaS의 인스턴스 생성 페이지

#### 4) 인스턴스 생성 전 정보 확인

- ① 사용자가 설정한 인스턴스에 대한 정보를 확인 할 수 있습니다.
- ② 설정한 정보가 맞으면 ❶ [서버 생성] 을 클릭하여 인스턴스를 생성합니다.

### 3. 인스턴스 생성

15

자본시장 IT 파트너 >koscom

laaS PaaS Market DevOps Guide

이정문님 한국어

laaS포탈 테스트 프로젝트

서버 > 인스턴스

+ 생성 삭제

--조건선택-- 검색

	이름	이미지	용도	상태	작업상태	키페어	내부IP	그룹
1	test_11	ubuntu-16.04-1	WAS	active		key01		
	testing	ubuntu-16.04-1	WAS	active		key01		
	snap_test			active				
	test_2	ubuntu-16.04-1	WEB	active		moon1key		
	test	ubuntu-16.04-1	WEB	active		moon1key		
	test1	ubuntu 16.04-cloud	WAS	active		moon1key	192.168.211.7	211.239.163.229 상세관리

building scheduling

active

IaaS의 인스턴스 생성 페이지

#### 5) 인스턴스 생성 완료

- ① 인스턴스 생성을 완료하면 ①번과 같이 인스턴스가 생성 된 것을 확인 할 수 있습니다.
- ② 인스턴스가 생성이 되면 인스턴스의 상태가 ②번과 같이 변경 되어 활성화 되는 것을 알 수 있습니다.

## 4. 공인 IP 생성

16

이제문님 한국어

laaS PaaS Market DevOps Guide

laaS포탈 테스트 프로젝트

네트워크/보안 > 공인 IP

+ 할당 - 반납

	공인IP	고정IP	인스턴스	풀	
<input type="checkbox"/>	211.239.163.229	192.168.211.7	test1	PUB_NET	🔗
<input type="checkbox"/>	211.239.163.235			PUB_NET	
<input type="checkbox"/>	211.239.163.243	192.168.211.12	testing	PUB_NET	🔗
<input type="checkbox"/>	211.239.163.246			PUB_NET	

IaaS의 공인 IP 생성 페이지

### 1) IaaS의 공인 IP 생성 페이지 이동

- ① IaaS 페이지 좌측에 위치한 ① [네트워크/보안] 을 클릭하여 하단메뉴에 위치한 ② [공인 IP] 메뉴를 클릭하면 위 이미지와 같은 공인 IP 페이지로 이동합니다.

## 4. 공인 IP 생성

17


1

+ 할당

반납

<input type="checkbox"/>	공인IP	고정IP	인스턴스	풀	
	211.239.163.229	192.168.211.7	test1	PUB_NET	🔗
<input type="checkbox"/>	211.239.163.235			PUB_NET	
	211.239.163.243	192.168.211.12	testing	PUB_NET	🔗
<input type="checkbox"/>	211.239.163.246			PUB_NET	

주의

 공인IP 할당  
※공인IP를 추가 할당 하시겠습니까?

2

확인

취소

IaaS의 공인 IP 생성

### 2) 공인 IP 생성

- ① 공인 IP 페이지 우측 상단에 위치한 1 [+할당] 버튼을 클릭하면 안내 팝업이 나타납니다.
- ② 안내 팝업 메시지의 하단부분에 위치한 2 [확인] 버튼을 클릭하여 공인 IP 할당을 받습니다.

## 4. 공인 IP 생성

18

laas포탈 테스트 프로젝트

이정문님 한국어

네트워크/보안 > 공인 IP

+ 할당    - 반납

<input type="checkbox"/>	공인IP	고정IP	인스턴스	풀	
<input checked="" type="checkbox"/>	211.239.163.229	192.168.211.7	test1	PUB_NET	🔗
<input type="checkbox"/>	211.239.163.235			PUB_NET	
<input type="checkbox"/>	211.239.163.243	192.168.211.12	testing	PUB_NET	🔗
<input type="checkbox"/>	211.239.163.246			PUB_NET	
<input type="checkbox"/>	211.239.163.251			PUB_NET	

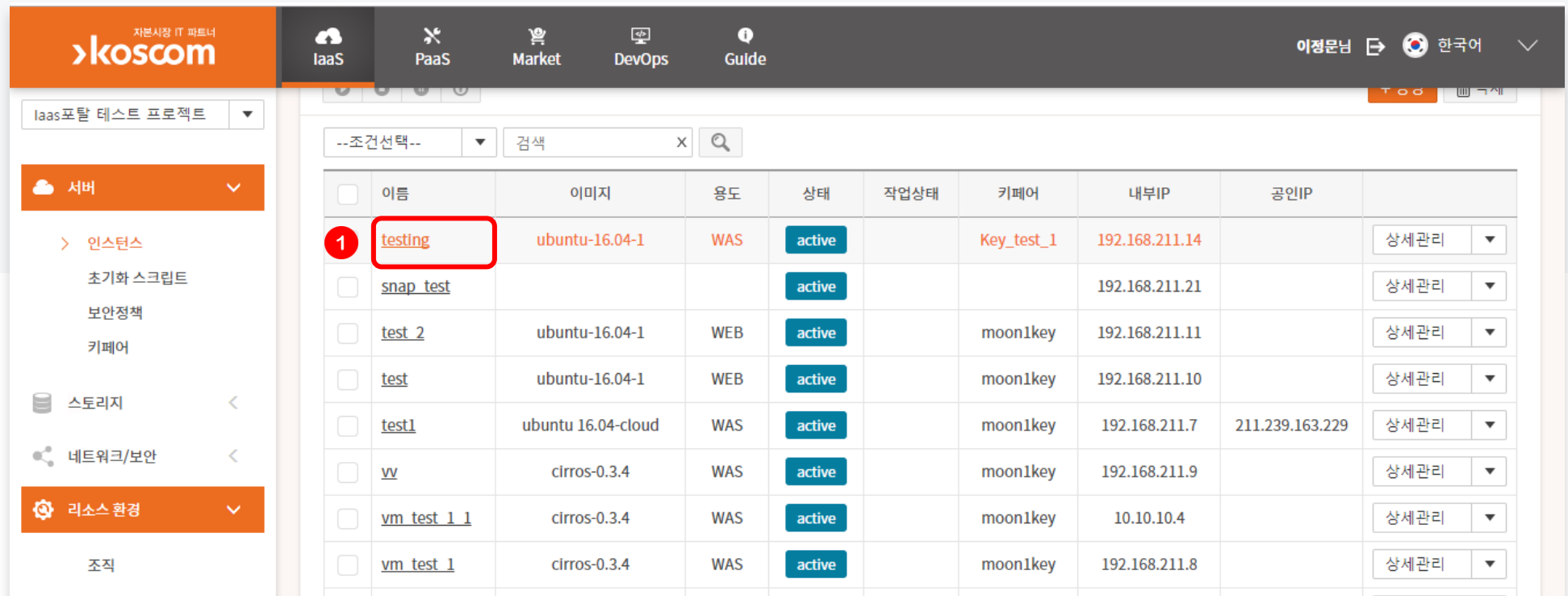
IaaS의 공인 IP 페이지

### 3) 공인 IP 생성 완료

- ① 공인 IP 할당을 받게 되면 ❶ 번과 같이 공인 IP가 생성 된 것을 확인 할 수 있습니다.

## 5. 인스턴스와 공인IP 연결

19



The screenshot shows the KOSCOM IaaS portal interface. On the left, there is a sidebar with navigation options: 서버 (Servers), 인스턴스 (Instances), 초기화 스크립트 (Init Scripts), 보안정책 (Security Policies), 키페어 (Key Pairs), 스토리지 (Storage), 네트워크/보안 (Network/Security), 리소스 환경 (Resource Environment), and 조직 (Organization). The main area displays a table of instances. The first instance, 'testing', is highlighted with a red box and a red circle with the number 1. The table has columns for 이름 (Name), 이미지 (Image), 용도 (Usage), 상태 (Status), 작업상태 (Operation Status), 키페어 (Key Pair), 내부IP (Private IP), 공인IP (Public IP), and actions (상세관리 - Detailed Management).

이름	이미지	용도	상태	작업상태	키페어	내부IP	공인IP	
1 testing	ubuntu-16.04-1	WAS	active		Key_test_1	192.168.211.14		상세관리 ▼
snap_test			active			192.168.211.21		상세관리 ▼
test_2	ubuntu-16.04-1	WEB	active		moon1key	192.168.211.11		상세관리 ▼
test	ubuntu-16.04-1	WEB	active		moon1key	192.168.211.10		상세관리 ▼
test1	ubuntu 16.04-cloud	WAS	active		moon1key	192.168.211.7	211.239.163.229	상세관리 ▼
vv	cirros-0.3.4	WAS	active		moon1key	192.168.211.9		상세관리 ▼
vm_test_1_1	cirros-0.3.4	WAS	active		moon1key	10.10.10.4		상세관리 ▼
vm_test_1	cirros-0.3.4	WAS	active		moon1key	192.168.211.8		상세관리 ▼

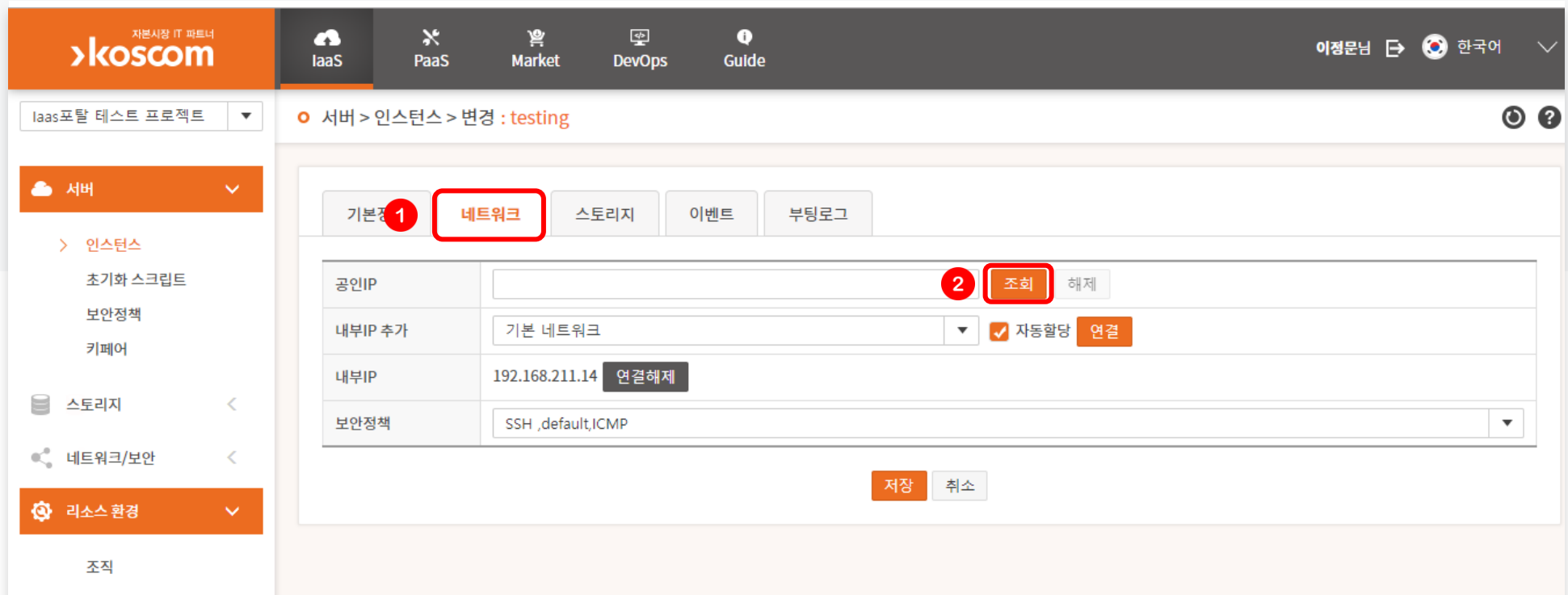
IaaS의 인스턴스페이지

### 1) 인스턴스 정보 페이지 이동

- ① 인스턴스 페이지로 이동하여 생성된 인스턴스 목록을 확인 합니다.
- ② 생성된 인스턴스 목록에서 공인 IP와 연결할 ① [인스턴스 이름] 을 클릭하여 인스턴스 정보 페이지로 이동합니다.

## 5. 인스턴스와 공인IP 연결

20



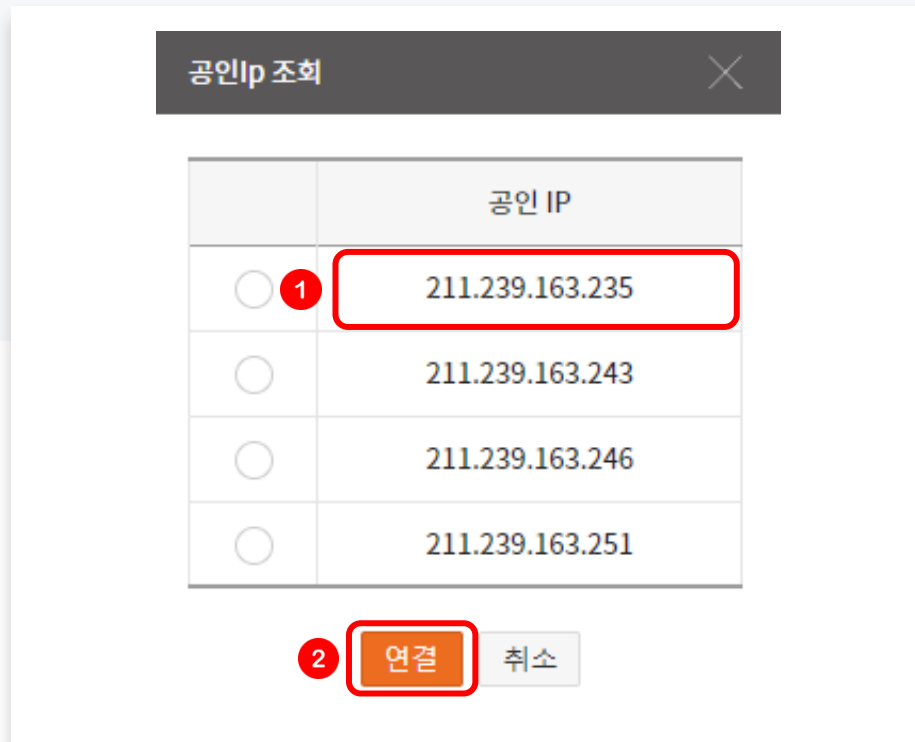
IaaS의 인스턴스 상세 페이지

### 2) 인스턴스 정보의 네트워크 탭 이동

- ① 인스턴스 정보 페이지에서 상단에 위치한 1 [네트워크] 탭을 클릭하여 공인 IP 연결 단계로 넘어갑니다.
- ② 인스턴스 정보 페이지에서 공인 IP 우측에 있는 2 [조회] 버튼을 클릭하면 공인 IP 조회 팝업 창이 생성됩니다.



## 5. 인스턴스와 공인IP 연결



공인 IP 생성 되어 있는 경우



공인 IP 없는 경우

### 3-1) 공인 IP 연결 ( 공인 IP 생성 되어 있는 경우 )

- ① 사용자가 생성한 공인 IP 중 사용할 ① [공인 IP] 를 선택 후 팝업 창 하단에 위치한 ② [연결] 버튼을 클릭하여 공인 IP를 연결합니다.

### 3-2) 공인 IP 연결 ( 공인 IP 없는 경우 )

- ① 공인 IP 조회 팝업 창 하단에 위치한 ① [공인IP할당] 을 클릭하여 공인 IP 를 할당 받습니다.
- ② 공인 IP 할당이 완료 되면 ② [공인 IP] 를 선택 후 팝업 창 하단에 위치한 ③ [연결] 버튼을 클릭하여 공인 IP 연결합니다.

## 5. 인스턴스와 공인IP 연결

22

The screenshot shows the KOSCOM IaaS console interface. The top navigation bar includes the KOSCOM logo and various service categories: IaaS, PaaS, Market, DevOps, and Guide. The user is logged in as '이정문님' and the language is set to '한국어'. The left sidebar shows the '서버' (Server) section expanded, with '인스턴스' (Instances) selected. The main content area displays the '네트워크' (Network) configuration for an instance named 'test1'. The configuration table includes fields for '공인IP' (Public IP), '내부IP 추가' (Add Internal IP), '내부IP' (Internal IP), and '보안정책' (Security Policy). The '공인IP' field contains the value '211.239.163.229' and is highlighted with a red box and a red circle with the number 1. The '내부IP 추가' dropdown is set to '기본 네트워크' (Basic Network), and the '자동할당' (Automatic Allocation) checkbox is checked. The '내부IP' field shows '192.168.211.7' with a '연결해제' (Disconnect) button. The '보안정책' field is set to 'SSH ,default,ICMP'. At the bottom right, the '저장' (Save) button is highlighted with a red box and a red circle with the number 2, next to a '취소' (Cancel) button.

IaaS의 인스턴스 상세 페이지

### 4) 공인 IP 연결 확인 및 저장

- ① 공인 IP 연결 설정이 완료 되면 공인 IP란에 ① 번과 같이 사용자가 선택한 공인 IP가 입력 된 것을 확인 할 수 있습니다.
- ② 인스턴스 정보 페이지 하단에 위치하고 있는 ② [저장] 버튼을 클릭 하시면 인스턴스와 공인 IP 연결이 완료 됩니다.

## 5. 인스턴스와 공인IP 연결

The screenshot shows the KOSCOM IaaS console interface. The top navigation bar includes 'IaaS', 'PaaS', 'Market', 'DevOps', and 'Guide'. The left sidebar shows a menu with '서버' (Server) expanded, containing '인스턴스' (Instances), '초기화 스크립트' (Init Scripts), '보안정책' (Security Policies), '키페어' (Key Pairs), '스토리지' (Storage), '네트워크/보안' (Network/Security), and '리소스 환경' (Resource Environment). The main content area is titled '서버 > 인스턴스' (Server > Instances) and displays a table of instances. The table has columns: '이름' (Name), '이미지' (Image), '용도' (Usage), '상태' (Status), '작업상태' (Operation Status), '키페어' (Key Pair), '내부IP' (Private IP), '공인IP' (Public IP), and '상세관리' (Detailed Management). The first instance, 'test1', is highlighted with a red box and a red circle with the number 1, indicating it is connected to a public IP.

이름	이미지	용도	상태	작업상태	키페어	내부IP	공인IP	상세관리
test1	ubuntu 16.04-cloud	WAS	active		moon1key	192.168.211.7	211.239.163.229	상세관리
vv	cirros-0.3.4	WAS	active		moon1key	192.168.211.9		상세관리
vm_test_1_1	cirros-0.3.4	WAS	active		moon1key	10.10.10.4		상세관리
vm_test_1	cirros-0.3.4	WAS	active		moon1key	192.168.211.8		상세관리
testvm	cirros	WAS	active		moon1key	192.168.211.6		상세관리
aaa	cirros	WAS	active		moon1key	192.168.211.5		상세관리

IaaS의 인스턴스페이지

### 5) 공인 IP 연결 완료

- ① 인스턴스와 공인 IP가 ① 번과 같이 연결된 것을 확인 할 수 있습니다.

## 5. 인스턴스와 공인IP 연결

```

C:\명령 프롬프트
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\₩₩₩ ① ping 211.239.163.229

Ping 211.239.163.229 32바이트 데이터 사용:
211.239.163.229의 응답: 바이트=32 시간=8ms TTL=53
211.239.163.229의 응답: 바이트=32 시간=4ms TTL=53
211.239.163.229의 응답: 바이트=32 시간=5ms TTL=53
211.239.163.229의 응답: 바이트=32 시간=4ms TTL=53

211.239.163.229에 대한 Ping 통계:
패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 4ms, 최대 = 8ms, 평균 = 5ms ②
  
```

Windows 환경

```

oper@operation: ~
oper@operat ③ : $ ping 211.239.163.229
PING 211.239.163.229 (211.239.163.229): 56(84) bytes of data.
64 bytes from 211.239.163.229: icmp_seq=1 ttl=53 time=5.70 ms
64 bytes from 211.239.163.229: icmp_seq=2 ttl=53 time=5.59 ms
64 bytes from 211.239.163.229: icmp_seq=3 ttl=53 time=5.00 ms
64 bytes from 211.239.163.229: icmp_seq=4 ttl=53 time=5.69 ms
64 bytes from 211.239.163.229: icmp_seq=5 ttl=53 time=5.08 ms
64 bytes from 211.239.163.229: icmp_seq=6 ttl=53 time=5.08 ms
64 bytes from 211.239.163.229: icmp_seq=7 ttl=53 time=8.92 ms
64 bytes from 211.239.163.229: icmp_seq=8 ttl=53 time=5.03 ms
64 bytes from 211.239.163.229: icmp_seq=9 ttl=53 time=5.78 ms
64 bytes from 211.239.163.229: icmp_seq=10 ttl=53 time=4.67 ms
64 bytes from 211.239.163.229: icmp_seq=11 ttl=53 time=4.95 ms
64 bytes from 211.239.163.229: icmp_seq=12 ttl=53 time=5.00 ms
64 bytes from 211.239.163.229: icmp_seq=13 ttl=53 time=5.40 ms
64 bytes from 211.239.163.229: icmp_seq=14 ttl=53 time=5.66 ms
64 bytes from 211.239.163.229: icmp_seq=15 ttl=53 time=5.78 ms
64 bytes from 211.239.163.229: icmp_seq=16 ttl=53 time=5.94 ms
64 bytes from 211.239.163.229: icmp_seq=17 ttl=53 time=14.1 ms
  
```

④

Linux 환경

### 6-1) 공인 IP 접속 확인 ( Windows 환경)

- ① Windows 환경의 명령 프롬프트(CMD)를 실행시켜 ① 번과 같은 ping 테스트를 실행합니다. (ping 할당 받은 공인IP 주소)
- ② ② 번과 같은 ping 테스트 로그가 성공적으로 실행되면 공인 IP와 인스턴스가 성공적으로 연결 된 것을 확인 할 수 있습니다.

### 6-2) 공인 IP 접속 확인 ( Linux 환경)

- ① Linux 환경의 터미널을 실행시켜 ③ 번과 같이 ping 테스트를 실행합니다. (ping 할당 받은 공인 IP 주소)
- ② ④ 번과 같은 ping 테스트 로그가 성공적으로 실행되면 공인 IP와 인스턴스가 성공적으로 연결 된 것을 확인 할 수 있습니다.

## 6. 인스턴스 ssh 접속

The screenshot shows the KOSCOM IaaS console interface. The top navigation bar includes 'IaaS', 'PaaS', 'Market', 'DevOps', and 'Guide'. The left sidebar shows a menu with '서버' (Server) expanded, containing '인스턴스' (Instances), '초기화 스크립트' (Init Scripts), '보안정책' (Security Policies), '키페어' (Key Pairs), '스토리지' (Storage), '네트워크/보안' (Network/Security), and '리소스 환경' (Resource Environment). The main content area is titled '서버 > 인스턴스' and displays a table of instances. The first instance, 'test1', is highlighted with a red box and a red circle with the number 1.

	이름	이미지	용도	상태	작업상태	키페어	내부IP	공인IP	
1	test1	ubuntu 16.04-cloud	WAS	active		moon1key	192.168.211.7	211.239.163.229	상세관리 ▼
	vv	cirros-0.3.4	WAS	active		moon1key	192.168.211.9		상세관리 ▼
	vm_test_1_1	cirros-0.3.4	WAS	active		moon1key	10.10.10.4		상세관리 ▼
	vm_test_1	cirros-0.3.4	WAS	active		moon1key	192.168.211.8		상세관리 ▼
	testvm	cirros	WAS	active		moon1key	192.168.211.6		상세관리 ▼
	aaa	cirros	WAS	active		moon1key	192.168.211.5		상세관리 ▼

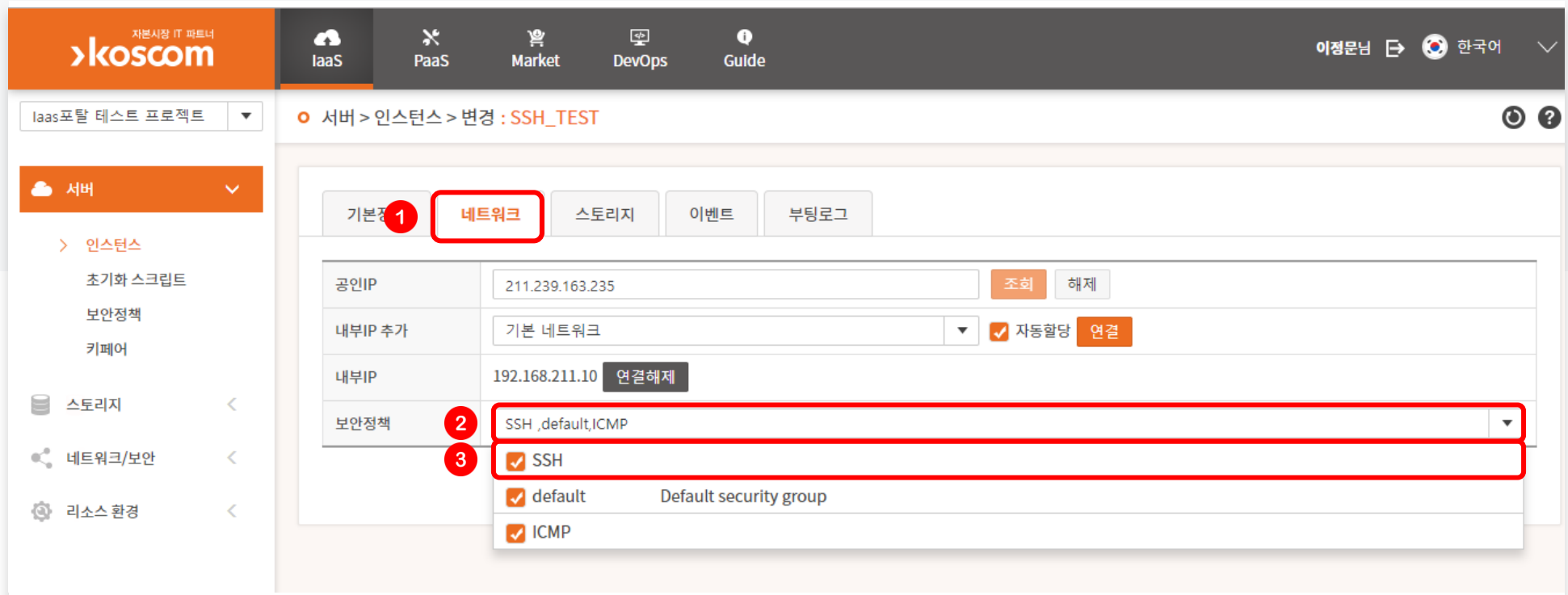
IaaS의 인스턴스페이지

### 1) IaaS의 인스턴스 정보 페이지 이동

- ① IaaS의 인스턴스 페이지로 이동하여 ssh연결을 할 ① [인스턴스]를 선택하여 인스턴스 정보 페이지로 이동합니다.

## 6. 인스턴스 ssh 접속

26



IaaS의 인스턴스 정보 페이지

### 2) 인스턴스 네트워크 보안정책 설정

- ① 인스턴스 정보 페이지 상단에 위치한 ① [네트워크] 탭을 클릭하여 페이지를 이동합니다.
- ② ① [네트워크] 탭 하단에 위치한 ② [보안정책] 을 클릭하여 ssh 연결을 위한 ③ [ssh] 탭을 클릭하여 저장합니다.

## 6. 인스턴스 ssh 접속

27

The screenshot shows the KOSCOM IaaS console interface. The left sidebar contains navigation links: 서버 (Servers), 인스턴스 (Instances), 초기화 스크립트 (Init Scripts), 보안정책 (Security Policies), 키페어 (Key Pairs), 스토리지 (Storage), 네트워크/보안 (Network/Security), and 리소스 환경 (Resource Environment). The main content area displays a table of key pairs. The table has columns: 이름 (Name), 설명 (Description), fingerprint, and 다운로드 (Download). The 'key02' row is highlighted with a red box around the download icon. A red arrow points from this icon to a tooltip that shows a padlock icon for 'private Key' and a key icon for 'public Key'.

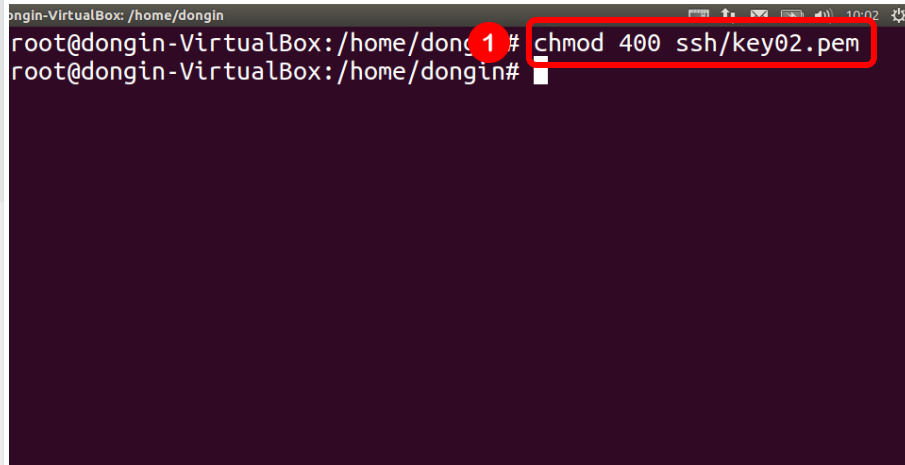
이름	설명	fingerprint	다운로드
key01	test	9b:0f:3a:22:ba:d0:9e:68:d4:98:d7:3f:be:f a:b5:69	
key02	test	...	
key03	test	...	
Key_test_1	test_1	...	
mm	테스트	...	

laaS의 키페어 페이지

### 3) ssh key 파일 다운 받기

- ① laaS의 키페어 페이지로 이동합니다.
- ② 키페어 페이지에서 사용자가 ssh 접속을 하고 싶은 인스턴스와 연결한 1 [ssh key 파일]을 다운받습니다.

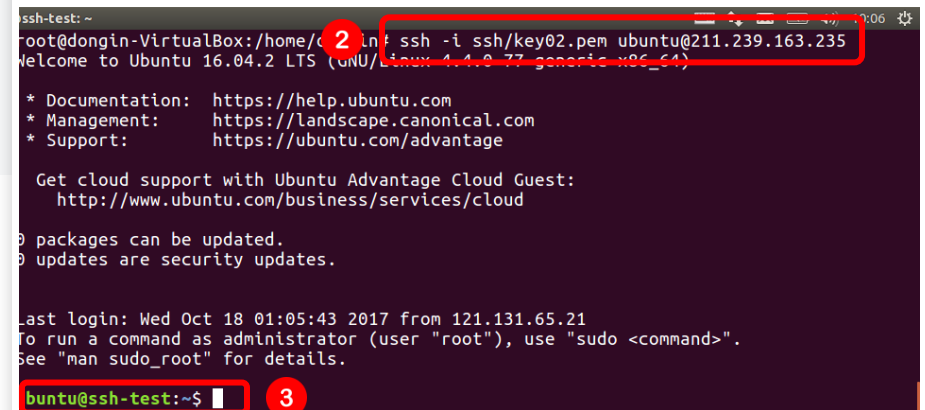
## 6. 인스턴스 ssh 접속



```

dongin-VirtualBox: /home/dongin
root@dongin-VirtualBox:/home/dongin# 1 chmod 400 ssh/key02.pem
root@dongin-VirtualBox:/home/dongin#
  
```

ssh 파일 chmod 명령어



```

ssh-test: ~
root@dongin-VirtualBox:/home/dongin# 2 ssh -i ssh/key02.pem ubuntu@211.239.163.235
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.

Last login: Wed Oct 18 01:05:43 2017 from 121.131.65.21
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ssh-test:~$ 3
  
```

ssh 접속 완료

### 4) ssh 접속

- ① 리눅스 환경의 터미널을 실행 시켜 ❶ 번과 같은 명령어를 입력합니다. (chmod 400 ssh 키 파일)
- ② chmod 명령어가 성공적으로 실행 후 ❷ 번과 같이 ssh 접속 명령어를 입력합니다. (ssh -i ssh키 파일 ubuntu@공인IP)
- ③ ssh 접속 명령이 성공적으로 완료 하면 ❸ 번과 같이 사용자와 환경이 바뀌며 ssh에 접속 완료를 확인 할 수 있습니다.



## 7. 인스턴스 apache 서비스

29

```
@ssh-test: /etc/resolvconf/resolv.conf.d
ubuntu@ssh-test:/etc/resolvconf/resolv.conf.d:1$ sudo apt-get update
sudo: unable to resolve host ssh-test
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [102 B]
Hit:2 http://archive.ubuntu.com/ubuntu xenial InRelease
Get:3 http://archive.ubuntu.com/ubuntu xenial-updates InRelease [102 B]
Get:4 http://security.ubuntu.com/ubuntu xenial-security/main Sources [102 B]
Get:5 http://security.ubuntu.com/ubuntu xenial-security/restricted Sources [2,600 B]
Get:6 http://security.ubuntu.com/ubuntu xenial-security/universe Sources [43.4 kB]
Get:7 http://archive.ubuntu.com/ubuntu xenial-backports InRelease [102 B]
Get:8 http://security.ubuntu.com/ubuntu xenial-security/multiverse Sources [1,140 B]
```

ssh 접속 후 업데이트

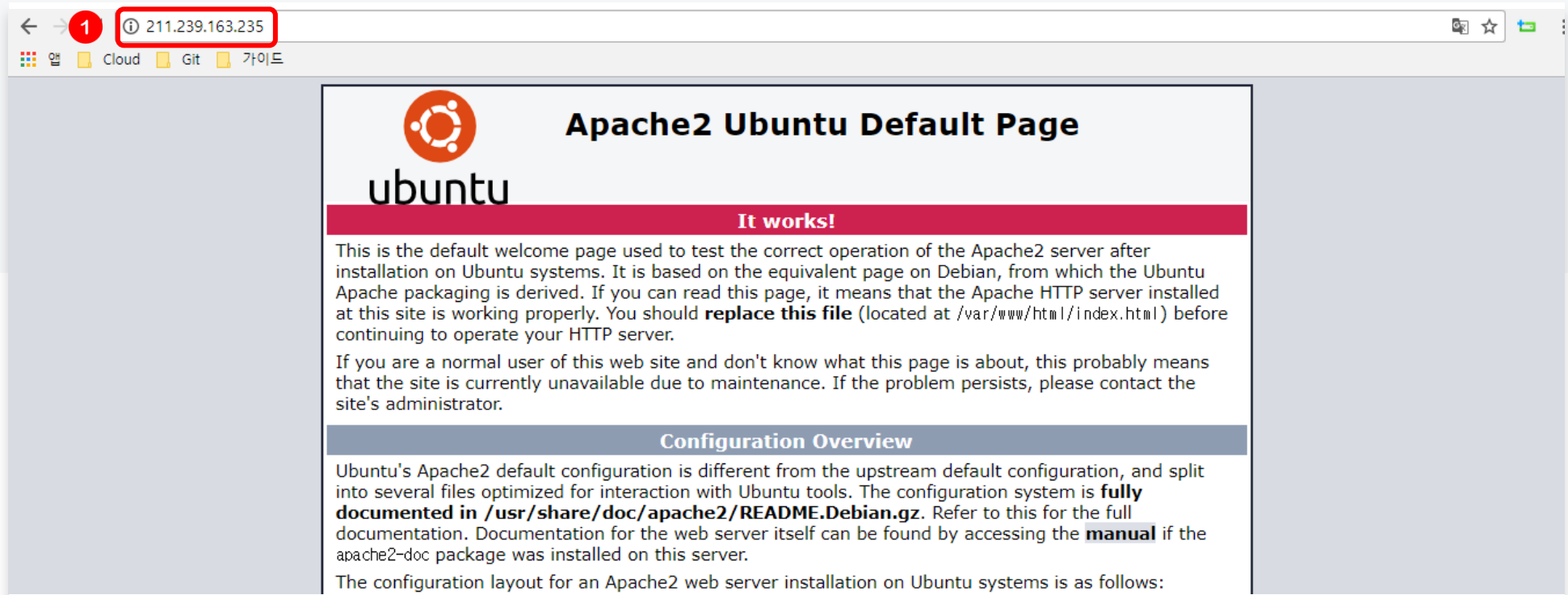
```
@ssh-test: /etc/resolvconf/resolv.conf.d
ubuntu@ssh-test:/etc/resolvconf/resolv.conf.d:2$ sudo apt install apache2
sudo: unable to resolve host ssh-test
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0 ssl-cert
Suggested packages:
  www-browser apache2-doc apache2-suexec-pristine
  | apache2-suexec-custom openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 134 not upgraded.
Need to get 1,557 kB of archives.
After this operation, 6,432 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Apache 설치

### 1) ssh 접속 후 apache 설치

- ① Apache 서비스를 실행할 인스턴스에 ssh 접속을 합니다.
- ② ssh 접속이 성공적으로 완료하면 ① [apt-get] 업데이트를 실행합니다. (sudo apt-get update)
- ③ ① [apt-get] 업데이트가 완료 하면 ② [apache2 설치] 를 실행합니다. (sudo apt install apache2)

## 7. 인스턴스 apache 서비스



아파치 설치 완료 페이지

### 2) apache 서비스 확인

- ① Apache 설치 완료 후 인터넷 브라우저를 실행 시킵니다.
- ② 인터넷 브라우저 주소 창에 인스턴스에 할당 된 ① [공인 IP 주소] 를 입력하여 확인합니다.
- ③ 위 안내 그림과 같이 apache 안내 페이지가 나오면 성공적으로 인스턴스에 apache 서비스가 적용 되었습니다.