kt ucloud biz

업데이트일 : 2018-11-01

VIII. 네트워크

3. LoadBalancer

목차

3.1 Load Balancer 서비스 소개

3.1.1 목적/용도

☐ 문서의 목적

본 문서는 KT ucloud server의 부가서비스인 로드밸런서의 기술적 특징과 ucloud biz 포탈에서의 서비스 신청 및 세부 실행 가이드를 제공하는데 목적을 두고 있습니다.

☐ 문서의 사용 범위

○ 로드밸런싱의 구조 및 원리 이해

○ ucloud biz 클라우드 콘솔을 통한 로드밸런서 서비스 이용

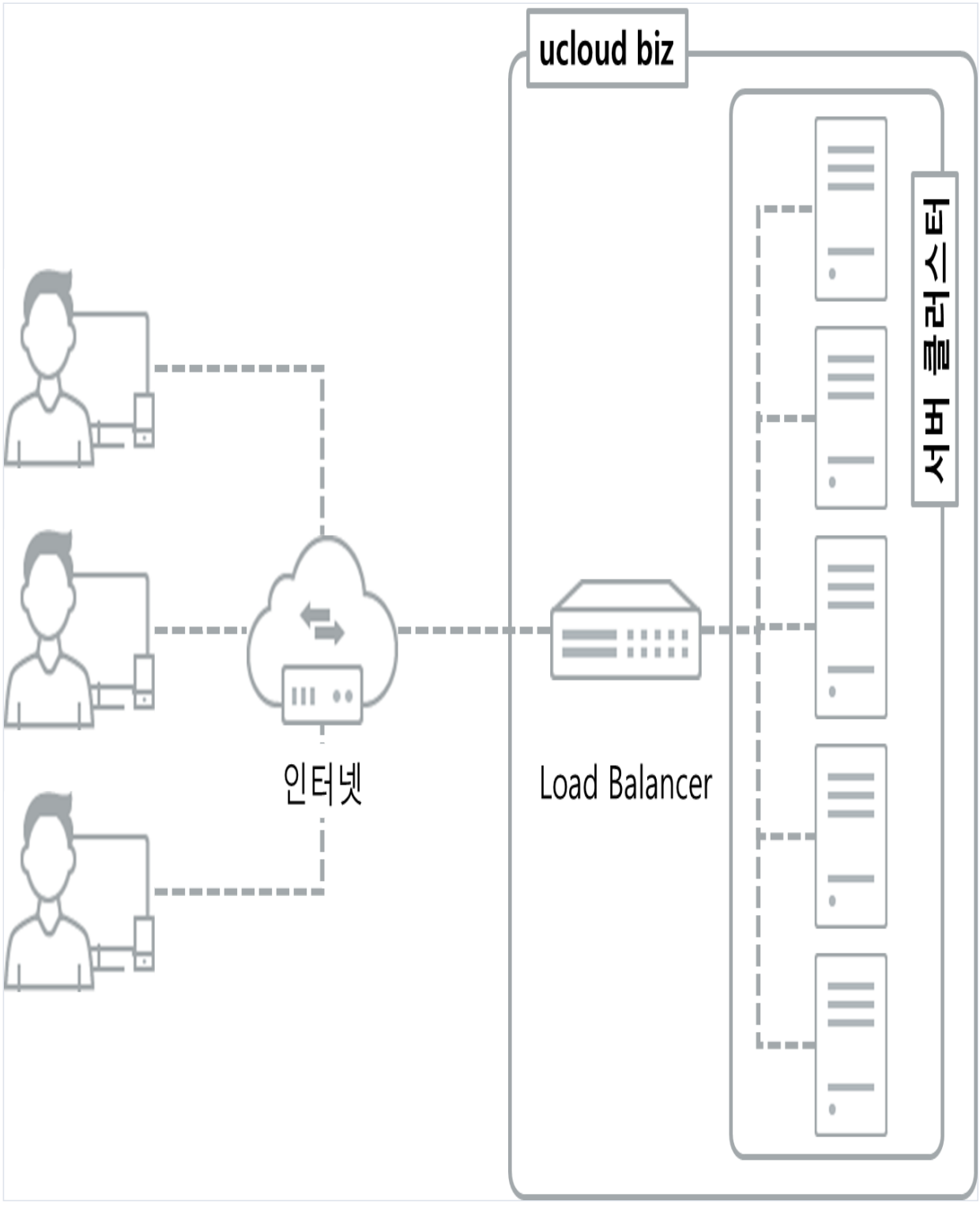
- 로드밸런서 화면 구성
- 로드밸런서 신청/해지
- 로드밸런서 생성/삭제
- 로드밸런서 세부 설정

☐ **KT ucloud 로드밸런서 특징**

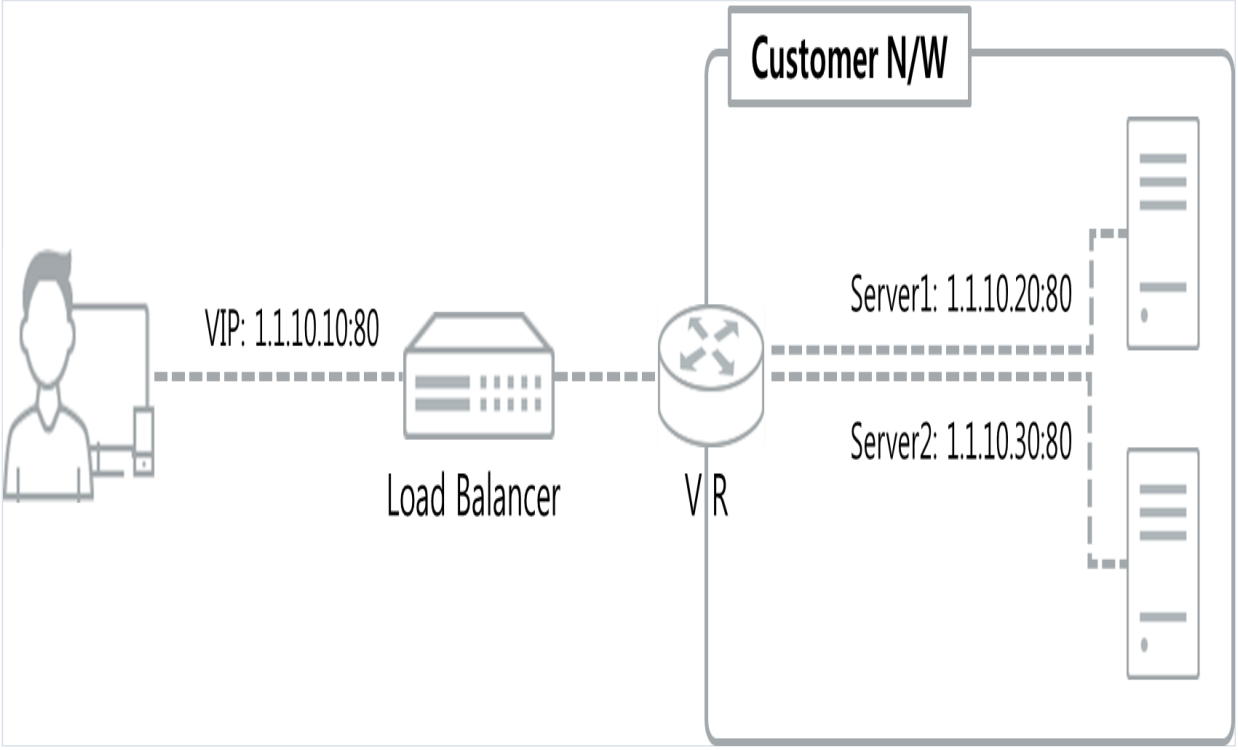
구분	종량제	정액제(별도 신청)
메소드	Round Robin, Hashing (Source IP/Source IP+Port), Least Connection, Least Response	Round Robin, Hashing (Source IP/Source IP+Port), Least Connection
모니터링	Throughput, Server Connections, TTFB, Request Connections, 상태(UP/DOWN)	Clients Connections, 상태(UP/DOWN)
서비스 타입	HTTP / TCP / HTTPS(Bridge) / HTTPS / FTP	HTTP
대역폭	On-Demand	100M/300M/500M: 포탈 제공 1G/3G: 전용 LB 제공
가격	LB 사용 시간: 20원/시간 데이터 처리량: 6원/GB 데이터 처리량(SSL): 9원/GB	용량 별 정액제 제공
안정성	이중화 구성(Active/Standby)	이중화 구성(Active/Standby)

3.1.2 구조/원리

☐ **로드밸런싱의 개념**



KT ucloud의 로드밸런싱(부하분산)은 리소스의 활용을 최적화 하기 위해 클라이언트의 요청을 여러 가상 서버(VM)에 분산시켜 주기 위한 기능입니다. 한 가지 종류의 서비스를 한 대의 서버에서 지원할 경우 많은 수의 클라이언트 요청에 대하여 과부하가 발생하고 서버 성능이 저하될 수 있습니다. 로드밸런서가 클라이언트의 요청을 수신하면 고객 서비스 영역 안에 있는 여러 가상 서버로 분산하여 정보를 처리할 수 있도록 합니다. 이때 고객은 필요에 따라 특정한 메소드(알고리즘)를 선택하여 부하를 분산 시키는 방법을 다르게 적용시킬 수 있습니다. 로드밸런싱의 처리 과정 대하여 간단한 도식을 해보면 다음과 같습니다.



위 그림에서와 같이 클라이언트는 실제 back-end에 위치한 서버의 주소가 아닌, 가상 IP주소(Virtual IP;VIP)로 접근합니다. VIP로 들어온 클라이언트 요청은 로드밸런서에 설정한 로드밸런서 옵션에 따라 back-end 서버들 중 적합한 대상 IP/Port를 설정합니다. 설정 된 대상 IP/Port 주소를 기반으로 클라이언트 요청은 포트포워딩 NAT기능을 하는 가상 라우터(Virtual Router; VR)를 통해 각 서비스에 도달하게 됩니다. KT ucloud biz에서 로드밸런싱 서비스를 사용하는 절차는 다음과 같습니다.

1. 로드밸런서 서비스를 신청하고 로드밸런서에 접근하기 위한 공인 IP(Public IP)를 할당합니다. 이 때 할당 방법은 미리 생성해 둔 가상 IP를 사용하거나 자동으로 신규 IP를 발급받도록 설정할 수 있습니다.
2. 로드밸런서에 등록 할 back-end 서버를 지정한 뒤, 최종 생성 신청을 완료 합니다.
3. 로드밸런서 생성 완료 직후 연결 상태는 'DOWN'로 나타나며 이는 네트워크 연결 과정이 진행 중인 상태로 back-end 서버가 정상적으로 동작하고 있다면 일정 시간 후 'UP'으로 변경 됩니다.

☐ 로드밸런싱의 핵심 특징

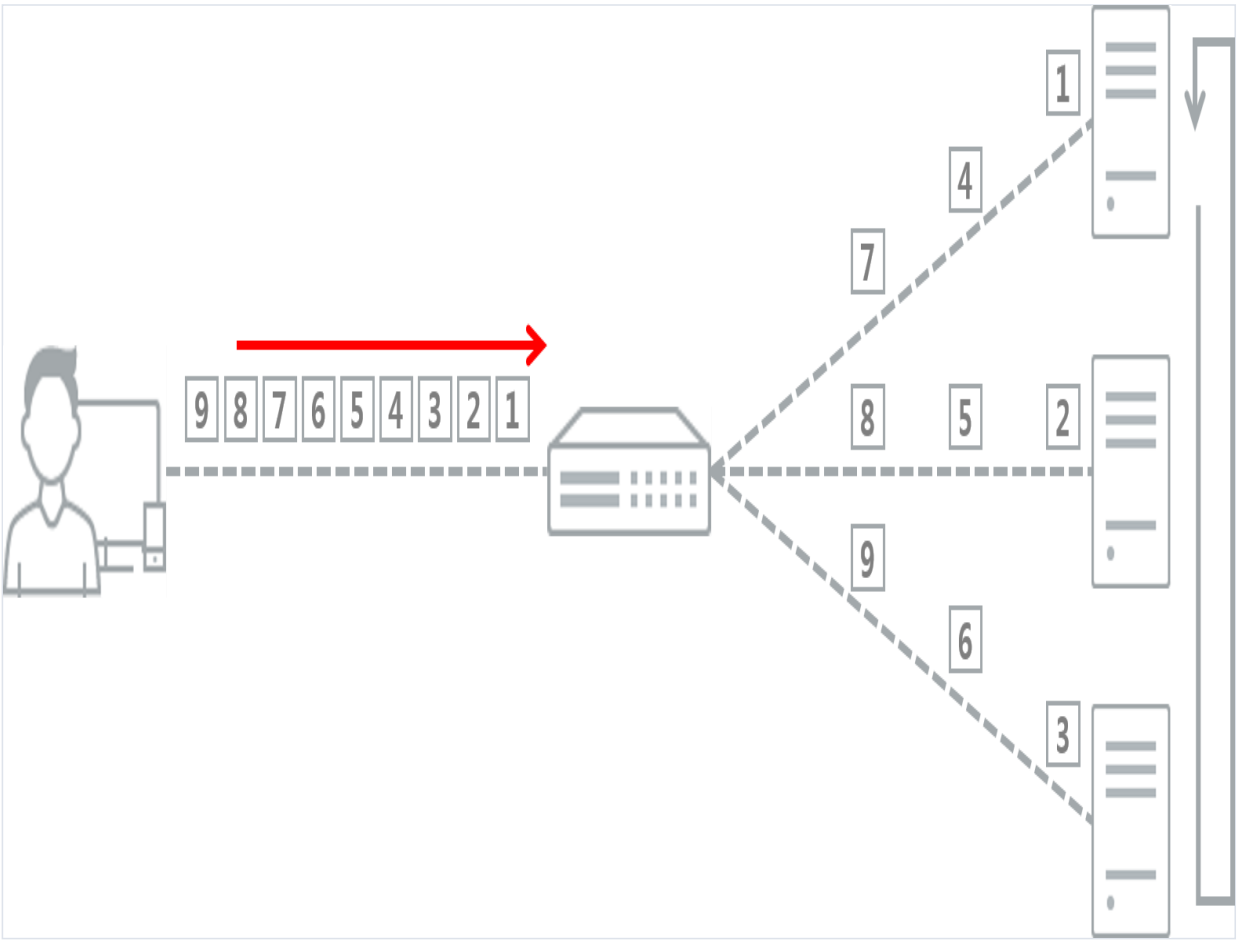
항목	특징
보안성	SynAttack 방어에 뛰어난 성능을 지님
수용성	로드밸런서는 고성능을 요구하는 중/대형 고객에 적합
서비스	HTTP/HTTPS(Bridge)/TCP/FTP 로드밸런싱 제공
성능	TCP Offload 를 이용한 웹서버 부하 경감 구현(HTTP 방식 사용시)
기타	http header(X-Forwarded-For)를 이용한 Client IP 제공(HTTP 방식 사용시)

☐ 로드밸런싱 메소드

KT ucloud server의 로드밸런싱 메소드(이하 옵션)는 총 5가지 옵션을 지원하고 있습니다.

○ Round Robin

Round Robin 방식은 클라이언트의 요청을 단순하게 들어온 순서대로 순환을 하여 로드밸런싱을 처리하는 방법입니다.



위 그림과 같이 back-end에 4개의 서버가 존재하는 경우 '서버 1' 부터 '서버 3' 까지 새로운 연결이 생길 때 마다, 1-2-3-1-2...과 같이 순환을 하는 방식입니다. 응답 시간이 빠르고 구성이 단순하다는 점이 장점입니다. 단, back-end 서버에 균등한 부하 분산이 이루어지지 않으며 무조건 순차적으로 포워딩 하므로 결제 시스템과 같이 연결 유지에 높은 신뢰가 요구되는 서비스인 경우 추천하지 않습니다.

○ Hasing(Source IP, Source IP+Port)

Hash 방식은 client 의 Source IP 정보 또는 Source IP + Port 정보를 바탕으로 hash 한 결과 값을 토대로 로드밸런싱을 수행합니다. 특정한 노드는 항상 동일한 Hash 값을 가지기 때문에, 동일한 클라이언트의 요청은 동일한 back-end 서버에서 응답을 받도록 하고자 할 때 주로 사용합니다.

- Source IP 방식

출발지(Source IP)주소를 기반으로 hash 값을 생성하여 hash 값을 기준으로 로드밸런싱을 수행합니다. 출발지가 동일한 주소는 항상 동일한 back-end 서버를 리턴 받기 때문에 결재 등을 지원하는 웹 서버의 경우 세션의 유지가 이루어 질 수 있으므로 추천하는 방식입니다. 하지만, 출발지 IP 주소가 NAT 환경과 같이 수 백대의 서버가 하나의 NAT Gateway를 이용하는 경우, 로드밸런서는 여러 대의 서버가 요청을 보내왔더라도, 동일한 hash값을 얻기 때문에 부하 분산 효과를 보기 어렵다는 단점이 존재 합니다.

- Source IP+Port 방식

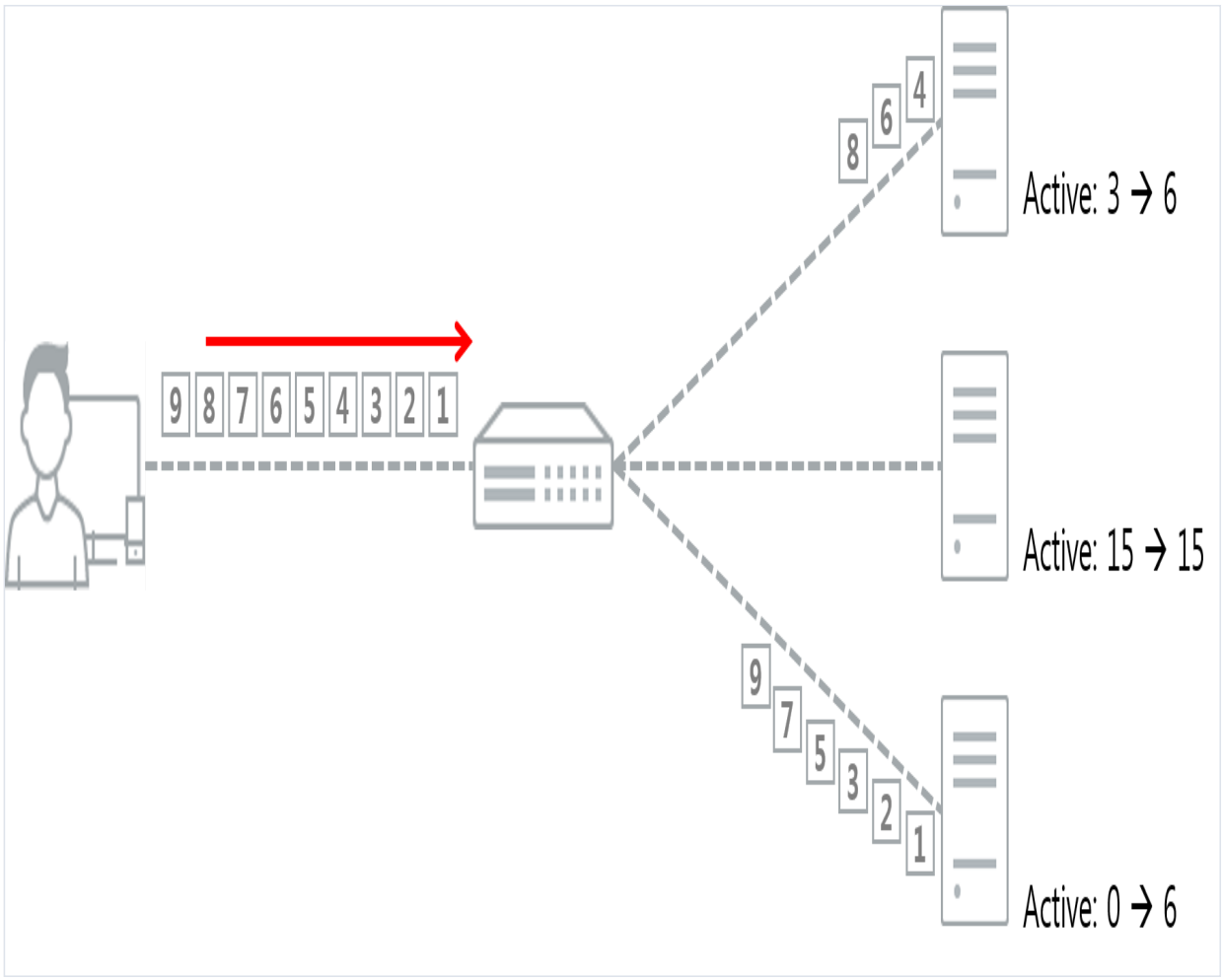
출발지(Source IP)주소와 Port 값을 기반으로 hash 값을 생성하여 hash 값을 기준으로 로드밸런싱을 수행합니다. 이 경우 특정 커넥션의 모든 패킷이 동일한 물리적 서버 내 서비스로 흐르도록 할 수 있습니다. Source IP 방식의 한계점인 NAT 환경에서의 단점을 극복할 수 있으나, 세션의 연속성은 끊어질 가능성이 있기 때문에 Source IP 방식과 달리 결제와 같은 시스템에는 적합하지 않습니다.

○ Least Response

Least Response 방식은 가장 빠른 Response Time(TTFB)을 제공하는 웹 서버로 로드밸런싱을 수행합니다. 로드밸런서는 back-end에 있는 가상 서버로부터 http(s) '200' 응답을 기준으로 TTFB 값을 계산 합니다. 따라서 고객이 제공하는 서비스가 웹 서버인 경우에만 본 알고리즘의 정상 동작을 보장할 수 있습니다. Least Response 방식은 back-end에 존재한 웹 서버들이 사용하는 가상 서버 자원양이 다른 경우, 서버까지 연결을 형성하는데 소요되는 시간, 각 서버가 처리하는 데이터 양이 서로 상이한 서비스 환경에서 유리하게 작용합니다.

○ Least Connection

Least Connection 방식은 새로운 클라이언트의 요청이 들어오는 경우, 로드밸런서에 연결 된 back-end 서버 중 활성(Active)화 되어 있는 연결의 수를 계산하여 가장 적은 커넥션 수를 보유한 서버로 로드밸런싱을 수행합니다.



로드밸런서에 연결 된 back-end 서버의 활성화 된 연결 수가 위 그림과 같을 경우, 새로운 연결 요청이 들어왔을 때 로드밸런서는 세 번째 서버로 연결을 설정하게 됩니다. 반복하여 연결이 수행 되는 동안 현재 활성화 된 연결 수를 점검한 뒤 적절한 back-end 서버로 연결을 넘겨주게 됩니다. 일반적인 웹 서비스 제공 환경에서는 Least Connection 알고리즘이 최적의 성능을 제공할 수 있습니다.

3.1.3 유의사항/제약사항

☐ **Port Forwarding과 보안**

로드밸런서를 생성한 뒤, 외부 공인 인터넷망에서 접근이 가능하게 하려면 [KT ucloud server - 네트워크]에서 포트포워딩 구성을 진행하게 됩니다. 이 때, 포트포워딩 추가 시 지정한 IP/Public Port로의 방화벽이 모든 Source IP에 대해 오픈 됩니다. 보안 강화를 위해 back-end 서버에 대한 방화벽 설정을 로드밸런서의 네트워크 대역에 해당하는 아래 CIDR만 접근 허용하는 정책 적용을 권고하고 있습니다.

Central A/B : 14.63.233.24/29

KOR-HA : 14.63.176.112/28

Seoul M : 211.253.15.48/29

Seoul M2 : 211.252.80.40/29

☐ 로드밸런서와 서버 응답 성능

로드밸런서는 사용자가 지정한 기준(옵션)에 따라 온전하게 네트워크 관점에서 분석하여 로드밸런싱을 수행합니다. 따라서, 각각의 back-end 서버의 성능 또는 파라미터 설정에 따라 실제 서버에 로드되는 부하량은 언제나 균등하지 않을 수 있습니다. 수 차례의 테스트와 성능 검증을 진행 하시어 운영하고자 하는 서비스에 최적화 된 옵션을 설정 하시는 것을 권고하고 있습니다.

☐ 로드밸런서 세션 수 제한

KT ucloud biz 로드밸런서는 타 고객/영역 서비스 보호를 위하여 LB당 최대 세션 수를 40만으로 제한하고 있습니다. 그 이상의 세션이 요구되는 서비스의 경우 기업 전용 클라우드 상품 또는 전용 로드밸런서 서비스 이용을 권고드리고 있습니다.

3.2 Load Balancer FAQ

ucloud biz 상품의 모든 상담 및 장애 신고 방법은 전화상담과 게시판 상담을 통해 이루어집니다.

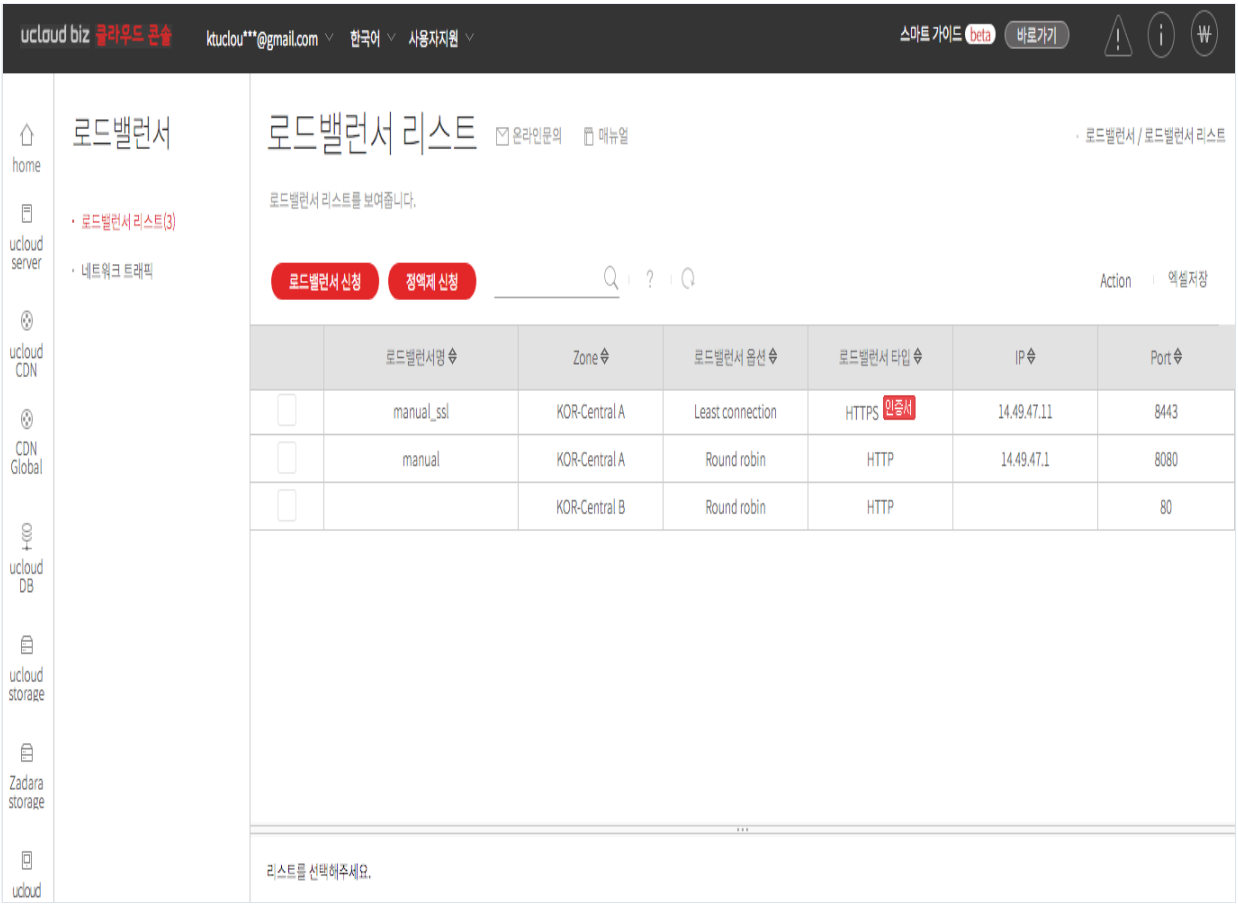
☐ FAQ 및 매뉴얼

각종 사용 매뉴얼 및 FAQ 는 ucloud biz 포탈 고객센터의 <u>FAQ 게시판 </u> 및 자료실을 통하여 확인 하실 수 있습니다..

3.3 Load Balancer 이용방법

☐ 로드밸런서 페이지 화면 구성

○ 로드밸런서 리스트

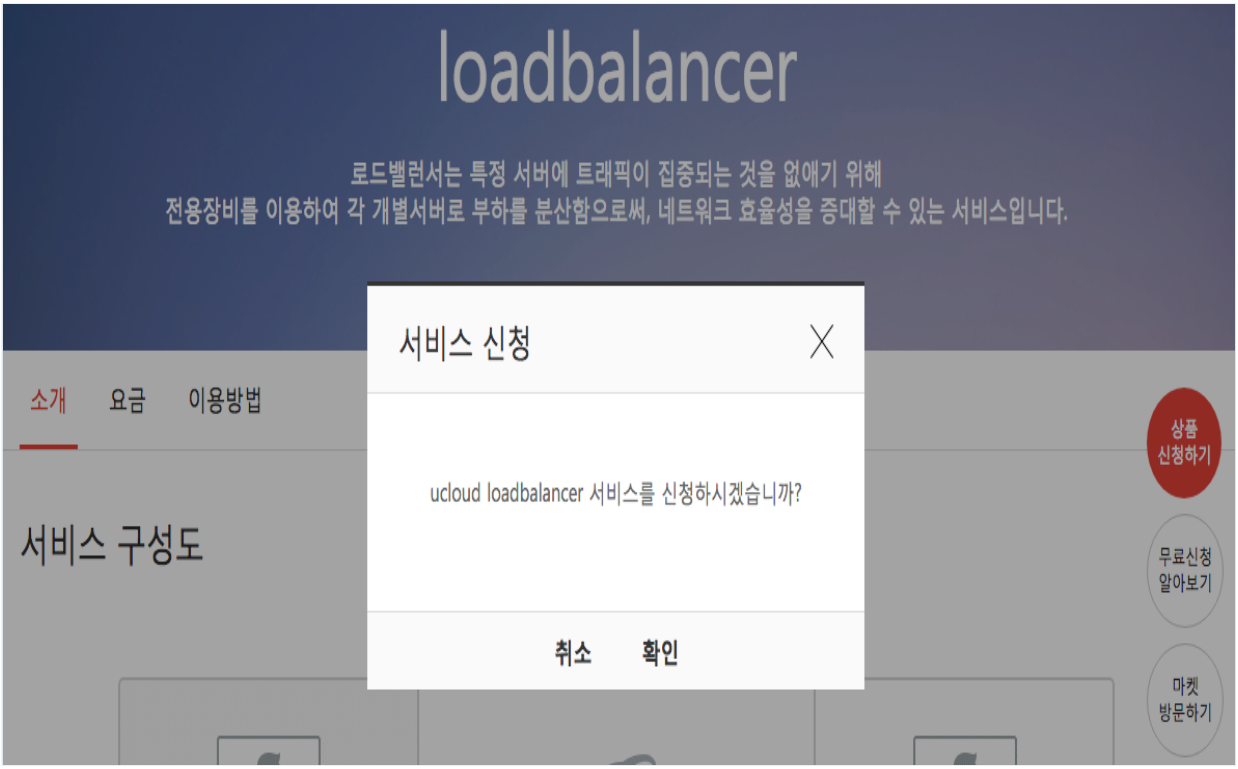


- 로드밸런서 신청: 새로운 로드밸런서를 생성하는 메뉴 입니다.
- 정액제 신청: 종량제(기본) 로드밸런서가 아닌 정액제 로드밸런서를 신청하는 메뉴로, 상담 정보를 입력하는 창으로 연결 됩니다.
- 로드밸런서 리스트: 사용중인 로드밸런서의 리스트를 보여줍니다. 로드밸런서를 사용중인 옵션과 타입, VIP 정보를 확인할 수 있습니다.
- Action(우측 상단): 로드밸런서 리스트 중 편집하고자 하는 로드밸런서의 체크박스를 선택한 뒤, 설정을 변경하거나 이용중인 로드밸런서를 삭제할 수 있습니다.
- 엑셀저장(우측 상단): 현재 사용중인 로드밸런서 리스트를 엑셀 정보로 저장하는 메뉴 입니다.
- 적용서버: 로드밸런서 리스트에서 로드밸런서를 선택하면 나타나는 화면입니다. 선택 한 로드밸런서에 등록된 back-end 서버의 목록과 서버의 모니터링 로드밸런싱 모니터링 정보를 보여줍니다.

3.3.1 Load Balancer 상품신청

☐ 상품 신청 (최초 이용 시)

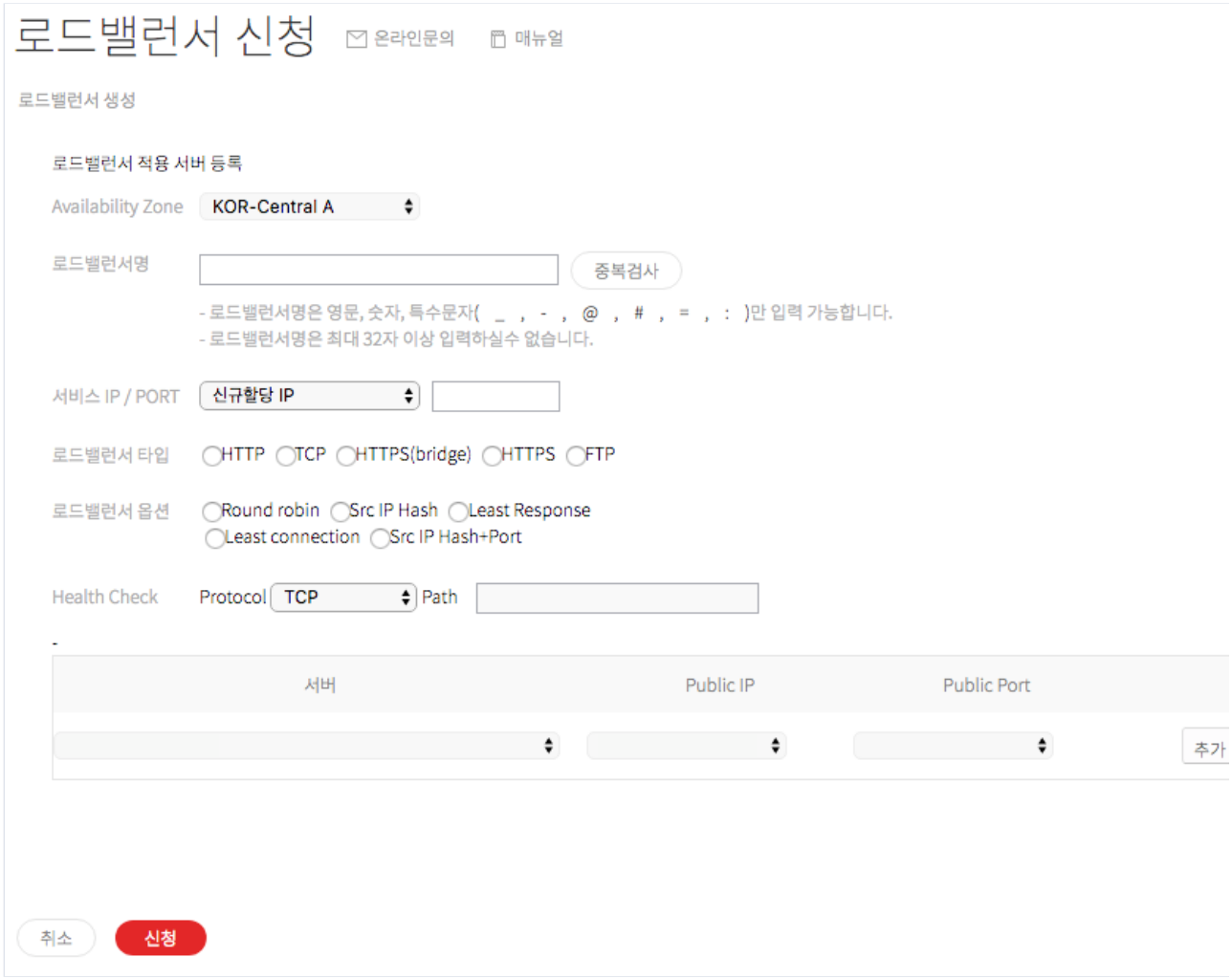
http://ucloudbiz.olleh.com 접속 후 상품 → 네트워크 → loadbalancer 선택 → 화면 우측 '상품 신청하기' 클릭 → 서비스 신청 확인 여부 팝업 창 생성 → '확인' 클릭



※ kt ucloud biz 사이트 내 최초로 상품 신청하는 경우, 1회에 한하여 결제 정보 입력창이 나타나게 됩니다. 약관 동의 및 결제 정보 입력 후 다음 단계를 진행 합니다.
※ 상품 신청 이후에는 화면 우측 상단의 '클라우드 콘솔' 메뉴를 통해 바로 접속하여 사용할 수 있습니다.

3.3.2 Load Balancer 생성 신청

☐ 로드밸런서 생성을 위한 입력 정보



○ Availability Zone: 로드밸런서를 사용할 클라우드 가용성 존을 선택 합니다.

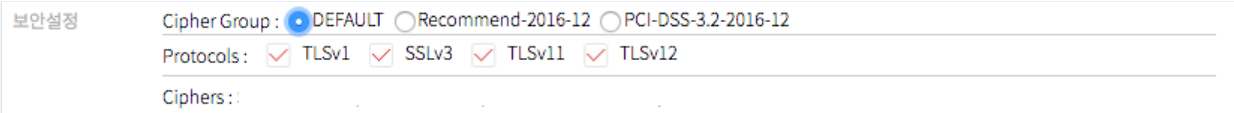
○ 로드밸런서명: 로드밸런서의 이름을 지정합니다. 로드밸런서 이름은 영문, 숫자, 지정된 특수문자만 사용 가능하며 32자 이내로 작성해야 합니다.

○ 서비스 IP/PORT: 로드밸런서에 할당 할 가상 IP(VIP)를 할당합니다. 이 때 공인 IP(Public IP)를 신규로 할당 받거나, 기존에 할당 된 IP를 지정할 수 있습니다. PORT는 외부 클라이언트가 back-end 서버에 접근할 때 사용할 PORT를 결정합니다. 예를 들면 1.1.1.1이라는 VIP를 할당 받는 로드밸런서의 지정 PORT가 8080번 이라면, 외부 클라이언트는 http://1.1.1.1:8080 이라는 주소로 웹 서버에 접근해야 합니다.

○ 로드밸런서 타입: 로드밸런서 back-end에 구동되는 서비스의 특징에 따라 로드밸런서 타입을 지정합니다.

- HTTP: SSL인증서를 사용하지 않는 일반 웹 서버와의 통신을 수행하며, 로드밸런서에서 HTTP 최적화 및 TCP Offload를 수행합니다. back-end 서버는 LB의 VIP를 클라이언트 IP(CIP)로 인식하기 때문에, CIP를 명확히 해야 하는 경우 X-forwarded-for 헤더를 적용하여 CIP를 확인할 수있습니다.
- HTTPS(bridge): 고객의 SSL 인증서는 back-end 서버에 직접 설치하여 사용하며, 클라이언트와 웹 서버가 암호화 통신을 end-to-end로 사용ㅇ합니다. 로드밸런서는 해당 패킷을 바이패스로 전송하며, 웹서버는 CIP를 구분할 수 없습니다.
- HTTPS: 고객의 SSL인증서를 로드밸런서에 배치하여 클라이언트와 로드밸런서 구간에서 암호화 통신을 수행합니다. 로드밸런서는 배치된 인증서를 통해 복호화를 진행한 후에 back-end 서버로 클라이언트 요청을 포워딩합니다. HTTP 방식과 마찬가지로 X-forwarded-for 헤더를 통해 CIP 정보를 확인할 수 있습니다. HTTPS 방식을 선택하는 경우 다음의 추가 정보 입력창이 나타나게 됩니다.

○ Cipher Group



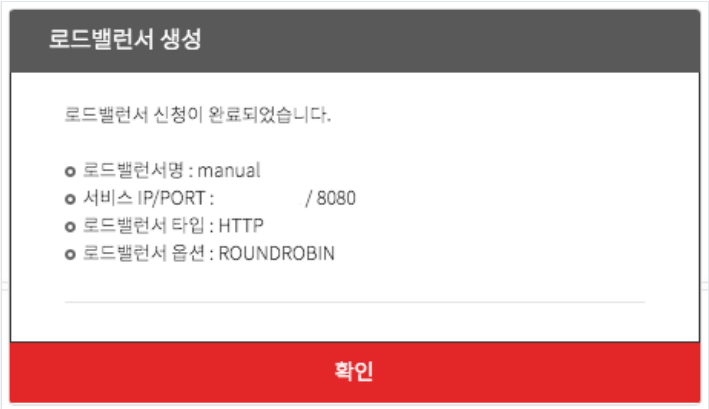
KT ucloud biz의 로드밸런서가 제공하는 암호화 알고리즘의 묶음 입니다. 암호화 알고리즘은 생성되는 각각의 로드밸런서에 바인딩 되어 동작합니다. 이 알고리즘의 그룹 안에는 키 교환, 인증, 암호화, 메시지 인증 코드 등이 복합적으로 구성됩니다. 또한 HTTPS 방식의 로드밸런서를 생성할 경우, 직접 로드밸런서에 SSL 인증서를 업로드 해야하며 이에 대한 내용은 3.3.6 Load Balancer 리스트 가이드 장에서 확인하실 수 있습니다.

※ 암호화 그룹은 새로운 알고리즘의 등장, 보안 취약점(CVE) 권고 사항등에 따라 default group의 cipher 구성 정보가 비 정기적으로 변동 될 수 있습니다.
※ 위 변동 등의 사유로 때때로 Cipher group에 구성된 알고리즘의 종류 따라 TPS(TRANSACTION PER SECOND)는 1K 내외로 제한될 수 있음을 유의하시기 바랍니다. (사유: 로드밸런서의 운영 안정)

○ 로드밸런서 옵션: 적용하고자 하는 로드밸런싱 메소드(알고리즘을) 선택합니다. 로드밸런싱 메소드에 관하여서는 3.1.2 항목의 로드밸런싱 메소드를 참고 하시기 바랍니다.
○ Health Check: back-end 서버의 정상 동작 여부를 확인합니다. back-end 서버와의 네트워크 정상 통신 여부를 확인합니다. HTTP 또는 HTTPS 방식을 적용하는 경우, 유효한 웹 페이지 주소를 지정해야 함을 참고 하시기 바랍니다.
○ 서버 리스트: 로드밸런서의 back-end 서버 리스트가 될 실제 가상 서버(VM)을 지정합니다. 최소 1개 이상의 ucloud server를 지정해야 합니다. IP/Port의 개방 범위 및 네트워크 보안에 관하여서는 3.1.3 유의사항/제약사항을 참고 하시기 바랍니다.

☐ 로드밸런서 생성 결과 확인

로드밸런서 생성 정보에 모든 정보를 입력한 뒤, [신청] 버튼을 누르고 [예]를 선택하면 로드밸런서 생성 프로세스가 진행됩니다. 로드밸런서가 정상적으로 생성 되었다면 다음과 같은 팝업창이 생성되게 됩니다.



3.3.3 Load Balancer 정액제 신청

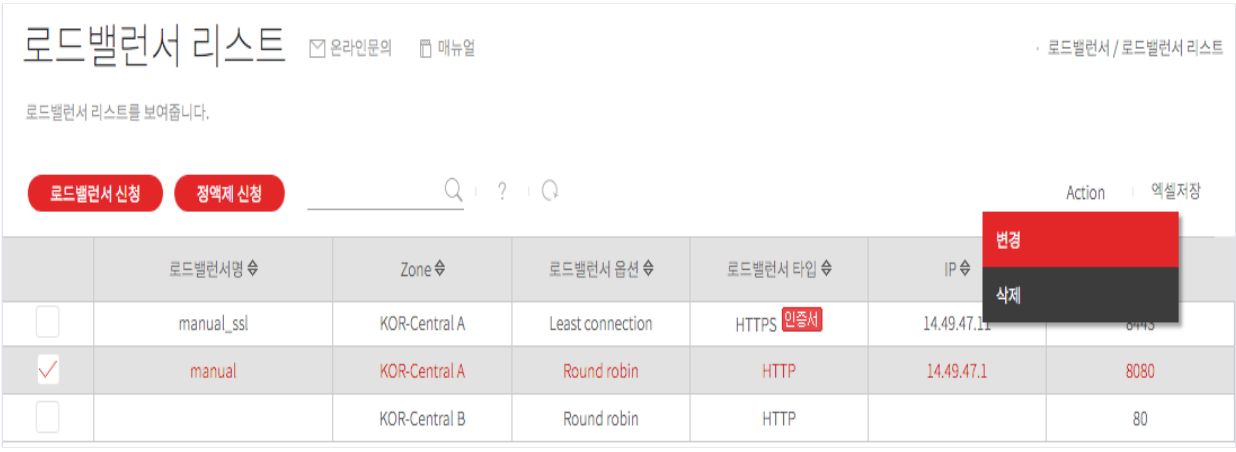
☐ 로드밸런서 정액제(전용 로드밸런서) 소개

KT ucloud biz의 로드밸런서는 종량제가 기본으로 적용됩니다. 정액제 서비스는 통상적으로 로드밸런싱 장비를 통해 접근하는 클라이언트 세션의 수가 100만 이상인 경우에, 전용으로 대역폭 보장을 원하시는 경우에 적합한 상품입니다. 정액제 상품 이용을 원하시는 경우 [정액제 상품 신청] 아이콘 클릭시 나타나는 양식에 맞추어 작성해주시면 상품 신청 처리 담당자가 확인한 후, 클라우드 기술 담당자가 고객에게 연락을 드리는 방법으로 상담 및 지원을 제공하고 있습니다.

3.3.4 Load Balancer 변경

☐ 로드밸런서 구성 설정 변경

아래 그림과 같이 로드밸런서 리스트에서 변경하고자 하는 로드밸런서를 선택한 뒤, 우측 상단의 [Action] 메뉴에서 [변경]을 선택합니다.



☐ 로드밸런서 구성 설정 변경 정보 입력

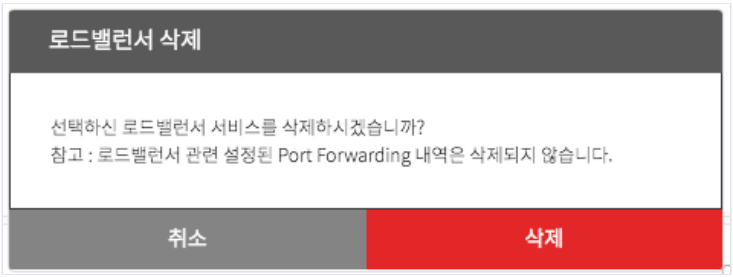
아래 그림과 같은 팝업창이 생성되면 변경하고자 하는 정보를 입력한 뒤 [신청] 버튼을 클릭 합니다.

정상적으로 처리 되었다면, 변경 된 로드밸런서 설정 정보를 로드밸런서 리스트에서 확인할 수 있습니다.

3.3.5 Load Balancer 삭제

아래 그림과 같이 로드밸런서 리스트에서 변경하고자 하는 로드밸런서를 선택한 뒤, 우측 상단의 [Action] 메뉴에서 [삭제]을 선택합니다.

다음 그림과 같은 팝업창을 확인한 뒤, [확인] 버튼을 클릭하면 일정 시간 뒤 삭제 완료 알림 팝업이 생성 됩니다. 정상적으로 처리 되었다면, 로드밸런서 리스트에서 삭제된 로드밸런서는 더 이상 표출되지 않습니다.



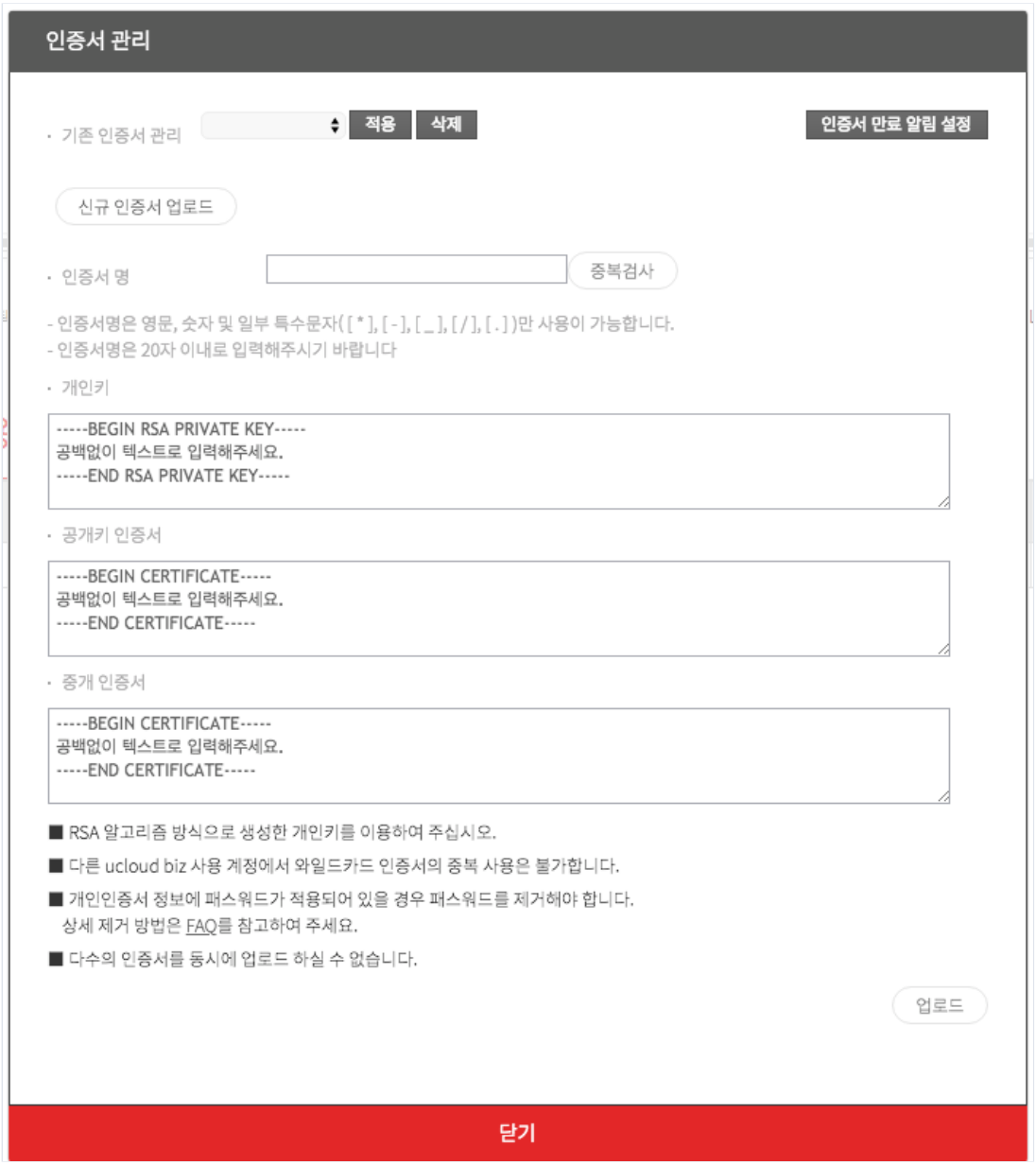
3.3.6 Load Balancer 리스트 가이드

☐ 로드밸런서 리스트를 통한 신청 내역 확인

로드밸런서가 생성된 뒤, 로드밸런서 리스트를 통해 사용중인 로드밸런서의 정보를 확인할 수 있습니다. 로드밸런서 리스트에서 체크박스를 선택 할 경우 콘솔 페이지의 하단 영역에 적용된 서버 리스트들이 조회 됩니다.

☐ HTTPS 타입의 로드밸런서에 SSL 인증서 배치하기

로드밸런서 리스트에서 HTTPS 타입을 이용중인 로드밸런서는 [인증서]라는 아이콘을 확인할 수 있습니다. 사용자는 이 [인증서]아이콘을 클릭하여 SSL 인증서를 직접 등록할 수 있습니다.



○ SSL 인증서 관리 페이지 상세 설명

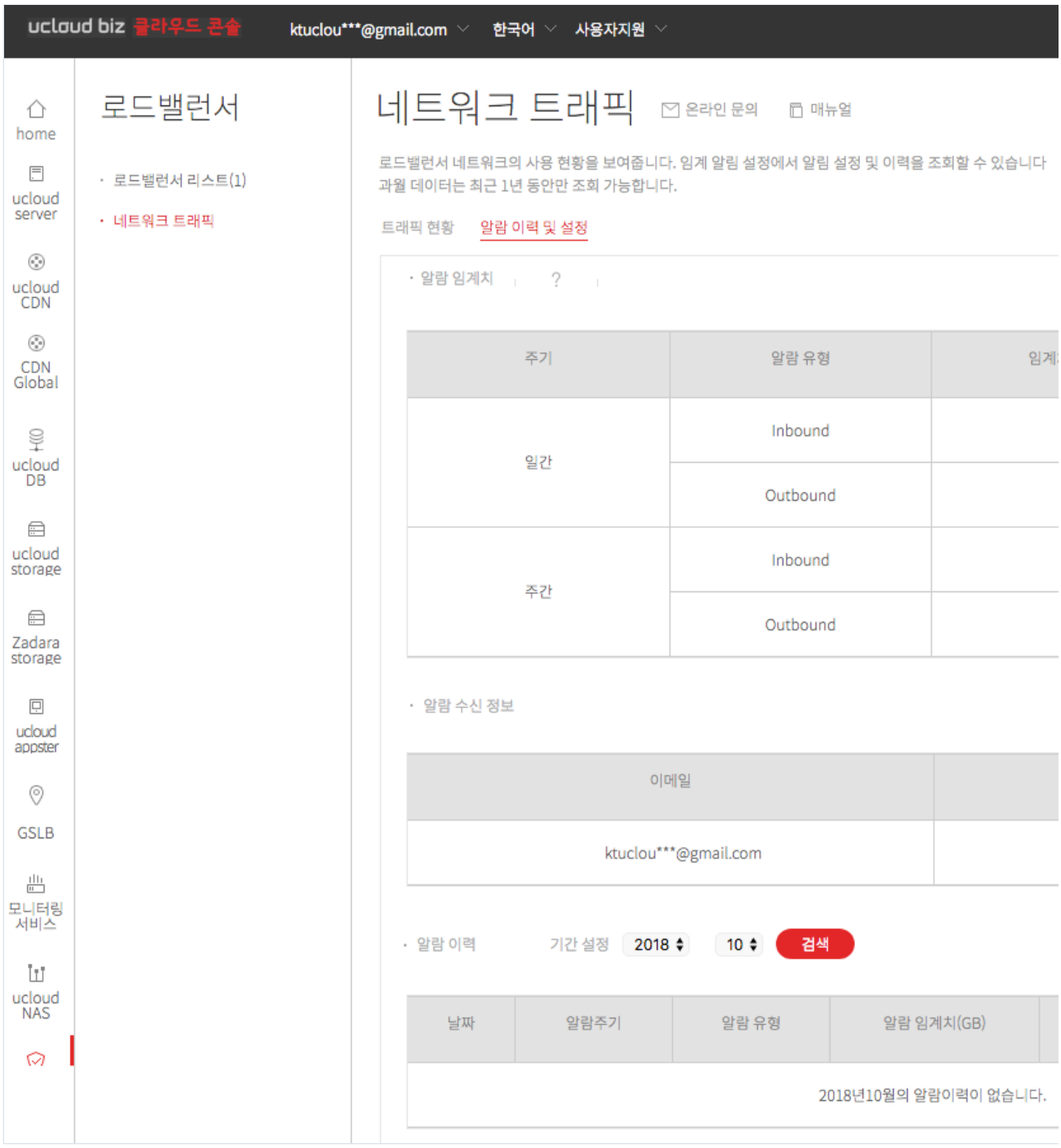
- 인증서 명: 원하는 인증서 명을 입력합니다. 인증서명은 영문, 숫자, 지정된 특수문자로만 사용 가능하며 20자 이내로 작성해야 합니다.
- 개인키: 도메인의 개인 키를 텍스트로 공백 없이 입력합니다.
- 공개키 인증서: 도메인의 인증서를 텍스트로 공백 없이 입력합니다.
- 중개 인증서(선택): 도메인 인증서에 중개키가 있는 경우, 텍스트로 공백 없이 입력합니다.

※ 보유하신 SSL 인증서에 암호(pass phrase)를 지정하신 경우 암호를 반드시 삭제해야 합니다. 아래 SSL 인증서의 암호를 제거 하는 방법에 대한 예시를 참고하시기 바랍니다.

```
#cp **********.key **********.key.old // 기존 key 백업
#openssl rsq -in **********.key -out new_**********.key
> 기존 암호(pass pharse) 입력
> 신규 암호 입력 요구 시 공백인 상태로 엔터 키 입력 // 암호가 제거 된 신규 키 생성 완료
※ 포탈을 통해 SSL인증서를 배치하시는 경우 텍스트에 어떠한 서식도 존재하지 않아야 합니다. 만일, 인증서의 텍스트 파일을 서식이 적용 가능한(rtf 등) 에디터로 편집하신 경우 메모장 등 텍스트 서식을 포함하지 않는 에디터로 복사/붙여넣기 하는 과정을 거쳐 입력창에 옮기셔야 합니다.
```

3.4 Load Balancer 네트워크 트래픽

3.4.1 Load Balancer 트래픽 현황

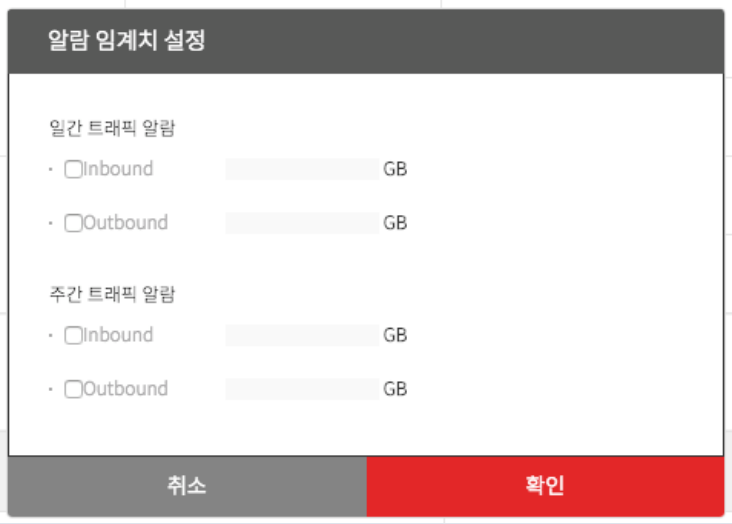


☐ Load Balancer 트래픽 통계

KT ucloud biz 로드밸런서는 일 단위로 트래픽 통계를 수집합니다. 사용하시고 계시는 로드밸런서들에 대하여 가용 존을 구분하여 모니터링 할 수 있습니다. 기간은 최대 1년 이전의 기록까지 월 단위로 조회가 가능합니다. 사용하시는 양에 따라서 트래픽 그래프는 MB / GB / TB 단위로 요약 정보를 선택하여 조회하실 수 있습니다.

3.4.2 Load Balancer 알람 설정 및 이력 조회

☐ 알람 임계치



KT ucloud biz 로드밸런서는 고객이 직접 설정 가능한 알람 기능을 제공하여, 고객에게 과다한 요금이 발생하지 않도록 하는 알람 정보 제공하고 있습니다. 알람 이력 및 설정에 대한 화면 구성은 다음과 같습니다.

먼저, 알람 임계치 항목에서 알람 주기는 일간과 주간으로 구분됩니다. 알람 유형은 인바운드와 아웃바운드 트래픽을 구분하여 설정이 가능합니다. 임계치는 GB 단위로 지정할 수 있습니다.

알람 임계치를 설정하는 화면은 위와 같이 인바운드와 아웃바운드 모니터링 여부를 체크박스로 선택할 수 있습니다. 원하시는 트래픽에 체크박스를 선택하신 뒤, 알람 값을 GB 단위로 입력하신 뒤 [확인] 버튼을 눌러 저장하면 설정이 적용 됩니다.

☐ 알람 수신 정보

알람 수신 정보 항목에서는 이메일과 휴대전화 SMS를 통해 알림을 수신하신 주소를 설정하실 수 있습니다.

알람 수신에 대한 설정은 이메일과 SMS 중 선호하시는 한 쪽 방법이나, 양 쪽 모두 선택이 가능합니다. 체크박스를 통해 수신 여부를 결정하실 수 있습니다. 이메일은 기존 가입하신 계정 정보를 토대로 메일이 발송 됩니다. SMS 수신은 설정 창에서 입력한 연락처 정보를 토대로 발송합니다. 또한, 수신 희망 시간을 설정하시어 원하지 않는 시간엔 알림을 차단 할 수 있습니다.

☐ 알람 이력

화면 구성 중, 알람 이력에서 1년 내 발생한 알람 이력에 대하여 월 단위로 알람 이력 목록을 조회하고 대상 리스트를 엑셀 파일로 저장할 수 있습니다.

3.6 Load Balancer 관련 Tool

3.6.1 네트워크 문제해결 가이드

웹 서버를 로드밸런서/GSLB에 등록 한 뒤, 웹 서버가 정상적으로 동작하지 않는 것 처럼 보일 수 있습니다. 이 때, 빠르고 쉽게 문제를 찾아볼 수 있는 방법으로서 일반적인 네트워크 문제해결(Trouble-shotting) 기법을 사용해 볼 수 있습니다. 로드밸런서/GSLB에 등록 된 포트 또는 주소를 향해 Ping을 요청하거나 back-end 서버에 Ping을 요청하여 어느 부분에서 정상 동작 하는지, 동작 하지 않는지를 1차적으로 선별할 수 있습니다.

☐ nc 명령어 사용하기 (Linux)

리눅스 환경에서 명령어는 다음과 같이 사용합니다

```
#nc -z <target ip> <port num>
```

목적지 Port가 정상적으로 열려있는(Listening) 상태인 경우 다음과 같은 응답 화면을 확인할 수 있습니다.

```
#nc -z 1.1.1.1
Connection to 1.1.1.1 port 80 [tcp/http] succeeded!
```

목적지 Port가 닫혀있어 정상적으로 통신이 되지 않을 경우 다음과 같은 응답이나, 아무 응답이 없을 수 있습니다.

```
#nc -z 1.1.1.1
<일정 시간 후(약 10초)>
14.63.212.122 port 8080 cloded.
```

☐ tcping 명령어 사용하기 (MS Windows)

Windows 환경에서 ping이 아닌 특정 포트와의 통신을 위해서는 tcping이라는 프로그램을 이용할 수 있습니다. 오픈소스 프로그램으로 링크에서 다운받으실 수 있습니다. tcping 명령어는 다음과 같이 사용합니다

```
c:₩> tcping <target ip> <port num>
Probing 1.1.1.1:80/tcp - Port is open - time=25.739ms
Probing 1.1.1.1:80/tcp - Port is open - time=21.842ms
Probing 1.1.1.1:80/tcp - Port is open - time=27.701ms
Probing 1.1.1.1:80/tcp - Port is open - time=27.489ms

Ping statistics for 1.1.1.1:80
4 probes sent.
4 successful, 0 failed.
Approximate trip times in milli-seconds:
Minimum = 21.842ms, Maximum = 27.701ms, Average = 25.693ms
```

3.6.2 로드밸런서/GSLB의 컨텐츠 정보 받아오기

로드밸런서/GSLB를 이용하여 웹 서비스를 제공하는 경우에 Port가 정상 동작 하더라도, 웹 페이지를 정상적으로 조회하기 어려운 경우가 발생할 수 있습니다. 이러한 경우 대부분 이용하시는 웹 서버(Apache, Nginx 등)의 환경 설정에 잘못 된 구성이 되어 있을 수 있습니다. 이 경우 'curl'이라는 명령어를 사용하여 간략하게 확인할 수 있습니다.

```
#curl -i 14.63.212.122
HTTP/1.1 403 Forbidden
Date: Sun, 14 Oct 2018 16:42:44 GMT
Server: Apache/2.2.15 (CentOS)
Accept-Ranges: bytes
Content-Length: 4961
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<후략>
```

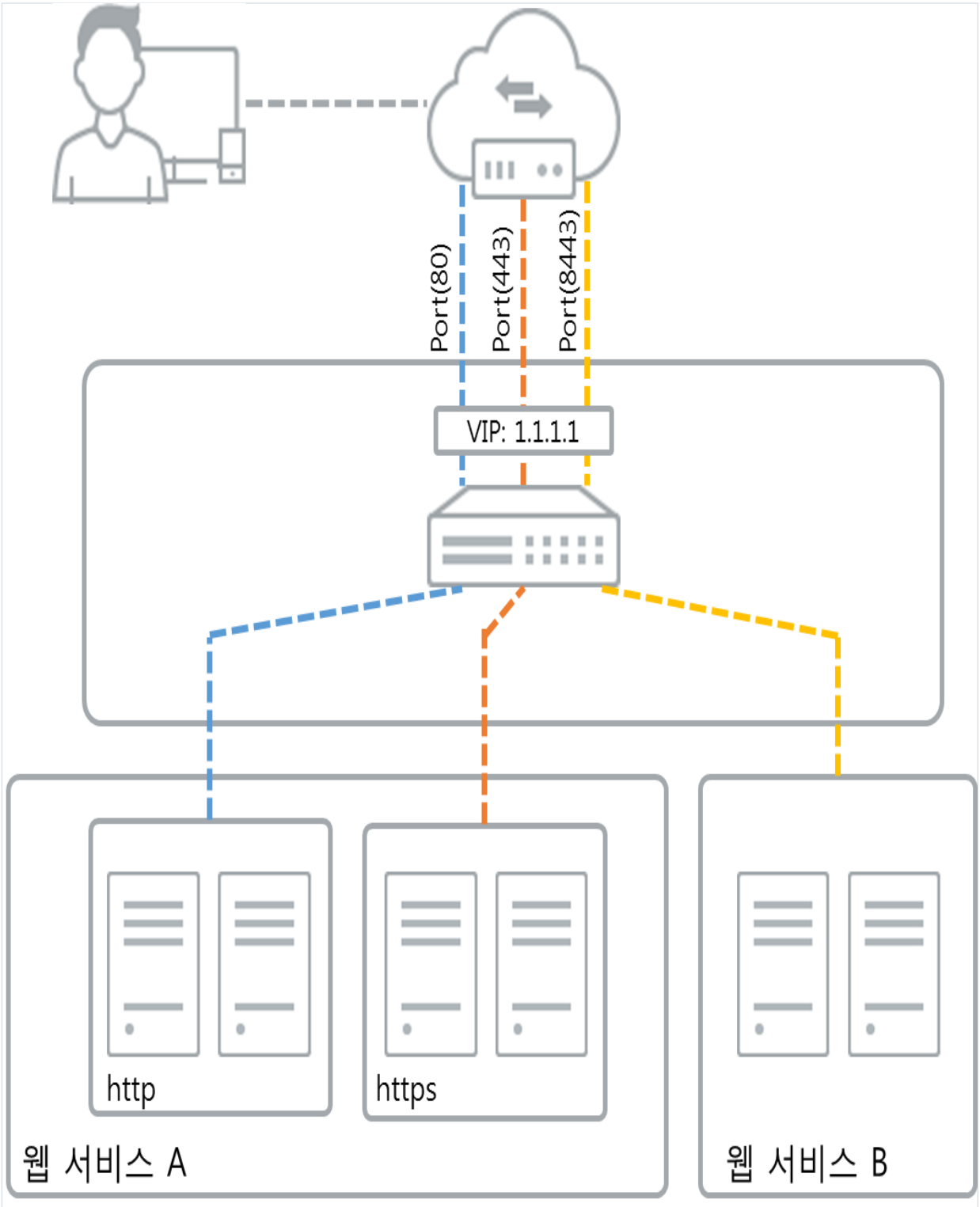
위 결과와 같이 curl 명령어에 -i 옵션을 주는 경우, 웹 서버가 보내는 HTTP 리턴에 대한 헤더 정보와 본문을 확인할 수 있습니다. 해당 결과를 통해 운영하시는 웹 서버에 어떤 부분이 잘못 설정 되었을 지 유추 해볼 수 있습니다.

3.7 Load Balancer 기타가이드

3.7.1 Load Balancer IP(VIP)의 멀티포트 설정

☐ 멀티포트(1 개 VIP 에 대해 여러 개의 서비스 포트 설정) 지원

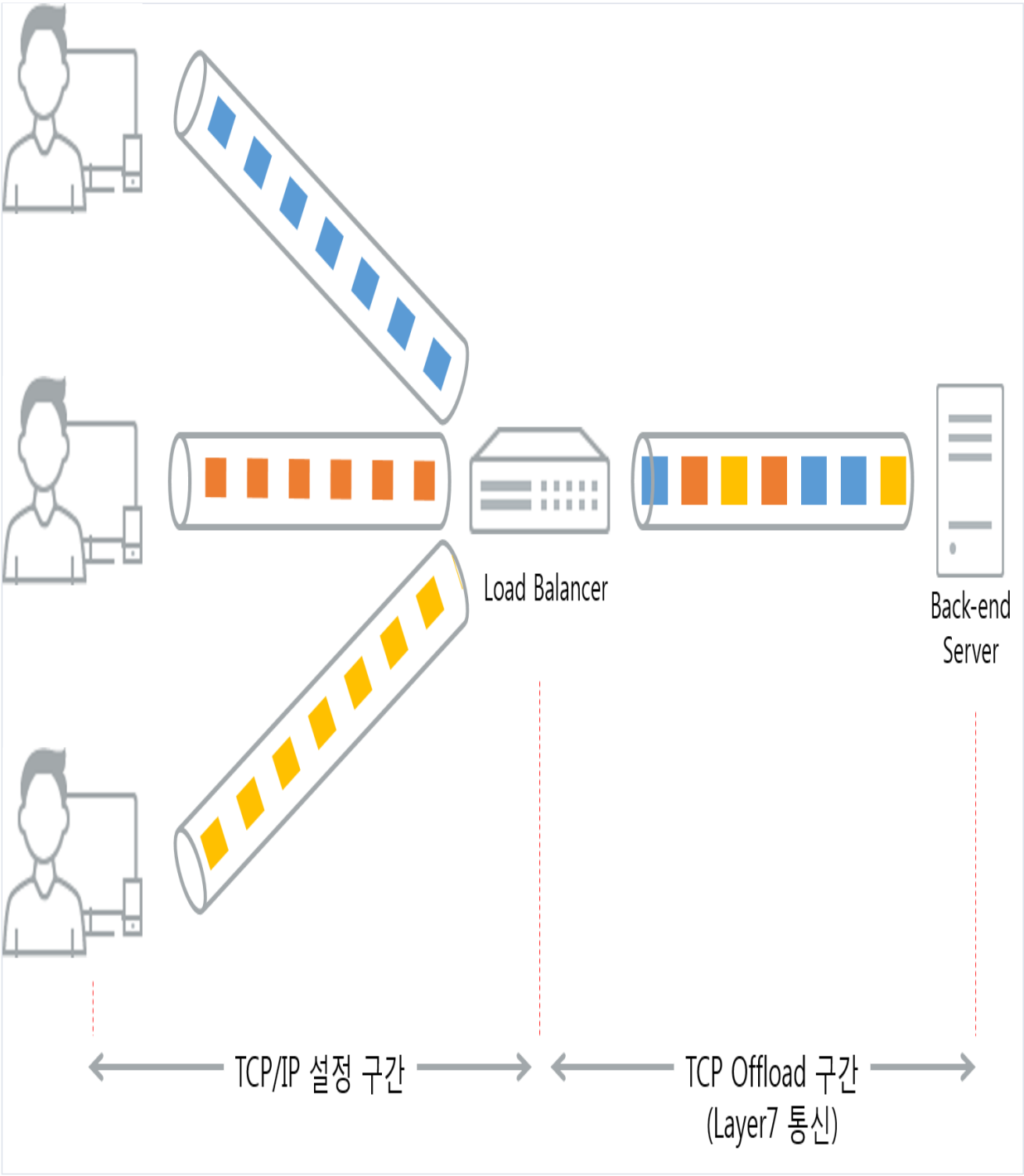
KT ucloud biz 로드밸런서는 로드밸런서가 사용하는 하나의 가상 IP(VIP)에 동시에 여러 개의 서비스 포트를 지정할 수 있습니다.



위 그림은 멀티포트를 사용하는 적절한 예 중 하나로 실제 사용하시는 방식에 따라 다양한 형태로 구성될 수 있습니다. 고객이 서비스 영역 내에서 웹 서비스를 http와 https를 동시에 운영 하고자 할 때, 로드밸런서에 동일한 VIP를 사용하고 PORT 숫자(e.g. 80/443)를 구분하여 back-end 서버와 매핑할 수 있습니다. 같은 방식으로 전혀 다른 웹 서비스를 운영하면서 동일한 VIP를 사용하게 하고자 할 때에도 PORT 번호를 달리하여 사용할 수 있습니다. 주의사항은 로드밸런서 신규 생성 시 같은 VIP에 같은 PORT가 중복이 되어서는 안됩니다. 즉, VIP상위의 네트워크인 인터넷-로드밸런서 구간 사이에서는 IP와 PORT를 동시에 중복시킬 수 없습니다.

3.7.2 TCP OFFLOAD

☐ TCP Multiplexing을 사용한 TCP Offload



KT ucloud biz 로드밸런서는 클라이언트의 전송 계층(TCP/IP)에 대한 요청을 back-end 서버를 대신하여 수행하며, 재사용 가능한 연결 유지 풀을 관리 합니다. 상세한 수행 과정은 다음과 같습니다.

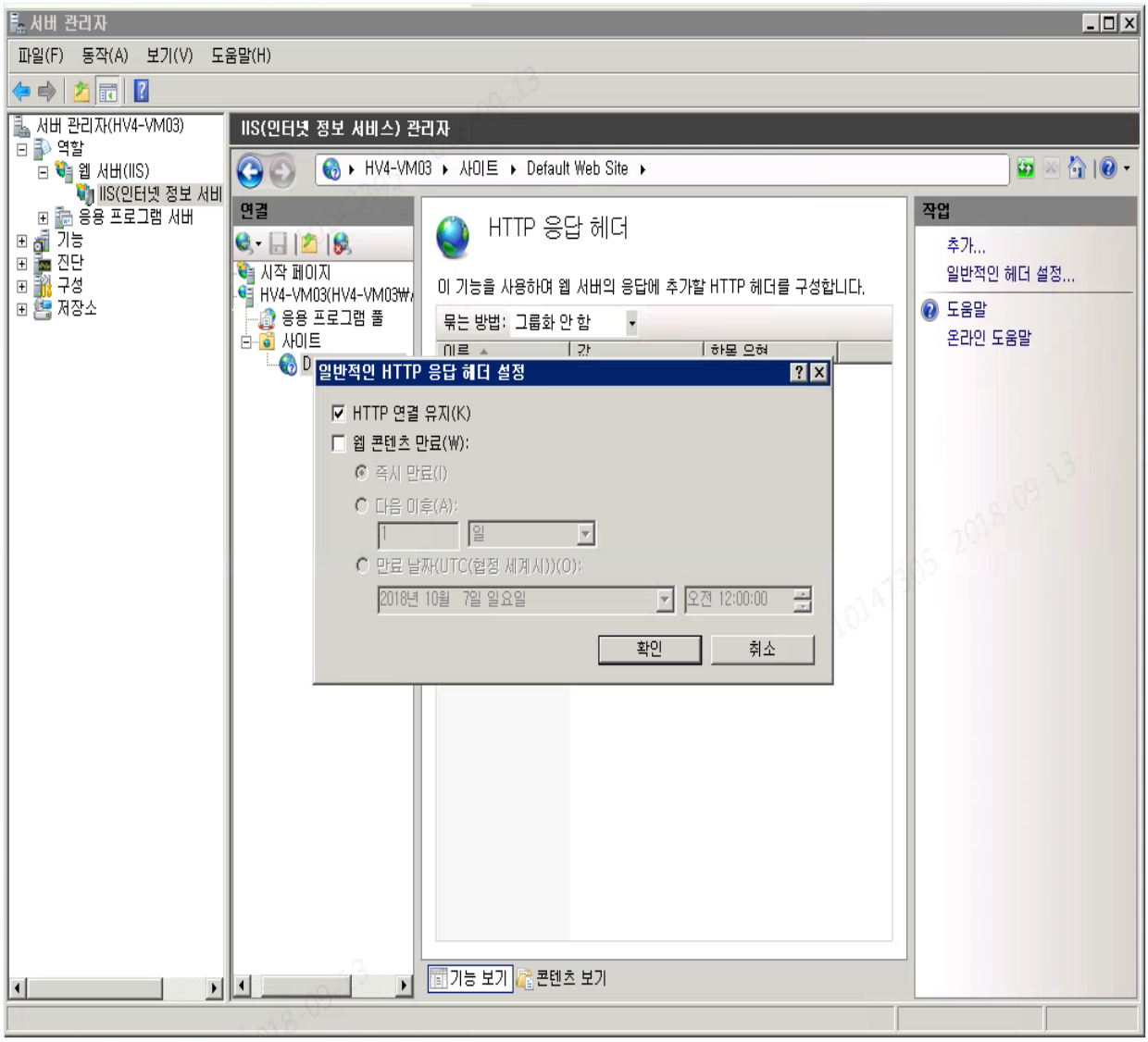
1. 새로운 클라이언트 요청이 들어오면 로드밸런서는 직접 클라이언트와 3-way handshake를 진행하고, 풀 안에서 사용 가능한 back-end 연결 정보가 있는지 확인합니다.
2. back-end에 대한 연결(Connection)이 풀 안에서 사용 가능한 경우, 해당 연결을 통해 고객의 요청 처리요청을 보내고 처리 받은 데이터를 서버에서 받아 와 클라이언트에 전달합니다.
3. 만약, 풀 안에 사용 가능한 연결이 존재하지 않는 경우, 로드밸런서가 back-end 서버와 새 연결을 생성합니다.
4. 기존 연결을 재사용하거나 새로운 연결을 생성하고 해당 연결에 대한 요청 처리가 종료 되면, 해당 연결은 연결 유지 풀안에 일정 시간 유지되며 새로운 요청이 들어왔을 때 지속적으로 재사용합니다.

이와 같은 TCP Multiplexing 기술을 사용한 TCP Offload 수행과정은 클라이언트의 요청을 최적화 할 수 있습니다. 이 최적화는 TCP 연결을 진행하는 전송계층(Transport Layer)과 데이터를 교환하는 응용계층(Application Layer) 데이터에 대한 간섭을 최소화 할 수 있습니다. 기존 웹 서버가 처리해야 했던 전송 계층(TCP/IP)의 프로세스를 로드밸런서에 넘기게 되어(Offload) back-end 서버의 CPU 사용률을 현저히 낮추는 효과를 기대할 수 있습니다. 이 기능은 HTTP 로드밸런서 사용 시 자동으로 적용 되며, back-end 서버에서 OS 종류에 따라 다음의 환경설정을 적용 하시기 바랍니다.

☐ 웹 서버에 TCP Offload 설정하기

○ MS Windows Server (IIS 7.0)

[서버 관리자] 실행 - [역할] 선택 - [IIS(인터넷 정보 서비스 관리자)] 선택 - 적용하고자하는 사이트 영역 선택 - [홈] 대쉬보드 에서 [HTTP 응답헤더] 선택 - [일반적인 헤더 설정] 선택 - 'HTTP 연결 유지' 선택 후 저장



○ Linux OS(Apache 2.0)

/etc/apache2/apache2.conf 에서 다음과 같이 설정합니다. (configuration 파일 경로는 설치 방법에 따라 다소 차이가 있을 수 있습니다.)

KeepAlive On

설정 파일 편집 후, 데몬을 재기동해야 변경 사항이 정상적으로 적용 됩니다.

아래 내용은 웹서버 성능 향상을 위한 설정값으로써 Apache에서 제공하는 권고하고 있는 사항입니다. 관련하여 더 자세한 사항은 링크(https://httpd.apache.org/docs/2.4/en/misc/perf-tuning.html)를 참고하시기 바랍니다.

- Apache 1.3 이전 버전의 경우

StartServers 256

MinSpareServers 50

MaxSpareServers 100

ServerLimit 8192

MaxClients 5000

MaxRequestsPerChild 4000

- Apache 2.x 이후 버전의 경우

MaxRequestsPerChild 30

KeepAliveTimeout 5

3.7.3 X-Forwarded Header

☐ 개요

HTTP 헤더는 클라이언트의 요청에 대한 메타 정보를 포함하고 있습니다. HTTP 헤더에 대한 필드(Field) 종류는 표준/비표준을 혼용하여 사용할 수 있습니다. 클라이언트의 요청은 로드밸런서와 같은 프록시(Proxy)환경에서 클라이언트 IP(CIP)를 구분해야 하는 경우가 존재할 수 있습니다. 이에 대해 오랜 기간동안 클라이언트 IP정보를 담을 수 있는 Forwarded 헤더를 비표준으로 사용해 왔으며, 현재 사실상 표준(De Facto Standard)으로 인정 받고 있으며 RFC 7239(https://tools.ietf.org/html/rfc7239.html)로 정의 되어 있습니다. KT ucloud biz 로드밸런서는 back-end 서버에 클라이언트의 요청을 전달할 때, 클라이언트의 요청을 받아 출발지 IP나 프로토콜에 대한 내용을 X-Fowarded 헤더로 저장하여 전달합니다.

☐ X-Fowarded-For

X-Forwarded-For 헤더의 필드값 을 확인하여 클라이언트 IP를 확인할 수 있습니다. 로드밸런서는 클라우드 서버에서 최소의 세션으로 클라이언트의 요청에 응답할 수 있도록 세션을 새로 만들어 사용합니다. 서버에서 로드밸런서가 아닌 클라이언트의 IP를 확인할 수 있도록, 로드밸런서는 클라이언트 IP주소를 헤더에 저장하여 서버로 전달합니다. X-Forwarded-For 헤더의 형식은 다음과 같습니다.

X-Forwarded-For: <client ip address>

☐ X-Fowarded-Proto

X-Forwarded-Proto 헤더의 필드값 을 확인하여 클라이언트와 로드밸런서 간 사용된 프로토콜(HTTP 또는 HTTPS)를 확인할 수 있습니다. 이를 통해 최초 클라이언트가 요청한 프로토콜을 확인할 수 있습니다. 단, 로드밸런서의 타입을 SSL인증서를 로드밸런서에 직접 등록하는 HTTPS 방식으로 사용하시는 경우, back-end 서버에서는 X-Forwarded-Proto 헤더 안에 HTTP로 확인 됩니다. X-Forwarded-Proto 헤더 형식은 다음과 같습니다.

X-Forwarded-Proto: <client origin protocol>