

kt cloud

Basic Course Hands on Lab

# (5) Network

Copyright© 2023 kt cloud corp. All rights reserved.

## 실습 1. Tier 관리

01

Tier 정보 보기

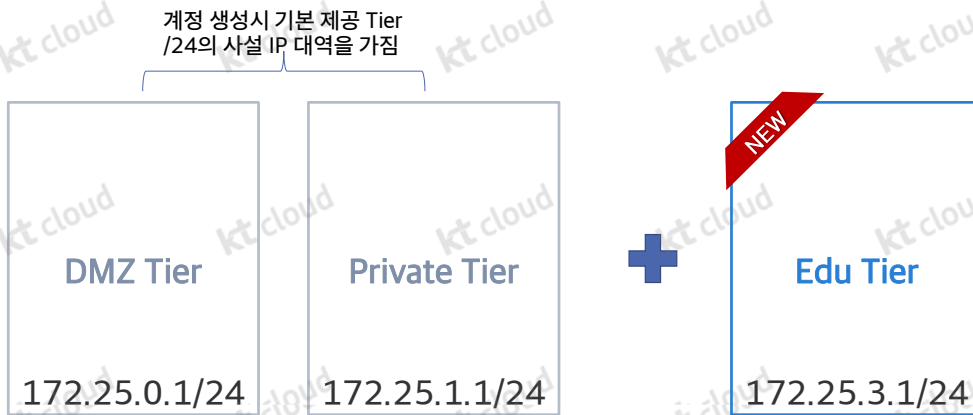
02

Tier 생성하기

03

생성된 Tier 확인하기

## 실습 1 개요



Copyright© 2023 kt cloud corp. All rights reserved.

kt cloud 계정에는 기본적으로 **DMZ Tier**와 **Private Tier**가 생성되어 있습니다. Tier는 계정내에 가상 네트워크 서브넷으로 Tier내에서 서버를 비롯한 다양한 서비스를 구성할 수 있도록 약 150개 정도의 사설 ip를 사용할 수 있습니다. 기본 Tier 외에 용도에 따라 추가 Tier를 생성할 수 있습니다.

## 1-1. Tier 정보 보기

① [Server] - [Tier]  
② DMZ Tier 선택 - [상세정보]

이름	위치	CIDR
Private	DX-M1	172.25.1.1/24
DMZ	DX-M1	172.25.0.1/24

tier이름	DMZ	CIDR	172.25.0.1/24
네트워크ID	f4df6988-8c81-41b4-8f7a-e78483fa19ac	시작 IP	172.25.0.6
연동대상	-	끝 IP	172.25.0.180
종류	PRIVATE	넷마스크	24
		게이트웨이	172.25.0.1

계정이 사용하고 있는 Tier 정보는 [Server]-[Tier] 메뉴를 선택하여 확인 가능합니다.

Tier의 상세 정보를 확인하면 가용한 사설 IP 정보를 알 수 있습니다.

- Tier 이름 / 종류
- CIDR
- 시작 IP / 끝IP
- 게이트 웨이

## 1-2. Tier 생성하기

Tier 생성하기.

가상 서버가 위치할 네트워크 대역

Tier 생성

기본 설정을 사용합니다. | 원하는 IP대역으로 설정합니다.

직접 IP 대역 설정

Tier 생성합니다.

네트워크 대역

기본 설정을 사용합니다. | 원하는 IP대역으로 설정합니다.

위치: DX-M1

이름: Edu

CIDR: 172.25.3/24

VM 사용 범위: 172.25.1.6 - 172.25.1.180

로드밸런서 사용 범위: 172.25.1.181 - 172.25.1.199

백어메일, 기타 범위: 172.25.1.201 - 172.25.1.250

iSCSI 사용 범위: 172.25.1.251 - 172.25.1.254

Gateway IP: 172.25.1.1

검증

취소 | Tier 생성

사설 IP의 세번째 옥텟을 지정하는 CIDR 형태의 대역 설정

- ① [Server] - [Tier]- Tier 생성
- ② 기본설정을 사용합니다 선택
- ③ Tier 이름 : Edu
- ④ CIDR의 세번째 옥텟 값 지정은 선택옵션

Copyright© 2023 kt cloud corp. All rights reserved.

Tier를 생성할 때, 사용할 사설 IP 대역이 정해지는데, 여기서 두가지 옵션이 있습니다.

기본 설정 옵션은 3번째 옥텟을 지정하게 되므로, 일반적으로는 **172.25.(지정 값).0/24**의 형태가 됩니다.

하나의 Tier는 /24bit의 IP대역을 제공하여 약 170개의 서버 사설IP를 사용할 수 있습니다.

### 1-3. 생성된 Tier 확인하기

**Tier**  
가상 서버가 위치할 네트워크 서브넷 단위의 Tier 관리합니다.

**Tier 생성** Data Lake Tier 생성 삭제 Private Subnet 상세정보 모든 위치 >

이름 ↓	위치	CIDR	VLAN	Type
<input type="checkbox"/> TestDT	DX-M1	172.24.153.1/24 *	253	Data Lake **
<input type="checkbox"/> Private	DX-M1	172.25.1.1/24	946	-
<input checked="" type="checkbox"/> Edu	DX-M1	172.25.3.1/24	381	새로 생성한 Tier
<input type="checkbox"/> DMZ	DX-M1	172.25.0.1/24	1077	-

Tier가 생성되면 일반적인 Tier는 Type에 '-'의 표시가 나오며, 사용하는 CIDR 정보를 알 수 있습니다.

[Data Lake Tier 생성]의 경우, 이름만 지정하며 CIDR 정보는 자동 할당됩니다.

Type 열을 보면 일반 Tier와 Data Lake Tier를 구분할 수 있습니다.

## 실습 2. 가상 네트워크 환경 내 VM 연결

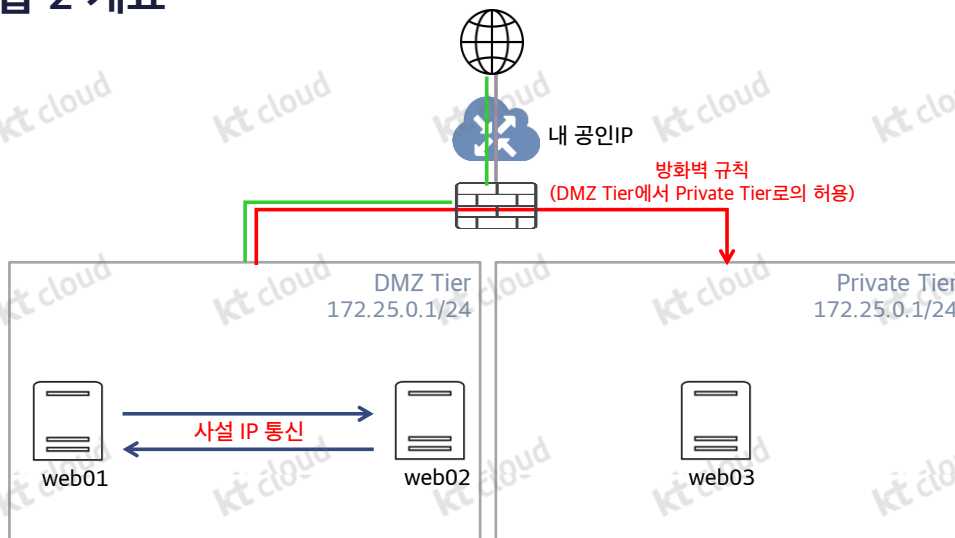
01

동일 Tier내 VM간 통신

02

한 계정의 서로 다른  
Tier간 VM 통신

## 실습 2 개요



Copyright© 2023 kt cloud corp. All rights reserved.

배스천 호스트란 내부와 외부 네트워크 사이에서 일종의 게이트 역할을 수행하는 호스트를 뜻합니다.

접근 제어 기능과 더불어 게이트웨이로서 가상 서버(Proxy Server)의 설치, 인증, 로그 등을 담당합니다. 특히 내부와 외부 사이에서 일종의 게이트 역할을 수행하는데요. 그만큼 위험에 노출되는 경우가 많기 때문에, 배스천 호스트는 네트워크 보안상 가장 중요한 방화벽 호스트입니다. 특히 내부 네트워크 전체의 보안을 담당하기 때문에 관리자의 감시 및 정기적인 점검이 뒷받침되어야 합니다. IT 보안 기업에서 제공하는 방화벽 솔루션은 이러한 배스천 호스트를 제공하는 것이 대부분입니다.



## 2-1. 서버의 사설 IP 확인

**Server**  
가상 서버를 관리합니다.

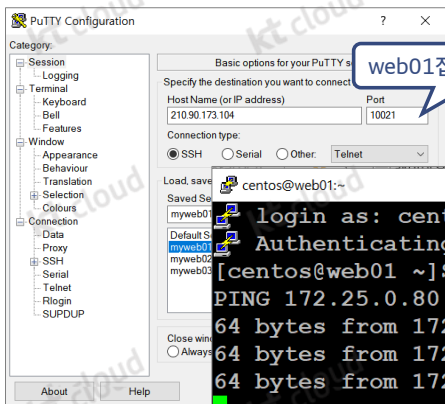
**서버 생성**   **시작**   **정지**   **재시작**   **강제재시작**   **삭제**   **접속설정**   ...   모든 위치 · 모든 상태 >

<input type="checkbox"/>	이름 ↓	상태	위치	운영체제	사양	상품	볼륨타입	사설IP	추가사설IP
<input type="checkbox"/>	web01	● 사용	DX-M1	centos-7.2-64bit	1vcore 1GB	표준	HDD	172.25.0.61	-
<input checked="" type="checkbox"/>	web02	● 사용	DX-M1	web01-image	1vcore 1GB	표준	HDD	172.25.0.80	-
<input type="checkbox"/>	web03	● 사용	DX-M1	centos-7.2-64bit	1vcore 1GB	표준	HDD	172.25.1.32	-

web02 서버의 사설 IP를 확인합니다.

클라우드 콘솔의 [Server]-[Server]페이지에서 각 서버의 가상사설 IP를 알 수 있습니다.  
web02 서버의 사설 IP를 복사해 둡니다.

## 2-2. 동일 Tier내 서버 간 통신 테스트



- ① PuTTY 실행 후 web01 서버로 로그인
- ② web02 서버의 사설 IP로 ping Test

동일한 Tier에 생성한 서버간에는 별도의 네트워크 설정 없이 사설IP만으로 통신이 가능합니다.  
이 실습을 통해 동일 Tier내 서버 간에는 네트워크 설정이 필요하지 않음을 알 수 있습니다.

## 2-3. web03 방화벽 규칙 변경

① [Server] - [Networking] - [방화벽]  
 ② external → Private\_Sub 삭제  
 ③ DMZ\_sub → Private\_Sub 추가

삭제	이동	No	Action	Protocol	Source	Destination	Port	Status	Priority	Direction	Icon	
<input type="checkbox"/>		5	allow	external	all	TCP	DMZ_Sub	PF_210.90.173.104_10023_...	---	●	-	✕
<input type="checkbox"/>		6	allow	external	all	TCP	DMZ_Sub	PF_210.90.173.104_10024_...	---	●	-	✕
<input type="checkbox"/>		7	allow	DMZ_Sub	172.25.0.14		18/32	---	●	-	✕	
<input type="checkbox"/>		8	allow	external	all		173.104_10042_...	10041-10041	●	-	✕	
<input type="checkbox"/>		9	allow	external	203.130.10		173.104_10042_...	10041-10041	●	-	✕	
<input type="checkbox"/>		10	allow	DMZ_Sub	172.25.0.72/32	ALL	external	all	●	-	✕	
<input checked="" type="checkbox"/>		11	allow	external	all	TCP	Private_Sub	PF_210.90.173.104_10026_...	---	●	-	✕

이전에 설정한 external로 부터 web03 서버로의 허용 정책 제거

DMZ Tier
→
Private Tier
+ 추가

Allow ▾ DMZ\_Sub ▾ 0.0.0.0/0 ▾ ALL ▾ Private\_Sub ▾ 0.0.0.0/0 or \*.kt.com Start - End

특정 Tier의 통신을 Tier간 통신으로만 제한할 수 있습니다.  
 방화벽에서 DMZ Tier에서 Private Tier로의 접근을 허용하는 정책을 추가하지 않으면 기본은 deny 이므로 접근이 불가능합니다.  
 그러므로, [Server]-[Networking]에서 방화벽 설정에 해당 정책을 추가합니다.  
 다양한 실습을 위해 프로토콜 유형을 ALL로 선택합니다.

## 2-4. 서버의 접속 설정 제거

① [Server] - [Networking] - [접속설정]  
② web03 서버의 포트 포워딩 항목 제거

서버	사설Port	공인IP	공인Port	프로토콜	설명
<input type="checkbox"/> web01	22	210.90.173.104	10021	TCP	
<input checked="" type="checkbox"/> web03	22	210.90.173.104	10026	TCP	
<input type="checkbox"/> web02	22	210.90.173.104	10023	TCP	
<input type="checkbox"/> web02	80	210.90.173.104	10024	TCP	
<input type="checkbox"/> web01	80	210.90.173.104	10022	TCP	

서버의 접속설정(포트포워딩) 항목을 삭제하기 위하여 [Server]-[Networking]-[접속설정]을 선택합니다.  
[Server]-[Server]-[접속설정]에서는 특정서버의 포트포워딩 설정만 가능합니다.

예제에서 web03 서버는 앞서 방화벽 규칙 및 접속설정 정보를 모두 제거했으므로 외부에서의 접근은 완전히 차단되었습니다.

다만, 방화벽 규칙에 따라 DMZ Tier의 서버들은 사설IP로 접근할 수 있습니다.

## 2-5. 다른 Tier의 서버 간 통신

**DMZ Tier**

**Server**  
가상 서버를 관리합니다.

<input type="checkbox"/>	이름 ↓	상태	위치	운영체제	사양	상품	볼륨타입	사설IP
<input type="checkbox"/>	web01	● 사용	DX-M1	centos-7.2-64bit	1vcore 1GB	표준	HDD	172.25.0.61
<input type="checkbox"/>	web02	● 사용	DX-M1	web01-image	1vcore 1GB	표준	HDD	172.25.0.80
<input type="checkbox"/>	web03	● 사용	DX-M1	centos-7.2-64bit	1vcore 1GB	표준	HDD	172.25.1.32

① [Server] - [Server]  
② web01, web02 서버의 사설 IP 복사

**사설 IP**

**Private Tier**

**Server**  
가상 서버를 관리합니다.

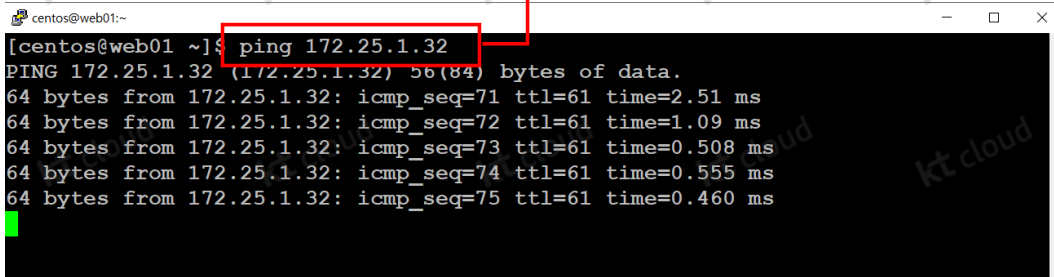
<input type="checkbox"/>	이름 ↓	상태	위치	운영체제	사양	상품	볼륨타입	사설IP
<input type="checkbox"/>	web01	● 사용	DX-M1	centos-7.2-64bit	1vcore 1GB	표준	HDD	172.25.0.61
<input type="checkbox"/>	web02	● 사용	DX-M1	web01-image	1vcore 1GB	표준	HDD	172.25.0.80
<input type="checkbox"/>	web03	● 사용	DX-M1	centos-7.2-64bit	1vcore 1GB	표준	HDD	172.25.1.32

Copyright© 2023 kt cloud corp. All rights reserved.

실습은 DMZ Tier의 임의의 서버가 Private Tier의 서버에 접근해 보는 것입니다.

## 2-6. 접속 확인

- web01 서버로 SSH 접속한 후 ping 테스트



```
centos@web01:~  
[centos@web01 ~]$ ping 172.25.1.32  
PING 172.25.1.32 (172.25.1.32) 56(84) bytes of data.  
64 bytes from 172.25.1.32: icmp_seq=71 ttl=61 time=2.51 ms  
64 bytes from 172.25.1.32: icmp_seq=72 ttl=61 time=1.09 ms  
64 bytes from 172.25.1.32: icmp_seq=73 ttl=61 time=0.508 ms  
64 bytes from 172.25.1.32: icmp_seq=74 ttl=61 time=0.555 ms  
64 bytes from 172.25.1.32: icmp_seq=75 ttl=61 time=0.460 ms
```

DMZ Tier의 서버가 Private Tier의 서버에 사설IP로 접근합니다.

## 실습 3. Bastion Host 구성

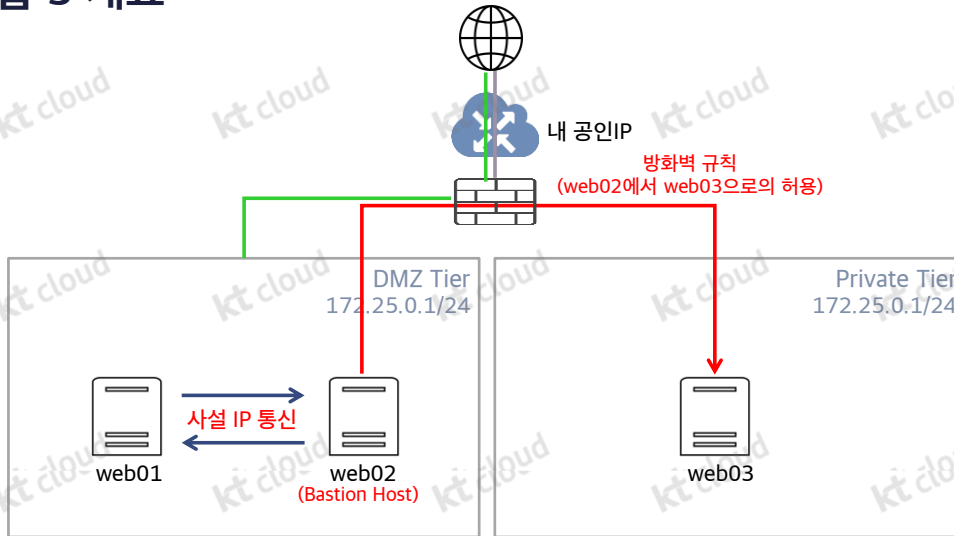
01

Bastion Host 구성

02

지정된 VM간 통신

## 실습 3 개요



배스천 호스트란 내부와 외부 네트워크 사이에서 일종의 게이트 역할을 수행하는 호스트를 뜻합니다.



### 3-1. 서로 다른 Tier의 지정된 서버 간 통신 규칙 설정

<input type="checkbox"/>	5	allow	external	all	TCP	DMZ_Sub	PF_210.90.173.104_1002			
<input type="checkbox"/>	6	allow	external	all	TCP	DMZ_Sub	PF_210.90.173.104_10024			
<input type="checkbox"/>	7	allow	DMZ_Sub	172.25.0.14/32	ALL	Private_Sub	172.25.1.118/32	--		
<input type="checkbox"/>	8	allow	external	all	TCP	DMZ_Sub	PF_210.90.173.104_10042	10041-10041		
<input type="checkbox"/>	9	allow	external	203.130.106.79/32	TCP	DMZ_Sub	PF_210.90.173.104_10042	10041-10041		
<input type="checkbox"/>	10	allow	DMZ_Sub	172.25.0.72/32	ALL	external	all	--		
<input checked="" type="checkbox"/>	11	allow	DMZ_Sub	all	ALL	Private_Sub	all	--		

- ① [Server] - [Networking] - [방화벽]
- ② DMZ\_Sub → Private\_Sub 규칙 제거
- ③ web02 IP --> web03 IP 규칙 추가

삭제 후  
추가

<input type="checkbox"/>	11	allow	DMZ_Sub	172.25.0.14/32	ALL	Private_Sub	172.25.1.118/32	--		
--------------------------	----	-------	---------	----------------	-----	-------------	-----------------	----	--	--

DMZ\_Sub web02

Private\_Sub web03

Allow

DMZ\_Sub

172.25.0.14/32

ALL

Private\_Sub

172.25.1.118/32

Start

End

web02 사설IP

web03 사설IP

Copyright© 2023 kt cloud corp. All rights reserved.

## 3-2. 지정된 서버 간 통신

**DMZ Tier**

**Server**  
가상 서버를 관리합니다.

서버 생성 시작 중지 재시작 강제재시작 삭제 접속설정 ... 모든 위치 · 모든 상태 >

이름	상태	위치	운영체제	사양	상품	볼륨타입	사설IP	추가사설IP	생성일시
web01	...	DX-M1	centos-7.2-64bit	1vcore 1GB	표준	HDD	172.25.0.5...	-	07/21/2023...
<input checked="" type="checkbox"/> web02	...	DX-M1	web01-image	1vcore 1GB	표준	HDD	172.25.0.1...	-	07/21/2023...
web03	...	DX-M1	centos-7.2-64bit	1vcore 1GB	표준	HDD	172.25.1.1...	-	07/21/2023...

**Private Tier**

**Server**  
가상 서버를 관리합니다.

서버 생성 시작 중지 재시작 강제재시작 삭제 접속설정 ... 모든 위치 · 모든 상태 >

이름	상태	위치	운영체제	사양	상품	볼륨타입	사설IP
web01	사용	DX-M1	centos-7.2-64bit	1vcore 1GB	표준	HDD	172.25.0.61
web02	사용	DX-M1	web01-image	1vcore 1GB	표준	HDD	172.25.0.80
<input checked="" type="checkbox"/> web03	사용	DX-M1	centos-7.2-64bit	1vcore 1GB	표준	HDD	172.25.1.32

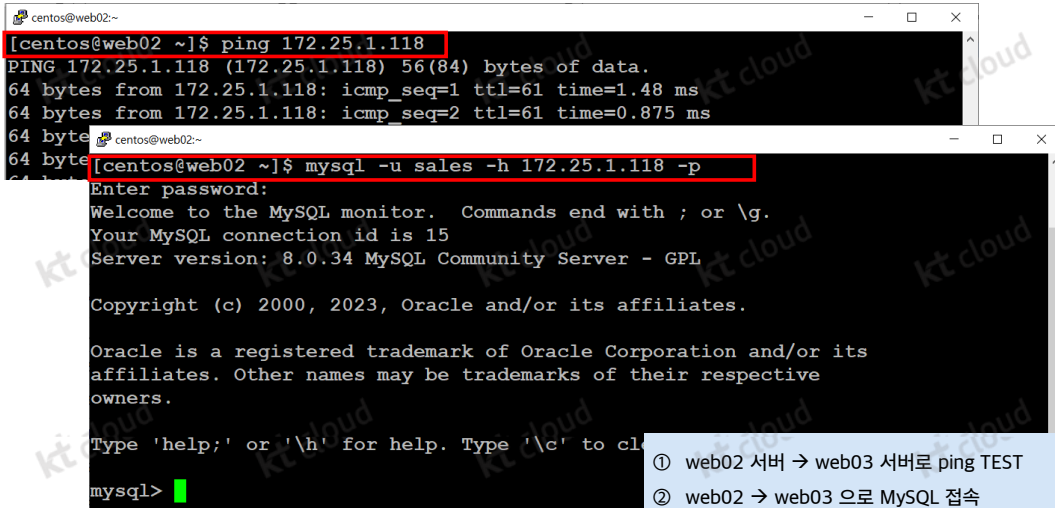
① [Server] - [Server]  
 ② web02 서버의 사설 IP 복사

사설 IP

Copyright© 2023 kt cloud corp. All rights reserved.

실습은 DMZ Tier와 Private Tier의 지정된 서버끼리의 통신입니다.  
 예제는 DMZ Tier의 web02 서버만 Private Tier의 web03 서버에게 접속합니다.

### 3-3. 접속 테스트



```
centos@web02~  
[centos@web02 ~]$ ping 172.25.1.118  
PING 172.25.1.118 (172.25.1.118) 56(84) bytes of data.  
64 bytes from 172.25.1.118: icmp_seq=1 ttl=61 time=1.48 ms  
64 bytes from 172.25.1.118: icmp_seq=2 ttl=61 time=0.875 ms  
64 bytes from 172.25.1.118: icmp_seq=3 ttl=61 time=0.875 ms  
64 bytes from 172.25.1.118: icmp_seq=4 ttl=61 time=0.875 ms  
64 bytes from 172.25.1.118: icmp_seq=5 ttl=61 time=0.875 ms  
[centos@web02 ~]$ mysql -u sales -h 172.25.1.118 -p  
Enter password:  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 15  
Server version: 8.0.34 MySQL Community Server - GPL  
Copyright (c) 2000, 2023, Oracle and/or its affiliates.  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
mysql>
```

- ① web02 서버 → web03 서버로 ping TEST
- ② web02 → web03 으로 MySQL 접속

Copyright© 2023 kt cloud corp. All rights reserved.

19

방화벽에 지정된 IP의 서버만 규칙에 지정된 대상 서버로의 접속에 성공합니다.

