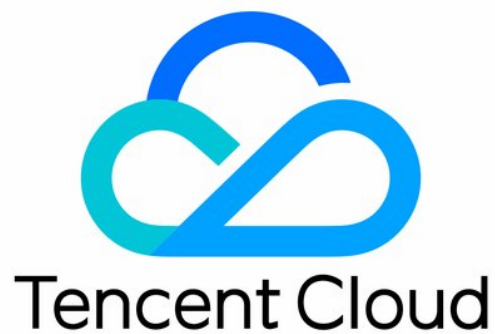


Cloud Load Balancer

운영 가이드

제품 문서



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

목록:

운영 가이드

CLB 인스턴스

도메인 이름 기반 CLB로 업그레이드

CLB 인스턴스 생성

IPv6 NAT64 CLB 인스턴스 생성

CLB 보안 그룹 구성

CLB 인스턴스 시작 및 중지

CLB 인스턴스 내보내기

CLB 인스턴스 업그레이드

CLB 인스턴스 삭제

인스턴스 공중망 구성 조정

CLB 리스너

CLB 리스너 개요

TCP 리스너 구성

UDP 리스너 구성

TCP SSL 리스너 구성

QUIC 리스너 구성

HTTP 리스너 구성

HTTPS 리스너 구성

로드 밸런싱 메소드

세션 지속성

레이어 7 리디렉션 구성

레이어 7 사용자 정의 구성

레이어 7 도메인 이름 포워딩 및 URL 규칙

CLB에서 QUIC 프로토콜 사용

CLB 인스턴스에 SNI 다중 인증서 바인딩 지원

리얼 서버

리얼 서버 개요

리얼 서버 관리

SCF 바인딩하기

리전 간 바인딩 2.0(New)

하이브리드 클라우드 배포

CVM 보안 그룹 구성

상태 확인

상태 확인 개요

상태 확인 구성

인증서 관리

인증서 관리

인증서 요구 사항 및 인증서 형식 변환

SSL 단방향 인증 및 양방향 인증

로그 관리

액세스 로그 개요

작업 로그 보기

액세스 로그 구성

로그 샘플링 및 수집

상태 확인 로그 구성

모니터링 및 알람

모니터링 데이터 가져오기

모니터링 지표

알람 정책 구성

알람 지표 설명

액세스 관리

개요

권한 정의

정책 예시

운영 가이드

CLB 인스턴스

도메인 이름 기반 CLB로 업그레이드

최종 업데이트 날짜: : 2023-05-06 11:28:22

기존 공중망 CLB 인스턴스를 도메인 이름 기반 CLB 인스턴스로 업그레이드할 수 있습니다. 업그레이드하면 CLB 서비스는 도메인 이름을 통해 제공되며, VIP는 더 이상 콘솔에 표시되지 않고, 비즈니스 요청에 따라 동적으로 변경됩니다.

업그레이드 전후 비교

항목	업그레이드 후	업그레이드 전
SLA	99.99%	99.95%
도메인 이름 지원 여부	Yes	No
자동 VIP 확장 지원 여부	Yes	No
VIP 변경 여부	VIP는 비즈니스 요청에 따라 동적으로 변경될 수 있으며 더 이상 콘솔에 표시되지 않습니다.	VIP 고정
상태 확인 소스 IP	기본적으로 100.64.0.0/10 IP 범위로 효과적으로 IP 충돌 방지	기본적으로 CLB 인스턴스 VIP, 100.64.0.0/10 IP 범위로 전환 가능

제한 설명

클래식 네트워크 기반 CLB 인스턴스는 업그레이드가 지원되지 않습니다. CLB 인스턴스가 클래식 네트워크에 있는 경우 먼저 인스턴스를 마이그레이션하시기 바랍니다. 자세한 내용은 [마이그레이션 가이드](#)를 참고하십시오.

클래식 CLB는 업그레이드가 지원되지 않습니다. 먼저 인스턴스를 CLB 인스턴스로 업그레이드하시기 바랍니다. 자세한 내용은 [클래식 CLB 업그레이드](#)를 참고하십시오.

컨테이너에서 생성한 CLB 인스턴스는 현재 콘솔에서 직접 업그레이드할 수 없습니다. 업그레이드하려면 [티켓 제출](#)을 통해 도움을 받으십시오.

Ant를-DDoS Pro는 현재 도메인화된 CLB 보호를 지원하지 않으며 도메인화된 CLB로 업그레이드하면 Anti-DDoS Pro가 작동하지 않아 비즈니스 보안에 심각한 영향을 미칠 수 있습니다. Anti-DDoS Pro가 이미 바인딩된 공중망 CLB 인스턴스 사용자 또는 DDoS 보호 요구 사항이 있는 공중망 CLB 인스턴스 사용자는 도메인화된 CLB 인스턴스로 업그레이드하지 않는 것이 좋습니다. 다른 질문이 있으면 [티켓 제출](#)하여 도움을 받으십시오.

전제 조건

1. CNAME 확인을 통해 비즈니스 서비스에 액세스할 수 있습니다.
2. 상태 확인 소스 IP를 100.64.0.0/10 IP 범위로 변경합니다. 자세한 내용은 [Changing Health Check Source IP](#)를 참고하십시오.

작업 단계

방법 1: 특정 인스턴스 업그레이드

1. [CLB 콘솔](#)에 로그인합니다.
2. 2. 인스턴스 관리 페이지의 왼쪽 상단에서 리전을 선택하고, 인스턴스 리스트에서 대상 인스턴스를 찾은 후, **자세히 > 도메인 이름 기반 인스턴스로 업그레이드**를 선택합니다.
3. 도메인 이름 기반 인스턴스로 업그레이드 팝업 창에서 **확인**을 클릭합니다.

Upgrade to domain name-based instance

Instances to upgrade: 1

ID/Name	Network type	Assign domain name ⓘ	Current VIP	VIP
lb- 	Public Network	lb-1  tencentclb.com	11  47	Dynamic IP

Benefits

Domain name-based instances provides service via a domain name with dynamic VIPs. The SLA increases from 99.95% to 99.99%.

Preparation

The health check source IP is changed to 100.64 IP range. You need to allow this IP range in other security policies (such as iptables) of the backend server. For details, see [The health check source IP supports 100.64.0.0/10 IP range.](#)

How to upgrade

1. Use load balancing service via a CNAME. For details, see the [usage guide](#).
2. to upgrade.

Impact

- The upgrade **does not affect the CLB forwarding service and pricing.**
- After the upgrade, the **VIP information is not visible** in the console. They are **changed dynamically.**
- The upgrade **cannot be undone.**

For any other questions, please [submit a ticket](#).

OK

Cancel

방법 2: 인스턴스 일괄 업그레이드

1. [CLB 콘솔](#)에 로그인합니다.
2. **인스턴스 관리** 페이지의 왼쪽 상단에서 리전을 선택하고 인스턴스 목록에서 업그레이드할 인스턴스를 선택합니다.
3. 인스턴스 목록 위에서 **추가 작업 > 도메인화된 인스턴스로 업그레이드**를 선택합니다.

Create
Delete
Assign to project
Edit tags
More ▼

ID/Name	Mon...	Status	Domain n...	VIP
lb-...				

Upgrade to LCU-supported
Upgrade to domain name-based instance

4. 도메인 이름 기반 인스턴스로 업그레이드 팝업 창에서 **확인**을 클릭합니다.

Upgrade to domain name-based instance

Instances to upgrade: 2

ID/Name	Network type	Assign domain name ⓘ	Current VIP	VIP
lb-...	Public Network	lb-... ...tencentclb.com	10...5	Dynamic IP
lb-...	Public Network	lb-... ...tencentclb.com	8...	Dynamic IP

Benefits

Domain name-based instances provides service via a domain name with dynamic VIPs. The SLA increases from 99.95% to 99.99%.

Preparation

The health check source IP is changed to 100.64 IP range. You need to allow this IP range in other security policies (such as iptables) of the backend server. For details, see [The health check source IP supports 100.64.0.0/10 IP range.](#)

How to upgrade

1. Use load balancing service via a CNAME. For details, see the [usage guide](#).
2. to upgrade.

Impact

- The upgrade **does not affect the CLB forwarding service and pricing.**
- After the upgrade, the **VIP information is not visible** in the console. They are **changed dynamically.**
- The upgrade **cannot be undone.**

For any other questions, please [submit a ticket](#).

OK
Cancel

CLB 인스턴스 생성

최종 업데이트 날짜: : 2024-01-04 19:37:43

Tencent Cloud는 공식 웹 사이트 구매 및 API 구매의 두 가지 CLB(Cloud Load Balancer) 구매 방식을 제공합니다. 이 섹션에서는 두 가지 구매 방식에 대해 자세히 설명합니다.

공식 웹사이트에서 구매

Tencent Cloud 공식 웹사이트에서 CLB 인스턴스를 구매할 수 있습니다. Tencent Cloud 계정에는 IP별 청구 계정과 CVM별 청구 계정의 두 가지 유형이 있습니다. 2020년 6월 17일(베이징 시간) 00:00:00 이후에 생성된 계정은 IP별 청구 유형입니다. 그 이전에 계정을 생성했다면 [Checking Account Type](#)의 안내에 따라 콘솔에서 계정 유형을 확인할 수 있습니다.

1. [CLB 구매 페이지](#)에 로그인합니다.
2. 필요에 따라 다음 CLB 구성 항목을 선택합니다.

IP별 청구 계정

매개변수	설명
과금방식	종량제 과금 방식이 지원됩니다.
리전	리전을 선택하십시오. CLB에서 지원하는 리전에 대한 자세한 내용은 Region List 를 참고하십시오.
인스턴스 유형	CLB 인스턴스 유형만 지원됩니다.
네트워크 유형	네트워크 유형에는 공중망과 사설망의 두 가지가 있습니다. 자세한 내용은 Network Types 를 참고하십시오. 공중망: CLB는 공중망의 요청을 분산하는 데 사용됩니다.

	<p>사설망: CLB는 Tencent Cloud 사설망의 요청을 분산하는 데 사용됩니다. 사설망 인스턴스는 EIP, IP 버전, ISP 유형, 인스턴스 사양, 네트워크 과금 방식 및 대역폭 한도와 같은 구성 항목을 지원하지 않으며 기본적으로 표시하지 않습니다.</p> <p>지원되는 네트워크 유형은 과금 방식에 따라 다릅니다.</p> <p>종량제 과금 방식에서는 공중망 및 사설망 유형이 모두 지원됩니다.</p>
IP 버전	IPv4, IPv6 및 IPv6 NAT64와 같은 CLB IP 버전이 지원됩니다. 종량제 인스턴스만 IPv6 버전을 지원합니다. 기타 제한 사항에 대한 자세한 내용은 IP Versions 를 참고하십시오.
네트워크	<p>CLB는 기본 네트워크와 VPC를 지원합니다.</p> <p>기본 네트워크는 모든 Tencent Cloud 사용자를 위한 공중망 리소스 풀입니다. 모든 CVM의 사설망 IP는 Tencent Cloud에서 할당합니다. IP 범위 또는 IP 주소를 사용자 지정할 수 없습니다.</p> <p>VPC는 Tencent Cloud에서 논리적으로 격리된 네트워크 공간입니다. VPC에서 IP 범위, IP 주소 및 라우팅 정책을 사용자 지정할 수 있습니다.</p> <p>두 옵션 중에서 VPC는 사용자 지정 네트워크 구성이 필요한 시나리오에 더 적합하며 기본 네트워크 제품은 2022년 12월 31일에 공식적으로 중단됩니다. VPC를 선택하는 것이 좋습니다.</p>
ISP 유형	<p>BGP, China Mobile, China Telecom 및 China Unicom과 같은 ISP 유형이 지원됩니다.</p> <p>종량제 과금 방식에서는 상기 네 가지 옵션이 모두 지원됩니다. 현재 고정 단일 회선 IP는 광저우, 상하이, 난징, 지난, 항저우, 푸저우, 베이징, 스자좡, 우한, 창사, 청두, 충칭에서만 지원됩니다. 다른 리전은 콘솔을 참고하십시오. 사용을 원하시면 영업 담당자에게 문의하여 신청하십시오. 승인되면 구매 페이지에서 ISP(China Mobile, China Unicom 또는 China Telecom)를 선택할 수 있습니다.</p>
기본/보조 가용 존	기본 가용 존(AZ)은 현재 트래픽을 유지하는 AZ입니다. 보조 AZ는 기본적으로 트래픽을 유지하지 않으며 기본 AZ를 사용할 수 없는 경우에만 사용됩니다. 현재 광저우, 상하이, 난징, 베이징, 중국 홍콩 및 서울 지역의 IPv4 CLB 인스턴스만 기본/보조 AZ를 지원합니다.
인스턴스	<p>공유 인스턴스가 지원됩니다.</p> <p>여러 공유 인스턴스는 리소스를 공유하고 단일 인스턴스는 성능을 보장하지 않습니다. 기본적으로 모든 인스턴스는 공유 인스턴스입니다.</p>

사 양	
네 트 워 크 과 금 방 식	<p>다음 네트워크 과금 방식이 지원됩니다: 대역폭 과금(월간 대역폭), 대역폭 과금(시간당 대역폭), 트래픽 별 과금 및 대역폭 패키지.</p> <p>종량제 인스턴스는 대역폭(시간당 대역폭) 과금과 트래픽 과금의 두 가지 네트워크 과금 방식을 지원합니다.</p>
대 역 폭 최 대 값	1-1024Mbps.
프 로 젝 트	프로젝트를 선택합니다.
태 그	태그 키와 값을 선택합니다. Creating Tags and Binding Resources 의 지침에 따라 태그를 생성할 수도 있습니다.
인 스 턴 스 이 름	이름에는 최대 60자의 영어 알파벳, 숫자, 중국어, 하이픈 '-', 밑줄 '_' 및 마침표 '.'를 사용할 수 있습니다. 지정하지 않으면 기본적으로 이름이 자동으로 생성됩니다.

CVM별 청구 계정

매 개 변 수	설명
과 금 방 식	종량제 과금 방식만 지원됩니다.

리전	리전을 선택하십시오. CLB에서 지원하는 리전에 대한 자세한 내용은 Region List 를 참고하십시오.
인스턴스 유형	CLB 인스턴스 유형만 지원됩니다.
네트워크 유형	<p>네트워크 유형에는 공중망과 사설망의 두 가지가 있습니다. 자세한 내용은 Network Types를 참고하십시오.</p> <p>공중망: CLB는 공중망의 요청을 분산하는 데 사용됩니다.</p> <p>사설망: CLB는 Tencent Cloud 사설망의 요청을 분산하는 데 사용됩니다. 사설 네트워크 인스턴스는 IP 버전, ISP 유형, 인스턴스 사양과 같은 구성 항목을 지원하지 않으며 기본적으로 표시되지 않습니다.</p>
IP 버전	IPv4, IPv6 및 IPv6 NAT64와 같은 CLB IP 버전이 지원됩니다. 사용 제한에 대한 자세한 내용은 IP Versions 를 참고하십시오.
네트워크	<p>CLB는 기본 네트워크와 VPC를 지원합니다.</p> <p>기본 네트워크는 모든 Tencent Cloud 사용자를 위한 공중망 리소스 풀입니다. 모든 CVM의 사설망 IP는 Tencent Cloud에서 할당합니다. IP 범위 또는 IP 주소를 사용자 지정할 수 없습니다.</p> <p>VPC는 Tencent Cloud에서 논리적으로 격리된 네트워크 공간입니다. VPC에서 IP 범위, IP 주소 및 라우팅 정책을 사용자 지정할 수 있습니다.</p> <p>두 옵션 중에서 VPC는 사용자 지정 네트워크 구성이 필요한 시나리오에 더 적합하며 기본 네트워크 제품은 2022년 12월 31일에 공식적으로 중단됩니다. VPC를 선택하는 것이 좋습니다.</p>
ISP 유형	BGP, China Mobile, China Telecom 및 China Unicom과 같은 ISP 유형이 지원됩니다. 현재 고정 단일 회선 IP는 광저우, 상하이, 난징, 지난, 항저우, 푸저우, 베이징, 스자좡, 우한, 창사, 청두, 충칭에서만 지원됩니다. 다른 리전은 콘솔을 참고하십시오. 사용을 원하시면 영업 담당자에게 문의하여 신청하십시오. 승인되면 구매 페이지에서 ISP(China Mobile, China Unicom 또는 China Telecom)를 선택할 수 있습니다.
인스턴스	<p>공유 인스턴스가 지원됩니다.</p> <p>여러 공유 인스턴스는 리소스를 공유하고 단일 인스턴스는 성능을 보장하지 않습니다. 기본적으로 모든 인스턴스는 공유 인스턴스입니다.</p>

사 양	
프 로 젝 트	프로젝트를 선택합니다.
태 그	태그 키와 값을 선택합니다. Creating Tags and Binding Resources 의 지침에 따라 태그를 생성할 수도 있습니다.
인 스 턴 스 이 름	이름에는 최대 60자의 영어 알파벳, 숫자, 중국어, 하이픈 '-', 밑줄 '_' 및 마침표 '.'를 사용할 수 있습니다. 지정하지 않으면 기본적으로 이름이 자동으로 생성됩니다.

3. 상기 구성을 완료한 후 수량과 요금을 확인하고 **즉시 구매**를 클릭합니다.

종량제 과금 방식: '확인' 팝업 창에서 **확인**을 클릭합니다.

4. 구매에 성공하면 CLB가 활성화되고 CLB 인스턴스를 구성하여 사용할 수 있습니다.

공유 인스턴스 구매 방법

1. [CLB 구매 페이지](#)에 로그인합니다.

2. [공식 웹 사이트에서 구매](#) 항목을 참고하여 공유 인스턴스 구성 항목을 설정하고 '인스턴스 사양'으로 **공유**를 선택합니다.

3. [공식 웹 사이트에서 구매](#)의 단계를 참고하여 후속 작업을 완료합니다.

LCU 인스턴스 구매 방법

1. [CLB 구매 페이지](#)에 로그인합니다.

2. [공식 웹사이트에서 구매](#)의 단계를 참고하여 LCU 지원 인스턴스 구성 항목을 설정하고 '인스턴스 사양'으로 **LCU**를 선택합니다.

3. [공식 웹 사이트에서 구매](#)의 단계를 참고하여 후속 작업을 완료합니다.

API를 통한 구매

API를 통해 CLB 인스턴스를 구매하려면 [CreateLoadBalancer](#)를 참고하십시오.

후속 작업

CLB 인스턴스에 대한 리스너를 생성하려면 [CLB Listener Overview](#)를 참고하시기 바랍니다.
[Real Server Overview](#)에 설명된 대로 CLB 리스너를 리얼 서버에 바인딩할 수 있습니다.

관련 문서

[Product Attribute Selection](#)

IPv6 NAT64 CLB 인스턴스 생성

최종 업데이트 날짜: : 2022-10-17 18:01:50

설명 :

IPv6 NAT64 CLB는 베이징, 상하이, 광저우의 세 리전에서만 생성할 수 있습니다.

IPv6 구현은 인터넷 전반에 걸쳐 아직 예비 단계에 있습니다. 접속 실패 시 [티켓을 제출](#)하십시오. SLA는 베타 테스트 기간 동안 보장되지 않습니다.

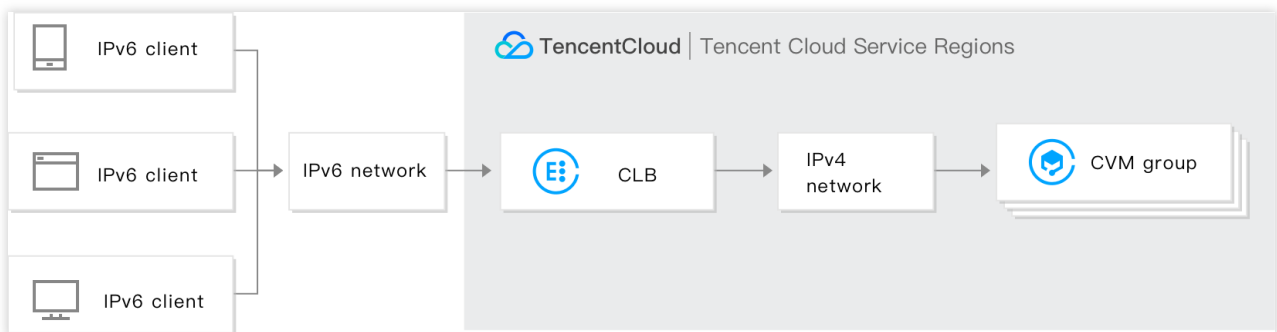
CLB는 IPv6 NAT64 CLB 인스턴스 생성을 지원합니다. Tencent Cloud는 IPv6 공개 IP 주소, 즉 IPv6 에디션의 VIP를 인스턴스에 할당하고 VIP는 IPv6 클라이언트의 요청을 실제 IPv4 CVM 인스턴스로 포워딩합니다.

IPv6 NAT64 CLB 인스턴스란 무엇입니까?

IPv6 NAT64 CLB 인스턴스는 IPv6 NAT64 전환 기술을 기반으로 구현된 로드 밸런서입니다. IPv6 NAT64 CLB 인스턴스를 통해 IPv6 사용자는 IPv6 수정 없이 리얼 서버에 빠르게 액세스할 수 있습니다.

IPv6 NAT64 CLB 아키텍처

IPv6 NAT64 CLB 아키텍처는 아래와 같습니다.



IPv6 NAT64 CLB가 IPv6 네트워크에서 액세스되면 CLB는 IPv6 주소를 IPv4 주소로 원활하게 변환하여 기존 서비스에 적용할 수 있습니다.

IPv6 NAT64 CLB 장점

Tencent Cloud IPv6 NAT64 CLB는 비즈니스가 IPv6에 빠르게 연결할 수 있도록 지원할 때 다음과 같은 이점이 있습니다.

빠른 액세스: CLB를 사용하면 몇 초 만에 IPv6에 연결할 수 있으며 구입 즉시 사용할 수 있습니다.

원활한 비즈니스 전환: 비즈니스를 IPv6으로 원활하게 전환하려면 리얼 서버에 필요한 수정 없이 클라이언트만 전환하면 됩니다. IPv6 NAT64 CLB는 IPv6 클라이언트의 액세스를 지원하고 IPv6 메시지를 IPv4 메시지로 변환합니다.

IPv6 전환은 여전히 원래 방식으로 작동하는 리얼 서버의 애플리케이션에서는 감지할 수 없습니다.

사용 용이성: IPv6 NAT64 CLB는 IPv4 CLB 순서도와 호환되며 추가 학습 비용이 발생하지 않고 사용하기 쉽습니다.

운영 가이드

IPv6 NAT64 CLB 인스턴스 생성

1. Tencent Cloud 콘솔에 로그인하여 [CLB 구매 페이지](#)로 이동합니다.

2. 다음 매개변수에 대한 옵션을 올바르게 선택하십시오.

과금 방식: 종량제를 지원합니다.

리전: 베이징, 상하이, 광저우만 지원됩니다.

인스턴스 유형: CLB.

네트워크 유형: 공중망.

IP 버전: IPv6 NAT64.

네트워크: VPC.

기타 구성은 일반 인스턴스 구성과 동일합니다.

3. 위의 항목을 구성한 후 **즉시 구매**를 클릭하고 방금 구매한 IPv6 CLB 인스턴스를 볼 수 있는 [인스턴스 관리 페이지](#)로 돌아갑니다.

IPv6 NAT64 CLB 사용

[CLB 콘솔](#)에 로그인하고 인스턴스 ID를 클릭하여 세부 정보 페이지로 이동합니다. 리스너 관리 탭에서 리스너 및 포워드 규칙을 구성하고 CVM 인스턴스를 바인딩할 수 있습니다. 자세한 내용은 [Getting Started with CLB](#)를 참고하십시오.

ID/Name	Monitor	Status	VIP	Network	Health Status	Project	Tag	Operation
[ID]	[Monitor]	Normal	72 (IPv6 NAT64)	Public Network	Health check not enabled (Configuration)	DEFAULT PROJECT	-	Configure listener More

관련 문서

Obtaining Real Client IPs via TOA in Hybrid Cloud Deployment

CLB 보안 그룹 구성

최종 업데이트 날짜: : 2024-01-04 19:32:11

CLB 인스턴스가 생성된 후 공중망 트래픽을 격리하도록 CLB 보안 그룹을 구성할 수 있습니다. 본문은 다양한 모드에서 CLB 보안 그룹을 구성하는 방법을 설명합니다.

사용 제한

하나의 CLB 인스턴스는 최대 5개의 보안 그룹에 바인딩될 수 있습니다. 할당을 늘리려면 [할당량 관리](#)로 이동하여 신청서를 제출하십시오.

보안 그룹에는 최대 512개의 규칙이 허용됩니다.

기본 네트워크의 사설망 CLB 인스턴스는 보안 그룹을 바인딩할 수 없습니다. 사설망 CLB가 [Anycast EIP](#)에 바인딩되어 있는 경우 해당 인스턴스에 바인딩된 보안 그룹은 적용되지 않습니다.

보안 그룹 기본 허용 기능은 클래식 사설망 CLB 및 기본 네트워크 기반 CLB에서 사용할 수 없습니다. 클라우드 베어 메탈은 현재 보안 그룹 기본 허용 기능을 지원하지 않습니다.

배경 정보

보안 그룹은 스테이트풀 데이터 패킷을 필터링하고 인스턴스 레벨에서 아웃바운드/인바운드 트래픽을 제어할 수 있는 가상 방화벽입니다. 자세한 내용은 [보안 그룹 개요](#)를 참고하십시오.

CLB 보안 그룹은 CLB 인스턴스에 바인딩되고 CVM 보안 그룹은 CVM 인스턴스에 바인딩됩니다. 그들은 다른 객체를 대상으로 합니다. CLB 보안 그룹의 경우 다음을 선택할 수 있습니다.

[보안 그룹 기본 허용 활성화](#)

[보안 그룹 기본 허용 비활성화](#)

설명:

IPv4 CLB 보안 그룹의 경우 보안 그룹 기본 허용은 기본적으로 비활성화되어 있으며 콘솔에서 활성화할 수 있습니다.

IPv6 CLB 보안 그룹의 경우 보안 그룹 기본 허용이 기본적으로 활성화되어 있으며 비활성화할 수 없습니다.

보안 그룹 기본 허용 활성화



기본 허용이 활성화된 경우:

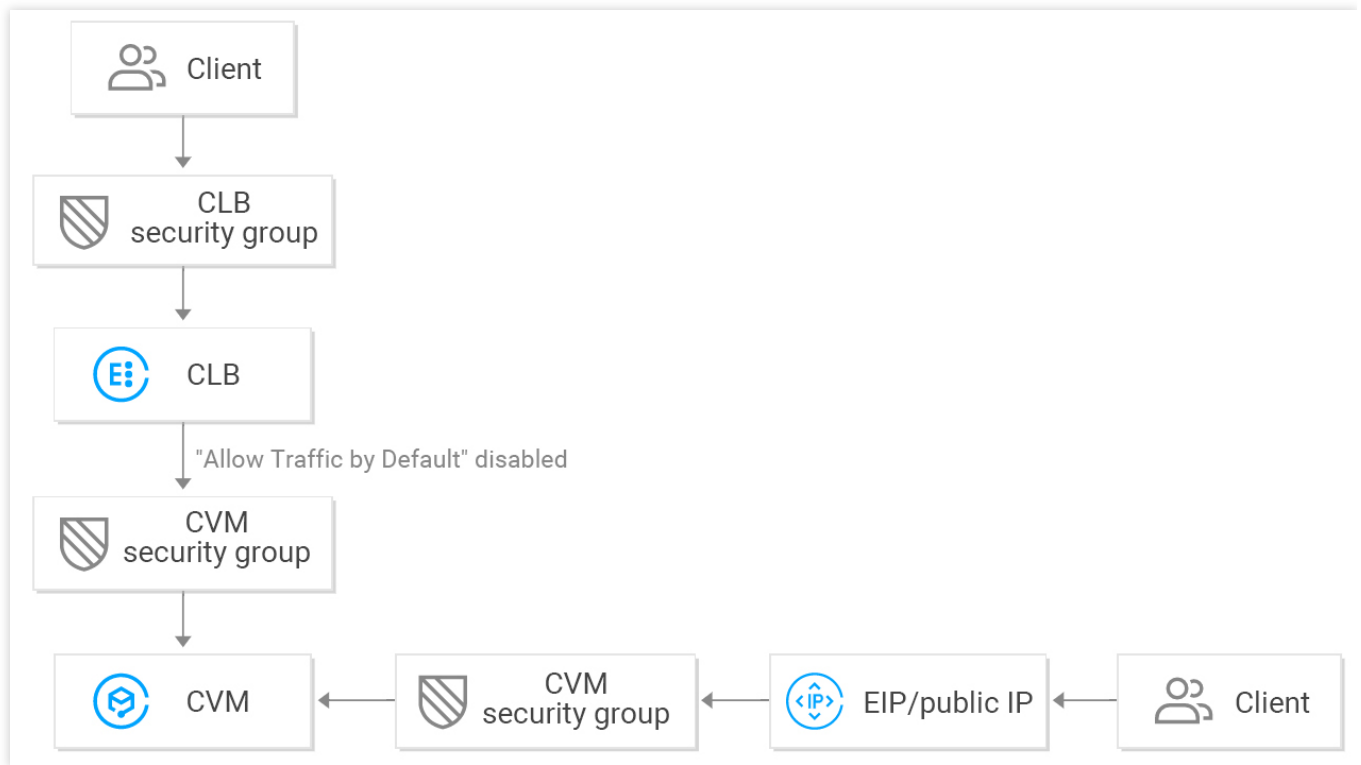
지정된 Client IP에서만 액세스를 허용하려면 해당 IP와 CLB 보안 그룹의 Client IP 및 수신 대기 포트를 허용해야 하지만 백엔드 CVM 보안 그룹의 Client IP 및 서비스 포트를 허용할 필요는 없습니다. 리얼 서버는 기본적으로 CLB의 트래픽을 허용하므로 CLB의 액세스 트래픽은 CLB 보안 그룹을 통해서만 전달됩니다.

공중망 IP(일반 공중망 IP 및 EIP 포함)의 트래픽은 여전히 CVM 보안 그룹을 통과해야 합니다.

CLB 인스턴스에 보안 그룹이 구성되지 않은 경우 모든 트래픽이 허용되며 CLB 인스턴스의 VIP에 리스너로 구성된 포트에만 액세스할 수 있습니다. 따라서 수신 포트는 모든 IP의 트래픽을 허용합니다.

지정된 Client IP의 트래픽을 거부하려면 CLB 보안 그룹에서 구성해야 합니다. CVM 보안 그룹의 Client IP 거부는 CLB의 트래픽에는 적용되지 않고 공중망 IP(일반 공중망 IP 및 EIP 포함)의 트래픽에만 적용됩니다.

보안 그룹 기본 허용 비활성화



보안 그룹 기본 허용이 비활성화된 경우:

지정된 Client IP에서만 액세스를 허용하려면 CLB 보안 그룹의 Client IP 및 수신 대기 포트를 허용하고 백엔드 CVM 보안 그룹의 Client IP 및 서비스 포트도 허용해야 합니다. 따라서 CLB를 통과하는 비즈니스 트래픽은 CLB 보안 그룹과 CVM 보안 그룹 모두에서 이중으로 확인됩니다.

공중망 IP(일반 공중망 IP 및 EIP 포함)의 트래픽은 여전히 CVM 보안 그룹을 통과해야 합니다.

CLB 인스턴스에 보안 그룹이 구성되어 있지 않으면 CVM 보안 그룹을 통과하는 트래픽만 허용됩니다.

CLB 보안 그룹 또는 CVM 보안 그룹에 대한 액세스를 거부하여 지정된 Client IP의 트래픽을 거부할 수 있습니다.

기본 허용이 비활성화된 경우 효과적인 상태 확인을 위해 CVM 보안 그룹을 다음과 같이 구성해야 합니다.

1. 공중망 CLB 구성

CLB 인스턴스가 VIP를 사용하여 백엔드 CVM의 상태를 확인할 수 있도록 백엔드 CVM의 보안 그룹에서 CLB VIP를 허용해야 합니다.

2. 사설망 CLB 구성

사설망 CLB(이전의 '애플리케이션 사설망 CLB')의 경우 CLB 인스턴스가 VPC에 있는 경우 상태 확인을 위해 백엔드 CVM의 보안 그룹에서 CLB VIP를 허용해야 합니다. CLB 인스턴스가 기본 네트워크에 있는 경우 기본적으로 상태 확인 IP가 허용되므로 추가 구성이 필요하지 않습니다.

사설망 클래식 CLB의 경우 CLB 인스턴스가 2016년 12월 5일 이전에 생성되었고 VPC에 있는 경우 백엔드 CVM 보안 그룹에서 CLB VIP를 허용(상태 확인을 위해)해야 합니다. 그렇지 않으면 상태 확인 IP가 기본적으로 허용되므로 추가 구성이 필요하지 않습니다.

작업 단계

다음 예시에서는 포트 80에서 CLB로의 인바운드 트래픽만 허용하도록 보안 그룹을 구성하고 CVM 포트 8080을 통해 서비스를 제공합니다. Client IP에는 제한이 없습니다.

주의사항:

이 예시에서 사용된 공중망 CLB 인스턴스의 경우 상태 확인을 위해 백엔드 CVM 보안 그룹에서 CLB VIP를 허용해야 합니다. 현재 IP는 `0.0.0.0/0` 으로 설정되어 모든 IP가 허용됩니다.

1단계: CLB 인스턴스 및 리스너 생성 및 CVM에 바인딩

자세한 내용은 [Getting Started with CLB](#)를 참고하십시오. HTTP:80 리스너가 생성되어 이 예시에서 서비스 포트가 8080인 백엔드 CVM 인스턴스에 바인딩됩니다.

2단계: CLB 보안 그룹 구성

1. CLB 보안 그룹 규칙 구성

[보안 그룹 콘솔](#)에서 보안 그룹 규칙을 구성합니다. 인바운드 규칙에서 모든 IP(예: `0.0.0.0/0`)의 포트 80에서 요청을 허용하고 다른 포트의 트래픽을 거부합니다.

설명

보안 그룹 규칙은 위에서 아래로 순서대로 적용됩니다. 새 규칙이 적용되면 다른 규칙은 기본적으로 거부됩니다. 그러므로 순서 구성에 주의를 기울이십시오. 자세한 내용은 [보안 그룹 개요](#)를 참고하십시오.

보안 그룹에는 인바운드 및 아웃바운드 규칙이 있습니다. 위의 구성은 인바운드 트래픽을 제한하기 위한 것이므로 **인바운드 규칙**이지만 아웃바운드 규칙은 특별히 구성할 필요가 없습니다.

Type	Source	Protocol port	Policy	Notes
Custom	0.0.0.0/0	TCP:80	Allow	

+ New Line

Completed Cancel

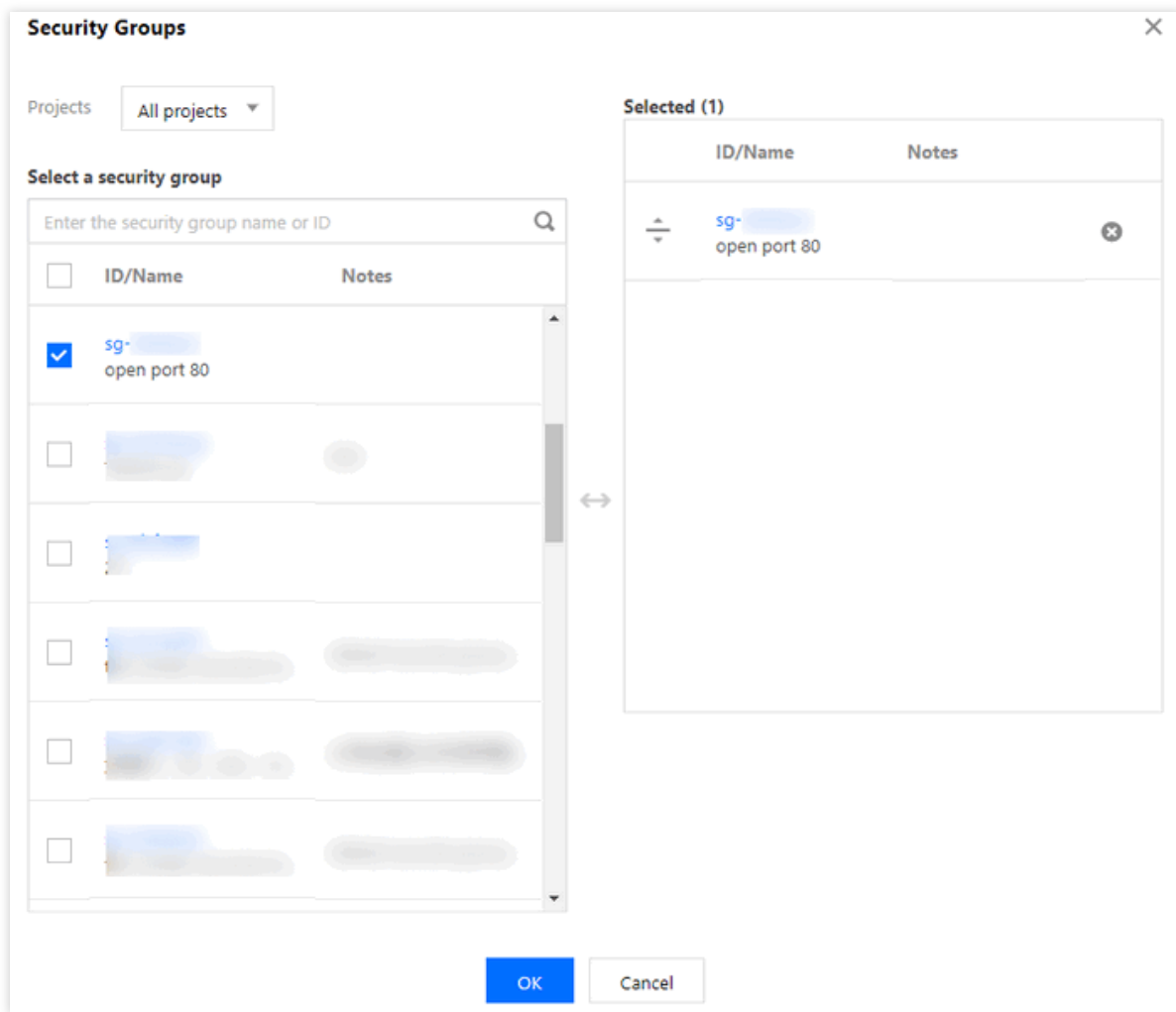
2. 보안 그룹을 CLB 인스턴스에 바인딩

2.1 CLB 콘솔에 로그인합니다.

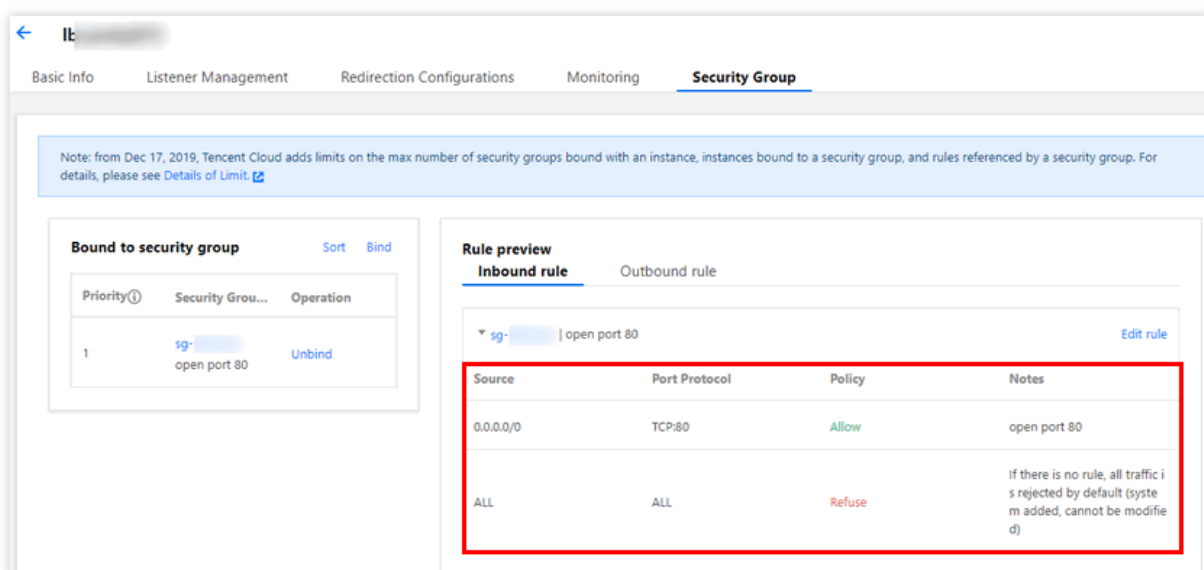
2.2 '인스턴스 관리' 페이지에서 대상 CLB 인스턴스의 ID를 클릭합니다.

2.3 인스턴스 세부 정보 페이지에서 **보안 그룹** 탭을 클릭하고 '바인딩된 보안 그룹' 모듈에서 **바인딩**을 클릭합니다.

2.4 '보안 그룹 구성' 팝업 창에서 CLB 인스턴스에 바인딩된 보안 그룹을 선택하고 **확인**을 클릭합니다.



CLB 보안 그룹 구성이 완료되면 포트 80에서만 CLB에 액세스할 수 있습니다.



3단계: 기본 허용 구성

다음과 같이 다양한 구성으로 기본 허용을 활성화 또는 비활성화할 수 있습니다.

방법1: 기본 허용을 활성화하여 리얼 서버에서 포트를 허용할 필요가 없도록 합니다.

설명:

이 기능은 클래식 사설망 CLB 및 기본 네트워크의 CLB에 대해 지원되지 않습니다.

방법2: 기본 허용을 비활성화합니다. CVM 보안 그룹에서 Client IP(이 예시에서는 0.0.0.0/0)도 허용해야 합니다.

방법1: 기본 허용 활성화

1. CLB 콘솔에 로그인합니다.
2. '인스턴스 관리' 페이지에서 대상 CLB 인스턴스의 ID를 클릭합니다.
3. 인스턴스 세부 정보 페이지에서 **보안 그룹** 탭을 클릭합니다.
4. '보안 그룹' 탭에서



을(를) 클릭하여 기본 허용을 활성화합니다.

5. 기본 허용이 활성화되면 아래와 같이 **규칙 미리 보기**의 보안 그룹 규칙만 확인됩니다.

Allow by Default ☒

When it's enabled, the access between CLB and CVM is allowed by default. Requests from CLB only need to be verified by the CLB security group. When it's disabled, requests from CLBs need to be verified by both security groups of CLB and CVM. If the CLB is not bound with a security group, all it's listening ports allow requests from all IPs.

Bound to security group [Sort](#) [Bind](#)

Priority①	Security Grou...	Operation
1	xx-allow80	Unbind

Rule preview ①

Inbound rule **Outbound rule**

Source	Port Protocol	Policy	Notes
xx-allow80	TCP:80	Allow	-
ALL	ALL	Refuse	If there is no rule, all traffic is rejected by default (system added, cannot be modified)

방법2: 기본 허용 비활성화

기본 허용이 비활성화된 경우 CVM 보안 그룹에서 Client IP를 허용해야 합니다. 비즈니스 트래픽은 CLB 포트 80에서만 CVM에 액세스하고 CVM 포트 8080에서 제공하는 서비스를 사용할 수 있습니다.

설명:

지정된 Client IP의 트래픽을 허용하려면 CLB 보안 그룹과 CVM 보안 그룹 모두에서 해당 IP를 허용해야 합니다. CLB에 보안 그룹이 없는 경우 CVM 보안 그룹에서 IP를 허용하십시오.

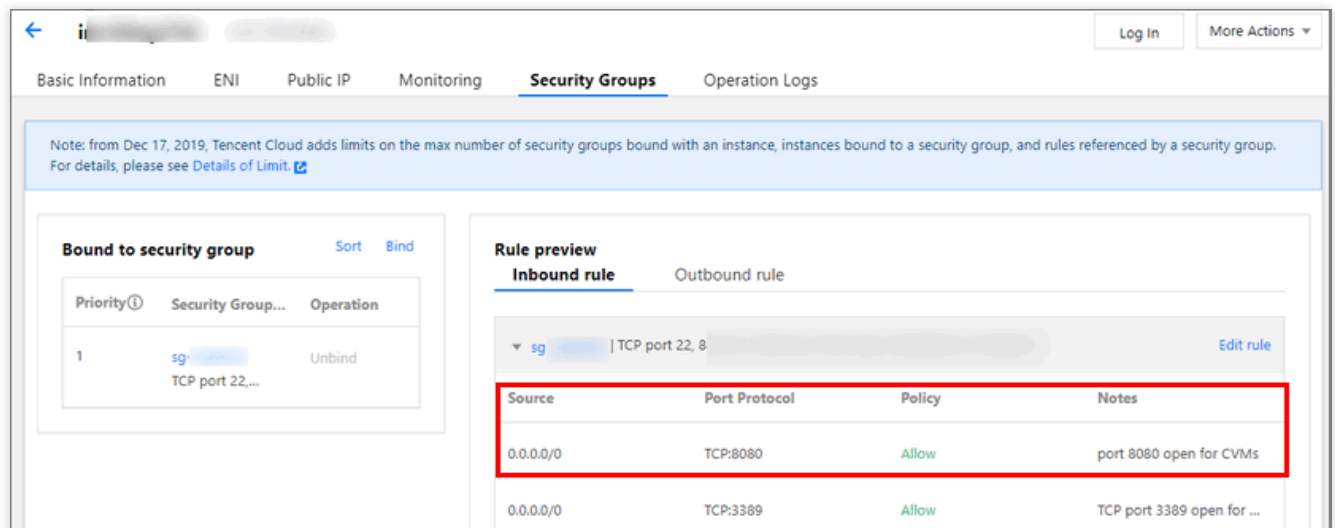
1. CVM 보안 그룹 규칙 구성

백엔드 CVM 인스턴스에 액세스하는 트래픽에 대해 서비스 포트의 액세스만 허용하도록 CVM 보안 그룹을 구성할 수 있습니다.

보안 그룹 콘솔로 이동하여 보안 그룹 정책을 구성합니다. 인바운드 규칙에서 모든 IP의 모든 포트는 8080입니다. 원활한 원격 CVM 로그인 및 Ping 서비스를 보장하려면 보안 그룹에서 22, 3389 및 ICMP 서비스를 엽니다.

2. 보안 그룹을 CVM 인스턴스에 바인딩

- 2.1 **CVM 콘솔**에서 CLB 인스턴스에 바인딩된 CVM 인스턴스의 ID를 클릭하여 세부 정보 페이지로 이동합니다.
- 2.2 **보안 그룹** 탭을 선택하고 '바인딩된 보안 그룹' 모듈에서 **바인딩**을 클릭하십시오.
- 2.3 '보안 그룹 구성' 팝업 창에서 CVM 인스턴스에 바인딩된 보안 그룹을 선택하고 **확인**을 클릭합니다.



CLB 인스턴스 시작 및 중지

최종 업데이트 날짜: : 2024-01-04 19:32:25

인스턴스를 시작하거나 중지할 수 있습니다. 인스턴스가 중지되면 더 이상 트래픽을 수신 또는 포워딩하거나 상태 확인을 수행하거나 Ping을 허용하지 않습니다.

설명:

이 기능은 현재 베타 테스트 중입니다. 사용해 보려면 [티켓 제출을 통해 신청](#)하십시오.

사용 사례

많은 수의 CLB 인스턴스를 구성했고 그 중 일부는 비즈니스 니즈를 고려해 일시적으로 사용되지 않지만 삭제할 수 없는 경우 인스턴스를 중지할 수 있습니다.

인스턴스가 중지되면 모든 리스너도 중지되고 더 이상 트래픽을 수신하거나 포워딩하지 않습니다.

인스턴스가 시작된 후 모든 리스너도 시작되고 정상적으로 트래픽을 수신 및 포워딩합니다.

리스너가 중지된 후에는 더 이상 트래픽을 수신하거나 포워딩하지 않습니다. 인스턴스의 모든 리스너가 중지되면 인스턴스가 중지됩니다.

리스너가 시작된 후에는 트래픽을 정상적으로 수신하고 포워딩합니다. 인스턴스의 모든 리스너가 시작된 후 인스턴스가 시작됩니다.

인스턴스가 중지된 후 해당 리스너가 시작되면 인스턴스가 시작되고 시작된 리스너와 함께 트래픽을 정상적으로 수신 및 포워딩하는 반면 다른 리스너는 중지된 상태로 유지됩니다.

제한 설명

이 기능은 클래식 CLB에서는 지원되지 않습니다.

이 기능은 VPC에서만 지원되며 클래식 네트워크에서는 지원되지 않습니다.

이 기능은 TLS 1.3 및 이전 버전에서는 지원되지 않습니다.

전제 조건

[CLB 인스턴스 생성](#)을 완료합니다.

[리스너 생성](#)을 완료합니다.

작업 단계

1. [CLB 콘솔](#)에 로그인합니다.
2. **인스턴스 관리** 페이지의 왼쪽 상단에서 리전을 선택하고 인스턴스 리스트에서 대상 인스턴스를 선택한 후 오른쪽의 작업 열에서 **더보기 > 시작** 또는 **더보기 > 중지**를 클릭합니다.
3. (선택 사항) **리스너 관리** 탭에서 대상 리스너를 찾고 **리스너 시작** 또는 **리스너 중지**를 클릭합니다.

CLB 인스턴스 내보내기

최종 업데이트 날짜: : 2023-04-24 15:34:36

리전 또는 기타 조건을 지정하여 구성 및 리소스 사용량 세부 정보가 포함된 CLB 인스턴스 리스트를 내보내기 할 수 있습니다.

작업 단계

1. [CLB 콘솔](#)에 로그인하고 '인스턴스 관리' 페이지의 왼쪽 상단 모서리에서 리전을 선택합니다.
2. 인스턴스 리스트에서 인스턴스를 선택하고 오른쪽 상단 모서리의



을(를) 클릭합니다.

3. '인스턴스 내보내기' 팝업 창에서 내보낼 필드와 범위를 선택하고 [확인]을 클릭하여 인스턴스 리스트를 로컬로 다운로드합니다.

Export instances

Exported files:

☒ Export All

Instance field:

☒ ID
☒ Name
☒ Status
☒ VIP

☒ Network type
☒ Network
☒ ISP
☒ Instance Specification

☒ Billing Mode
☒ Bandwidth Cap
☒ Project
☒ Tags

☒ VIP features
☒ Bind with Custom
☒ Creation Time

Rule filed:

☒ Listener ID, listener protocol, listener port, forwarding rule ID, forwarding domain, forwarding URL, CVM ID, RS IP, RS port, RS weight

Backend service type:

☒ Non-target group
☐ Target Group

In case some of the CLB's listeners are bound with the target group and the rest listeners don't, you need you export them separately.

Exported range:

☐ All Instances
☐ Only search results
☒ Only selected instances

Confirm

Cancel

매개변수	설명
필드	<p>다음 필드를 내보낼 수 있습니다.</p> <p>인스턴스 필드</p> <p>규칙 필드</p> <p>규칙 필드의 'RS 상태'는 규칙 필드가 선택되고 내보내기 범위가 '선택한 인스턴스만'인 경우에만 표시됩니다.</p>
범위	<p>다음 범위를 내보낼 수 있습니다.</p> <p>모든 인스턴스</p> <p>검색결과만</p> <p>선택한 인스턴스만</p> <p>선택된 인스턴스가 없으면 '선택한 인스턴스만' 필드가 회색으로 표시됩니다.</p>

©2013-2022 Tencent Cloud. All rights reserved.

Page 28 of 233

CLB 인스턴스 업그레이드

최종 업데이트 날짜: : 2024-01-04 19:33:05

CLB 인스턴스는 공유 CLB 인스턴스와 LCU 지원 인스턴스의 두 가지 유형으로 제공됩니다. 공유 CLB 인스턴스를 LCU 지원 CLB 인스턴스로 업그레이드할 수 있습니다.

LCU 지원 CLB의 장점

공유 CLB 인스턴스는 최대 5만개의 동시 접속, 초당 5000개의 신규 접속 및 5000개의 QPS(초당 쿼리 수)를 유지할 수 있습니다. 보장된 성능 범위 내에서 전용 포워딩 성능을 누리고 과도한 성능을 위해 공유 클러스터 리소스를 사용하므로 성능 선점이 발생할 수 있습니다.

각 LCU 지원 CLB 인스턴스는 최대 100만 동시 접속, 10만개의 새 연결 및 5만 QPS를 지원합니다. 능력을 높이려면 [Submit Ticket](#)하십시오.

업그레이드 영향

속도 제한

업그레이드 중 사설망 LCU 지원 인스턴스의 기본 대역폭은 10Gbps이며 조정할 수 있는 반면, 공중망 LCU 지원 인스턴스의 인스턴스는 동일하게 유지되며 조정할 수 없습니다(업그레이드 후 콘솔에서 조정할 수 있음).

최대 용량은 100만 동시 접속, 10만 개의 새로운 연결/초, 50만 개의 QPS입니다. 상한을 초과하면 속도 제한 및 패킷 손실이 발생합니다. LCU 지원 인스턴스의 속도 제한 지표는 아래를 참고하십시오. 자세한 내용은 [모니터링 지표](#)를 참고하십시오.

ClientConcurConn(클라이언트-CLB 동시 접속)

ClientNewConn(클라이언트-CLB 신규 연결)

TotalReq(초당 쿼리 수)

ClientOuttraffic(클라이언트-CLB 아웃바운드 대역폭)

ClientIntraffic(클라이언트-CLB 인바운드 대역폭)

업그레이드된 인스턴스의 최대 용량을 초과하지 않으면 기존 연결은 영향을 받지 않습니다.

과금

과금 방식은 변경되지 않습니다.

LCU 요금은 시간당 사용된 LCU 수를 기준으로 청구됩니다. 자세한 내용은 [LCU Pricing](#)을 참고하십시오.

네트워크 연결

업그레이드는 네트워크 연결을 방해하지 않으며 1분 이내에 완료될 수 있습니다.

롤백

한 번 업그레이드된 인스턴스는 공유 인스턴스로 다운그레이드할 수 없습니다.

제한 사항

현재 LCU 지원 인스턴스 유형은 베타 버전입니다. 업그레이드하거나 구매하려면 [Submit Ticket](#)하여 신청하십시오.

여러 종량제 공유 CLB 인스턴스 업그레이드가 지원됩니다.

기존 CLB 인스턴스 업그레이드는 허용되지 않습니다.

기본 네트워크 CLB 인스턴스 업그레이드는 허용되지 않습니다.

업그레이드 방법

1. [CLB 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **인스턴스 관리**를 클릭합니다.
2. CLB 인스턴스 목록에서 대상 공유 인스턴스를 선택하고 인스턴스 목록 위에서 **업그레이드**를 클릭합니다.
3. '인스턴스 업그레이드' 팝업 창에서 **확인**을 클릭합니다.

관련 문서

[LCU Pricing](#)

CLB 인스턴스 삭제

최종 업데이트 날짜: : 2022-10-17 18:01:50

설명 :

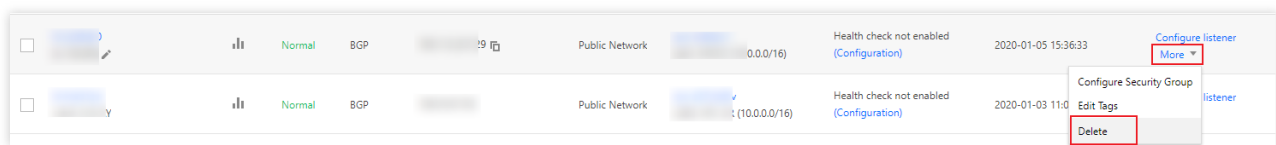
‘월간’ 구독 인스턴스는 삭제할 수 없지만 만료 시 갱신을 중지할 수 있습니다.

CLB 인스턴스에 트래픽이 없고 더 이상 필요하지 않은 경우 CLB 콘솔 또는 API를 통해 삭제할 수 있습니다.

삭제된 CLB 인스턴스는 완전히 종료되어 복구할 수 없습니다. 모든 실제 서버의 바인딩을 해제하고 인스턴스를 삭제하기 전에 잠시 관찰하는 것이 좋습니다.

콘솔을 통해 CLB 인스턴스 삭제

1. CLB 콘솔에 로그인합니다.
2. 삭제하려는 CLB 인스턴스를 찾아 우측 작업 열에서 [더 보기]>[삭제]를 클릭합니다.



3. 확인 창이 팝업되면, 작업 보안 프롬프트를 읽은 후 [확인]을 클릭하여 삭제합니다.

대화 상자는 아래와 같습니다. 바인딩된 규칙이 '0'개 있고 바인딩된 CVM 인스턴스가 '없음'이며 작업 보안에 대한 참고 사항 열 아래에 '녹색' 체크 표시가 나타났을 때 삭제하는 것이 좋습니다.

Confirm to delete the following load balancers? ×

ID/Name	Bound rules	Bound CVM	Notes About Oper...
lb-2jrl6dv0 lb-162309	0	None	✓

Submit

Close

API를 통해 CLB 인스턴스 삭제

자세한 내용은 [DeleteLoadBalancers](#)를 참고하십시오.

인스턴스 공중망 구성 조정

최종 업데이트 날짜: : 2024-01-04 19:34:35

필요에 따라 실시간으로 공중망 CLB 인스턴스의 대역폭 또는 과금 방식을 조정할 수 있습니다.

제한 설명

IPv4 CLB 인스턴스: 네트워크 구성 조정은 IP별 청구 계정에 대해서만 지원되고, CVM별 청구 계정에는 지원되지 않습니다.

IPv6 CLB 인스턴스: 네트워크 구성 조정은 IP별 청구 및 CVM별 청구 계정 모두에 대해 지원됩니다.

계정 유형 확인에 대한 자세한 내용은 [Checking Account Type](#)을 참고하십시오.

대역폭 최댓값

인스턴스 과금 방식	네트워크 과금 방식	대역폭 제한 범위(Mbps)
종량제 과금	대역폭 과금(시간당)	0 - 2048(포함)
	트래픽 과금	
	대역폭 패키지	

설명 :

더 높은 대역폭 한도를 설정해야 하는 경우 [티켓 제출](#)하거나 Tencent Cloud 영업 담당자에게 문의하십시오.

대역폭 조정

1. [CLB 콘솔](#)에 로그인합니다.
2. '인스턴스 관리' 페이지에서 리전을 선택하고 공중망 CLB 인스턴스 오른쪽의 '작업' 열에서 [더 보기]>[대역폭 조정]을 클릭합니다.
3. '대역폭 조정' 대화 상자에서 대역폭 한도를 설정하고 [제출]을 클릭합니다.

과금 방식 조정

1. CLB 콘솔에 로그인합니다.

2. '인스턴스 관리' 페이지에서 리전을 선택하고 공중망 CLB 인스턴스의 오른쪽의 '작업' 열에서 [더 보기]를 클릭한 후 네트워크 과금 방식을 계속 조정합니다.

인스턴스 과금 방식	네트워크 과금 방식	조정
종량제 과금	대역폭 과금 (시간 당)	대역폭 패키지에 IP 추가: 인스턴스 과금 방식은 동일하게 유지됩니다. 네트워크 과금 방식이 대역폭 패키지를 사용하도록 전환됩니다. 각 인스턴스는 과금 방식을 한 번만 전환할 수 있습니다.
	트래픽 과금	월간 구독으로 전환: 인스턴스 과금 방식이 월간 구독으로 전환됩니다. 네트워크 과금 방식이 대역폭 과금(월별)으로 전환됩니다. 각 인스턴스는 과금 방식을 한 번만 전환할 수 있습니다. 공유 대역폭 패키지 추가 지원: 인스턴스 과금은 변경되지 않고 네트워크 과금은 공유 대역폭 패키지 과금으로 변환됩니다. 각 인스턴스는 과금 방식을 횟수 제한 없이 전환할 수 있습니다.
	대역폭 패키지	대역폭 패키지에서 IP 제거: 인스턴스 과금 방식은 동일하게 유지됩니다. 네트워크 과금 방식이 트래픽 과금으로 전환됩니다. 각 인스턴스는 과금 방식을 횟수 제한 없이 전환할 수 있습니다.

3. 팝업 창에서 [제출]을 클릭합니다.

CLB 리스너

CLB 리스너 개요

최종 업데이트 날짜: : 2024-01-04 19:41:11

CLB 인스턴스를 생성한 후에는 이에 대한 리스너를 구성해야 합니다. 리스너는 인스턴스에 대한 요청을 수신하고 로드 밸런싱 정책에 따라 트래픽을 리얼 서버로 라우팅합니다.

다음 항목을 사용하여 CLB 리스너를 구성해야 합니다.

1. 수신 프로토콜 및 포트. 수신 포트 또는 프론트엔드 포트는 요청을 수신하고 리얼 서버로 포워딩하는 데 사용됩니다.
2. 로드 밸런싱 정책 및 [Session Persistence](#) 등의 수신 정책.
3. [Health Check](#) 정책.
4. 리얼 서버. 리얼 서버의 IP와 포트를 선택하여 바인딩합니다. 서비스 포트 또는 백엔드 포트는 리얼 서버에서 요청을 수신하는 데 사용됩니다.

지원되는 프로토콜 유형

CLB 리스너는 CLB 인스턴스에서 레이어 4 및 레이어 7 요청을 수신하고 처리를 위해 리얼 서버로 라우팅할 수 있습니다. 레이어 4 CLB와 레이어 7 CLB의 주요 차이점은 레이어 4 프로토콜(예: TCP 또는 UDP) 또는 레이어 7 프로토콜(예: HTTP 또는 HTTPS)이 사용자 요청의 로드 밸런싱을 위해 트래픽을 포워딩하는 데 사용되는지 여부입니다.

레이어 4 프로토콜: 요청을 수신하고 주로 **VIP + Port**를 통해 트래픽을 리얼 서버로 포워딩하는 전송 레이어 프로토콜입니다.

레이어 7 프로토콜: URL 및 HTTP 헤더와 같은 애플리케이션 레이어 정보를 기반으로 트래픽을 분산하는 애플리케이션 레이어 프로토콜입니다.

레이어 4 리스너(즉, 레이어 4 프로토콜 포워딩)를 사용하는 경우 CLB 인스턴스는 수신 포트에서 리얼 서버와 TCP 연결을 설정하고 요청을 리얼 서버로 직접 포워딩합니다. 이 프로세스는 데이터 패킷을 수정하지 않으며(통과 모드에서) 포워딩 효율성이 높습니다.

Tencent Cloud CLB는 다음 프로토콜을 통한 요청 포워딩을 지원합니다.

TCP(전송 레이어)

UDP(전송 레이어)

TCP SSL(전송 레이어)

QUIC(전송 레이어)

HTTP(애플리케이션 레이어)

HTTPS(애플리케이션 레이어)

설명 :

TCP SSL 리스너는 현재 공중망 CLB 인스턴스를 지원하지만 사설망 또는 클래식 CLB 인스턴스는 지원하지 않습니다.

프로토콜 유형	프로토콜	설명	사용 사례
레이어 4 프로토콜	TCP	<p>연결 지향적이고 안정적인 전송 레이어 프로토콜 소스 및 타깃 엔드는 데이터 전송 전에 연결을 설정하기 위해 3방향 핸드셰이크를 수행해야 합니다. 클라이언트 IP(소스 IP) 기반 세션 지속성을 지원합니다. 클라이언트 IP는 네트워크 레이어에서 찾을 수 있습니다. 서버는 클라이언트 IP를 직접 가져올 수 있습니다.</p>	<p>파일 전송, 이메일 송수신, 원격 로그인과 같이 신뢰성과 데이터 정확도에 대한 요구 사항은 높지만 전송 속도에 대한 요구 사항은 상대적으로 낮은 시나리오에 적합합니다. 자세한 내용은 TCP 리스너 구성을 참고하십시오.</p>
	UDP	<p>연결 없는 전송 레이어 프로토콜 소스 및 타깃 엔드는 연결을 설정하지 않으며 연결 상태를 유지하지도 않습니다. 각 UDP 연결은 지점 간입니다. 일대일, 일대다, 다대일 및 다대다 통신이 지원됩니다. 클라이언트 IP(소스 IP) 기반 세션 지속성을 지원합니다. 서버는 클라이언트 IP를 직접 가져올 수 있습니다.</p>	<p>인스턴트 메시징 및 온라인 비디오와 같이 전송 효율성에 대한 요구 사항은 높지만 정확도에 대한 요구 사항은 상대적으로 낮은 시나리오에 적합합니다. 자세한 내용은 UDP 리스너 구성을 참고하십시오.</p>
	TCP SSL	<p>보안 TCP TCP SSL 리스너는 무단 액세스 요청을 방지하기</p>	<p>TCP를 사용할 때 보안 요구 사항이 높은 시나리오에 적합하며 TCP 기반 사용자 지정 프로토콜을 지원합니다. 자세한 내용은 TCP SSL 리스너 구성을 참고하십시오.</p>

레이어 7 프로토콜		<p>위해 인증서 구성을 지원합니다.</p> <p>CLB가 복호화를 구현할 수 있도록 통합 인증서 관리가 제공됩니다.</p> <p>단방향 및 양방향 인증이 지원됩니다.</p> <p>서버는 클라이언트 IP를 직접 가져올 수 있습니다.</p>	
	QUIC	<p>UDP 기반 다중화 동시 전송 레이어 프로토콜입니다.</p> <p>UDP를 통한 안정적인 데이터 전송, 보안 및 HTTP2를 구현하며 TCP + TLS + HTTP2와 유사합니다.</p> <p>QUIC 연결에서는 IP나 포트에 무슨 일이 일어나도 연결이 끊기지 않아 끊김 없는 연결 마이그레이션이 가능합니다.</p>	<p>오디오/비디오 서비스, 게임 서비스 등에 적합합니다. 4G 네트워크와 Wi-Fi 네트워크 간의 빈번한 전환 등 네트워크가 불안정한 경우 중단 없이 원활하게 서비스 마이그레이션 및 연결할 수 있습니다. 자세한 내용은 QUIC 리스너 구성을 참고하십시오.</p>
	HTTP	<p>애플리케이션 레이어 프로토콜</p> <p>요청된 도메인 이름 및 URL을 기반으로 하는 포워딩이 지원됩니다.</p> <p>Cookie 기반 세션 지속성이 지원됩니다.</p>	<p>Web 애플리케이션, 모바일 App 등 요청 내용을 식별해야 하는 애플리케이션에 적합합니다. 자세한 내용은 HTTP 리스너 구성을 참고하십시오.</p>
	HTTPS	<p>암호화된 애플리케이션 레이어 프로토콜</p> <p>요청된 도메인 이름 및 URL을 기반으로 하는 포워딩이 지원됩니다.</p> <p>Cookie 기반 세션 지속성이 지원됩니다.</p> <p>CLB가 복호화를 구현할 수 있도록 통합 인증서 관리가 제공됩니다.</p> <p>단방향 및 양방향 인증이 지원됩니다.</p>	<p>암호화된 전송이 필요한 HTTP 애플리케이션에 적합합니다. 자세한 내용은 HTTPS 리스너 구성을 참고하십시오.</p>

포트 구성

포트 유형	설명	제한 사항
수신 포트 (프론트 엔드 포트)	수신 포트는 CLB 인스턴스에서 요청을 수신하고 리얼 서버로 포워딩하는 데 사용됩니다. 포트 21(FTP), 25(SMTP), 80(HTTP) 및 443(HTTPS) 등과 같은 포트 1 - 65535에 대해 CLB 인스턴스를 구성할 수 있습니다.	하나의 CLB 인스턴스에서: UDP의 수신 포트는 TCP에 사용할 수 있습니다. 예를 들어 TCP:80 리스너와 UDP:80 리스너가 공존할 수 있습니다. 수신 포트는 동일한 유형의 프로토콜에 대해 고유해야 합니다. TCP, TCP SSL, HTTP, HTTPS는 TCP이므로 TCP:80 리스너와 HTTP:80 리스너가 공존할 수 없습니다.
서비스 포트 (백엔드 포트)	서비스 포트는 CVM 인스턴스에서 서비스를 제공하고 CLB 인스턴스에서 트래픽을 수신 및 처리하는 데 사용됩니다. 하나의 CLB 인스턴스에서 하나의 수신 포트는 여러 CVM 인스턴스의 포트에 트래픽을 포워딩할 수 있습니다.	하나의 CLB 인스턴스에서: 다른 수신 프로토콜의 서비스 포트는 고유할 필요가 없습니다. 예를 들어 리스너 HTTP:80 및 HTTPS:443은 모두 CVM 인스턴스의 동일한 포트에 바인딩될 수 있습니다. 동일한 수신 프로토콜을 사용할 때 각 실제 서버 포트는 하나의 리스너에만 바인딩될 수 있습니다. 즉, 쿼드러플(VIP, 리스닝 프로토콜, 실제 서버의 사설망 IP 및 실제 서버 포트)이 고유해야 합니다.

관련 문서

[Use Limits](#)

TCP 리스너 구성

최종 업데이트 날짜: : 2023-05-05 18:00:39

CLB 인스턴스에 대한 TCP 리스너를 생성하여 클라이언트의 TCP 요청을 포워딩할 수 있습니다. TCP는 파일 전송, 이메일 메시징 및 원격 로그인과 같이 안정성과 데이터 정확도에 대한 요구 사항은 높지만 전송 속도에 대한 요구 사항은 상대적으로 낮은 시나리오에 적합합니다. TCP 리스너의 경우 리얼 서버가 실제 클라이언트 IP를 직접 가져올 수 있습니다.

전제 조건

먼저 [CLB 인스턴스 생성](#)을 완료해야 합니다.

작업 단계

1단계: 리스너 구성

1. [CLB 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **인스턴스 관리**를 클릭합니다.
2. CLB 인스턴스 목록 페이지의 왼쪽 상단 모서리에서 리전을 선택하고 오른쪽의 작업 열에서 **리스너 구성**을 클릭합니다.

ID/Name	Mon...	Status	VIP	Availability Z...	Network ...	Carrier	Instance Spe...	Health Status	Billing
<input type="checkbox"/> lb- lb-		Normal		Beijing Zone 4	Public Network	BGP	Dedicated	Health check not enabled Configuration	Pay-as- - banc Createc 2022-0 11:32

3. TCP/UDP/TCP SSL/QUIC 리스너에서 **생성**을 클릭하고 '리스너 생성' 팝업 창에서 TCP 리스너를 구성합니다.

3.1 기본 구성

리스너 기본 구성	설명	예시
이름	리스너 이름입니다.	test-tcp-80
리스너 프로토콜 및 포트	리스너 프로토콜: 이 예시에서는 TCP가 사용됩니다. 리스너 포트: 요청을 수신하고 리얼 서버로 포워딩하는 데 사용되는 포트입니다. 포트 범위: 1 - 65535. 리스너 포트는 동일한 CLB 인스턴스에서 고유해야 합니다.	TCP:80
밸런싱 메소드	TCP 리스너의 경우 CLB는 WRR(가중 라운드 로빈) 및 WLC(가중 최소 연결)	WRR

	<p>의 두 가지 스케줄링 알고리즘을 지원합니다.</p> <p>WRR: 가중치에 따라 다른 리얼 서버에 요청을 순차적으로 전달합니다. 스케줄링은 새 연결 수를 기반으로 수행되며 가중치가 높은 서버는 더 많은 폴링(즉, 더 높은 확률)을 거치고 가중치가 같은 서버는 같은 수의 연결을 처리합니다.</p> <p>WLC: 서버에 대한 활성 연결 수에 따라 서버 로드가 예상됩니다. 스케줄링은 서버 로드 및 가중치를 기반으로 수행됩니다. 가중치가 같으면 활성 연결이 적은 서버가 더 많은 폴링을 받게 됩니다(즉, 더 높은 확률).</p> <p>설명: 리스너는 로드 밸런싱을 위해 가장 최소 연결을 선택한 후 세션 선호도 기능 활성화를 지원하지 않습니다.</p>	
양방향 RST	이 옵션을 선택하면 해당 작업에서 RST 패킷을 양쪽 끝(클라이언트 및 서버)으로 보내 연결을 닫습니다. 그렇지 않으면 양방향 RST 패킷이 전송되지 않으며 시간이 초과될 때까지 영구 연결이 유지됩니다.	미선택

3.2 상태 확인

자세한 내용은 [TCP 상태 확인](#)을 참고하십시오.

3.3 세션 지속성

세션 지속성 구성	설명	예시
세션 지속성 스위치	<p>세션 지속성이 활성화된 후 CLB 리스너는 동일한 클라이언트의 액세스 요청을 동일한 리얼 서버로 배포합니다.</p> <p>TCP 세션 지속성은 클라이언트 IP 주소를 기반으로 구현됩니다. 동일한 IP 주소의 액세스 요청은 동일한 리얼 서버로 포워딩됩니다.</p> <p>WRR 스케줄링에는 세션 지속성을 활성화할 수 있지만 WLC 스케줄링에는 활성화할 수 없습니다.</p>	활성화
세션 지속 시간	<p>세션 지속 시간</p> <p>세션 지속 시간 이후에 연결 내에 새로운 요청이 없으면 세션 지속성이 자동으로 비활성화됩니다.</p> <p>값 범위: 30 - 3600초.</p>	30s

2단계: 리얼 서버 바인딩

1. '리스너 관리' 페이지에서 생성된 리스너 `TCP:80` 을 클릭하면 리스너 오른쪽에 바인딩된 리얼 서버가 표시됩니다.

2. **바인딩**을 클릭하고 대상 리얼 서버를 선택하고 팝업 창에서 서버 포트 및 가중치를 구성합니다.

설명


기본 포트: '기본 포트'를 먼저 입력한 다음 CVM 인스턴스를 선택합니다. 모든 CVM 인스턴스의 포트는 기본 포트입니다.


3단계: 보안 그룹 구성(선택 사항)

공중망 트래픽을 격리하도록 CLB 보안 그룹을 구성할 수 있습니다. 자세한 내용은 [Configuring CLB Security Group](#)을 참고하십시오.

4단계: 리스너 수정 및 삭제(선택 사항)

생성된 리스너를 수정하거나 삭제해야 하는 경우 '리스너 관리' 페이지에서 해당 리스너를 클릭한 후

을(를)  클릭하여 수정하거나

을(를)  클릭하여 삭제합니다.

UDP 리스너 구성

최종 업데이트 날짜: : 2024-01-04 19:41:56

CLB 인스턴스에 대한 UDP 리스너를 생성하여 클라이언트의 UDP 요청을 포워딩할 수 있습니다. UDP는 인스턴트 메시징 및 온라인 비디오와 같이 전송 속도에 대한 요구 사항이 높지만 정확도에 대한 요구 사항이 상대적으로 낮은 시나리오에 적합합니다. UDP 리스너의 경우 리얼 서버는 실제 클라이언트 IP를 직접 가져올 수 있습니다.

제한 설명

UDP 리스너의 포트 4789는 시스템 예약 포트이며 아직 사용할 수 없습니다.

전제 조건

[CLB 인스턴스 생성](#)의 안내에 따라 CLB 인스턴스를 생성해야 합니다.

작업 단계

1단계: 리스너 구성

1. [CLB 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **인스턴스 관리**를 선택합니다.
2. CLB 인스턴스 목록 페이지의 왼쪽 상단 모서리에서 리전을 선택하고 오른쪽의 작업 열에서 **리스너 구성**을 클릭합니다.

<input type="checkbox"/>	ID/Name ↕	Mon...	Status	VIP	Availability Z...	Network ...	Carrier	Instance Spe...	Health Status	Billing
<input type="checkbox"/>	lb- lb-		Normal		Beijing Zone 4	Public Network	BGP	Dedicated	Health check not enabled Configuration	Pay-as- - banc Create 2022-0 11:32

3. TCP/UDP/TCP SSL/QUIC 리스너에서 **생성**을 클릭하고 **리스너 생성** 팝업 창에서 UDP 리스너를 구성합니다.

3.1 기본 구성

구성 항목	설명	예시
이름	리스너 이름.	test-udp-8000
리스너 프로토콜 및 포트	리스너 프로토콜: 이 예시에서는 UDP가 사용됩니다.	UDP:8000

	<p>리스너 포트: 요청을 수신하고 리얼 서버로 포워딩하는 데 사용되는 포트입니다. 포트 범위: 1 - 65535. 포트 4789는 시스템 예약 포트이며 아직 사용할 수 없습니다.</p> <p>리스너 포트는 동일한 CLB 인스턴스에서 고유해야 합니다.</p>	
밸런싱 메소드	<p>UDP 리스너의 경우 CLB는 WRR(가중 라운드 로빈) 및 WLC(가중 최소 연결)의 두 가지 스케줄링 알고리즘을 지원합니다.</p> <p>WRR: 요청은 가중치에 따라 다른 리얼 서버에 순차적으로 전달됩니다. 스케줄링은 새 연결 수를 기반으로 수행되며 가중치가 높은 서버는 더 많은 폴링(즉, 더 높은 확률)을 거치고 가중치가 같은 서버는 같은 수의 연결을 처리합니다.</p> <p>WLC: 서버에 대한 활성 연결 수에 따라 서버 로드가 예상됩니다. 스케줄링은 서버 로드 및 가중치를 기반으로 수행됩니다. 가중치가 같으면 활성 연결이 적은 서버가 더 많은 폴링을 받게 됩니다(즉, 더 높은 확률).</p> <p>설명: WLC가 선택된 경우 리스너는 세션 지속성을 지원하지 않습니다.</p>	WRR
QUIC ID로 스케줄링	<p>이 기능이 활성화되면 CLB는 QUIC ID로 클라이언트 요청을 스케줄링하므로 동일한 QUIC Connection ID를 가진 요청은 동일한 리얼 서버로 스케줄링됩니다. 요청에 QUIC Connection ID가 없으면 일반 WRR 스케줄링, 즉 4중(소스 IP + 대상 IP + 소스 포트 + 대상 포트)에 따른 스케줄링으로 다운그레이드됩니다.</p>	활성화

3.2 상태 확인

상태 확인에 대한 자세한 내용은 [상태 확인 구성](#)을 참고하십시오.

3.3 세션 지속성

세션 지속성 구성	설명	예시
세션 지속성 스위치	<p>세션 지속성이 활성화되면 CLB 리스너는 동일한 클라이언트의 액세스 요청을 동일한 리얼 서버로 전달합니다.</p> <p>TCP 세션 지속성은 클라이언트 IP 주소를 기반으로 구현됩니다. 즉, 동일한 IP 주소의 액세스 요청이 동일한 리얼 서버로 포워딩됩니다.</p> <p>WRR 스케줄링에는 세션 지속성을 활성화할 수 있지만 WLC 스케줄링에는 활성화할 수 없습니다.</p>	활성화
세션 지속 시간	<p>세션 지속 시간</p> <p>세션 지속 시간 이후에 연결 내에 새로운 요청이 없으면 세션 지속성이 자동으로 비활성화됩니다.</p> <p>값 범위는 30 - 3600s입니다.</p>	30s

2단계: 백엔드 CVM 바인딩

1. **리스너 관리** 페이지에서 생성된 리스너 `UDP:8000` 을 클릭하면 리스너 오른쪽에 바인딩된 리얼 서버가 표시됩니다.

2. **바인딩**을 클릭하고 대상 리얼 서버를 선택하고 팝업 창에서 서버 포트 및 가중치를 구성합니다.

설명:


기본 포트: '기본 포트'를 먼저 입력한 후 CVM 인스턴스를 선택합니다. 모든 CVM 인스턴스의 포트는 기본 포트입니다.


3단계: 보안 그룹 구성(선택 사항)

공중망 트래픽을 격리하도록 CLB 보안 그룹을 구성할 수 있습니다. 자세한 내용은 [Configuring CLB Security Group](#)을 참고하십시오.

4단계: 리스너 수정 및 삭제(선택 사항)

생성된 리스너를 수정하거나 삭제해야 하는 경우 '리스너 관리' 페이지에서 해당 리스너를 클릭한 후

을(를)  클릭하여 수정하거나

을(를)  클릭하여 삭제합니다.

TCP SSL 리스너 구성

최종 업데이트 날짜: : 2023-05-05 18:00:39

CLB 인스턴스에 대한 TCP SSL 리스너를 생성하여 클라이언트에서 암호화된 TCP 요청을 포워딩할 수 있습니다. TCP SSL은 초고성능 및 대규모 TLS 오프로딩이 필요한 시나리오에 적용할 수 있습니다. TCP SSL 리스너의 경우 리얼 서버가 실제 클라이언트 IP를 직접 가져올 수 있습니다.

설명:

TCP SSL 리스너는 현재 CLB에서만 지원되고 클래식 CLB에서는 지원되지 않습니다.

사용 사례

TCP SSL은 TCP 사용 시 보안 요구 사항이 높은 시나리오에 적합합니다. TCP SSL 리스너는 무단 액세스 요청을 방지하기 위해 인증서 구성을 지원합니다. CLB가 복호화를 구현할 수 있도록 통합 인증서 관리가 제공됩니다. 단방향 및 양방향 인증이 지원됩니다. 서버는 클라이언트 IP를 직접 가져올 수 있습니다.

전제 조건

먼저 [CLB 인스턴스 생성](#)을 완료해야 합니다.

작업 단계

1단계: 리스너 구성

1. [CLB 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **인스턴스 관리**를 클릭합니다.
2. CLB 인스턴스 목록 페이지의 왼쪽 상단 모서리에서 리전을 선택하고 오른쪽의 작업 열에서 **리스너 구성**을 클릭합니다.

<input type="checkbox"/>	ID/Name ↕	Mon...	Status	VIP	Availability Z...	Network ...	Carrier	Instance Spe...	Health Status	Billing
<input type="checkbox"/>	lib- lib-		Normal		Beijing Zone 4	Public Network	BGP	Dedicated	Health check not enabled Configuration	Pay-as- - banc Createt 2022-0 11:32

3. TCP/UDP/TCP SSL/QUIC 리스너에서 **생성**을 클릭하고 **리스너 생성** 팝업 창에서 TCP SSL 리스너를 구성합니다.

3.1 기본 구성

리스너 기본 구성	설명	예시
이름	리스너 이름입니다.	test-tcpsl-9000
리스너 프로토콜 및 포트	리스너 프로토콜: 이 예시에서는 TCP SSL이 사용됩니다. 리스너 포트: 요청을 수신하고 리얼 서버로 포워딩하는 데 사용되는 포트입니다. 포트 범위: 1 - 65535. 리스너 포트는 동일한 CLB 인스턴스에서 고유해야 합니다.	TCP SSL:9000
SSL 파싱 방법	단방향 인증과 양방향 인증을 지원합니다.	단방향 인증
서버 인증서	SSL 인증서 서비스 에서 기존 인증서를 선택하거나 인증서를 업로드할 수 있습니다.	기존 인증서
밸런싱 메소드	TCP SSL 리스너의 경우 CLB는 WRR(가중 라운드 로빈) 및 WLC(가중 최소 연결)의 두 가지 스케줄링 알고리즘을 지원합니다. WRR: 가중치에 따라 다른 리얼 서버에 요청을 순차적으로 전달합니다. 스케줄링은 신규 연결 수를 기반으로 수행되며 가중치가 높은 서버는 더 많은 폴링(즉, 더 높은 확률)을 거치고 가중치가 같은 서버는 같은 수의 연결을 처리합니다. WLC: 서버에 대한 활성 연결 수에 따라 서버 로드가 예상됩니다. 스케줄링은 서버 로드 및 가중치를 기반으로 수행됩니다. 가중치가 같으면 활성 연결이 적은 서버가 더 많은 폴링을 받게 됩니다(즉, 더 높은 확률).	WRR

3.2 상태 확인

자세한 내용은 [TCP SSL 상태 확인](#)을 참고하십시오.

3.3 세션 지속성(현재 지원되지 않음)

TCP SSL 리스너는 현재 세션 지속성을 지원하지 않습니다.

2단계: 리얼 서버 바인딩

1. **리스너 관리** 페이지에서 생성된 리스너 `TCP SSL:9000` 을 클릭하여 리스너 오른쪽에 바인딩된 리얼 서버를 확인합니다.

2. **바인딩**을 클릭하고 대상 리얼 서버를 선택하고 팝업 창에서 서버 포트 및 가중치를 구성합니다.

설명:


기본 포트: '기본 포트'를 먼저 입력한 다음 CVM 인스턴스를 선택합니다. 모든 CVM 인스턴스의 포트는 기본 포트입니다.


3단계: 보안 그룹 구성(선택 사항)

공중망 트래픽을 격리하도록 CLB 보안 그룹을 구성할 수 있습니다. 자세한 내용은 [Configuring CLB Security Group](#)을 참고하십시오.

4단계: 리스너 수정 및 삭제(선택 사항)

생성된 리스너를 수정하거나 삭제해야 하는 경우 '리스너 관리' 페이지에서 해당 리스너를 클릭한 후

을(를)  클릭하여 수정하거나

을(를)  클릭하여 삭제합니다.

QUIC 리스너 구성

최종 업데이트 날짜: : 2023-03-27 18:04:11

클라이언트에서 암호화된 QUIC 요청을 전달하기 위해 CLB 인스턴스에 대한 QUIC 리스너를 생성할 수 있습니다. QUIC 리스너의 경우 리얼 서버는 리얼 클라이언트 IP를 직접 가져올 수 있습니다.

QUIC(Quick UDP Internet Connection)는 Google에서 설계한 전송 레이어 네트워크 프로토콜로 UDP를 사용하여 동시 데이터 스트림을 다중화합니다. 널리 사용되는 TCP+TLS+HTTP2 프로토콜과 비교하여 QUIC에는 다음과 같은 장점이 있습니다.

연결 설정 시간이 단축되었습니다.

혼잡 제어를 개선합니다.

HOL(head-of-line) 차단을 피하기 위해 멀티플렉스를 채택합니다.

연결 마이그레이션을 지원합니다.

사용 사례

QUIC 리스너는 연결 마이그레이션을 지원합니다. 4G와 Wi-Fi 네트워크 간의 빈번한 전환과 같이 네트워크가 변경되어도 중단 없이 연결을 원활하게 마이그레이션할 수 있습니다. 오디오/비디오 서비스, 게임 서비스 등에 적합합니다.

제한 설명

QUIC 리스너는 CLB에만 지원되며 클래식 CLB에는 지원되지 않습니다.

QUIC 리스너는 클래식 네트워크가 아닌 VPC의 CLB 인스턴스에만 지원됩니다.

IPv4 및 IPv6 NAT64 CLB 인스턴스만 QUIC 리스너를 지원합니다.

전제 조건

먼저 [CLB 인스턴스를 생성](#)해야 합니다.

작업 단계

1단계: 리스너 구성

1. [CLB 콘솔](#)에 로그인하고 왼쪽 사이드바에서 인스턴스 관리를 클릭합니다.

2. CLB 인스턴스 목록 페이지의 왼쪽 상단 모서리에서 리전을 선택하고 오른쪽의 작업 열에서 리스너 구성을 클릭합니다.

<input type="checkbox"/>	ID/Name ↕	Mon...	Status	VIP	Availability Z...	Network ... ▾	Carrier	Instance Spe...	Health Status	Billing
<input type="checkbox"/>	lb- lb-		Normal		Beijing Zone 4	Public Network	BGP	Dedicated	Health check not enabled Configuration	Pay-as- - banc Createt 2022-0 11:32

3. TCP/UDP/TCP SSL/QUIC 리스너에서 생성을 클릭하고 리스너 생성 팝업 창에서 QUIC 리스너를 구성합니다.

3.1 기본 구성

구성 항목	설명	예시
이름	리스너의 이름입니다.	test-quic-443
리스너 프로토콜 및 포트	리스너 프로토콜: 이 예시에서는 QUIC가 사용됩니다. QUIC이 선택된 후 CLB는 클라이언트의 QUIC 요청을 수신할 수 있지만 CLB와 리얼 서버 간에는 여전히 TCP가 사용됩니다. 리스너 포트: 요청을 수신하여 리얼 서버로 포워딩하는 데 사용되는 포트입니다. 포트 범위: 1 - 65535. 리스너 포트는 동일한 CLB 인스턴스에서 고유해야 합니다.	QUIC:443
SSL 파싱 메소드	단방향 인증 및 양방향 인증이 지원됩니다.	단방향 인증
서버 인증서	SSL 인증서 서비스 에서 기존 인증서를 선택하거나 인증서를 업로드할 수 있습니다.	기존 인증서
밸런싱 방식	QUIC 리스너의 경우 CLB는 WRR(가중 라운드 로빈) 및 WLC(가중 최소 연결)의 두 가지 스케줄링 알고리즘을 지원합니다. WRR: 요청이 가중치에 따라 다른 리얼 서버에 순차적으로 전달됩니다. 스케줄링은 새 연결 수를 기반으로 수행됩니다. 여기서 가중치가 더 높은 서버는 더 많은 폴링(즉, 더 높은 확률)을 받는 반면 동일한 가중치를 가진 서버는 동일한 수의 연결을 처리합니다. WLC: 서버에 대한 활성 연결 수에 따라 서버 부하가 추정됩니다. 스케줄링은 서버 로드 및 가중치를 기반으로 수행됩니다. 가중치가 같으면 활성 연결이 적은 서버가 더 많은 폴링을 받게 됩니다(즉, 더 높은 확률).	WRR

3.2 상태 확인

상태 확인에 대한 자세한 내용은 [TCP SSL 상태 확인](#)을 참고하십시오.

3.3 세션 지속성

QUIC 리스너는 현재 세션 지속성을 지원하지 않습니다.

2단계: 리얼 서버 바인딩

1. 리스너 관리 페이지에서 생성된 리스너 **QUIC:443**을 클릭하면 리스너 오른쪽에 바인딩된 리얼 서버가 표시됩니다.
2. 바인딩을 클릭하고 대상 리얼 서버를 선택하고 팝업 창에서 서버 포트 및 가중치를 구성합니다.

설명 :

기본 포트: 기본 포트를 먼저 입력한 다음 **CVM** 인스턴스를 선택합니다. 모든 **CVM** 인스턴스의 포트는 기본 포트입니다.

3단계: 보안 그룹 구성.

공중망 트래픽을 격리하려면 **CLB** 보안 그룹을 구성해야 합니다. 자세한 내용은 [CLB 보안 그룹 구성](#)을 참고하십시오.

4단계: 리스너 수정 및 삭제(선택 사항)

생성된 리스너를 수정하거나 삭제해야 하는 경우 '리스너 관리' 페이지에서 리스너를 클릭한 후

수정  또는

 삭제를 클릭합니다.

관련 문서

[CLB에서 QUIC 프로토콜 사용](#)

HTTP 리스너 구성

최종 업데이트 날짜: : 2024-01-04 19:43:20

CLB 인스턴스에 대한 HTTP 리스너를 만들어 클라이언트의 HTTP 요청을 포워딩할 수 있습니다. HTTP는 Web 애플리케이션 및 모바일 App과 같이 요청 내용을 식별해야 하는 애플리케이션에 적합합니다.

전제 조건

먼저 [CLB 인스턴스 생성](#)에 설명된 대로 CLB 인스턴스를 생성해야 합니다.

작업 단계

1단계: 리스너 구성

1. [CLB 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **인스턴스 관리**를 클릭합니다.
2. CLB 인스턴스 목록 페이지의 왼쪽 상단 모서리에서 리전을 선택하고 오른쪽의 작업 열에서 **리스너 구성**을 클릭합니다.

<input type="checkbox"/>	ID/Name	Mon...	Status	VIP	Availability Z...	Network ...	Carrier	Instance Spe...	Health Status	Billing
<input type="checkbox"/>	lb- lb-		Normal		Beijing Zone 4	Public Network	BGP	Dedicated	Health check not enabled Configuration	Pay-as- - banc Createc 2022-0 11:32

3. HTTP/HTTPS 리스너에서 **생성**을 클릭하고 '리스너 생성' 팝업 창에서 HTTP 리스너를 구성합니다.

3.1 리스너 생성

리스너 기본 구성	설명	예시
이름	리스너 이름입니다.	test-http-80
리스너 프로토콜 및 포트	리스너 프로토콜: 이 예시에서는 HTTP를 사용합니다. 리스너 포트: 요청을 수신하고 리얼 서버로 포워딩하는 데 사용되는 포트입니다. 포트 범위: 1 - 65535. 리스너 포트는 동일한 CLB 인스턴스에서 고유해야 합니다.	HTTP:80
영구 연결 활성화	이 기능이 활성화되면 CLB와 리얼 서버 간에 영구 연결이 사용되며 CLB는 XFF에서 얻을 수 있는 소스 IP를 더 이상 통과하지 않습니다. 정상적인 포워딩을 위해서는 CLB 보안 그룹에서 기본적으로 허용 기능을 활성화하거나 CVM 보안 그룹에서 100.127.0.0/16을 허용하십시오.	비활성화

설명: 이 기능이 활성화되면 CLB와 백엔드 서비스 간의 연결 수는 연결 재사용률에 따라 [QPS, QPS*60] 범위에서 변동됩니다. 백엔드 서비스에 최대 연결 수에 대한 제한이 있는 경우 이 기능을 활성화할 때 주의하는 것이 좋습니다. 이 기능은 현재 베타 테스트 중입니다. 사용해 보려면 [티켓 제출](#)하십시오.

3.2 포워딩 규칙 생성

포워딩 규칙 구성	설명	예시
도메인 이름	<p>포워딩 도메인 이름: 길이: 1 - 80자. _ 로 시작할 수 없습니다. 정확한 와일드카드 도메인 이름이 지원됩니다. 정규식이 지원됩니다. 자세한 구성 규칙은 Layer-7 도메인 이름 포워딩 및 URL 규칙을 참고하십시오.</p>	www.example.com
기본 도메인 이름	리스너의 모든 도메인 이름이 일치하지 않으면 시스템은 요청을 기본 도메인 이름으로 보내 기본 액세스를 제어할 수 있게 합니다. 각 리스너는 하나의 기본 도메인 이름으로만 구성할 수 있습니다.	기본적으로 활성화
URL 경로	<p>포워딩 URL 경로: 길이: 1 - 200자. 정규식이 지원됩니다. 자세한 구성 규칙은 Layer-7 도메인 이름 포워딩 및 URL 규칙을 참고하십시오.</p>	/index
밸런싱 메소드	<p>HTTP 리스너의 경우 CLB는 WRR(가중 라운드 로빈), WLC(가중 최소 연결) 및 IP Hash의 세 가지 스케줄링 알고리즘을 지원합니다. WRR: 가중치에 따라 다른 리얼 서버에 요청을 순차적으로 전달합니다. 스케줄링은 새 연결 수를 기반으로 수행되며 가중치가 높은 서버는 더 많은 폴링(즉, 더 높은 확률)을 거치고 가중치가 같은 서버는 같은 수의 연결을 처리합니다. WLC: 서버에 대한 활성 연결 수에 따라 서버 로드가 예상됩니다. 스케줄링은 서버 로드 및 가중치를 기반으로 수행됩니다. 가중치가 같으면 활성 연결이 적은 서버가 더 많은 폴링을 받게 됩니다(즉, 더 높은 확률). IP Hash: Hash Key는 요청의 소스 IP를 기반으로 정적 해시 테이블에서 해당 서버를 찾는 데 사용됩니다. 서버가 사용 가능하고 오버로드되지 않은 경우 요청이 전달됩니다. 그렇지 않으면 null 값이 반환됩니다.</p>	WRR
클라이언트 IP 가져오기	기본적으로 활성화	활성화됨
Gzip 압축	기본적으로 활성화	활성화됨

3.3 상태 확인

자세한 내용은 [HTTP 상태 확인](#)을 참고하십시오.

3.4 세션 지속성

세션 지속성 구성	설명	예시
세션 지속성 스위치	세션 지속성이 활성화된 후 CLB 리스너는 동일한 클라이언트의 액세스 요청을 동일한 리얼 서버로 배포합니다. TCP 세션 지속성은 클라이언트 IP 주소를 기반으로 구현됩니다. 동일한 IP 주소의 액세스 요청은 동일한 리얼 서버로 포워딩됩니다. WRR 스케줄링에는 세션 지속성을 활성화할 수 있지만 WLC 스케줄링에는 활성화할 수 없습니다.	활성화
세션 지속 시간	세션 지속 시간 이후에 연결 내에 새로운 요청이 없으면 세션 지속성이 자동으로 비활성화됩니다. 값 범위: 30 - 3600초.	30s

2단계: 백엔드 CVM 바인딩

1. '리스너 관리' 페이지에서 생성된 리스너 `HTTP:80` 을 선택합니다. 왼쪽의 ****+****를 클릭하여 도메인 이름과 URL 경로를 확장하고 원하는 URL 경로를 선택하면 리스너 오른쪽의 경로에 바인딩된 리얼 서버를 볼 수 있습니다.
2. **바인딩**을 클릭하고 대상 리얼 서버를 선택하고 팝업 창에서 서버 포트 및 가중치를 구성합니다.

설명:

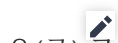
기본 포트: '기본 포트'를 먼저 입력한 후 CVM 인스턴스를 선택합니다. 모든 CVM 인스턴스의 포트는 기본 포트입니다.

3단계: 보안 그룹 구성(선택 사항)

공중망 트래픽을 격리하도록 CLB 보안 그룹을 구성할 수 있습니다. 자세한 내용은 [Configuring CLB Security Group](#)을 참고하십시오.

4단계: 리스너 수정 및 삭제(선택 사항)

생성된 리스너를 수정하거나 삭제해야 하는 경우 '리스너 관리' 페이지에서 해당 리스너를 클릭한 후



을(를) 클릭하여 수정하거나



을(를) 클릭하여 삭제합니다.

HTTPS 리스너 구성

최종 업데이트 날짜: : 2024-01-04 19:52:30

CLB 인스턴스에 대한 HTTPS 리스너를 생성하여 클라이언트의 HTTPS 요청을 포워딩할 수 있습니다. HTTPS는 데이터 전송을 암호화해야 하는 HTTP 애플리케이션에 적합합니다.

전제 조건

먼저 [CLB 인스턴스를 생성](#)해야 합니다.

작업 단계

1단계: 리스너 구성

1. [CLB 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **인스턴스 관리**를 클릭합니다.
2. CLB 인스턴스 목록 페이지의 왼쪽 상단 모서리에서 리전을 선택하고 오른쪽의 작업 열에서 **리스너 구성**을 클릭합니다.

HTTP/HTTPS 리스너에서 **생성**을 클릭하고 '리스너 생성' 팝업 창에서 HTTPS 리스너를 구성합니다.

a. 리스너 생성

구성 항목	설명	예시
이름	리스너 이름입니다.	test-https-443
리스너 프로토콜 및 포트	리스너 프로토콜: 이 예시에서는 HTTPS가 사용됩니다.리스너 포트: 요청을 수신하여 리얼 서버로 포워딩하는 데 사용되는 포트입니다. 포트 범위: 1 - 65535.	HTTPS:443
지속 연결 활성화	이 기능이 활성화되면 CLB와 리얼 서버 간에 지속 연결이 사용되며 CLB는 XFF에서 얻을 수 있는 소스 IP를 더 이상 통과하지 않습니다. 정상적인 포워딩을 위해서는 CLB 보안 그룹에서 기본적으로 허용 기능을 활성화하거나 CVM 보안 그룹에서 '100.127.0.0/16'을 허용합니다.	비활성화
SNI 활성화	SNI가 활성화된 경우 리스너의 여러 도메인 이름을 다른 인증서로 구성할 수 있습니다. 비활성화된 경우 하나의 인증서로만 리스너의 여러 도메인 이름을 구성할 수 있습니다.	비활성화
SSL 파	단방향 인증 및 양방향 인증이 지원됩니다. CLB는 액세스 보안을 보장하기 위해	단방향 인증

싱 메소드	SSL 암호화 및 복호화의 오버헤드를 인수합니다.	
서버 인증서	SSL 인증서 서비스 에서 기존 인증서를 선택하거나 인증서를 업로드할 수 있습니다.	단방향 인증

b. 포워딩 규칙 생성

포워딩 규칙 구성	설명	예시
도메인 이름	<p>포워딩 도메인 이름: 길이: 1 - 80자. 밑줄 `_`로 시작할 수 없습니다. 정확한 도메인 이름과 와일드카드 도메인 이름이 지원됩니다. 정규식이 지원됩니다. 자세한 구성 규칙은 레이어 7 도메인 이름 포워딩 및 URL 규칙을 참고하십시오.</p>	www.example.com
기본 도메인 이름	<p>리스너의 모든 도메인 이름이 일치하지 않으면 시스템은 요청을 기본 도메인 이름으로 보내 기본 액세스를 제어할 수 있게 합니다. 각 리스너는 기본 도메인 이름 하나만으로 구성할 수 있습니다.</p>	활성화
HTTP 2.0	<p>HTTP 2.0이 활성화된 후 CLB 인스턴스는 HTTP 2.0 요청을 수신할 수 있습니다. CLB 인스턴스는 클라이언트가 CLB 인스턴스에 액세스하는 데 사용하는 HTTP 버전에 관계없이 HTTP 1.1을 통해 리얼 서버에 액세스합니다.</p>	활성화
URL 경로	<p>포워딩 URL 경로: 길이: 1 - 200자. 정규식이 지원됩니다. 자세한 구성 규칙은 레이어 7 도메인 이름 포워딩 및 URL 규칙을 참고하십시오.</p>	/index
분산 방식	<p>HTTP 리스너의 경우 CLB는 WRR(가중 라운드 로빈), WLC(가중 최소 연결) 및 IP Hash의 세 가지 스케줄링 알고리즘을 지원합니다. WRR: 요청이 가중치에 따라 다른 리얼 서버에 순차적으로 전달됩니다. 스케줄링은 **새 연결 수**를 기반으로 수행됩니다. 여기서 가중치가 더 높은 서버는 더 많은 폴링(즉, 더 높은 확률)을 받는 반면 동일한 가중치를 가진 서버는 동일한 수의 연결을 처리합니다. WLC: 서버에 대한 활성 연결 수에 따라 서버 부하가 추정됩니다. 스케줄링은 서버 로드 및 가중치를 기반으로 수행됩니다. 가중치가 같으면 활성 연결이 적은 서버가 더 많은 폴링을 받게 됩니다(즉, 더 높은 확률). IP Hash: 해시 키(Hash Key)는 요청의 소스 IP를 기반으로 정적 해시 테이블에서 해당 서버를 찾는 데 사용됩니다. 서버를 사용할 수 있고 오버로드</p>	WRR

	되지 않은 경우 요청이 해당 서버로 전달됩니다. 그렇지 않으면 null 값이 반환됩니다.	
백엔드 프로토콜	백엔드 프로토콜은 CLB 인스턴스와 리얼 서버 사이에 배포됩니다. .백엔드 프로토콜로 HTTP를 선택한 경우 리얼 서버에 HTTP 서비스를 배포해야 합니다. 백엔드 프로토콜로 HTTPS를 선택한 경우 리얼 서버에 HTTPS 서비스를 배포해야 하며 HTTPS 서비스의 암호화 및 암호 해독은 리얼 서버에서 더 많은 리소스를 소모합니다.	HTTP
클라이언트 IP 가져오기	기본적으로 활성화	활성화됨
Gzip 압축	기본적으로 활성화	활성화됨

c. 상태 확인 자세한 내용은 [HTTP 상태 확인](#)을 참고하십시오.

b. 세션 지속성

세션 지속성 구성	설명	예시
세션 지속성 스위치	세션 지속성이 활성화되면 CLB 리스너는 동일한 클라이언트에서 동일한 리얼 서버로 액세스 요청을 분산합니다. TCP 세션 지속성은 클라이언트 IP 주소를 기반으로 구현됩니다. 동일한 IP 주소의 액세스 요청은 동일한 리얼 서버로 포워딩됩니다. 세션 지속성은 WRR 스케줄링에 대해 활성화할 수 있지만 WLC 스케줄링에는 활성화할 수 없습니다.	활성화
세션 지속 시간	세션 지속 기간을 초과하여 연결 내에서 새 요청이 없으면 세션 지속이 자동으로 비활성화됩니다. 값 범위: 30 - 3600초.	30s

2단계: 리얼 서버 바인딩

1. '리스너 관리' 페이지에서 생성된 리스너 `HTTP:443` 을 선택합니다. 왼쪽의 **+**를 클릭하여 도메인 이름과 URL 경로를 확장하고 원하는 URL 경로를 선택하면 리스너 오른쪽의 경로에 바인딩된 리얼 서버를 볼 수 있습니다.

2. **바인딩**을 클릭하고 대상 리얼 서버를 선택하고 팝업 창에서 서버 포트 및 가중치를 구성합니다.

설명 :

기본 포트: '기본 포트'를 먼저 입력한 다음 CVM 인스턴스를 선택합니다. 모든 CVM 인스턴스의 포트는 기본 포트입니다.

3단계: 보안 그룹 구성(선택 사항)

공중망 트래픽을 격리하도록 CLB 보안 그룹을 구성할 수 있습니다. 자세한 내용은 [Configuring CLB Security Group](#)을 참고하십시오.

4단계: 리스너 수정 및 삭제(선택 사항)

생성된 리스너를 수정하거나 삭제해야 하는 경우 '리스너 관리' 페이지에서 리스너를 클릭한 후

 수정 또는

 삭제를 클릭합니다.

로드 밸런싱 메소드

최종 업데이트 날짜: : 2024-01-04 19:52:43

부하 분산 방식은 [Real Server](#)에 트래픽을 할당하는 알고리즘입니다. 각 방법은 서로 다른 부하 분산 효과를 생성합니다.

가중 라운드 로빈 스케줄링

가중 라운드 로빈 스케줄링(Weighted Round-Robin Scheduling) 알고리즘은 풀링을 기반으로 다른 서버에 대한 요청을 스케줄링하는 것입니다. 다른 서버의 불균형 성능 문제를 해결할 수 있습니다. 가중치를 사용하여 서버의 처리 성능을 나타내고 풀링 방식으로 가중치별로 다른 서버에 대한 요청을 스케줄링합니다. 새로운 연결 수를 기반으로 서버를 스케줄링합니다. 여기서 가중치가 더 높은 서버가 더 일찍 연결을 수신하고 풀링할 가능성이 더 높습니다. 동일한 가중치를 가진 서버는 동일한 수의 연결을 처리합니다.

장점: 이 알고리즘은 단순성과 높은 실용성을 특징으로 합니다. 모든 연결의 상태를 기록할 필요가 없으므로 상태 비저장 스케줄링 알고리즘입니다.

단점: 이 알고리즘은 비교적 단순하여 요청의 서비스 시간이 크게 변경되거나 각 요청에 다른 시간을 소비해야 하는 상황에는 적합하지 않습니다. 이러한 경우 서버 간에 부하 분산이 불균형하게 발생합니다.

적용 가능한 시나리오: 이 알고리즘은 각 요청이 기본적으로 최고의 로드 성능으로 백엔드에서 동일한 시간을 소비하는 시나리오에 적합합니다. 일반적으로 HTTP 서비스와 같은 비지속 연결 서비스에서 사용됩니다.

권장 사항: 각 요청이 기본적으로 백엔드에서 동일한 시간을 소비한다는 것을 알고 있는 경우(예시: 리얼 서버에서 처리되는 요청이 동일한 유형 또는 유사한 유형임) 가중 라운드 로빈 스케줄링을 사용하는 것이 좋습니다. 각 요청 간의 시간 차이가 작은 경우, 이 알고리즘도 순회가 필요 없고, 효율성이 높으므로 권장됩니다.

가중 최소 연결 스케줄링

실제 상황에서는 클라이언트의 요청이 서버에 머무르는 데 소요되는 시간이 크게 다를 수 있습니다. 작업 시간이 길어질수록 단순 라운드 로빈 또는 랜덤 로드 밸런싱 알고리즘을 사용하면 각 서버의 연결 프로세스 수가 크게 달라져 로드 밸런싱 효과를 얻을 수 없습니다.

라운드 로빈 스케줄링과 달리 최소 연결 스케줄링은 활성 연결 수량으로 서버의 부하를 추정하는 동적 스케줄링 알고리즘입니다. 스케줄러는 각 서버에 현재 설정된 연결 수를 기록해야 합니다. 서버에 대한 요청이 스케줄링된 경우 연결 수는 1 증가합니다. 연결이 중지되거나 시간 초과되면 연결 수는 1 감소합니다.

최소 연결 스케줄링에 기반한 가중 최소 연결 스케줄링(Weighted Least-Connection Scheduling) 알고리즘에서는 서버의 처리 능력에 따라 서로 다른 가중치를 할당합니다. 이러한 방식으로 서버는 가중치에 따라 해당 수의 요청을 수신할 수 있으며, 이는 최소 연결 스케줄링의 개선입니다.

설명 :

리얼 서버의 가중치는 w_i 이고 현재 연결 수는 c_i 라고 가정합니다. 각 서버의 c_i/w_i 값은 순서대로 계산됩니다. c_i/w_i 값이 가장 작은 리얼 서버는 새 요청을 받는 다음 서버가 됩니다. 동일한 c_i/w_i 값을 가진 리얼 서버가 있는 경우 가중치 라운드 로빈 스케줄링을 기반으로 스케줄링됩니다.

장점: 이 알고리즘은 FTP와 같이 오랜 시간 처리가 필요한 요청에 적합합니다.

단점: API 제한으로 인해 최소 연결과 세션 지속성을 동시에 활성화할 수 없습니다.

적용 가능한 시나리오: 이 알고리즘은 백엔드에서 각 요청에 사용되는 시간이 크게 달라지는 시나리오에 적합합니다. 일반적으로 지속적 연결 서비스에 사용됩니다.

권장 사항: 다른 요청을 처리해야 하고 백엔드에서 필요한 서비스 시간이 크게 다른 경우(예시: 3ms 및 3s) 부하 분산을 달성하기 위해 가장 최소 연결 스케줄링을 사용하는 것이 좋습니다.

소스 해싱 스케줄링

소스 해싱 스케줄링 알고리즘(`ip_hash`)은 요청의 소스 IP 주소를 해시 키로 사용하고 정적으로 할당된 해시 테이블에서 해당 서버를 찾습니다. 사용 가능하고 오버로드되지 않은 경우 요청이 이 서버로 전송됩니다. 그렇지 않으면 null이 반환됩니다.

장점: `ip_hash`는 클라이언트의 요청을 해시 테이블을 통해 동일한 리얼 서버에 매핑할 수 있습니다. 따라서 세션 지속성이 지원되지 않는 시나리오에서는 간단한 세션 지속성 효과를 얻기 위해 사용할 수 있습니다.

권장 사항: 이 알고리즘은 요청 소스 주소의 해시 값을 계산하고 가중치를 기반으로 일치하는 리얼 서버에 요청을 배포합니다. 이러한 방식으로 동일한 클라이언트 IP의 모든 요청을 동일한 서버에 배포할 수 있습니다. 이 알고리즘은 Cookie를 지원하지 않는 프로토콜에 적합합니다.

부하 분산 알고리즘 선택 및 가중치 구성

리얼 서버 클러스터가 다양한 시나리오에서 안정적으로 비즈니스를 수행할 수 있도록 로드 밸런싱 알고리즘을 선택하고 가중치를 구성하는 방법에 대한 몇 가지 사례가 아래에 참고용으로 제공됩니다.

시나리오1:

1.1 동일한 구성(CPU/메모리)을 가진 3개의 리얼 서버가 있고 동일한 성능을 가지므로 모든 가중치를 10으로 설정했다고 가정합니다.

1.2 각각의 리얼 서버와 클라이언트 사이에 100개의 TCP 연결이 설정되고 새로운 리얼 서버가 추가됩니다.

1.3 이 시나리오에서는 4번째 리얼 서버의 부하를 빠르게 증가시키고 나머지 3개 서버에 대한 압력을 줄일 수 있는 최소 연결 스케줄링 알고리즘을 사용하는 것이 좋습니다.

시나리오2:

1.1 Tencent Cloud 서비스를 처음 사용하고 웹사이트가 방금 낮은 부하로 구축되었다고 가정합니다. 모두 동일한 액세스 레이어 서버이므로 동일한 구성의 리얼 서버를 구입하는 것이 좋습니다.

1.2 이 시나리오에서는 모든 리얼 서버의 가중치를 기본값인 10으로 설정하고 가중치 기반 라운드 로빈 스케줄링 알고리즘을 사용하여 트래픽을 분산할 수 있습니다.

시나리오3:

1.1 정적 페이지에 대한 단순 액세스 요청을 수행하는 5개의 리얼 서버가 있고 이러한 서버의 컴퓨팅 성능(CPU 및 메모리로 계산) 비율이 9:3:3:3:1이라고 가정합니다.

1.2 이 시나리오에서는 리얼 서버의 가중치를 각각 90, 30, 30, 30, 10으로 설정할 수 있습니다. 정적 웹 페이지에 대한 대부분의 액세스 요청은 비지속적 연결 유형이므로 가중 라운드 로빈 스케줄링 알고리즘을 사용하여 CLB 인스턴스가 서버의 성능 비율에 따라 요청을 할당할 수 있습니다.

시나리오4:

1.1 10개의 리얼 서버가 방대한 양의 Web 액세스 요청을 처리하며 추가 서버를 구입하지 않을 경우 지출이 증가하고 서버 중 하나가 과부하로 인해 다시 시작되는 경우가 종종 있다고 가정합니다.

1.2 이 시나리오에서는 기존 서버의 성능에 따라 가중치를 설정하고 부하가 높은 서버에 상대적으로 작은 가중치를 설정하는 것이 좋습니다. 또한 서버 과부하를 피하기 위해 최소 연결 스케줄링 알고리즘을 사용하여 활성 연결이 적은 리얼 서버에 요청을 할당할 수 있습니다.

시나리오5:

1.1 일부 지속적 연결을 처리하기 위해 3개의 리얼 서버가 있다고 가정하고 이러한 서버의 컴퓨팅 성능 비율(CPU 및 메모리로 계산)은 3:1:1입니다.

1.2 성능이 가장 좋은 서버는 더 많은 요청을 처리하지만 과부하를 원하지 않고 유휴 서버에 새 요청을 할당하려고 합니다.

1.3 이 시나리오에서는 최소 연결 스케줄링 알고리즘을 사용하고 사용량이 많은 서버의 가중치를 적절하게 줄여 CLB 인스턴스가 활성 연결이 적은 리얼 서버에 요청을 할당하여 로드 밸런싱을 구현할 수 있습니다.

시나리오6:

1.1 클라이언트의 후속 요청이 동일한 서버에 할당되기를 원한다고 가정합니다. 가중 라운드 로빈 또는 가중 최소 연결 스케줄링은 동일한 클라이언트의 요청이 동일한 서버에 할당되도록 보장할 수 없습니다.

1.2 특정 응용 프로그램 서버의 요구 사항을 충족하고 클라이언트 세션의 '고정성'(또는 '연속성')을 유지하려면 ip_hash를 사용하여 트래픽을 분산할 수 있습니다. 이 알고리즘은 서버 수가 변경되거나 서버를 사용할 수 없게 되지 않는 한 동일한 클라이언트의 모든 요청이 동일한 리얼 서버에 배포되도록 할 수 있습니다.

세션 지속성

최종 업데이트 날짜: : 2024-01-04 19:52:57

세션 지속성은 동일한 IP에서 동일한 리얼 서버로 요청을 포워딩할 수 있습니다. 기본적으로 CLB 인스턴스는 로드 밸런싱을 위해 요청을 다른 리얼 서버로 라우팅합니다. 그러나 세션 지속성을 사용하여 지정된 사용자의 요청을 동일한 리얼 서버로 라우팅할 수 있으므로 세션을 유지해야 하는 일부 애플리케이션(예시: 장바구니)이 제대로 실행될 수 있습니다.

레이어 4 세션 지속성

레이어 4 프로토콜(TCP/UDP)은 소스 IP 기반 세션 지속성을 지원합니다. 세션 지속 기간은 30 - 3600초 사이의 정수로 설정할 수 있습니다. 시간 임계값이 초과되고 세션에 새 요청이 없으면 세션 지속성이 종료됩니다. 세션 지속성은 로드 밸런싱 모드의 영향을 받습니다.

리얼 서버의 가중치를 기반으로 요청을 분산하는 '가중 라운드 로빈' 모드에서는 소스 IP 기반 세션 지속성을 지원합니다.

전체 스케줄링이 서버 부하와 가중치에 따라 달라지는 '가중 최소 연결' 모드에서는 세션 지속성이 지원되지 않습니다.

레이어 7 세션 지속성

레이어 7 프로토콜(HTTP/HTTPS)은 Cookie 삽입을 기반으로 세션 지속성을 지원합니다(CLB는 Cookie를 클라이언트에 삽입). 세션 지속 기간은 30 - 3600초 사이의 값으로 설정할 수 있습니다. 세션 지속성은 로드 밸런싱 모드의 영향을 받습니다.

리얼 서버의 가중치를 기반으로 요청을 분산하는 '가중 라운드 로빈' 모드에서는 Cookie 삽입을 기반으로 하는 세션 지속성을 지원합니다.

전체 스케줄링이 서버 부하와 가중치에 따라 달라지는 '가중 최소 연결' 모드에서는 세션 지속성이 지원되지 않습니다.

'IP Hash' 모드는 소스 IP를 기반으로 세션 지속성을 지원하지만 Cookie 삽입에는 지원하지 않습니다.

연결 제한 시간

현재 HTTP 연결 제한 시간(keepalive_timeout)은 기본적으로 75초입니다. 조정하려면 [Custom Configuration](#)을 활성화하십시오. 임계값을 초과하고 세션에 데이터 전송이 없으면 연결이 끊어집니다.

현재 TCP 연결 제한 시간은 기본적으로 900초이며 사용자 지정할 수 없습니다. 임계값을 초과하고 세션에 데이터 전송이 없으면 연결이 끊어집니다.

세션 지속성 구성

1. **CLB 콘솔**에 로그인하고 세션 지속성을 구성할 CLB 인스턴스의 ID를 클릭하여 세부 정보 페이지로 이동합니다.
2. [리스너 관리] 탭을 선택합니다.
3. 세션 지속성으로 구성할 CLB 리스너 다음에 [수정]을 클릭합니다.
4. 세션 지속성 기능 활성화 여부를 선택합니다. 버튼을 클릭하여 활성화하고 지속 시간을 입력한 다음 [확인]을 클릭합니다.

지속 연결과 세션 지속성의 관계

시나리오1: HTTP 레이어 7 비즈니스

Client가 HTTP/1.1 프로토콜에 액세스하고 헤더 정보에 **Connection:keep-alive**가 구성되어 있다고 가정합니다. 클라이언트는 세션 지속성을 활성화하지 않고 CLB 인스턴스를 통해 CVM에 액세스합니다. 클라이언트가 다음에 동일한 CVM에 액세스할 수 있습니까?

A: 아니오.

첫째, HTTP keep-alive는 요청이 전송된 후에도 TCP 연결이 연결된 상태를 유지하므로 브라우저가 동일한 연결을 통해 요청을 보낼 수 있음을 나타냅니다. 지속 연결은 각 요청에 대해 새 연결을 설정하는 데 필요한 시간을 줄이고 대역폭 소비를 줄입니다. CLB 클러스터의 기본 타임 아웃 시간은 75초입니다(75초 이내에 새 요청이 없으면 기본적으로 TCP 연결이 끊어집니다).

HTTP keep-alive는 Client와 CLB 인스턴스 간에 설정됩니다. Cookie 세션 지속성이 비활성화된 경우 CLB 인스턴스는 폴링 정책에 따라 CVM 인스턴스를 무작위로 선택합니다. 이전 지속 연결은 더 이상 유효하지 않습니다.

따라서 세션 지속성을 활성화하는 것이 좋습니다.

Cookie 세션 지속 기간이 1000초로 구성된 경우 Client는 다시 요청을 시작합니다. 두 요청 사이의 간격이 75초를 초과하므로 TCP 연결을 다시 설정해야 합니다. 애플리케이션 레이어는 Cookie를 식별하고 Client가 마지막으로 액세스한 CVM 인스턴스를 찾아 이번에는 다시 평가됩니다.

시나리오2: TCP 레이어 4 비즈니스

Client가 액세스를 시작하고 TCP가 전송 레이어 프로토콜이며 지속 연결이 활성화되어 있지만 소스 IP를 기반으로 하는 세션 지속성이 비활성화되어 있는 경우, 동일한 Client가 다음 액세스 요청에서 동일한 서버에 액세스할 수 있습니까?

A: 반드시 그렇지는 않습니다.

첫 번째, 레이어 4 구현 메커니즘에 따르면 TCP에 대해 지속 연결이 활성화되고 닫히지 않고 두 요청에서 동일한 연결에 액세스되면 동일한 클라이언트가 동일한 서버에 액세스할 수 있습니다. 두 번째 액세스 요청 중에 어떤 이유로(예시: 네트워크 재시작 또는 연결 시간 초과) 연결이 닫히면 요청이 다른 실제 서버로 스케줄링될 수 있습니다. 지속 연결의 기본 전역 제한 시간은 900초입니다. 즉, 900초 동안 새 요청이 없으면 지속 연결이 릴리스됩니다.

레이어 7 리디렉션 구성

최종 업데이트 날짜: : 2024-01-04 19:53:11

CLB는 레이어 7 리디렉션을 지원하므로 레이어 7 HTTP/HTTPS 리스너에서 리디렉션을 구성할 수 있습니다.

설명 :

세션 지속성: 클라이언트가 `example.com/bbs/test/123.html` 에 액세스하고 백엔드 CVM에서 세션 지속성이 활성화된 경우 `example.com/bbs/test/456.html` 로 트래픽을 포워딩하기 위해 리디렉션이 활성화된 후 원래 세션 지속성 메커니즘이 적용되지 않습니다.

TCP / UDP 리디렉션: IP + Port 수준의 리디렉션은 현재 지원되지 않지만 이후 버전에서 사용할 수 있습니다.

리디렉션 개요

자동 리디렉션

개요

기존 `HTTPS:443` 리스너의 경우 포워딩을 위해 시스템에서 HTTP 리스너(포트 80)를 자동으로 생성합니다.

`HTTP:80` 으로 전송된 요청은 자동으로 `HTTPS:443` 으로 리디렉션됩니다.

사용 사례

강제 HTTPS 리디렉션, 즉 HTTP 요청을 HTTPS로 리디렉션합니다. 사용자가 HTTP를 통해 PC 또는 모바일 브라우저에서 Web 서비스에 액세스하면 CLB는 포워딩을 위해 `HTTP:80` 으로 전송된 모든 요청을 `HTTPS:443` 으로 리디렉션합니다.

강점

Set-and-Forget 구성: 하나의 구성 작업만 필요하면 도메인 이름에 대해 강제 HTTPS 리디렉션을 구현할 수 있습니다.
편리한 업데이트: HTTPS 서비스의 URL 수가 변경되면 이 기능을 콘솔에서 다시 사용하여 새로고침하기만 하면 됩니다.

수동 리디렉션

개요

일대일 리디렉션을 구성할 수 있습니다. 예를 들어 CLB 인스턴스에서 `리스너1 / 도메인 이름1 / URL1` 을 `리스너2 / 도메인 이름2 / URL2` 로 리디렉션을 구성할 수 있습니다.

설명 :

도메인 이름이 자동 리디렉션으로 구성된 경우 수동 리디렉션을 구성할 수 없습니다.

사용 사례

단일 경로 리디렉션. 예를 들어, 제품 품질, 페이지 유지보수, 업데이트 및 업그레이드 등의 경우 Web 비즈니스를 일시적으로 비활성화하려면 원래 페이지를 새 페이지로 리디렉션해야 합니다. 리디렉션이 수행되지 않으면 방문자의 즐겨찾기 및 검색 엔진 데이터베이스의 이전 주소가 `404/503` 오류 메시지 페이지를 반환하여 사용자 경험을 저하시키고 트래픽 낭비를 초래합니다.

자동 리디렉션

CLB는 HTTP에서 HTTPS로의 원클릭 강제 리디렉션을 지원합니다.

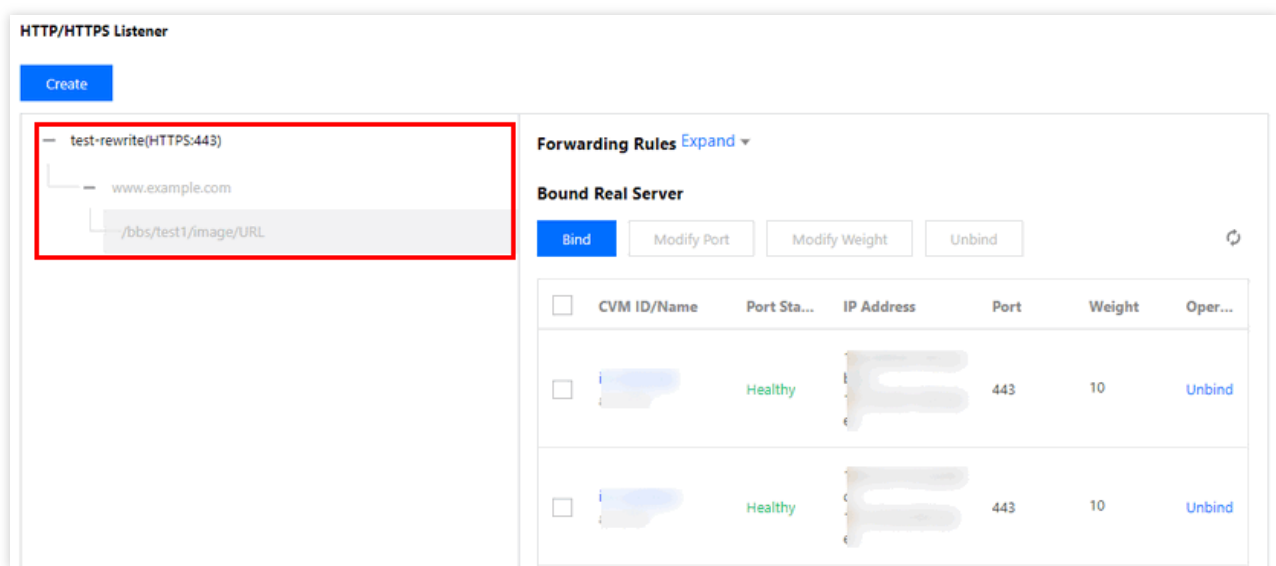
웹 사이트 `https://www.example.com` 을 구성해야 한다고 가정합니다. 최종 사용자가 브라우저에서 HTTP 요청(`http://www.example.com`)을 보내든 HTTPS 요청(`https://www.example.com`)을 보내든 상관없이 HTTPS를 통해 안전하게 방문할 수 있습니다.

전제 조건

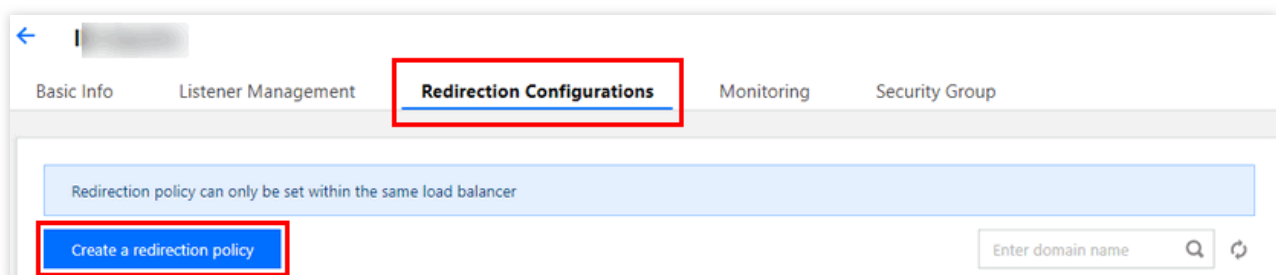
HTTPS:443 리스너가 구성되었습니다.

작업 단계

1. CLB 콘솔에서 CLB HTTPS 리스너를 구성하고 `https://example.com` 의 Web 환경을 설정합니다. 자세한 내용은 [Configuring HTTPS Listener](#)를 참고하십시오.
2. HTTPS 리스너 구성 결과는 아래와 같습니다.



3. CLB 인스턴스 세부 정보의 '리디렉션 구성' 탭에서 리디렉션 정책 생성을 클릭합니다.



4. 자동 리디렉션 구성을 선택하고 구성된 HTTPS 리스너 및 도메인 이름을 선택한 후 다음: 경로 구성을 클릭합니다.

New redirection policy

1 Select domain name > 2 Configure Directory

☐ Manual Redirection Configuration

If you configure the original address and redirection address manually, the system will redirect the requests from the original address to the related target address. You can configure multiple directories for one domain name for redirection, so as to implement auto-redirection between HTTP/HTTPS.

☒ Auto-redirection Configuration

For the existing HTTPS:443 listener, an HTTP listener (port 80) is created by the system for forwarding. Requests sent to HTTP:80 will be redirected to HTTPS:443.

Front-end protocol and port: HTTPS:443 Domain Name: www.example.com

Next: Configure directory

5. 제출을 클릭합니다.

New redirection policy

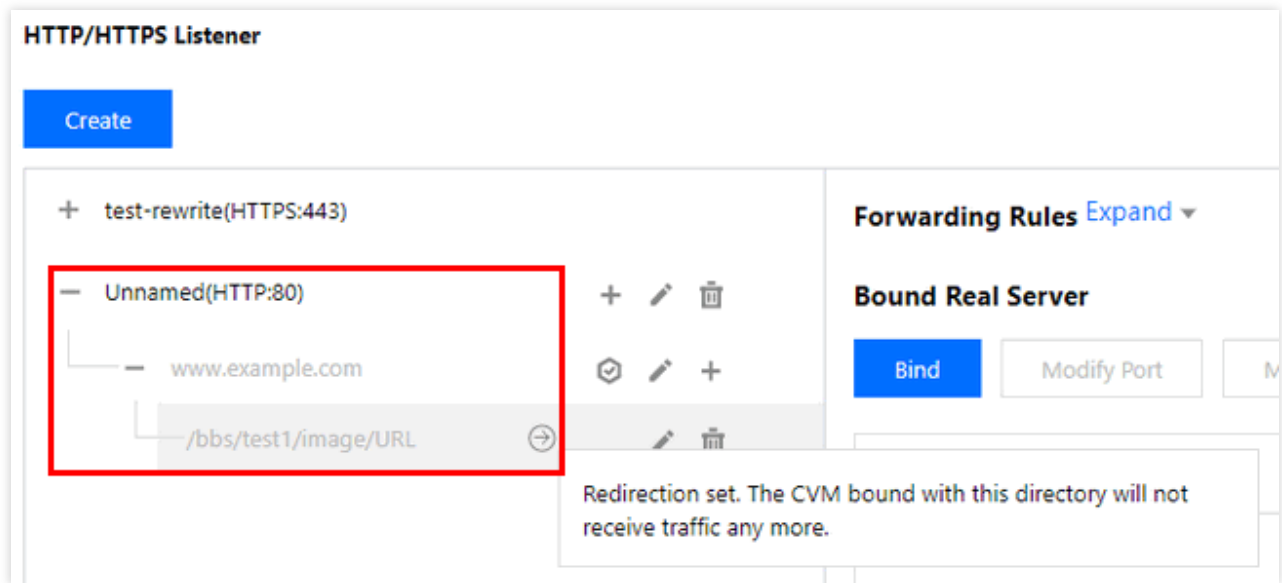
1 Select domain name > 2 Configure Directory

You've set 1 redirection policies

Original Path	Redirect to a path
/bbs/test1/image/URL	/bbs/test1/image/URL

Back: Select domain name Submit

6. 리디렉션을 구성한 후의 결과는 다음과 같습니다. HTTP:80 리스너는 HTTPS:443 수신기에 대해 자동으로 구성되었으며 모든 HTTP 트래픽은 자동으로 HTTPS로 리디렉션됩니다.



수동 리디렉션

CLB는 일대일 리디렉션 구성을 지원합니다.

예를 들어, 귀하의 비즈니스는 프로모션 캠페인에 `forsale` 페이지를 사용하고 캠페인 종료 후 캠페인 페이지 `https://www.example.com/forsale` 을 새 홈페이지 `https://www.new.com/index` 로 리디렉션해야 합니다.

전제 조건

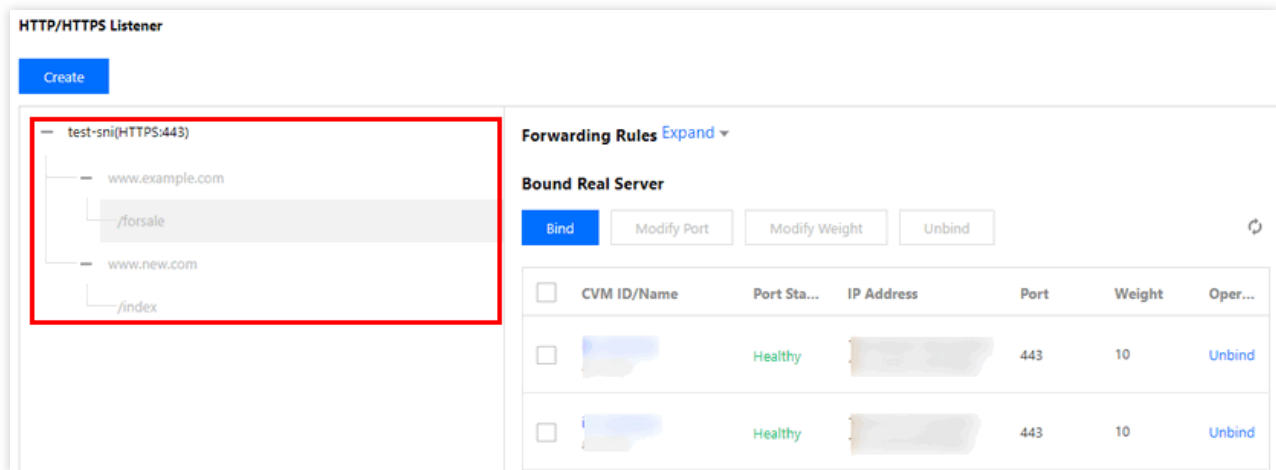
HTTPS 리스너가 구성되어 있어야 합니다.

포워딩 도메인 이름 `https://www.example.com/forsale` 이 구성되어 있어야 합니다.

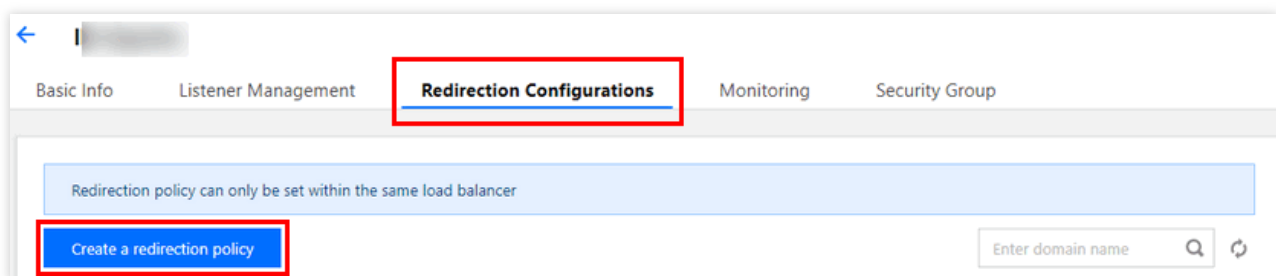
포워딩 도메인 이름 및 경로 `https://www.new.com/index` 가 구성되어 있어야 합니다.

작업 단계

1. CLB 콘솔에서 CLB HTTPS 리스너를 구성하고 `https://example.com` 의 Web 환경을 설정합니다. 자세한 내용은 [Configuring HTTPS Listener](#)를 참고하십시오.
2. HTTPS 구성의 결과는 다음과 같습니다.



3. CLB 인스턴스 세부 정보의 '리디렉션 구성' 탭에서 리디렉션 정책 생성을 클릭합니다.



4. 수동 리디렉션 구성을 선택하고, 원래 액세스한 프론트엔드 프로토콜 포트 `HTTPS:443` 및 도메인 이름 `https://www.example.com/forsale` 을 선택하고, 리디렉션 후 프론트엔드 프로토콜 포트 `HTTPS:443` 및 도메인 이름 `https://www.new.com/index` 를 선택하고, 다음: 경로 구성을 클릭합니다.

← New redirection policy

1 Select domain name > 2 Configure Directory

☒ Manual Redirection Configuration

If you configure the original address and redirection address manually, the system will redirect the requests from the original address to the related target address. You can configure multiple directories for one domain name for redirection, so as to implement auto-redirection between HTTP/HTTPS.

Original Access

Front-end protocol and port: HTTPS:443 Domain Name: www.example.com

Redirect to

Front-end protocol and port: HTTPS:443 Domain Name: www.new.com

☐ Auto-redirection Configuration

For the existing HTTPS:443 listener, an HTTP listener (port 80) is created by the system for forwarding. Requests sent to HTTP:80 will be redirected to HTTPS:443.

Next: Configure directory

5. 원래 액세스 경로로 `/forsale` 을 선택하고 리디렉션 후 액세스 경로로 `/index` 를 선택하고 **제출**을 클릭하여 구성을 완료합니다.

← New redirection policy

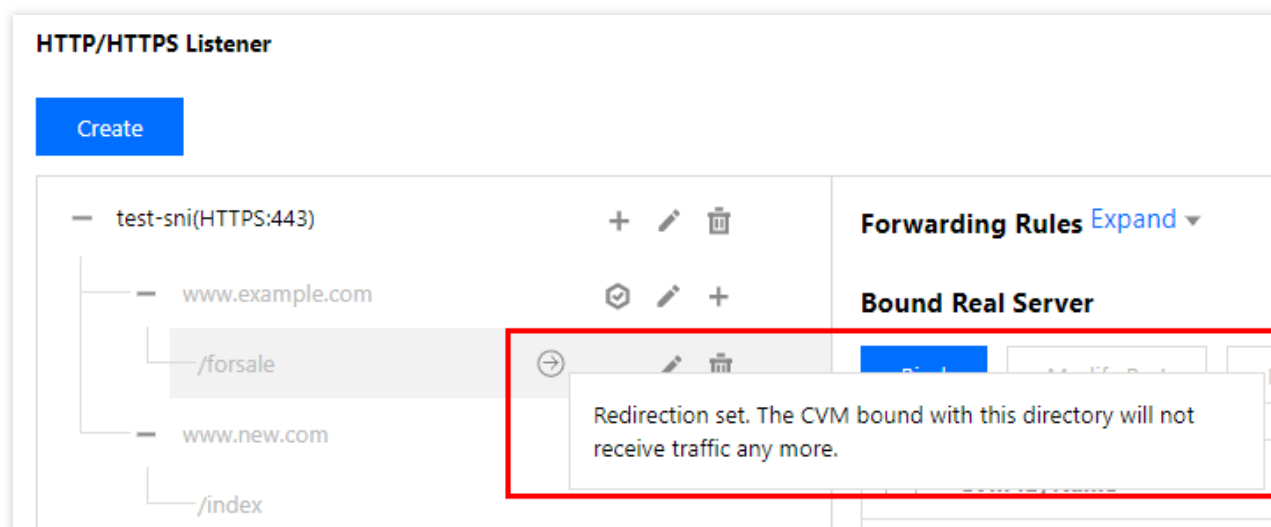
✓ Select domain name > 2 Configure Directory

Original Path	Redirect to a path①	Operation
/forsale	/index	Delete

+ New Redirection Policy

Back: Select domain name Submit

6. 리디렉션 구성의 결과는 다음과 같습니다. HTTP:443 리스너에서 `https://www.example.com/forsale` 이 `https://www.new.com/index` 로 리디렉션되었습니다.



레이어 7 사용자 정의 구성

최종 업데이트 날짜: : 2024-01-29 15:56:19

CLB는 사용자 지정 구성을 지원하므로 `client_max_body_size` 및 `ssl_protocols`와 같은 단일 CLB 인스턴스에 대한 구성 매개변수를 설정하여 고유한 요구 사항을 충족할 수 있습니다.

설명 :

각 리전에는 최대 200개의 사용자 지정 구성 항목이 있을 수 있습니다.

사용자 지정 구성은 64k 바이트로 제한됩니다.

각 인스턴스는 사용자 지정 구성의 하나의 항목에만 바인딩될 수 있습니다.

사용자 지정 구성은 레이어 7 HTTP/HTTPS CLB(이전 '애플리케이션 CLB') 리스너에만 유효합니다.

CLB 사용자 지정 구성 매개변수

CLB 사용자 지정 구성은 다음 구성을 지원합니다.

구성	기본값/권장값	매개변수 범위	설명
<code>ssl_protocols</code>	기본값: TLSv1, TLSv1.1, TLSv1.2 권장값: TLSv1.2, TLSv1.3	TLSv1, TLSv1 .1, TLSv1.2, TLSv1.3	사용된 TLS 프로토콜 버전
<code>ssl_ciphers</code>	ssl_ciphers 기본값	ssl_ciphers 매개변수 범위	암호 제품군.
<code>client_header_timeout</code>	60s	[30-120]s	Client 요청 헤더를 가져오는 타임아웃 시간. 타임아웃의 경우 408 오류가 반환됩니다.
<code>client_header_buffer_size</code>	4k	[1-256]k	Client 요청 헤더가 저장되는 기본 Buffer의 크기입니다.
<code>client_body_timeout</code>	60s	[30-120]s	Client 요청 Body 획득의 타임아웃 시간은, 전체 Body를 획득하는 시간이 아니라 데이터 전송이 없는 유ힴ 기간을 나타냅니다. 타임아웃의 경우 408 오류가 반환됩니다.

client_max_body_size	60M	[1-10240]M	기본값: 1M-256M. 최대 크기: 10240M (10GB). client_max_body_size가 256M보다 크면 proxy_request_buffering 값이 off여야 합니다.
keepalive_timeout	75s	[0-900]s	Client-Server 지속 연결 유지 시간, 0으로 설정하면 지속 연결이 금지됩니다. 900s 이상으로 설정하시려면 티켓을 제출 하십시오. 설정할 수 있는 최대값은 3600s입니다.
add_header	사용자 지정	-	add_header xxx yyy 형식으로 클라이언트에 반환되는 특정 헤더 필드입니다. 예를 들어 크로스 도메인 시나리오의 경우: <code>add_header Access-Control-Allow-Methods 'POST, OPTIONS';</code> <code>add_header Access-Control-Allow-Origin *;</code> 으로 구성할 수 있습니다.
more_set_headers	사용자 지정	-	more_set_headers "A:B"형식으로 클라이언트에 반환되는 특정 헤더 필드입니다.
proxy_connect_timeout	4s	[4-120]s	upstream 백엔드 연결의 타임아웃 시간입니다.
proxy_read_timeout	60s	[30-3600]s	upstream 백엔드 응답을 읽는 타임아웃 시간입니다.
proxy_send_timeout	60s	[30-3600]s	upstream 백엔드에 요청을 보내는 타임아웃 시간입니다.
server_tokens	on	on, off	on: 버전 정보를 표시합니다. off: 버전 정보를 숨깁니다.
keepalive_requests	100	[1-10000]	Client-Server 지속 연결을 통해 보낼 수 있는 최대 요청 수입니다.
proxy_buffer_size	4k	[1-32]k	기본적으로 proxy_buffer에 설정된 단일 버퍼의 크기인 Server 응답 헤더의 크기입니다. proxy_buffer_size를 사용하려면 proxy_buffers가 동시에 설정되어야 합니다.

proxy_buffers	8 4k	[3-8] [4-16]k	버퍼 수량 및 크기.
proxy_request_buffering	off	on, off	<p>on: 클라이언트 요청 본문을 캐시합니다. CLB 인스턴스는 요청을 캐시하고 요청이 완전히 수신된 후 여러 부분에서 이를 백엔드 CVM 인스턴스로 포워딩합니다.</p> <p>off: 클라이언트 요청 본문을 캐시하지 않습니다. 요청을 수신한 후 CLB 인스턴스는 이를 백엔드 CVM 인스턴스로 직접 포워딩하여 백엔드 CVM 성능에 대한 부담을 높입니다.</p>
proxy_set_header	X-Real-Port \$remote_port	X-Real-Port \$remote_port X-clb-stgw-vip \$server_addr Stgw-request-id \$stgw_request_id X-Forwarded-Port \$vport X-Method \$request_method X-Uri \$uri	<p>X-Real-Port \$remote_port 클라이언트 포트.</p> <p>X-clb-stgw-vip \$server_addr CLB VIP.</p> <p>Stgw-request-id \$stgw_request_id 요청 ID(CLB에서만 사용됨).</p> <p>X-Forwarded-Port CLB 리스너 포트.</p> <p>X-Method 클라이언트 요청 메소드.</p> <p>X-Uri 클라이언트 요청 URI.</p>
send_timeout	60s	[1-3600]s	서버에서 클라이언트로의 데이터 전송 타임아웃 시간으로, 전체 요청 전송 시간이 아니라 두 개의 연속 데이터 전송 작업 사이의 시간 간격입니다.
ssl_verify_depth	1	[1, 10]	클라이언트 인증서 체인의 검증 Depth입니다.
proxy_redirect	http:// https://	http:// https://	업스트림 서버가 리디렉션 또는 새로 고침 요청(코드 301 또는 302)을 반환하면 proxy_redirect는 안전한 리디렉션을 위해 HTTP 헤더의 Location 또는 Refresh 필드에서 http를 https로 재설정합니다.
ssl_early_data	off	on, off	<p>TLS 1.3 0-RTT를 활성화하거나 비활성화합니다. ssl_protocols의 필드 값에 TLSv1.3이 포함된 경우에만 ssl_early_data가 적용됩니다.</p> <p>ssl_early_data를 활성화하기 전에</p>

			리플레이 공격의 위험을 고려해야 합니다.
http2_max_field_size	4k	[1-256]k	HPACK으로 압축된 요청 헤더의 최대 크기(Size)를 제한합니다.
proxy_intercept_errors	off	on, off	error_page를 구성하려면 반드시 사전에 proxy_intercept_errors를 on으로 설정해야 합니다.
error_page	-	error_page code [= [response]] uri	특정 오류 코드(Code)에 대해 미리 정의된 URI가 표시됩니다. 기본 응답(Response) 코드의 기본값은 302입니다. URI는 / 로 시작해야 합니다.error_page를 구성하려면 반드시 사전에 proxy_intercept_errors를 on으로 설정해야 합니다.
proxy_ignore_client_abort	off	on, off	클라이언트가 응답을 기다리지 않고 CLB 인스턴스와 연결을 끊는 경우 실제 서버와 CLB 인스턴스를 연결하거나 연결을 끊습니다.

설명 :

proxy_buffer_size 및 proxy_buffers 값에 대한 요구 사항: $2 * \max(\text{proxy_buffer_size}, \text{proxy_buffers.size})$

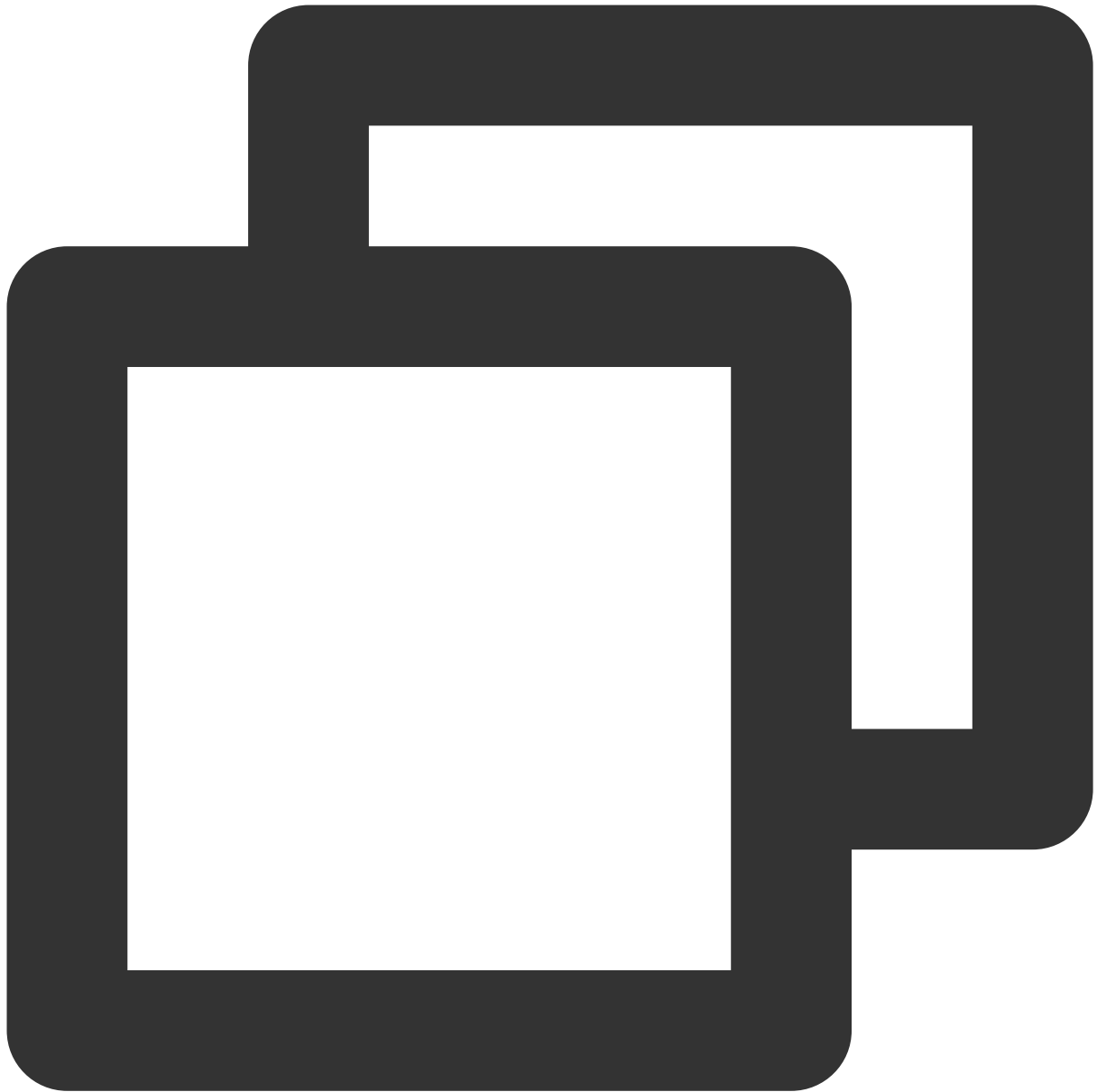
$\leq (\text{proxy_buffers.num} - 1) * \text{proxy_buffers.size}$. 예를 들어 proxy_buffer_size가 24k이면 proxy_buffers는 8 8k입니다. $2 * 24k = 48k$, $(8 - 1) * 8k = 56k$ 및 $48k \leq 56k$ 이므로 구성 오류가 없습니다.

ssl_ciphers 구성 설명

구성 중인 ssl_ciphers 암호화 제품군은 OpenSSL에서 사용하는 것과 동일한 형식이어야 합니다. 알고리즘 목록은 하나 이상의 <cipher strings> 입니다. 여러 알고리즘은 ':'로 구분해야 합니다. ALL은 모든 알고리즘을 나타냅니다. '!'는 알고리즘을 활성화하지 않음을 나타내고 '+'는 알고리즘을 마지막 위치로 이동함을 나타냅니다.

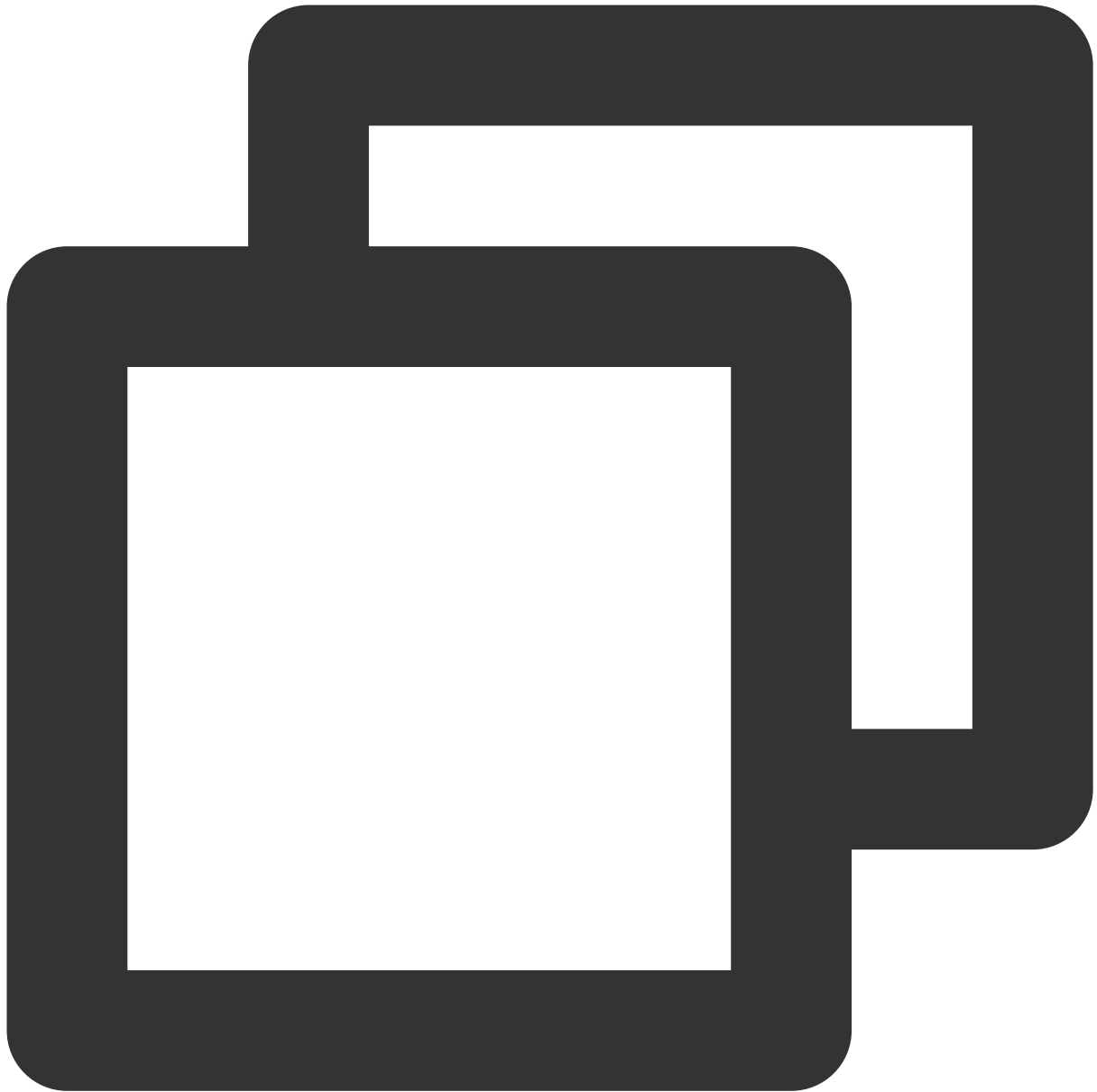
기본 강제 비활성화에 대한 암호화 알고리즘은 !aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!DHE 입니다.

기본값:



ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA3

매개변수 범위:




ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES256-SHA:ECDH-ECDSA-AES256-SHA:SRP-DSS-AES-256-

CLB 사용자 지정 구성 예시

1. [CLB 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **사용자 지정 구성**을 클릭합니다.
2. '사용자 지정 구성' 페이지 상단에서 리전을 선택하고 **생성**을 클릭합니다.

3. '사용자 지정 구성 생성' 페이지에서 각 항목이 세미콜론 ; 으로 끝나는 구성 이름과 코드 구성 항목을 입력합니다. 모든 정보를 입력한 후 **완료**를 클릭합니다.

 **Create custom configuration**

Specifications

Configuration Name

test

Region

Guangzhou

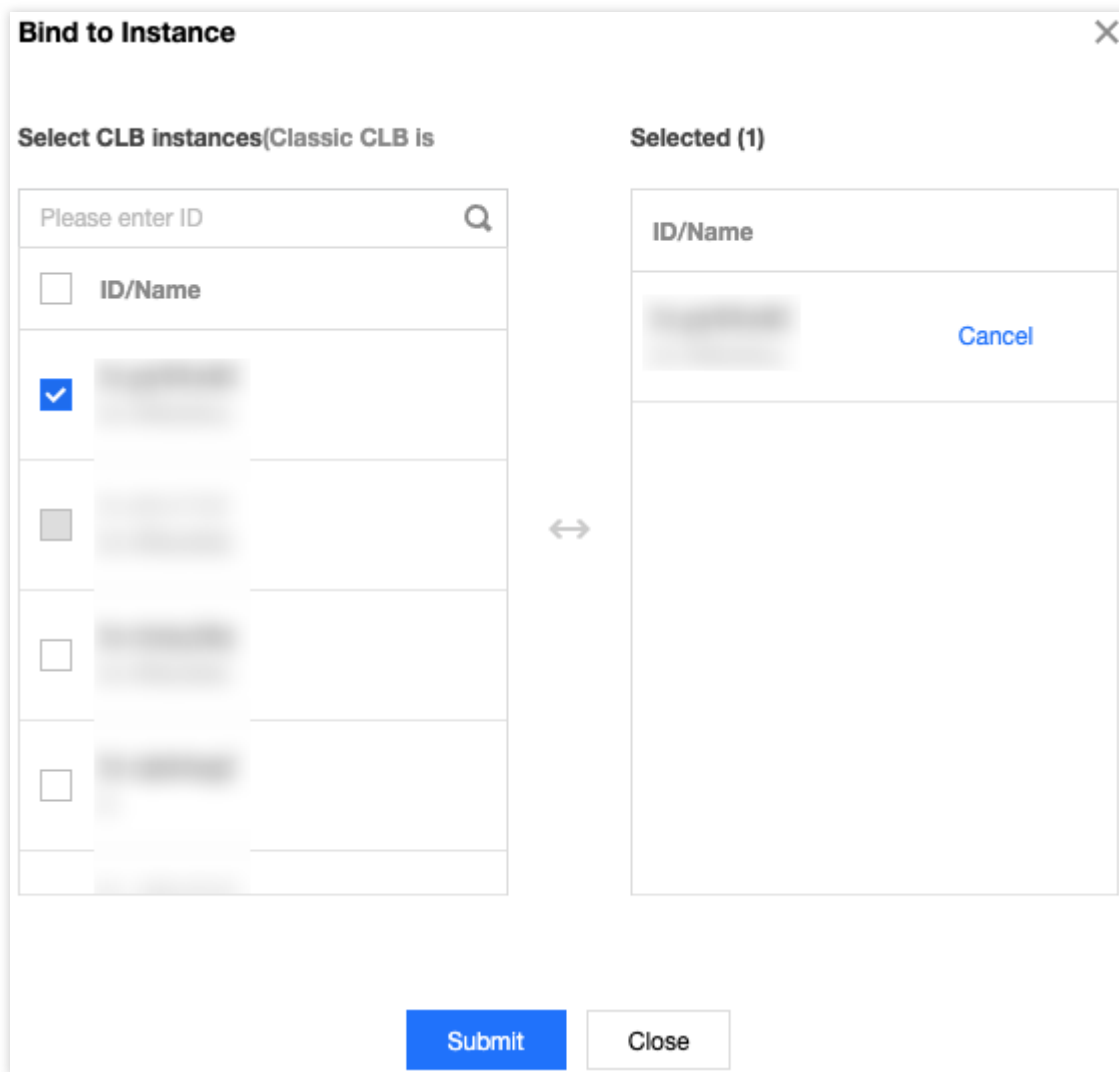
Code Configuration

```
1 client_max_body_size 2048M;
2 proxy_request_buffering off;
```

Parameters should accord with the supported configuration items and requirements, [Parameter De](#)

Completed

4. '사용자 지정 구성' 페이지로 돌아가십시오. 오른쪽에서 **인스턴스에 바인딩**을 클릭합니다.
5. '인스턴스에 바인딩' 팝업 페이지에서 바인딩할 CLB 인스턴스를 선택하고 **제출**을 클릭합니다.







6. '사용자 지정 구성' 페이지에서 구성된 ID를 클릭하여 세부 정보 페이지를 입력합니다. 바인딩된 인스턴스는 **바인딩 인스턴스** 탭에서 확인할 수 있습니다.

7. (선택 사항) 이제 인스턴스 목록 페이지에서 해당 사용자 지정 구성 정보를 볼 수 있습니다.

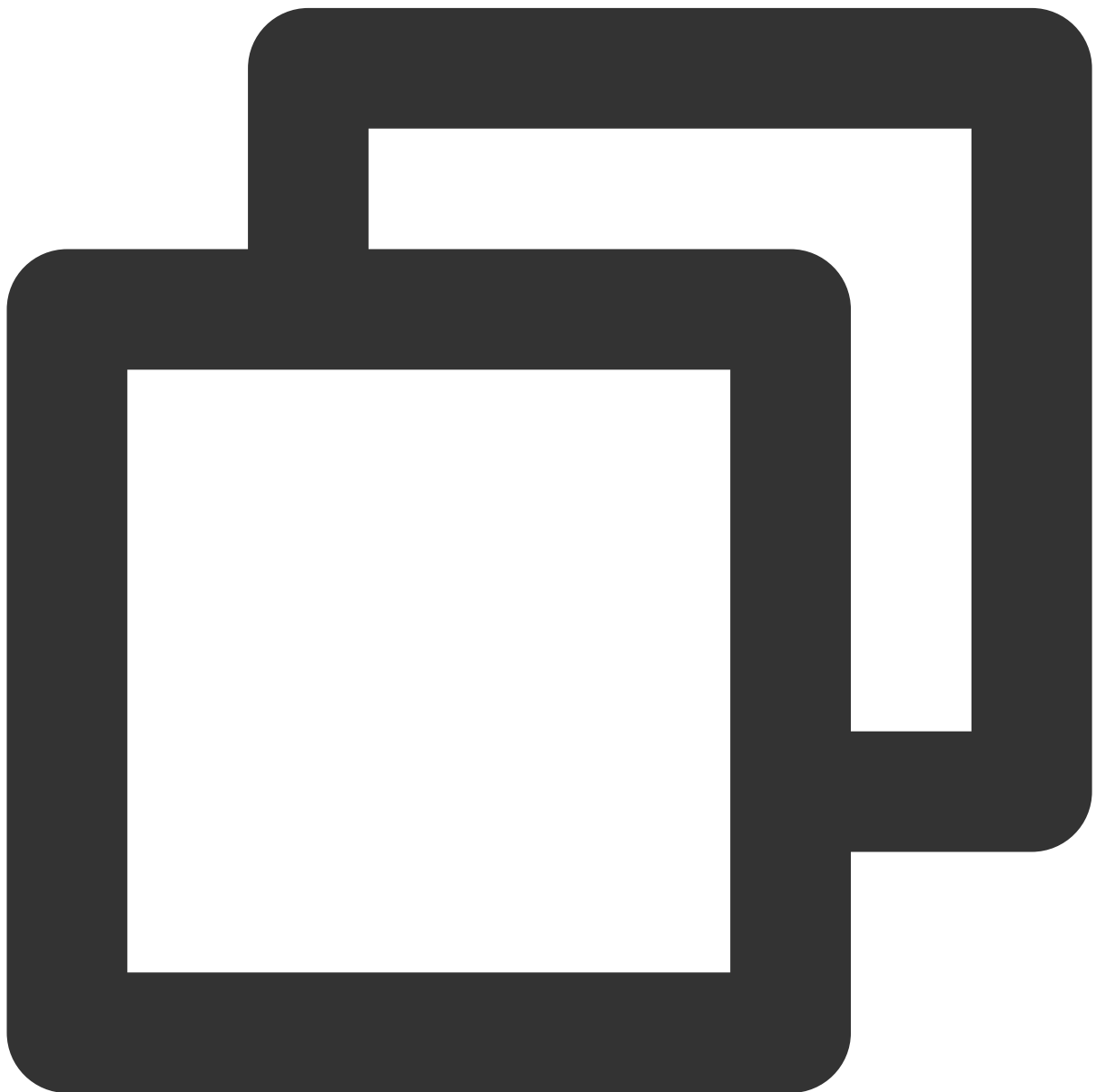
설명 :

'사용자 지정 구성 바인딩'이 인스턴스 목록에 표시되지 않으면 오른쪽 상단 모서리에 있는

을(를)  클릭합니다. 팝업 '사용자 지정 목록 필드' 대화 상자에서 '사용자 지정 구성 바인딩'을 선택하고 **확인**을 클릭합니다. 목록 페이지에 '사용자 지정 구성 바인딩' 열이 표시되어야 합니다.

<input type="checkbox"/>	ID/Name ↕	Mon...	Status	VIP	Availability Z...	Network ... ▾	Network	Health Status	Bill
<input type="checkbox"/>			Normal		Guangzhou Zone 4	Public Network	Basic Network	Health check not enabled (Configuration)	Pay — 1 Cre 20% 13:

기본 구성 샘플 코드:



```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

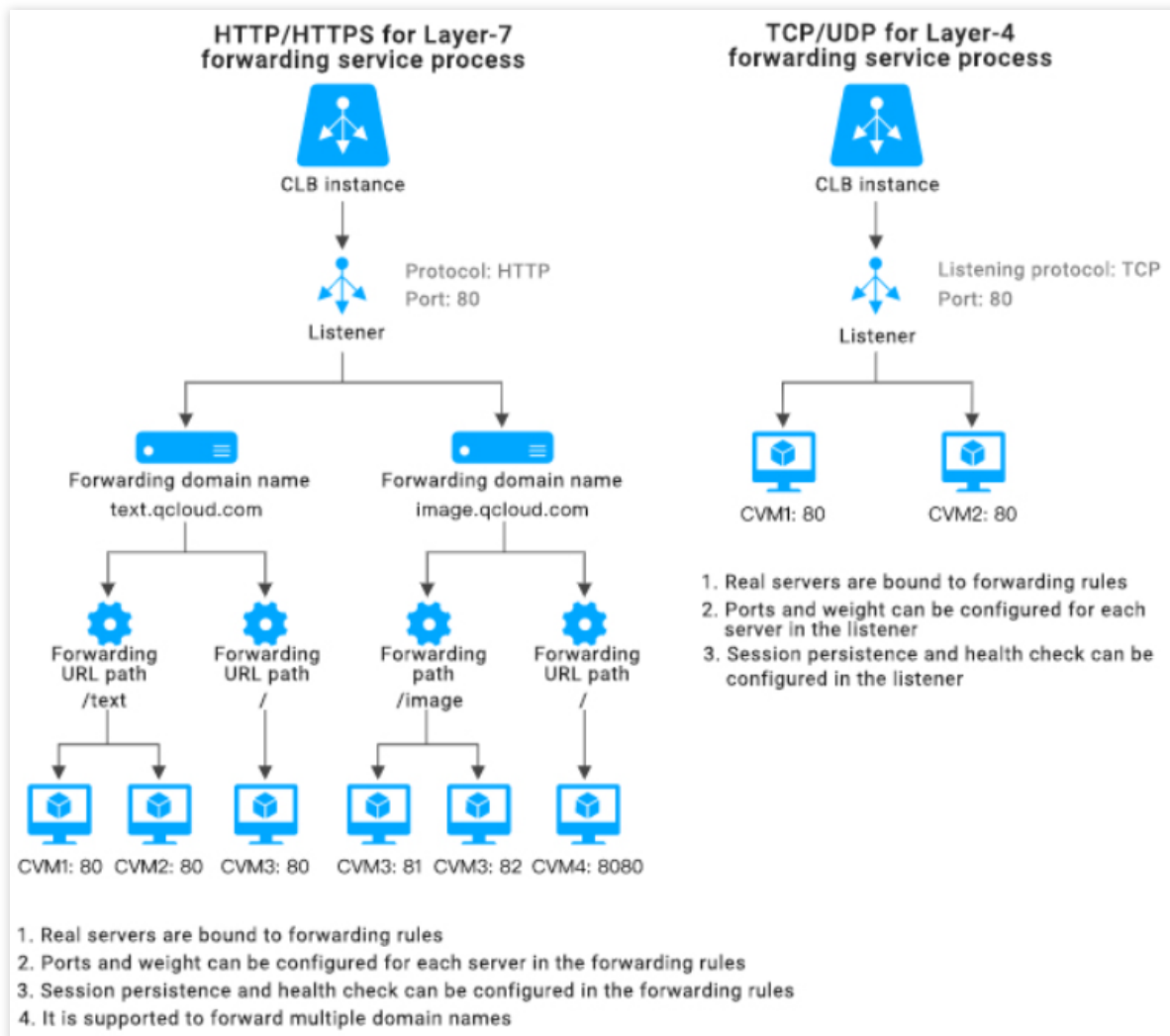
```
client_header_timeout    60s;
client_header_buffer_size 4k;
client_body_timeout      60s;
client_max_body_size     60M;
keepalive_timeout        75s;
add_header               xxx yyy;
more_set_headers          "A:B";
proxy_connect_timeout     4s;
proxy_read_timeout        60s;
proxy_send_timeout        60s;
```

레이어 7 도메인 이름 포워딩 및 URL 규칙

최종 업데이트 날짜: : 2024-01-04 19:54:02

프로세스 흐름

레이어 7 및 레이어 4 CLB(기존 애플리케이션 CLB)의 프로세스는 다음과 같습니다.



레이어 7 CLB를 사용하여 HTTP/HTTPS 프로토콜을 포워딩하는 경우 CLB 리스너에서 포워딩 규칙을 생성할 때 해당 도메인 이름을 추가할 수 있습니다.

하나의 포워딩 규칙만 생성된 경우 VIP + URL을 통해 해당 포워딩 규칙 및 서비스에 액세스할 수 있습니다.

여러 포워딩 규칙이 생성된 경우 VIP + URL을 사용한다고 해서 지정된 도메인 이름 + URL에 대한 액세스가 보장되는 것은 아닙니다. 포워딩 규칙이 적용되었는지 확인하려면 도메인 이름 + URL에 직접 액세스해야 합니다. 즉, 여러 포워딩 규칙을 구성할 때 VIP는 여러 도메인 이름에 해당할 수 있습니다. 이 경우 VIP + URL이 아닌 지정된 도메인 이름 + URL을 통해 서비스에 액세스하는 것을 권장합니다.

레이어 7 포워딩 구성

도메인 포워딩 구성

레이어 7 CLB는 다른 도메인 이름과 URL의 요청을 다른 서버로 포워딩할 수 있습니다. 레이어 7 리스너는 여러 도메인 이름으로 구성할 수 있으며, 각 도메인 이름은 여러 포워딩 경로로 구성할 수 있습니다.

포워딩된 도메인 이름의 길이 제한: 1 - 80자.

`_` 로 시작할 수 없습니다.

`www.example.com` 과 같은 정확한 도메인이 지원됩니다.

와일드카드 도메인 이름이 지원되지만 현재는 `*.example.com` 또는 `www.example.*` 형식의 도메인 이름만 지원됩니다. 즉, 와일드카드 도메인 이름은 `*` 로 시작하거나 끝나며 한 번만 나타납니다.

비정규식 포워딩 도메인 이름의 경우 유효한 문자 세트에는 `a-z` `0-9` `.` `-` `_` 가 포함됩니다.

포워딩된 도메인 이름은 정규식을 지원합니다. 정규식 도메인 이름:

지원되는 문자 세트: `a-z` ``` `0-9` ``` `.` `-` `?` `=` `~` `_` `-` `+` `\\` `^` `*` `!` `$` `&` `|` `(` `)` `[` `]` `.`

`~` 로 시작해야 하며, 한 번만 나타날 수 있습니다.

CLB에서 지원하는 정규식 도메인 이름의 예시는: `~^www\\d+\\.example\\.com$` 입니다.

포워딩된 도메인 이름 매칭

일반 매칭 정책

1. 포워딩 규칙에 도메인 이름 대신 IP 주소를 입력하고 포워딩 그룹에 여러 URL을 구성하면 VIP + URL을 사용하여 서비스에 액세스합니다.
2. 포워딩 규칙에서 전체 도메인 이름을 구성하고 포워딩 그룹에서 여러 URL을 구성하면 도메인 이름 + URL을 사용하여 서비스에 액세스합니다.
3. 포워딩 규칙에 와일드카드 도메인 이름을 설정하고 포워딩 그룹에 여러 개의 URL을 설정하면 요청한 도메인 이름과 URL의 매칭을 통해 서비스에 액세스하게 됩니다. 다른 도메인 이름이 동일한 URL을 가리키도록 하려면 이 방법을 구성에 사용할 수 있습니다. `example.qcloud.com` 을 예로 들면 형식은 다음과 같습니다.

정확히 매칭: 입력한 도메인 `example.qcloud.com` 과 완전히 일치하는 도메인 이름

`example.qcloud.com` 을 매칭합니다.

접두사 와일드카드: `*.qcloud.com` 과 같이 지정된 두 번째 및 최상위 레벨 도메인이 있는 모든 도메인 이름과 매칭합니다.

접미사 와일드카드: `example.qcloud.*` 와 같이 지정된 세 번째 및 두 번째 레벨 도메인이 있는 모든 도메인 이름과 매칭합니다.

정규식 일치: `~^www\\d+\\.example\\.com$` .

우선 순위: 정확히 일치 > 접두사 와일드카드 > 접미사 와일드카드 > 정규식 일치. 여러 매칭 규칙이 활성화되지 않도록 보다 정확한 도메인 이름을 사용하는 것이 좋습니다. 그렇지 않으면 같은 레벨의 여러 도메인 이름이 한 번에 히트될 때 부정확한 매칭 결과가 나올 수 있습니다.

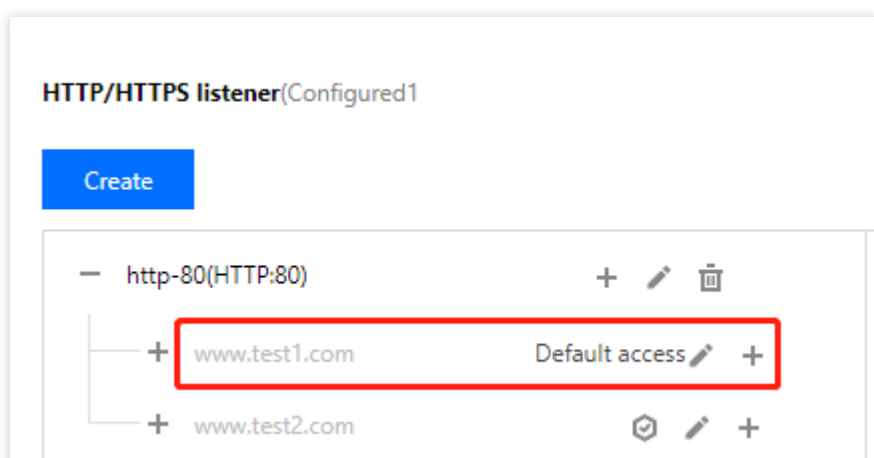
4. 포워딩 규칙에서 도메인 이름을 구성하고 포워딩 그룹에서 퍼지 매칭을 위한 URL을 구성하는 경우 접두사 일치 항목을 사용하고 접미사가 붙은 와일드카드 \$를 추가하여 전체 매칭을 시작할 수 있습니다.

예를 들어 URL ~*(gif|jpg|bmp)\$ 를 입력하면 모든 gif , jpg 및 bmp 파일과 일치합니다.

기본 도메인 이름 정책

요청된 도메인 이름이 규칙과 일치하지 않으면 CLB는 요청을 기본 도메인 이름(Default Server)으로 포워딩합니다. 하나의 리스너는 기본 도메인 이름을 하나만 가질 수 있습니다.

예를 들어, CLB1의 HTTP:80 리스너는 www.test1.com 및 www.test2.com 이라는 두 개의 도메인 이름으로 구성되며, 여기서 www.test1.com 은 기본 도메인 이름입니다. 사용자가 www.example.com 을 방문하면 일치하는 도메인 이름이 없으므로 CLB는 요청을 기본 도메인 이름인 www.test1.com 으로 포워딩합니다.



설명:

2020년 5월 18일 이전에는 레이어 7 리스너에 기본 도메인 이름 구성 여부는 선택 사항이며 기본 도메인 이름 구성 여부를 선택할 수 있습니다.

레이어 7 리스너에 기본 도메인 이름이 구성된 경우 다른 규칙과 일치하지 않는 클라이언트 요청은 기본 도메인 이름으로 포워딩됩니다.

레이어 7 리스너에 기본 도메인 이름이 구성되어 있지 않은 경우 다른 규칙과 일치하지 않는 클라이언트 요청은 CLB에서 로드한 첫 번째 도메인 이름으로 포워딩됩니다(로드 순서는 콘솔에서 구성된 순서와 다를 수 있으므로 콘솔에서 구성된 첫 번째 순서가 아닐 수 있습니다).

2020년 5월 18일부터:

모든 새 레이어 7 리스너에는 기본 도메인 이름이 있어야 합니다. 레이어 7 리스너의 첫 번째 규칙이 기본 도메인 이름으로 설정됩니다. API를 통해 레이어 7 규칙을 생성하면 DefaultServer 필드가 true로 설정됩니다.

기본 도메인 이름이 구성된 모든 리스너의 경우 기존 기본 도메인 이름을 수정하거나 삭제할 때 새 기본 도메인 이름을 지정해야 합니다. 콘솔에서 작업을 수행할 때 새 기본 도메인 이름을 지정해야 합니다. API를 호출하여 작업을 수행할 때 새 기본 도메인 이름을 설정하지 않으면 CLB는 나머지 도메인 이름 중 가장 먼저 생성된 이름을 새 기본 도메인 이름으로 설정합니다.

기본 도메인 이름이 없는 기존 규칙의 경우 아래 '작업4'에 설명된 대로 비즈니스 요구 사항에 따라 기본 도메인 이름을 직접 구성할 수 있습니다. 그렇게 하지 않으면 Tencent Cloud는 CLB가 로드한 첫 번째 도메인 이름을 기본 도메인 이름으로 설정합니다. 기존 리스너는 2020년 06월 19일 이전에 모두 처리됩니다.

상기 정책은 2020년 5월 18일부터 점진적으로 시행 중이며, 각 사례별 시행일자는 다소 상이할 수 있습니다. 2020년 6월 20일부터 도메인 이름이 포워딩된 모든 레이어 7 리스너는 기본 도메인 이름을 갖게 됩니다.

기본 도메인 이름에 대해 다음 네 가지 작업을 수행할 수 있습니다.

작업1: 레이어 7 리스너에 대한 첫 번째 포워딩 규칙을 구성할 때 기본 도메인 이름이 활성화 상태여야 합니다.

CreateForwarding rule

1 Basic configuration > 2 Health check > 3 Session persistence

Domain name ⓘ

Default domain name **Enable**

If a client request does not match any domain names of this listener, the CLB instance will forward the request to the default domain name (Default Server). Each listener only can configure one listener and must configure one. [Details](#)

URL ⓘ

Balancing method ⓘ

WRR scheduling is based on the number of new connections. The real server with higher weight stands more chances to be polled.

작업2: 현재 기본 도메인 이름을 비활성화합니다.

리스너 아래에 여러 도메인 이름이 있는 경우 현재 기본 도메인 이름을 비활성화할 때 새 기본 도메인 이름을 지정해야 합니다.

EditDomain name

Domain name ⓘ

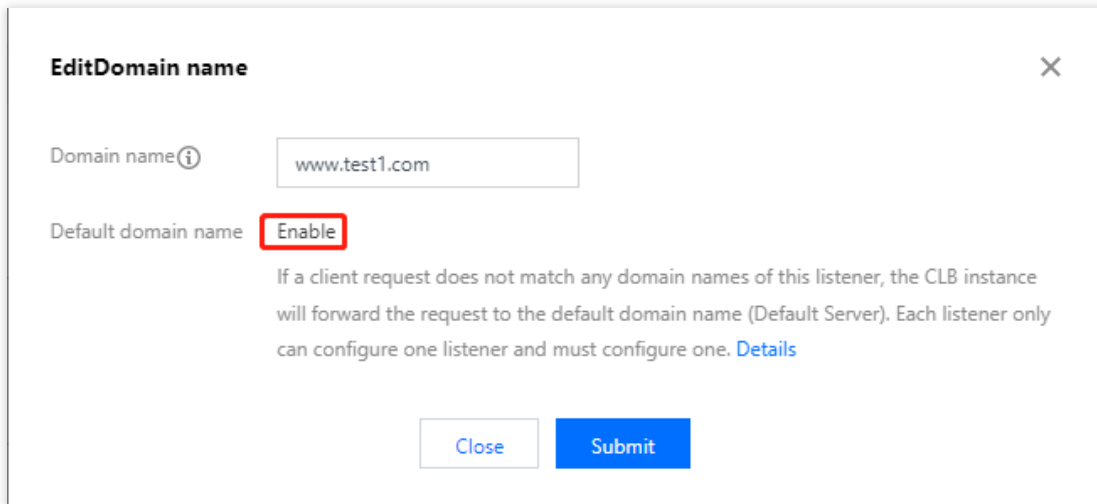
Default domain name ☐

If a client request does not match any domain names of this listener, the CLB instance will forward the request to the default domain name (Default Server). Each listener only can configure one listener and must configure one. [Details](#)

New default domain name

Please configure a new default domain name

리스너에 도메인 이름이 하나만 있고 해당 도메인 이름이 기본 도메인 이름인 경우 비활성화할 수 없습니다.



EditDomain name

Domain name ⓘ

Default domain name **Enable**

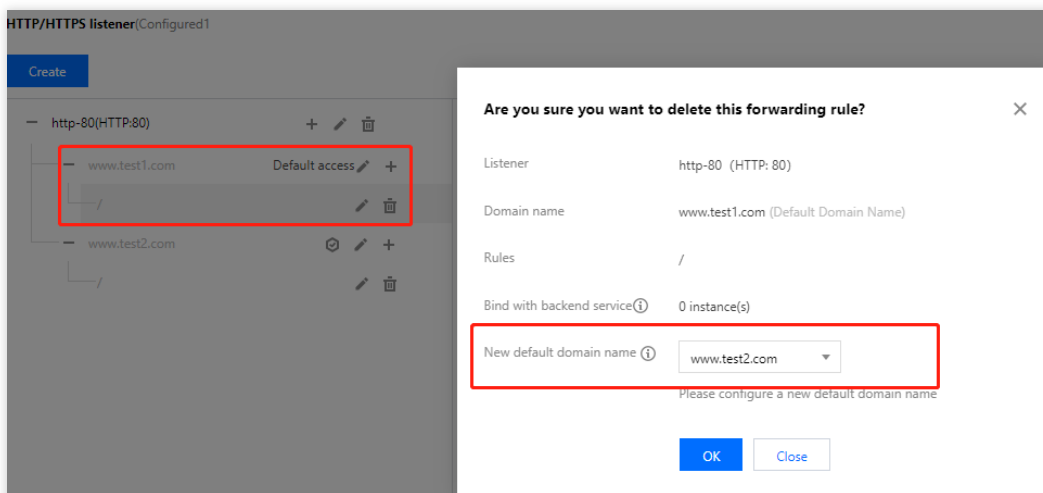
If a client request does not match any domain names of this listener, the CLB instance will forward the request to the default domain name (Default Server). Each listener only can configure one listener and must configure one. [Details](#)

작업3: 기본 도메인 이름을 삭제합니다.

리스너 아래에 여러 도메인 이름이 있는 경우 기본 도메인 이름 아래의 규칙을 삭제:

규칙이 기본 도메인 이름의 마지막 규칙이 아닌 경우 직접 삭제할 수 있습니다.

규칙이 기본 도메인 이름의 마지막 규칙인 경우 새 기본 도메인 이름을 설정해야 합니다.



HTTP/HTTPS listener(Configured1)

Create

http-80(HTTP:80)

www.test1.com Default access +

www.test2.com +

Are you sure you want to delete this forwarding rule?

Listener http-80 (HTTP: 80)

Domain name www.test1.com (Default Domain Name)

Rules /

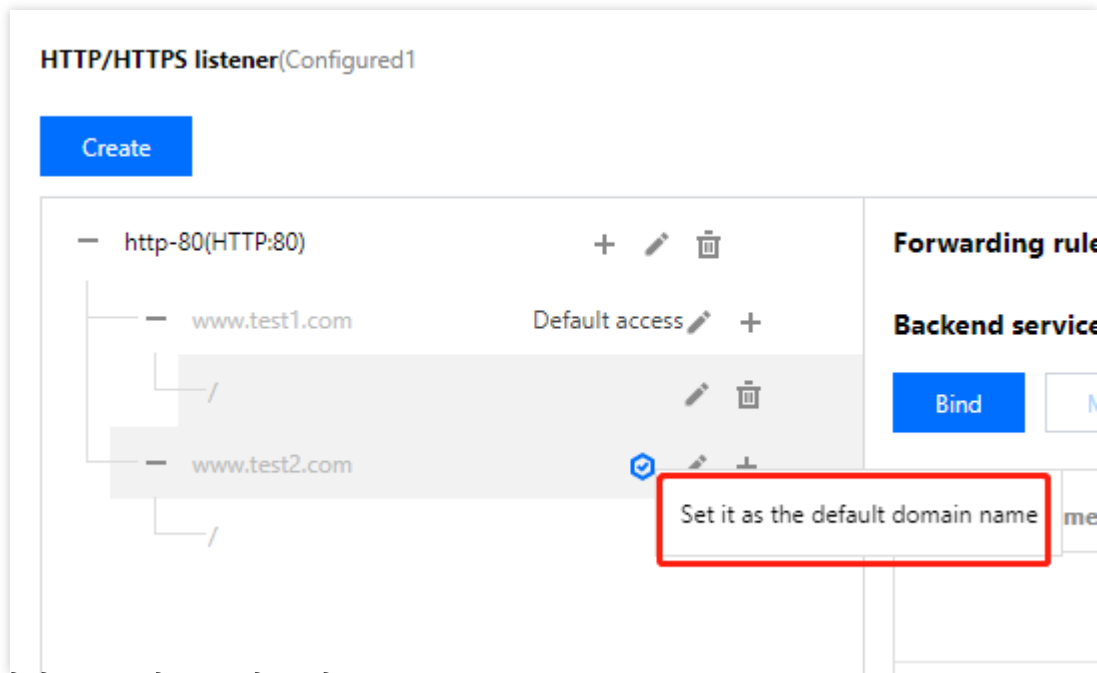
Bind with backend service ⓘ 0 instance(s)

New default domain name ⓘ

Please configure a new default domain name

리스너 아래에 도메인 이름이 하나만 있는 경우 새 기본 도메인 이름을 설정하지 않고 모든 규칙을 직접 삭제할 수 있습니다.

작업4: 리스너 목록에서 기본 도메인 이름을 빠르게 수정할 수 있습니다.



포워딩된 URL 경로 구성 규칙

레이어 7 CLB는 처리를 위해 다른 URL의 요청을 다른 서버로 포워딩할 수 있으며 단일 도메인 이름에 대해 여러 포워딩된 URL 경로를 구성할 수 있습니다.

포워딩된 URL의 길이 제한: 1-200자.

비정규식 포워딩 URL은 '/'로 시작해야 하며 a-z A-Z 0-9 . - _ / = ? : 를 포함한 유효한 문자 세트를 사용해야 합니다. 대소문자를 구분합니다.

포워딩된 URL은 정규식을 지원하지 않습니다.

정규식 URL은 ~ 로 시작해야 하며, 한 번만 나타날 수 있습니다.

정규식 URL의 경우 유효한 문자 집합: a-z A-Z 0-9 . - _ / = ? ~ ^ * \$:

() [] + | .

정규식 URL의 예는 ~* .png\$ 일 수 있습니다.

포워딩된 URL에 대한 매칭 규칙은 다음과 같습니다.

= 로 시작하는 것은 정확히 일치함을 나타냅니다.

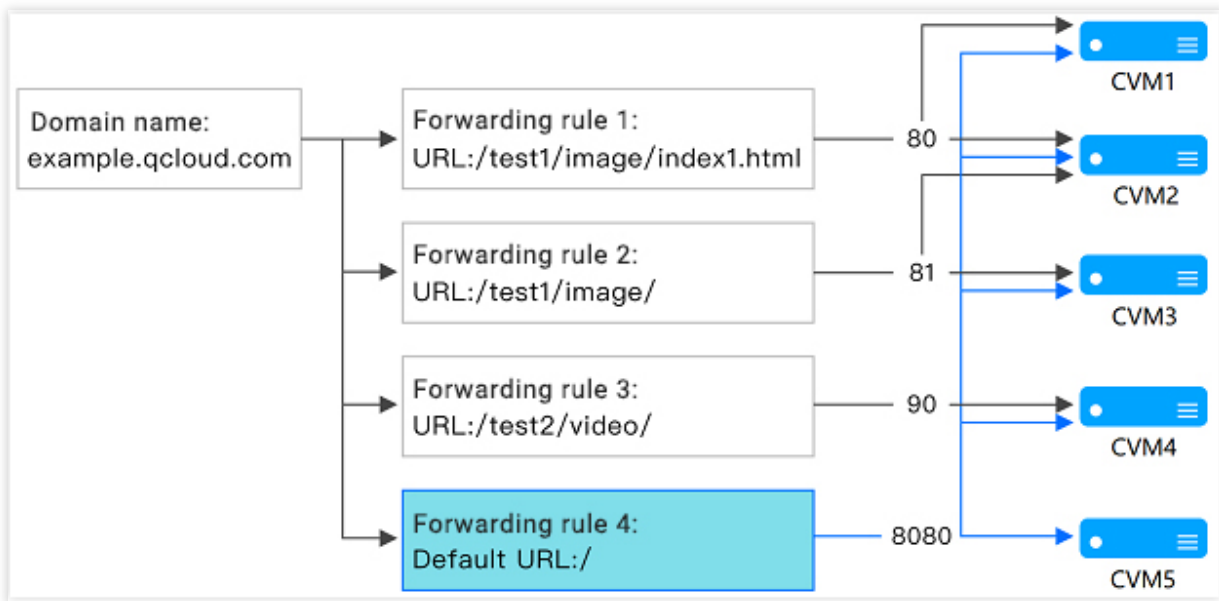
^~ 로 시작하는 URL은 정규 문자열로 시작하고 정규식 일치를 위한 것이 아님을 나타냅니다.

~ 로 시작하는 것은 대소문자를 구분하는 정규식 일치를 나타냅니다.

~* 로 시작하는 것은 대소문자를 구분하지 않는 정규식 일치를 나타냅니다.

/ 는 다른 일치 항목이 없는 경우 모든 요청이 일치하는 일반 일치를 나타냅니다.

포워딩된 URL 경로 일치 설명



1. 매칭 규칙: 가장 긴 접두어 일치룰 기반으로 정확한 일치가 먼저 수행되고 퍼지 일치가 수행됩니다.

예를 들어 위와 같이 포워딩 규칙 및 포워딩 그룹을 구성한 후 다음 요청이 다른 포워딩 규칙과 순서대로 일치합니다.

1.1 `example.qcloud.com/test1/image/index1.html` 은 포워딩 규칙1에 의해 구성된 URL 규칙과 정확히 일치하므로, 요청은 포워딩 규칙1과 연결된 실제 서버, 즉 그림에서 CVM1 및 CVM2의 포트 80으로 포워딩됩니다.

1.2 `example.qcloud.com/test1/image/hello.html` 에는 정확히 일치하는 항목이 없으므로 가장 긴 접두어 일치룰 기준으로 포워딩 규칙2와 일치합니다. 따라서 요청은 포워딩 규칙2와 연결된 실제 서버, 즉 그림에서 CVM2 및 CVM3의 포트 81로 전달됩니다.

1.3 `example.qcloud.com/test2/video/mp4/` 에는 정확히 일치하는 항목이 없으므로 가장 긴 접두어 일치룰 기반으로 포워딩 규칙3과 일치합니다. 따라서 요청은 포워딩 규칙3과 관련된 실제 서버, 즉 그림에서 CVM4의 포트 90으로 전달됩니다.

1.4 `example.qcloud.com/test3/hello/index.html` 에는 정확히 일치하는 항목이 없기 때문에 루트 디렉터리의 Default URL인 `example.qcloud.com/` 과 가장 긴 접두어 일치로 일치합니다. 이 경우 Nginx는 요청을 FastCGI/php) 또는 Tomcat(jsp)과 같은 실제 서버로 전달하고 Nginx는 역방향 프록시 서버로 존재합니다.

1.5 `example.qcloud.com/test2/` 에는 정확히 일치하는 항목이 없기 때문에 루트 디렉터리의 Default URL인 `example.qcloud.com/` 과 가장 긴 접두어 일치로 일치합니다.

2. 설정된 URL 규칙에서 서비스가 제대로 작동하지 않을 경우, 매칭 성공 후 다른 페이지로 리디렉션되지 않습니다.

예를 들어 클라이언트가 `example.qcloud.com/test1/image/index1.html`을 요청하여 포워딩 규칙1과 일치시킵니다. 하지만 포워딩 규칙1의 실제 서버는 예외가 있고 404 오류 페이지가 나타납니다. 404 오류 페이지가 표시되지만 다른 페이지로 리디렉션되지는 않습니다.

3. Default URL을 안정적인 페이지(예: 정적 페이지 또는 홈페이지)로 지정하고 모든 실제 서버에 바인딩하는 것이 좋습니다. 일치하는 규칙이 없으면 시스템은 요청을 Default URL 페이지로 지정합니다. 그렇지 않으면 404 오류가 발생할 수 있습니다.

4. Default URL을 설정하지 않고, 일치하는 포워딩 규칙이 없으면, 서비스에 액세스할 때 404 오류가 반환됩니다.

5. 레이어 7 URL 경로 끝에 있는 슬래시 참고: 설정한 URL이 `/` 로 끝나지만 클라이언트의 액세스 요청에 `/` 가 포함되지 않은 경우 요청은 `/` 로 끝나는 규칙으로 리디렉션됩니다(301 리디렉션).

예를 들어 HTTP:80 리스너에서 구성된 도메인 이름은 `www.test.com` 입니다.

5.1 이 도메인 이름 아래에 설정된 URL이 `/abc/` 인 경우:

클라이언트가 `www.test.com/abc` 에 액세스하면 `www.test.com/abc` 로 리디렉션됩니다.

클라이언트가 `www.test.com/abc/` 에 액세스하면 `www.test.com/abc/` 와 일치합니다.

5.2 이 도메인 이름 아래에 설정된 URL이 `/abc` 인 경우:

클라이언트가 `www.test.com/abc` 에 액세스하면 `www.test.com/abc` 와 일치합니다.

클라이언트가 `www.test.com/abc/` 에 액세스하면 `www.test.com/abc/` 와도 일치합니다.

레이어 7 상태 확인 구성 설명

상태 확인 도메인 이름 구성 규칙

상태 확인 도메인 이름은 레이어 7 CLB에서 실제 서버의 상태를 감지하는 데 사용하는 도메인 이름입니다.

길이 제한: 1 - 80자.

기본값: 포워딩된 도메인 이름.

정규식은 지원되지 않습니다. 포워딩된 도메인 이름이 와일드카드 도메인 이름인 경우 고정된 이름(비정규식)을 지정해야 합니다.

유효한 문자 집합에는 `a-z` `0-9` `.` `-` `_` 가 포함됩니다. 예시: `www.example.qcould.com` .

상태 확인 경로 구성 규칙

상태 확인 경로는 레이어 7 CLB가 실제 서버의 상태를 감지하는 데 사용하는 URL 경로입니다.

길이 제한: 1 - 200자.

기본: `/` . `/` 로 시작하는 사용자 정의 경로를 입력할 수 있습니다.

정규식은 지원되지 않습니다. 상태 확인을 위해 고정 URL(정적 페이지)을 지정하는 것이 좋습니다.

유효한 문자 집합에는 `a-z` `A-Z` `0-9` `.` `-` `_` `/` `=` `?` `:` 가 있습니다. 예: `/index` .

CLB에서 QUIC 프로토콜 사용

최종 업데이트 날짜: : 2024-01-04 19:54:41

QUIC 프로토콜을 사용하면 네트워크가 약하거나 Wi-Fi와 4G 간의 빈번한 전환과 같은 시나리오에서 재연결이 필요 없이 App에 더 빠르게 액세스하고 다중화를 달성할 수 있습니다. 본문은 CLB 콘솔에서 QUIC 프로토콜을 구성하는 방법을 소개합니다.

QUIC 개요

QUIC(Quick UDP Internet Connection)는 Google에서 설계한 전송 레이어 네트워크 프로토콜로 UDP를 사용하여 동시 데이터 스트림을 다중화합니다. 널리 사용되는 TCP+TLS+HTTP2 프로토콜과 비교하여 QUIC에는 다음과 같은 장점이 있습니다.

연결 설정 시간이 단축되었습니다.

혼잡 제어를 개선합니다.

HOL(head-of-line) 차단을 피하기 위해 멀티플렉스를 채택합니다.

연결 마이그레이션을 지원합니다.

QUIC가 활성화되면 클라이언트는 CLB(Cloud Load Balancer) 인스턴스와 QUIC 연결을 설정할 수 있습니다. 클라이언트와 CLB 인스턴스 간의 협상으로 인해 QUIC 연결이 실패하면 HTTPS 또는 HTTP/2가 사용됩니다. 그러나 CLB 인스턴스와 리얼 서버는 여전히 HTTP1.x 프로토콜을 사용합니다.

사용 제한

CLB 인스턴스만 QUIC 프로토콜을 지원합니다.

IPv4 및 IPv6 NAT64 CLB만 QUIC 프로토콜이 지원되며 IPv6 버전은 현재 지원되지 않습니다.

레이어 7 HTTPS 리스너가 있는 공중망 CLB만 QUIC 프로토콜을 지원합니다.

지원되는 QUIC 버전: Q050, Q046, Q043, h3-29 및 h3-27.

작업 순서

1. 필요에 따라 CLB 인스턴스를 생성합니다. 자세한 내용은 [Creating CLB Instances](#)를 참고하십시오.

설명 :

CLB 인스턴스를 생성할 때 리전으로 '베이징', '상하이' 또는 '뮌바이'를 선택하고 네트워크 유형으로 '공중망'을 선택합니다.

2. [CLB 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **CLB 인스턴스 관리**를 클릭합니다.

3. 'CLB 인스턴스 관리' 페이지에서 **Cloud Load Balancer** 탭을 선택합니다.

4. 'CLB' 태그 페이지에서 '베이징', '상하이' 또는 '몸바이' 리전에서 생성된 공중망 CLB 인스턴스를 찾고 작업 열 아래에서 **리스너 구성**을 클릭합니다.
5. '리스너 관리' 페이지의 "HTTP/HTTPS 리스너"에서 **생성**을 클릭합니다.
6. '리스너 생성' 페이지에서 수신 포트의 프로토콜로 HTTPS를 선택합니다. 다른 구성을 완료하고 **제출**을 클릭합니다.
7. **리스너 관리** 탭에서 생성된 리스너 오른쪽의 **+** 를 클릭합니다.
8. '포워딩 규칙 생성' 페이지에서 QUIC를 활성화하고 레이어 7 규칙을 생성합니다. 관련 필드를 채우고 **다음**을 클릭하여 기본 구성을 완료합니다.

설명 :

HTTPS 포워딩 규칙을 생성할 때 QUIC 프로토콜을 활성화한 경우 나중에 필요에 따라 QUIC 프로토콜을 활성화하거나 비활성화할 수 있습니다. HTTPS 포워딩 규칙을 생성할 때 QUIC 프로토콜을 활성화하지 않은 경우 나중에 활성화할 수 없습니다.

UDP 프로토콜을 기반으로 QUIC는 CLB 인스턴스의 UDP 포트를 사용합니다. HTTPS 리스너에 대해 QUIC를 활성화하면 UDP 및 TCP 포트가 사용됩니다. 예를 들어 HTTPS:443 리스너에 대해 QUIC를 활성화하면 TCP:443 및 UDP:443 포트가 모두 사용되며 TCP:443 또는 UDP:443 리스너를 생성할 수 없습니다.

후속 작업

기본 구성이 완료된 후 [Health Check](#) 및 [Session Persistence](#)를 구성할 수 있습니다.

CLB 인스턴스에 SNI 다중 인증서 바인딩 지원

최종 업데이트 날짜: : 2024-01-04 19:54:55

서버 이름 표시(Server Name Indication, SNI)는 서버와 클라이언트의 SSL/TLS 확장을 개선하기 위해 하나의 서버가 하나의 인증서만 사용할 수 있는 문제를 해결하기 위해 설계되었습니다. 서버가 SNI를 지원하는 경우 서버가 여러 인증서에 바인딩될 수 있음을 의미합니다. 클라이언트에 SNI를 사용하려면 서버에 대한 SSL/TLS 연결이 설정되기 전에 연결할 도메인 이름을 지정해야 합니다. 그러면 서버는 도메인 이름을 기반으로 적절한 인증서를 반환합니다.

시나리오

레이어 7 HTTPS CLB 리스너는 수신 규칙에서 서로 다른 도메인 이름에서 사용할 수 있는 여러 인증서 바인딩과 같은 SNI를 지원합니다. 예를 들어, CLB 인스턴스의 동일한 `HTTPS:443` 리스너에서 `*.test.com` 및 `*.example.com`에 대해 각각 인증서 1 및 인증서 2를 사용하여 이러한 도메인 이름의 요청을 두 개의 다른 서버 세트로 전달할 수 있습니다.

전제 조건

CLB 인스턴스 구매를 완료해야 합니다.

작업 단계

1. CLB 콘솔에 로그인합니다.
2. [Configuring HTTPS Listener](#)를 참고하여 리스너를 구성하고 SNI를 활성화합니다.

CreateListener ✕

Name

test-sni

Listen Protocol Ports

HTTPS ▾

:

443

Enable SNI ⓘ

☒

✕

1. If you select HTTPS protocol for forwarding, the accesses from client to load balancer is encrypted with HTTPS protocol. HTTP protocol is adopted to forward requests from load balancers to backend CVM.

2. The load balancer serves as an agent for the overhead of SSL encryption and decryption, and ensures Web access security.

3. You can go to [SSL Certificate Management Platform](#) to apply for an SSL certificate for free.

4. To enable SNI, you do not need to configure the certificate here. Please configure it on the domain configuration page.

Close

Submit

3. 리스너에 포워딩 규칙을 추가할 때 서로 다른 도메인 이름에 대해 서로 다른 서버 인증서를 구성합니다. 그런 다음 [다음]을 클릭하고 상태 확인 및 세션 지속성을 구성합니다.

Create Forwarding rules

1 Basic Configuration

2 Health Check

3 Session Persistence

Domain Name ⓘ

*.example.com

Default Domain Name

☒

If the client request does not match any domain name of this listener, CLB will forward the request to the default domain name. Each listener can only be configured with one default domain name, [Details](#)

HTTP2.0

☒

URL ⓘ

/

Balance Method

Weighted Round Robin

If you set a same weighted value for all CVMs, requests will be distributed by a simple pooling policy.

Backend Protocol ⓘ

HTTP

SSL Phrasing

One-way Authentication(Recommended)

[Detailed Comparison](#)

Note: Choose SSL two-way authentication if you also need a certificate from the client.

Server Certificate

☒ Select existing ☐ Create

Please select

Get client IP

Enabled

Gzip compression

Enabled ⓘ

Close

Next

리얼 서버

리얼 서버 개요

최종 업데이트 날짜: : 2024-01-04 19:55:13

리얼 서버란?

리얼 서버는 생성된 CLB 인스턴스에 바인딩되어 요청을 처리하는 [CVM 인스턴스](#)입니다. [CLB Listener](#)를 구성할 때 CVM 인스턴스를 리얼 서버로 바인딩해야 합니다. CLB는 다양한 [Round-Robin Methods](#)를 통해 요청을 리얼 서버로 포워딩하여 애플리케이션의 안정성과 신뢰성을 보장합니다. CLB 인스턴스가 있는 리전의 하나 이상의 가용존에서 CVM 인스턴스를 바인딩하여 애플리케이션 견고성을 향상하고 단일 실패 지점을 차단할 수 있습니다.

주의 사항

리얼 서버를 추가할 때 다음을 수행하는 것이 좋습니다.

CLB 인스턴스에 바인딩할 모든 CVM 인스턴스에 Web 서버(예: Apache 또는 IIS)를 설치하고 애플리케이션 일관성을 보장합니다.

CLB가 여러 요청에서 재사용할 수 있도록 더 긴 TCP 연결을 유지할 수 있도록 [Session Persistence](#)를 활성화하여 Web 서버의 부하를 줄이고 CLB 처리량을 개선하는 것이 좋습니다.

실제 인스턴스의 보안 그룹에 CLB 리스너 포트 및 상태 확인 포트에 대한 인바운드 규칙이 있는지 확인하십시오. 자세한 내용은 [Configuring CVM Security Groups](#)를 참고하십시오.

리얼 서버 관리

최종 업데이트 날짜: : 2024-01-04 19:55:28

CLB는 정상적으로 실행되는 리얼 서버 인스턴스로 요청을 라우팅합니다. 본문은 필요에 따라 또는 CLB를 처음 사용할 때 리얼 서버를 추가하거나 삭제하는 방법에 대해 설명합니다.

전제 조건

CLB 인스턴스를 생성하고 리스너를 구성합니다. 자세한 내용은 [Getting Started with CLB](#)를 참고하십시오.

작업 단계

CLB에 리얼 서버 추가

설명:

CLB 인스턴스가 Auto Scaling 그룹과 연결되어 있으면 해당 그룹의 CVM이 CLB의 리얼 서버에 자동으로 추가됩니다. CVM 인스턴스가 Auto Scaling 그룹에서 제거되면 CLB의 리얼 서버에서 자동으로 삭제됩니다.

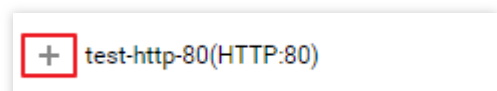
API를 사용하여 리얼 서버를 추가하는 방법에 대한 자세한 내용은 [RegisterInstancesWithLoadBalancer](#)를 참고하십시오.

CVM별 청구 계정이 있고 비 BGP ISP(China Mobile/China Unicom/China Telecom)를 선택한 경우, 트래픽별 청구 및 대역폭별 청구 패키지 CVM 인스턴스만 바인딩할 수 있습니다. 계정 및 ISP 유형에 대한 자세한 내용은 [Checking Account Type](#) 및 [Product Attribute Selection](#)을 참고하십시오.

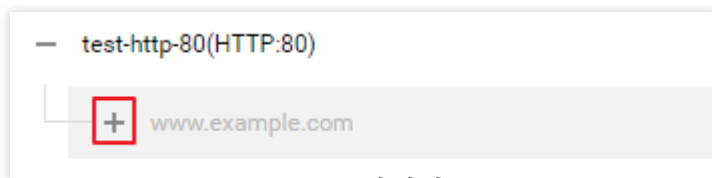
1. [CLB 콘솔](#)에 로그인합니다.
2. '인스턴스 관리' 페이지에서 'CLB' 인스턴스의 오른쪽에 있는 **리스너 구성**을 클릭합니다.
3. 리스너 구성 페이지에서 백엔드 CVM에 바인딩할 리스너를 선택합니다.

HTTP/HTTPS 리스너

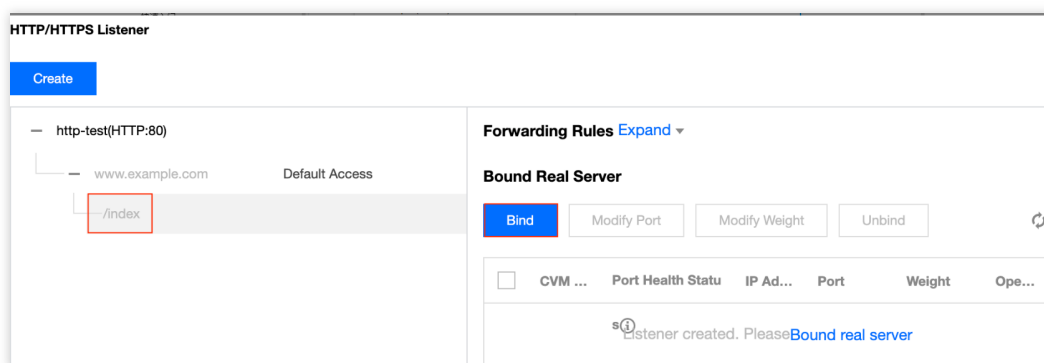
3.1.1 HTTP/HTTPS 리스너 섹션에서 선택한 리스너 왼쪽의 +를 클릭합니다.



3.1.2 펼쳐진 도메인 이름의 왼쪽에 있는 +를 클릭합니다.

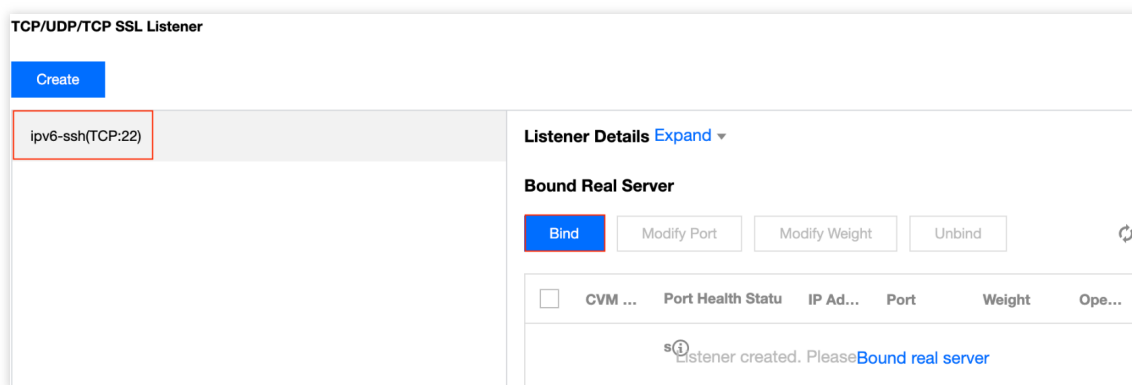


3.1.3 펼쳐진 URL 경로를 선택하고 **바인딩**을 클릭합니다.



TCP/UDP/TCP SSL 리스너

TCP/UDP/TCP SSL 리스너 섹션 왼쪽의 목록에서 백엔드 CVM과 바인딩할 리스너를 선택하여 **바인딩**을 클릭합니다.



4. CLB 인스턴스를 리얼 서버와 바인딩합니다.

방법1: '리얼 서버와 바인딩' 대화 상자에서 **CVM**을 클릭하고 CVM 인스턴스를 하나 이상 선택하고 포워딩 포트와 가중치를 입력하고 **확인**을 클릭합니다. 포트에 대한 자세한 내용은 [서버 상용 포트](#)를 참고하십시오.

설명:

'리얼 서버와 바인딩' 팝업 창에는 동일한 리전, 동일한 네트워크 환경에서 격리되거나 만료되지 않고 최대 대역폭이 0보다 큰 사용 가능한 CVM만 표시됩니다.

CLB 인스턴스가 여러 리얼 서버와 바인딩될 때 Hash 알고리즘을 사용하여 트래픽을 포워딩합니다.

가중치가 클수록 요청이 더 많이 포워딩됩니다. 값 범위는 0 - 100(기본값: 10)입니다. 0으로 설정하면 리얼 서버는 새 요청 수신을 중지합니다. 세션 지속성을 활성화하면 리얼 서버의 요청이 고르게 분산되지 않을 수 있습니다. 자세한

내용은 [Load Balancing Algorithm Selection and Weight Configuration Examples](#)를 참고하십시오.

Bind with backend service

Select an instance

CVM

ENI

Please enter the d...

IP address

Search by IP address,

Instance ID/name

10

/ page

1

/ 1 page

Selected (2)

Instance ID/name	Port	Weight	
	80	10	Add a port Delete
	80	10	Add a port Delete

Confirm

Cancel

방법2: 일괄 바인딩할 CVM 인스턴스의 사전 설정 포트 값이 동일한 경우 ‘리얼 서버와 바인딩’ 팝업 창에서 **CVM**을 클릭하고 포트 값을 입력하고 해당 CVM 인스턴스를 선택하고 가중치를 설정한 다음 **확인**을 클릭하여 일괄 바인딩합니다. 포트에 대한 자세한 내용은 [서버 상용 포트](#)를 참고하십시오.

Bind with backend service

CVM

ENI

80

IP address

Search by IP address,

Instance ID/name

✓

Instance ID/name

✓

Instance ID/name

✓

Instance ID/name

10 / page

1

/ 1 page

Press Shift key to select more

Selected (2)

Instance ID/name	Port	Weight		
...	80	10	+	Add a port Delete
...	80	10	+	Add a port Delete

Confirm

Cancel

CLB의 리얼 서버 가중치 수정

리얼 서버 가중치는 포워딩할 CVM 요청 수를 결정합니다. 리얼 서버를 바인딩할 때 가중치를 미리 설정해야 합니다. 다음은 'HTTP/HTTPS 리스너'(TCP/UDP/TCP SSL 리스너에도 적용됨)를 사용할 때 리얼 서버 가중치를 변경하는 예를 보여줍니다.

설명:

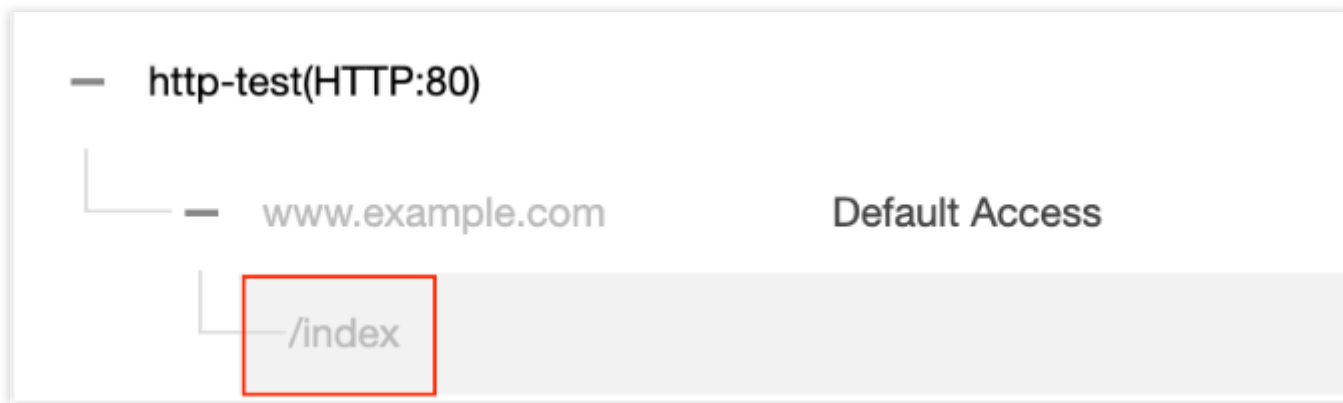
API로 리얼 서버 가중치를 수정하는 방법에 대한 자세한 내용은 [ModifyLoadBalancerBackends](#)를 참고하십시오.

CLB 리얼 서버의 가중치에 대한 자세한 내용은 [CLB Round-Robin Methods](#)를 참고하십시오.

1. CLB 콘솔에 로그인합니다.
2. '인스턴스 관리' 페이지에서 'CLB' 인스턴스의 오른쪽에 있는 **리스너 구성**을 클릭합니다.
3. HTTP/HTTPS 리스너 섹션 왼쪽에 있는 목록에서 인스턴스 및 리스너 규칙을 펼쳐 표시하고 URL을 선택합니다.

©2013-2022 Tencent Cloud. All rights reserved.

Page 98 of 233



4. HTTP/HTTPS 리스너 섹션 오른쪽의 서버 목록에서 해당 서버 가중치를 수정합니다.

설명:

가중치가 클수록 요청이 더 많이 포워딩됩니다. 값 범위는 0 - 100(기본값: 10)입니다. 0으로 설정하면 리얼 서버는 새 요청 수신을 중지합니다. 세션 지속성을 활성화하면 리얼 서버의 요청이 고르게 분산되지 않을 수 있습니다. 자세한 내용은 [Load Balancing Algorithm Selection and Weight Configuration Examples](#)를 참고하십시오.

방법1: 단일 백엔드 CVM의 가중치 수정

4.1.1 가중치를 수정할 CVM 인스턴스를 찾아 마우스를 해당 가중치에 갖다 대고



아이콘을 클릭합니다.

<div>Bind Modify Port Modify Weight Unbind</div>						
<input type="checkbox"/>	CVM ID/Name	Port Health Statu	IP Address	Port	Weight	Ope...
<input type="checkbox"/>		Abnormal		80	10	Unbind
						Edit
<input type="checkbox"/>		Abnormal		80	10	Unbind


4.1.2 '가중치 수정' 팝업 창에서 새 가중치를 입력하고 **제출**을 클릭합니다.

방법2: 여러 백엔드 CVM의 가중치를 수정합니다.

설명:

일괄 수정을 수행한 후 백엔드 CVM은 동일한 가중치를 사용합니다.

4.1.1 수정할 CVM 인스턴스 앞의 체크 박스를 클릭하고 **가중치 수정**을 클릭합니다.

Bind	Modify Port	Modify Weight	Unbind			
✓	CVM ID/Name	Port Health Status	IP Address	Port	Weight	Ope...
✓		 Abnormal		80	10	Unbind
✓		Abnormal		80	10	Unbind

4.1.2 '가중치 수정' 팝업 창에서 새 가중치를 입력하고 **제출**을 클릭합니다.

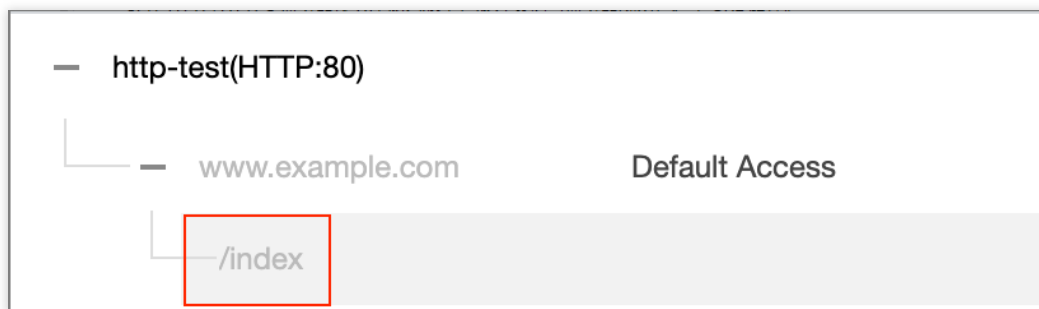
CLB용 리얼 서버 포트 수정

CLB 콘솔에서 리얼 서버 포트를 수정할 수 있습니다. 다음은 'HTTP/HTTPS 리스너'(TCP/UDP/TCP SSL 리스너에도 적용됨)를 사용할 때 리얼 서버 포트를 변경하는 예시를 보여줍니다.

설명:

API로 리얼 서버 포트를 수정하는 방법에 대한 자세한 내용은 [ModifyTargetPort](#)를 참고하십시오.

1. CLB 콘솔에 로그인합니다.
2. '인스턴스 관리' 페이지에서 'CLB' 인스턴스의 오른쪽에 있는 **리스너 구성**을 클릭합니다.
3. HTTP/HTTPS 리스너 섹션 왼쪽에 있는 목록에서 인스턴스 및 리스너 규칙을 펼쳐 표시하고 URL을 선택합니다.



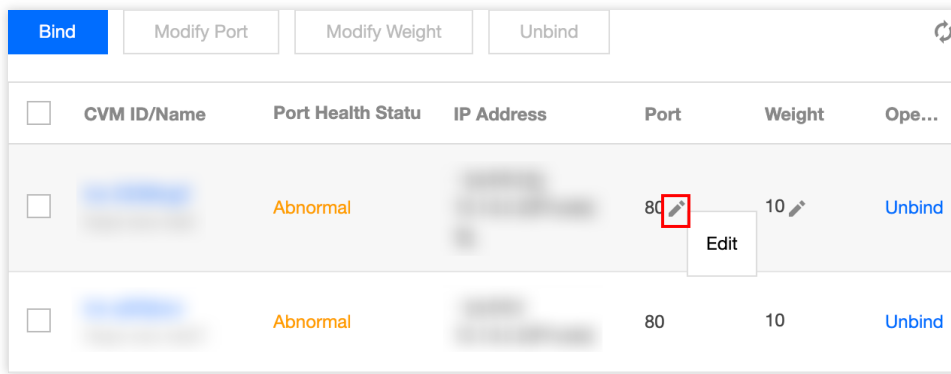
4. HTTP/HTTPS 리스너 섹션의 오른쪽 목록에서 해당 서버 포트를 수정합니다. 포트 선택 방법에 대한 자세한 내용은 [서버 상용 포트](#)를 참고하십시오.

방법1: 단일 백엔드 CVM의 포트 수정.

4.1.1 수정할 CVM 인스턴스를 찾아 마우스를 해당 포트에 갖다 대고



아이콘을 클릭합니다.



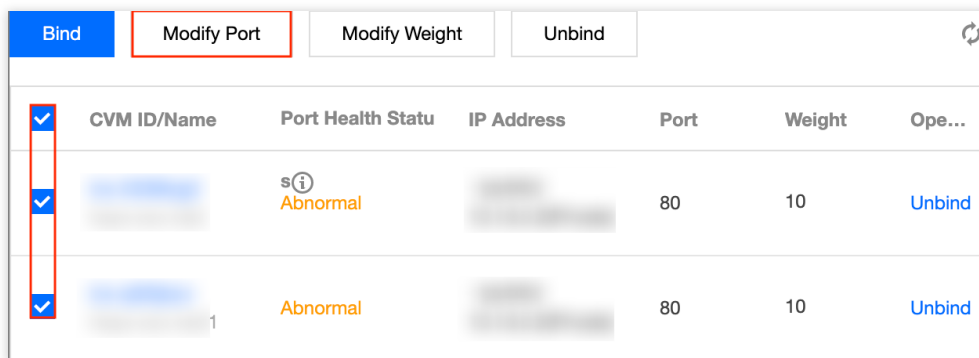
4.1.2 '포트 수정' 팝업 창에서 새 포트 값을 입력하고 **제출**을 클릭합니다.

방법2: 여러 백엔드 CVM 포트 일괄 수정.

설명:

일괄 수정을 수행한 후 백엔드 CVM은 동일한 포트를 사용합니다.

4.1.1 수정할 CVM 인스턴스 앞의 체크 박스를 클릭하고 **포트 수정**을 클릭합니다.



4.1.2 '포트 수정' 팝업 창에서 새 포트 값을 입력하고 **제출**을 클릭합니다.

CLB에서 리얼 서버 바인딩 해제

CLB 콘솔에서 바인딩된 리얼 서버를 바인딩 해제할 수 있습니다. 다음은 'HTTP/HTTPS 리스너'(TCP/UDP/TCP SSL 리스너에도 적용됨)를 사용할 때 리얼 서버의 바인딩을 해제하는 방법의 예시를 보여줍니다.

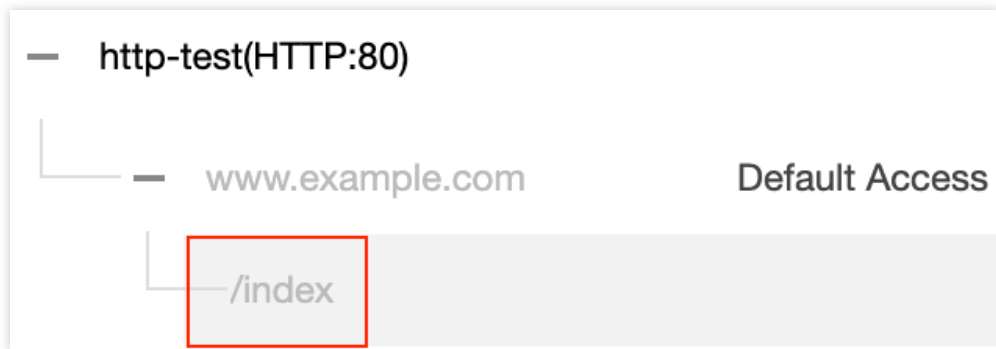
설명:

리얼 서버를 바인딩 해제하면 CVM 인스턴스에서 CLB 인스턴스가 바인딩 해제되고 CLB는 즉시 해당 서버에 대한 요청 포워딩을 중지합니다.

리얼 서버의 바인딩을 해제해도 CVM 인스턴스의 라이프사이클에는 영향을 미치지 않으며 리얼 서버 클러스터에 다시 추가될 수도 있습니다.

API를 사용하여 리얼 서버의 바인딩을 해제하는 방법에 대한 자세한 내용은 [DeregisterTargets](#)를 참고하십시오.

1. CLB 콘솔에 로그인합니다.
2. '인스턴스 관리' 페이지에서 'CLB' 인스턴스의 오른쪽에 있는 **리스너 구성**을 클릭합니다.
3. HTTP/HTTPS 리스너 섹션 왼쪽에 있는 목록에서 인스턴스 및 리스너 규칙을 펼쳐 표시하고 URL을 선택합니다.



4. HTTP/HTTPS 리스너 섹션의 오른쪽 목록에서 바인딩된 리얼 서버의 바인딩을 해제합니다.

방법1: 단일 백엔드 CVM을 바인딩 해제합니다.

4.1.1 대상 CVM 인스턴스를 선택하고 오른쪽 작업 열에서 **바인딩 해제**를 클릭합니다.

Bind		Modify Port	Modify Weight	Unbind		
<input type="checkbox"/>	CVM ID/Name	Port Health Status	IP Address	Port	Weight	Ope...
<input type="checkbox"/>		<div><div>s<i>i</i></div><div>Abnormal</div></div>		80	10	Unbind
<input type="checkbox"/>		Abnormal		80	10	Unbind

4.1.2 '바인딩 해제' 팝업 창에서 선택한 CVM 인스턴스를 확인하고 **제출**을 클릭합니다.

방법2: 여러 백엔드 CVM을 바인딩 해제합니다.

4.1.1 바인딩을 해제하려는 CVM 인스턴스 앞의 확인란을 클릭하고 **바인딩 해제**를 클릭합니다.

Bind

Modify Port

Modify Weight

Unbind

<input checked="" type="checkbox"/>	CVM ID/Name	Port Health Status	IP Address	Port	Weight	Oper...
<input checked="" type="checkbox"/>		<div> <div></div> <div>Abnormal</div> </div>		80	10	Unbind
<input checked="" type="checkbox"/>		Abnormal		80	10	Unbind

4.1.2 '바인딩 해제' 팝업 창에서 선택한 CVM 인스턴스를 확인하고 **제출**을 클릭합니다.

SCF 바인딩하기

최종 업데이트 날짜: : 2024-01-04 19:56:12

SCF 함수를 작성하여 백엔드 Web 서비스를 구현하고 CLB 인스턴스와 바인딩하여 서비스를 제공할 수 있습니다.

배경 정보

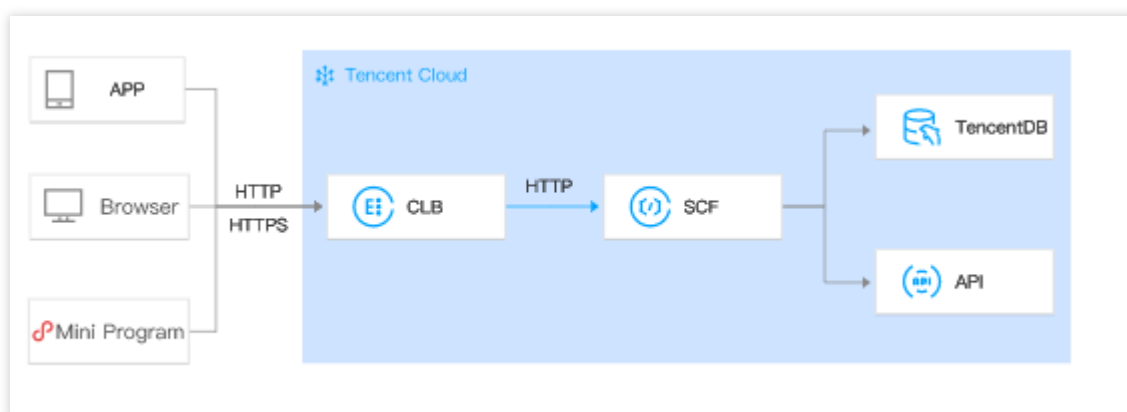
Tencent Cloud [Serverless Cloud Function\(SCF\)](#)은 서버를 구매하고 관리할 필요 없이 애플리케이션을 구축하고 실행할 수 있는 서버리스 실행 환경입니다. 함수를 생성한 후 CLB 트리거를 생성하여 함수와 이벤트를 바인딩할 수 있습니다. CLB 트리거는 요청 내용을 매개변수로 함수에 전달하고 함수의 결과를 요청자에게 응답으로 다시 반환합니다.

사용 사례

HTTP/HTTPS 일반 액세스

전자상거래, 소셜 미디어 및 톨 등 기타 서비스용 App과 개인 블로그, 이벤트 페이지 등을 위한 Web 응용 프로그램에 적용할 수 있습니다. 워크플로는 다음과 같습니다.

1. App, 브라우저, H5 페이지 또는 미니 프로그램에서 시작된 HTTP/HTTPS 요청은 CLB 인스턴스를 통해 SCF 기능에 액세스합니다.
2. CLB 인스턴스가 인증서 제거를 완료한 후 SCF는 HTTP 서비스만 제공하면 됩니다.
3. 그 다음 요청은 클라우드 데이터베이스에 쓰기 및 다른 API 호출과 같은 후속 처리를 위해 SCF 기능으로 전송됩니다.



CVM/SCF 간 전환

특히 장애 조치 시 HTTP/HTTPS 서비스를 CVM에서 SCF로 마이그레이션하는 데 적용할 수 있습니다. 워크플로는 다음과 같습니다.

1. App, 브라우저, H5 또는 미니프로그램 등이 HTTP/HTTPS 요청을 시작합니다.
2. 그 다음 요청은 DNS에 의해 두 CLB 인스턴스의 VIP로 레졸루션됩니다.

3. 하나의 CLB 인스턴스는 요청을 CVM으로 포워딩하고 다른 인스턴스는 이를 SCF로 포워딩합니다.
4. 백엔드에서 CVM에서 SCF로의 전환은 클라이언트측에 영향을 주지 않습니다.

CVM/SCF 비즈니스 전환

SCF를 사용하여 고탄력 서비스를 처리하고 CVM을 사용하여 타임 세일 및 스냅업 구매와 같은 시나리오에서 일상적인 비즈니스를 처리하는 데 적용할 수 있습니다.

1. DNS 확인을 통해 도메인 이름 A는 한 CLB 인스턴스의 VIP로 확인되고 도메인 이름 B는 다른 CLB 인스턴스의 VIP로 확인됩니다.
2. 하나의 CLB 인스턴스는 요청을 CVM으로 포워딩하고 다른 CLB 인스턴스는 요청을 SCF로 포워딩합니다.

제한 설명

SCF와의 바인딩은 광저우, 상하이, 베이징, 청두, 중국홍콩, 싱가포르, Mumbai, 도쿄 및 실리콘밸리에서만 사용할 수 있습니다.

SCF 기능은 IP별 청구 계정의 CLB 인스턴스에만 바인딩할 수 있지만 CVM별 청구 계정에는 바인딩할 수 없습니다. CVM별 청구 계정을 사용하는 경우 IP별 청구 계정으로 업그레이드하는 것이 좋습니다. 자세한 내용은 [Checking Account Type](#)을 참고하십시오.

SCF 함수는 클래식 CLB 인스턴스와 바인딩할 수 없습니다.

SCF 기능은 기본 네트워크 기반 CLB 인스턴스와 바인딩할 수 없습니다.

동일한 리전의 SCF 기능은 CLB 인스턴스와 바인딩될 수 있습니다. SCF 기능은 VPC에서만 바인딩할 수 있지만 리전에서는 바인딩할 수 없습니다.

SCF 기능은 IPv4 및 IPv6 NAT64 CLB 인스턴스에만 바인딩할 수 있지만 현재 IPv6 CLB 인스턴스에는 바인딩할 수 없습니다.

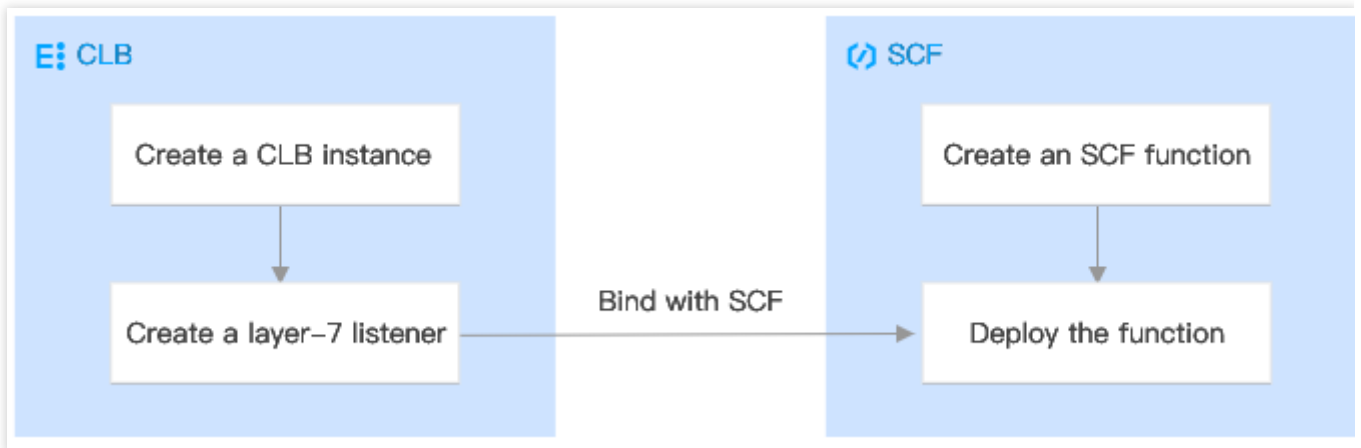
SCF 기능은 레이어 7 HTTP 및 HTTPS 리스너에만 바인딩할 수 있지만 레이어 7 QUIC 리스너 또는 레이어 4(TCP, UDP 및 TCP SSL) 리스너에는 바인딩할 수 없습니다.

SCF 'Event 함수'만 CLB 인스턴스와 바인딩할 수 있습니다.

전제 조건

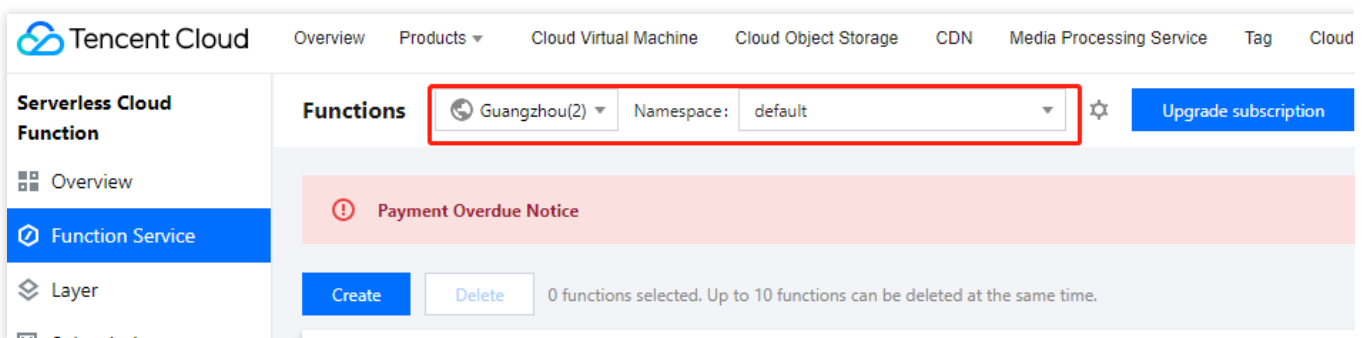
1. [CLB 인스턴스 생성](#)
2. [Configuring HTTP Listener](#) 또는 [Configuring HTTPS Listener](#)

작업 단계



1단계: 함수 생성

1. [Serverless 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **함수 서비스**를 클릭합니다.
2. 함수 서비스 페이지에서 함수를 생성할 리전과 네임스페이스를 선택하고 **생성**을 클릭하여 함수 생성 프로세스로 들어갑니다.



3. '함수 생성' 페이지에서 실제 필요에 따라 함수 생성 방법을 선택할 수 있습니다. 자세한 생성 방법은 [함수 생성](#)을 참고하십시오.

템플릿 생성: 함수 이름을 입력하여(필수) 함수 템플릿의 구성을 사용하여 함수 생성을 완료합니다.

처음부터 시작: 함수 이름과 실행 환경을 입력하여(필수) 함수를 생성합니다.

컨테이너 이미지 사용: 컨테이너 이미지를 기반으로 함수를 생성합니다. 자세한 내용은 [이미지를 사용하여 함수 배포](#)를 참고하십시오.

4. 본문은 **처음부터 시작**을 예로 들어 함수의 기본 정보를 구성합니다.

함수 유형: **이벤트 함수**와 **Web 함수**의 선택을 지원합니다.

이벤트 함수: 클라우드 API 및 다양한 트리거를 수신하는 JSON 형식의 이벤트 트리거 함수를 실행합니다. 자세한 내용은 [이벤트 함수 개요](#)를 참고하십시오.

Web 함수: HTTP 요청을 직접 수신하여 함수를 트리거하며, Web 서비스 시나리오에 적합합니다. 자세한 내용은 [Web 함수 개요](#)를 참고하십시오.

함수 이름: 함수 이름은 기본적으로 입력되며 필요에 따라 수정할 수 있습니다.

리전: CLB 인스턴스와 동일한 리전을 선택합니다.

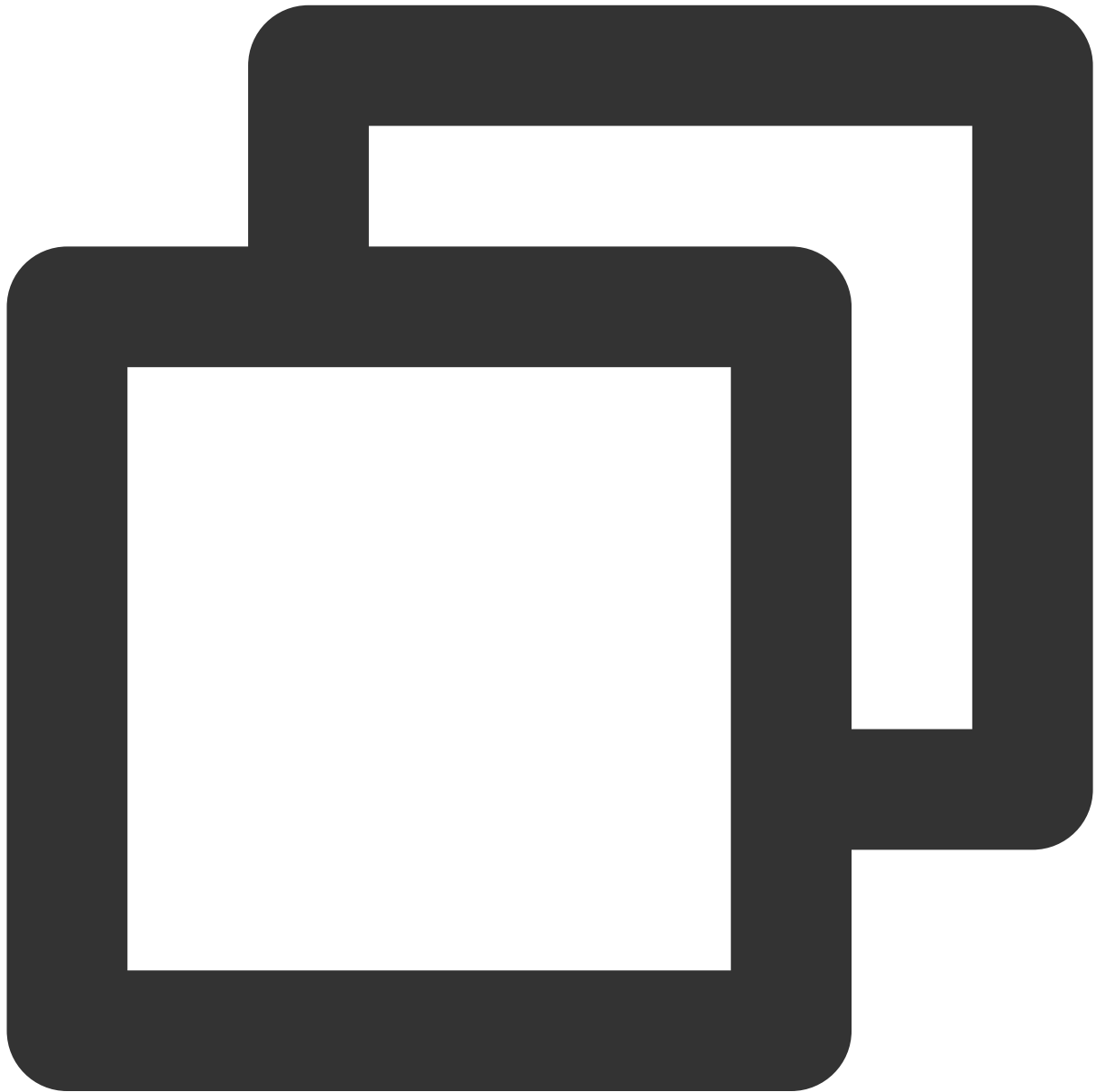
실행 환경: 실행 환경으로 'Python3.6'을 선택합니다. 필요에 따라 수정할 수 있습니다.

시간대: SCF는 기본적으로 UTC 시간을 사용하며 환경 변수 TZ를 구성하여 수정할 수 있습니다. 시간대를 선택하면 해당 시간대에 해당하는 TZ 환경 변수가 자동으로 추가됩니다.

5. 함수 코드 입력란에 다음 코드를 입력합니다.

주의사항:

CLB가 SCF에 바인딩되면 특정 응답 통합 형식으로 반환되어야 합니다. 자세한 내용은 [통합 응답](#)을 참고하십시오.



```
# -*- coding: utf8 -*-
import json
def main_handler(event, context):
```

```
return {
  "isBase64Encoded": False,
  "statusCode": 200,
  "headers": {"Content-Type": "text/html"},
  "body": "<html><body><h1>Hello CLB</h1></body></html>"
}
```

6. 로그 구성에서 로그 전달을 활성화할지 선택합니다.

Log Configuration ⓘ When log shipping is enabled, the function invocation logs are shipped to the SCF log topic in CLS by default, which will incur charges. For details, see [Log Shipping](#).

Log delivery ☐ Enable ⓘ

Log template ☒ Default ☐ Simplified ⓘ

로그 전달은 기본적으로 비활성화되어 있습니다. 활성화 시 함수 실행 로그를 지정된 위치에 실시간으로 전달할 수 있습니다. 자세한 내용은 [로그 전달 구성](#)을 참고하십시오.

주의사항

이미지 배포 함수 및 **Web** 함수는 현재 로그 형식 선택을 지원하지 않습니다.

7. 고급 구성에서는 실제 필요에 따라 함수에 대한 환경 구성, 권한 구성, 레이어 구성, 네트워크 구성 등을 진행할 수 있으며, 자세한 내용은 [함수 관련 구성](#)을 참고하십시오.

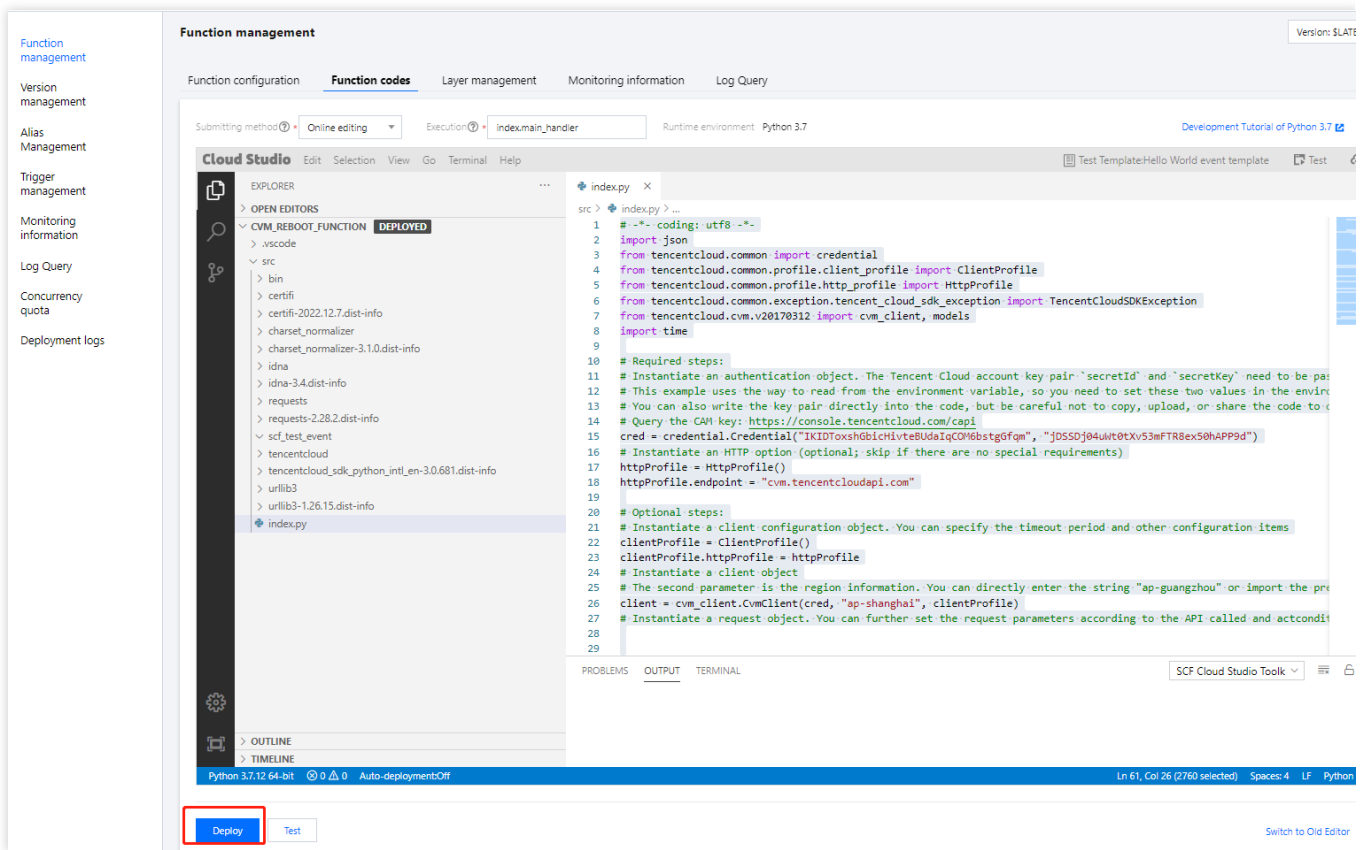
8. 트리거 구성에서 트리거 생성 여부를 선택합니다. '사용자 지정 생성'을 선택한 경우, 자세한 내용은 [트리거 개요](#)를 참고하십시오.

9. **완료**를 클릭합니다. 생성된 함수는 [함수 서비스](#)에서 확인할 수 있습니다.

2단계: 함수 배포

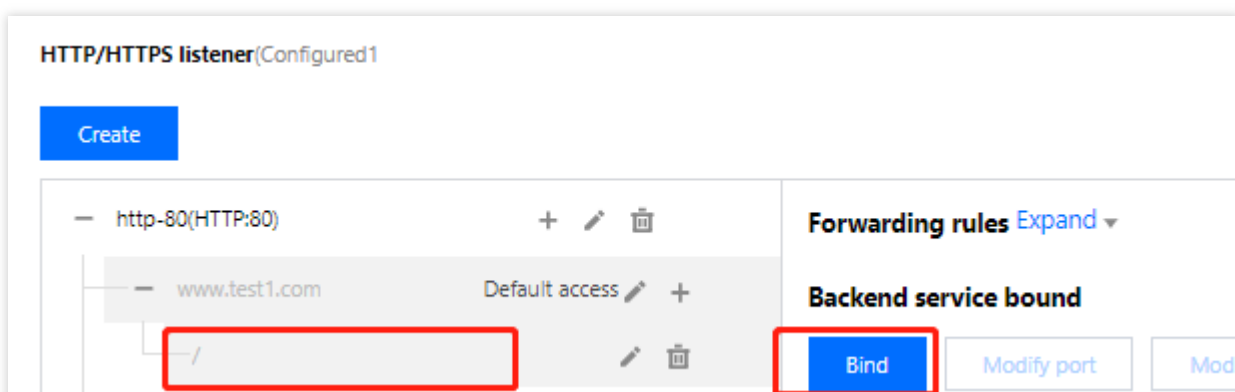
1. **함수 서비스** 목록 페이지에서 생성한 함수의 이름을 클릭합니다.

2. **함수 관리** 페이지에서 **함수 코드** 탭을 선택하고 하단의 **배포**를 클릭합니다.



3단계: 함수 바인딩

1. CLB 콘솔에 로그인하고 왼쪽 사이드바에서 **인스턴스 관리**를 클릭합니다.
2. 인스턴스 관리 페이지 **CLB** 탭에서 대상 인스턴스 오른쪽의 **작업** 열에서 **리스너 구성**을 클릭합니다.
3. HTTP/HTTPS 리스너 섹션에서 SCF 함수와 바인딩할 리스너를 선택합니다. 리스너 왼쪽에 있는 **+** 아이콘과 펼쳐진 도메인 이름 왼쪽에 있는 **+**를 클릭하고 펼쳐진 **URL** 경로를 선택한 다음 바인딩을 클릭합니다.



4. 팝업된 **리얼 서버 바인딩** 창에서 대상 유형을 **SCF**로 선택하고 구성 항목을 설정한 후 **확인**을 클릭합니다.

Bind with backend service

Target type ⓘ ☐ Instance ☐ IP type ☒ SCF

Namespace	Function name	Version/Alias	Weight ⓘ
<input type="text"/>	<input type="text"/>	Version <input type="text"/> \$LATEST	<input type="text" value="10"/> <input type="button" value="-"/> <input type="button" value="+"/>

5. 리스너 관리 탭의 포워딩 규칙 섹션에서 CLB 트리거가 생성되었음을 나타내는 CLB 인스턴스에 바인딩된 함수를 볼 수 있습니다.

Forwarding rules Expand

Backend service bound

<input type="checkbox"/>	Namespace	Function name	Port health status ⓘ	Version/Alias	Weight
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	Healthy	Version: \$LATEST	10

설명:

SCF 콘솔에서 CLB 트리거를 생성하여 CLB 인스턴스를 SCF 기능과 바인딩할 수도 있습니다. 자세한 내용은 [Creating Triggers](#)를 참고하십시오.

결과 검증

1. [SCF 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **함수 서비스**를 클릭합니다.
2. **함수 서비스** 목록 페이지에서 생성한 함수의 이름을 클릭합니다.
3. 함수 페이지에서 왼쪽의 **트리거 관리**를 클릭합니다.
4. **트리거 관리** 페이지에서 **액세스 경로**를 클릭합니다.

Trigger management

Tencent Cloud CMQ will be discontinued by June 2022. No more CMQ triggers can be created. Existing CMQ triggers are not affected. For details:

Create trigger

CLB trigger Triggered version: \$LATEST

Instance ID [redacted]

Listener [redacted] (HTTP:80)

Domain name/server [redacted]

Path /

Access path [redacted] ✓

5. 브라우저에서 액세스 경로를 엽니다. **Hello CLB**가 표시되면 함수가 성공적으로 배포된 것입니다.



관련 문서

[SCF 함수 생성](#)

리전 간 바인딩 2.0(New)

최종 업데이트 날짜: : 2023-04-28 10:31:35

CLB는 CCN을 통해 리전 간 CVM 인스턴스 바인딩을 지원하므로 다른 리전의 리얼 서버를 선택하고 CLB 인스턴스를 VPC 또는 리전 간에 바인딩할 수 있습니다.

이 기능은 현재 베타 테스트 중입니다. 사용해 보시려면 [베타 신청](#) 하십시오.

설명

리전 간 CVM 바인딩은 현재 클래식 CLB 인스턴스에서 지원되지 않습니다.

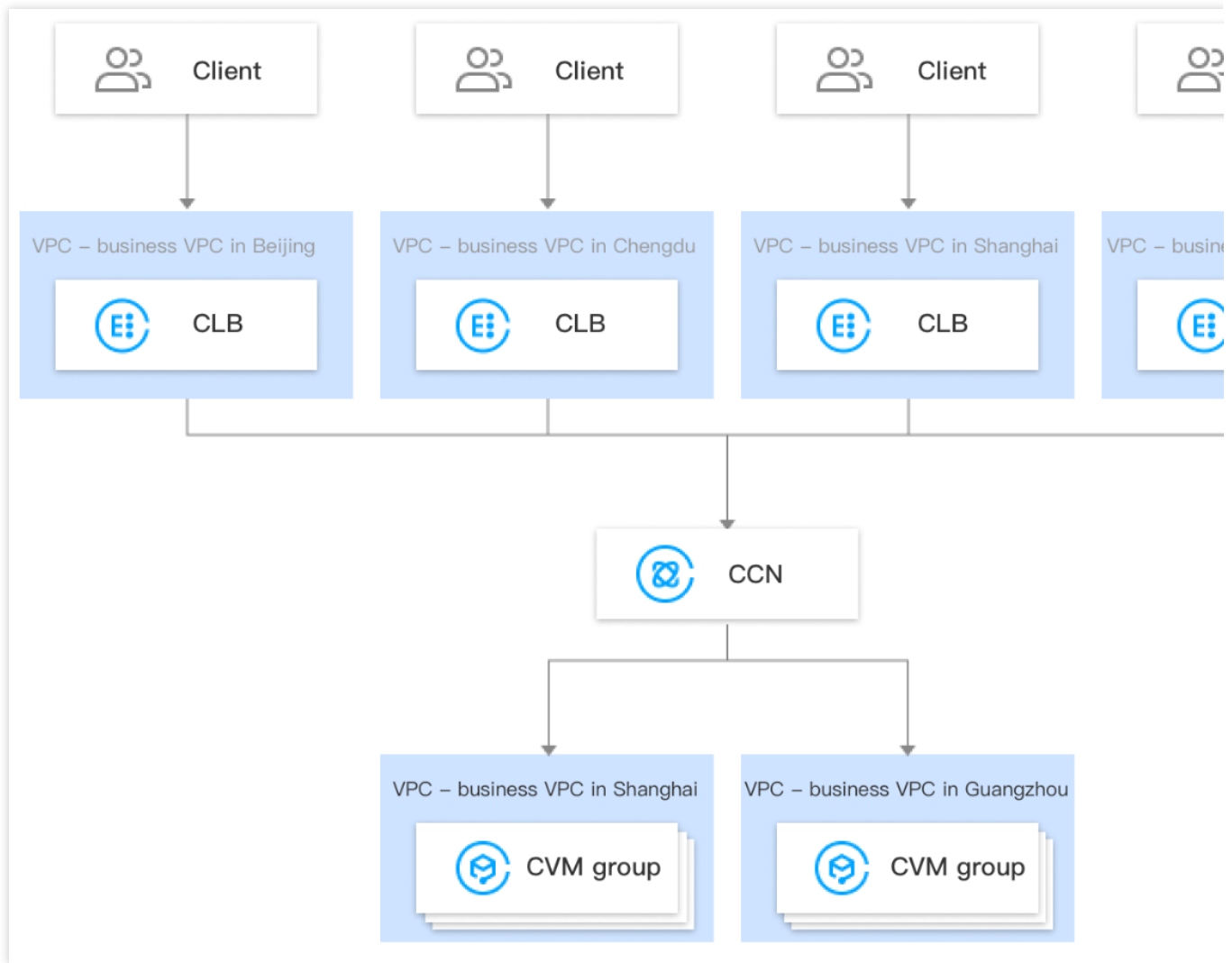
이 기능은 IP별 청구 계정에서만 사용할 수 있습니다. 계정 유형을 확인하려면 [Checking Account Type](#)을 참고하십시오.

리전 간 바인딩 2.0 및 하이브리드 클라우드 배포는 리얼 서버에서 Client IP 및 서비스 포트를 허용해야 하는 [보안 그룹 기본 허용 활성화](#)를 지원하지 않습니다.

리전 간 바인딩 2.0 및 하이브리드 클라우드 배포 시나리오에서는 다른 CLB 인스턴스를 바인딩할 수 없습니다(CLB에 CLB 바인딩 불가).

사용 사례

1. 리전 간 바인딩 기능은 다른 리전의 플레이어가 동일한 서버를 공유하는 P2P 게임 시나리오의 요구 사항을 잘 충족할 수 있습니다. 예를 들어 리얼 서버 클러스터가 광저우에 배포된 경우 상하이와 베이징에 CLB 인스턴스를 생성하고 광저우의 동일한 리얼 서버 클러스터에 바인딩하여 게임 가속화 및 트래픽 수렴을 구현하여 데이터 전송 품질을 보장하고 대기 시간을 줄일 수 있습니다.
2. 이 기능은 금융 산업 및 지불 시나리오의 엄격한 요구 사항을 충족하면서 주요 비즈니스 거래에서 전송 품질 및 데이터 일관성을 보장할 수 있습니다.



레거시 리전 간 바인딩과의 차이점

비교 항목	리전 간 바인딩 2.0(New)	리전 간 바인딩 1.0(Legacy)
동시에 여러 리전 내 서비스 바인딩 지원 여부	지원: 새 버전에서는 CLB 인스턴스를 여러 리전의 CVM 인스턴스에 동시에 바인딩할 수 있습니다. 예를 들어 베이징 리전의 CLB 인스턴스는 베이징과 상하이 리전의 CVM 인스턴스에 동시에 바인딩될 수 있습니다.	미지원: 레거시 버전에서 CLB 인스턴스는 한 리전에서만 CVM 인스턴스에 바인딩될 수 있습니다. 예를 들어 베이징 리전의 CLB 인스턴스는 상하이 리전의 CVM 인스턴스에 바인딩할 수 있지만 동시에 베이징 및 상하이 리전의 CLB 인스턴스에 바인딩할 수 없습니다.
리전 간 바인딩 사용 후 리전 내 바인딩으로 재 전환 가능 여부	지원: 새 버전에서는 리전 간 바인딩을 사용한 후 기존 리전 내 바인딩으로 다시 전환할 수 있습니다.	미지원: 레거시 버전에서 리전 간 바인딩을 위해 리얼 서버 리전 속성을 수정한 후 새 리전이 CLB 인스턴스의 리전과 다른 경우 기존

		리전 내 바인딩으로 다시 변경할 수 없습니다.
지원되는 CLB 유형	공중망 CLB 및 사설망 CLB.	공중망 CLB.
CVM 인스턴스 릴리스 시 CLB 자동 바인딩 해제 여부	<p>리전 내 바인딩 시 자동 바인딩 해제: CLB 인스턴스가 동일한 리전의 CVM 인스턴스에 바인딩된 경우 CVM 인스턴스가 릴리스되면 CLB 인스턴스는 자동으로 바인딩 해제됩니다.</p> <p>리전 간 바인딩 시 자동 바인딩 해제: CLB 인스턴스가 다른 리전의 CVM 인스턴스에 바인딩된 경우 CVM 인스턴스가 해제될 때 CLB 인스턴스가 자동으로 바인딩 해제되지 않으므로 수동으로 바인딩을 해제해야 합니다.</p>	<p>리전 내 바인딩 시 자동 바인딩 해제: CLB 인스턴스가 동일한 리전의 CVM 인스턴스에 바인딩된 경우 CVM 인스턴스가 릴리스되면 CLB 인스턴스는 자동으로 바인딩 해제됩니다.</p> <p>리전 간 바인딩 시 자동 바인딩 해제: CLB 인스턴스가 다른 리전의 CVM 인스턴스에 바인딩된 경우 CVM 인스턴스가 릴리스되면 CLB 인스턴스가 자동으로 바인딩 해제됩니다.</p>
가격이 유리한지 여부	CCN에서 과금됩니다. 비용은 세분화된 방식으로 제어되므로 가격이 낮아집니다.	일일 95번째 백분위수.

제한 조건

네트워크 간 CVM 인스턴스 바인딩은 현재 클래식 CLB 인스턴스에 대해 지원되지 않습니다.

이 기능은 IP별 청구 계정에서만 사용할 수 있습니다. 계정 유형을 확인하려면 [Checking Account Type](#)을 참고하십시오.

이 기능은 클래식 네트워크가 아닌 VPC에서만 지원됩니다.

이 기능은 IPv4 및 IPv6 NAT64 CLB 인스턴스에서 지원됩니다. 레이어 7 IPv6 CLB 인스턴스는 리전 간 바인딩 2.0 및 하이브리드 클라우드 배포를 지원하기 위해 이중 스택 바인딩을 활성화하여 IPv4 및 IPv6 CVM 인스턴스를 동시에 바인딩해야 합니다. IPv6 인스턴스가 IPv6 리얼 서버에 바인딩되면 리전 간 바인딩 2.0 및 하이브리드 클라우드 배포는 지원되지 않습니다.

리전 간 바인딩 2.0 및 하이브리드 클라우드 배포는 리얼 서버에서 Client IP 및 서비스 포트를 허용해야 하는 [보안 그룹 기본 허용 활성화](#)를 지원하지 않습니다.

리전 간 바인딩 2.0 및 하이브리드 클라우드 배포 시나리오에서는 다른 CLB 인스턴스를 바인딩할 수 없습니다(CLB에 CLB 바인딩 불가).

레이어 4 및 레이어 7(HTTP/HTTPS) CLB 서비스 모두 클라이언트 IP 가져오기를 지원합니다. 레이어 4 CLB의 경우 백엔드 CVM 인스턴스에서 얻은 소스 IP는 클라이언트 IP입니다. 레이어 7 CLB의 경우 X-Forwarded-For 또는 remote_addr 필드를 사용하여 클라이언트 IP를 직접 가져올 수 있습니다. 자세한 내용은 [IPv4 CLB를 통해 리얼 클라이언트 IP 가져오기](#)를 참고하십시오.

전제 조건

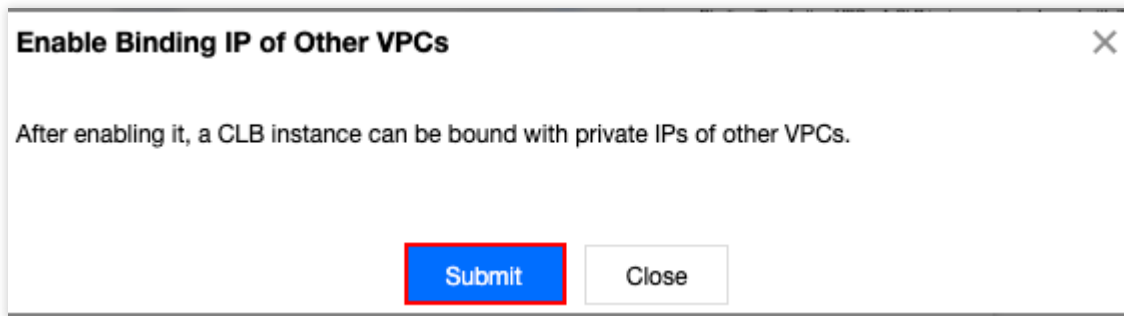
1. 베타 테스트 신청서를 제출했습니다. 중국 본토 내의 리전 간 바인딩의 경우 [베타 신청](#)을 통해, 중국 본토 외의 리전 간 바인딩의 경우 [Tencent Cloud 담당자에게 문의](#)하여 신청하십시오.
2. CLB 인스턴스 생성을 완료합니다. 자세한 내용은 [Creating CLB Instances](#)를 참고하십시오.
3. CCN 인스턴스 생성을 완료합니다. 자세한 내용은 [CCN 인스턴스 생성](#)을 참고하십시오.
4. 대상 VPC를 생성된 CCN 인스턴스와 연결합니다. 자세한 내용은 [네트워크 인스턴스 연결](#)을 참고하십시오.

작업 단계

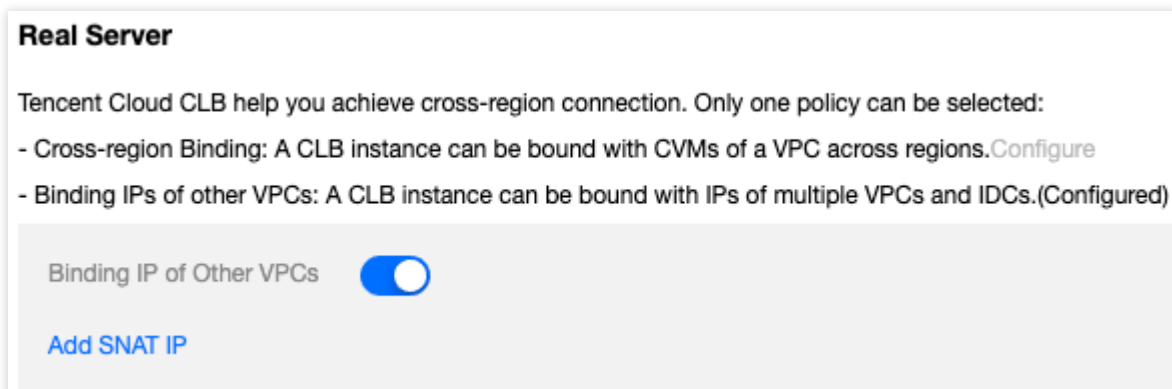
1. [CLB 콘솔](#)에 로그인합니다.
2. 인스턴스 관리 페이지에서 대상 CLB 인스턴스의 ID를 클릭합니다.
3. '리얼 서버' 섹션의 '기본 정보' 탭에서 [구성 클릭](#)을 클릭하여 다른 VPC의 사설망 IP를 바인딩합니다.

The screenshot shows the Tencent Cloud CLB console interface. The top navigation bar includes tabs for Basic Info, Listener Management, Redirection Configurations, Monitoring, and Security Group. The 'Basic Info' tab is selected, displaying details for instance lb-kyqjxnhg. The instance is in a 'Normal' status, located in the 'Guangzhou' region, 'Guangzhou Zone 4' availability zone, and is a 'Public Network' instance type. The 'Real Server' section on the right provides information about binding methods, including 'Cross-region Binding' and 'Binding IPs of other VPCs'.

4. '다른 VPC의 IP 열기 및 사용' 팝업 창에서 [제출](#)을 클릭합니다.



5. '기본 정보' 탭의 '리얼 서버' 섹션에서 '다른 VPC의 바인딩 IP'가 활성화되어 있는 것을 볼 수 있으며 이는 클라우드 내 IP를 바인딩할 수 있음을 나타냅니다.



6. 인스턴스 세부 정보 페이지에서 '리스너 관리' 탭을 열고 리스너 구성 섹션에서 리얼 서버를 CLB 인스턴스에 바인딩합니다. 자세한 내용은 [CLB에 리얼 서버 추가](#)를 참고하십시오.

7. 팝업 창에서 '다른 VPC'를 선택하고 **CVM**을 클릭한 후 하나 이상의 대상 CVM 인스턴스를 선택한 후 포워딩 포트와 가중치를 입력합니다. 그 다음 **확인**을 클릭합니다. 포트에 대한 자세한 내용은 [서버 상용 포트](#)를 참고하십시오.

Bind with backend service

Target type ⓘ ☒ Instance ☐ Other Private IP

Network type ⓘ ☐ Current VPC ☒ Other VPC

Network

Shanghai

Select an instance

CVM

ENI

Please enter the d

IP address

Search by IP address,

Instance ID/name

☒

☒

☐

☐

☐

10 / page

1

/ 1 page

Press Shift key to select more

Selected (2)

Instance ID/name	Port	Weight ⓘ
	80	<div>-</div> 10 <div>+</div>
	80	<div>-</div> 10 <div>+</div>

Confirm

Cancel

8. 이제 '바인딩된 리얼 서버' 섹션에서 다른 리전의 바인딩된 CVM 인스턴스를 볼 수 있습니다.

하이브리드 클라우드 배포

최종 업데이트 날짜: : 2023-08-01 11:34:45

하이브리드 클라우드 배포 시나리오에서는 CLB 인스턴스를 클라우드 외부의 로컬 IDC에 있는 IP에 직접 바인딩하여 VPC 및 IDC 전체의 리얼 서버에 바인딩할 수 있습니다.

이 기능은 베타 테스트 중입니다. 중국 본토 내의 리전 간 바인딩은 [베타 신청](#)을 통해, 중국 본토 외의 리전 간 바인딩은 [Tencent Cloud 담당자에게 문의](#)를 통해 체험해 볼 수 있습니다.

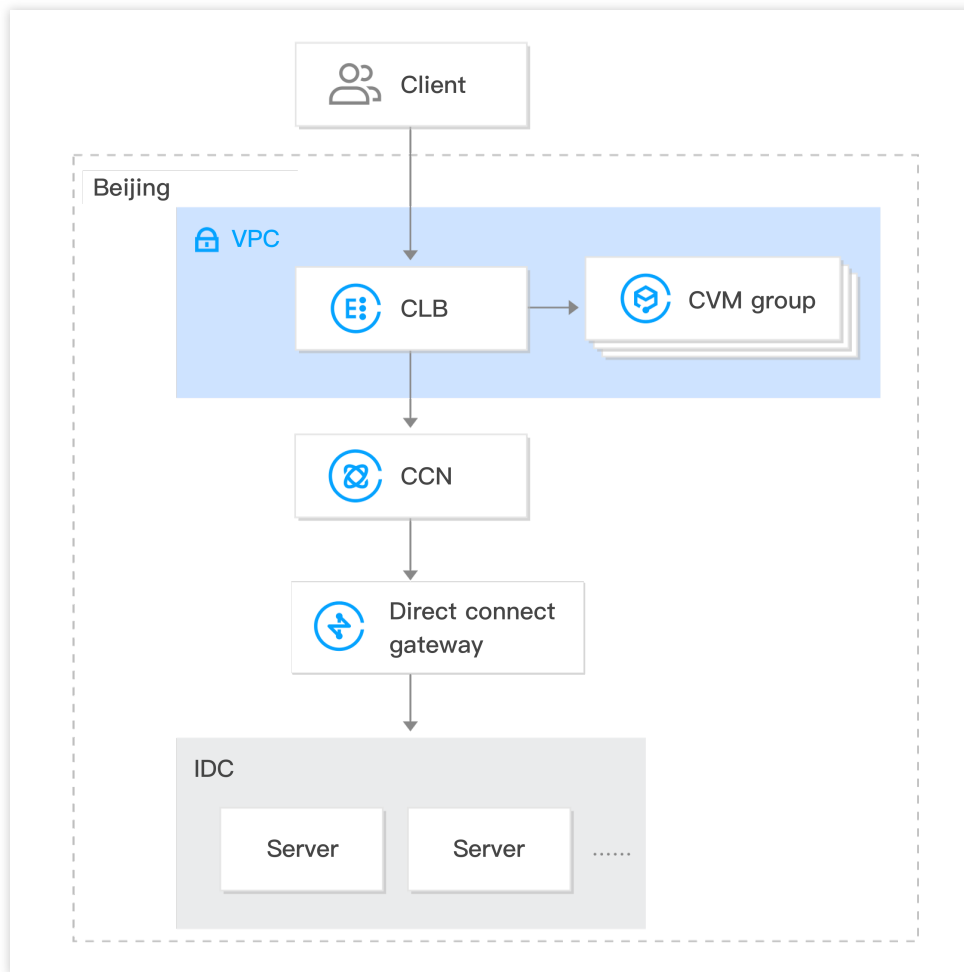
솔루션 장점

하이브리드 클라우드를 빠르게 구축하여 클라우드 안팎의 환경을 원활하게 연결할 수 있습니다. CLB는 클라우드 내의 VPC와 클라우드 밖의 IDC의 CVM 인스턴스에 요청을 동시에 전달할 수 있습니다.

Tencent Cloud의 고품질 공중망 액세스 기능을 재사용할 수 있습니다.

레이어 4/7 액세스, 상태 확인 및 세션 지속성과 같은 CLB의 풍부한 기능을 재사용할 수 있습니다.

사설망은 [CCN](#)을 통해 상호 연결될 수 있으며, 품질을 보장하기 위해 세분화된 라우팅이 지원되며, 비용 절감을 위해 다양한 계층별 가격이 지원됩니다.



제한

리전 간 바인딩 2.0은 현재 클래식 CLB를 지원하지 않습니다.

이 기능은 IP별 청구 계정에서만 사용할 수 있습니다. 계정 유형을 확인하려면 [Checking Account Type](#)을 참고하십시오.

이 기능은 클래식 네트워크가 아닌 VPC에서만 지원됩니다.

이 기능은 IPv4 및 IPv6 NAT64 CLB 인스턴스에서 지원됩니다. 레이어 7 IPv6 CLB 인스턴스는 리전 간 바인딩 2.0 및 하이브리드 클라우드 배포를 지원하기 위해 이중 스택 바인딩을 활성화하여 IPv4 및 IPv6 CVM 인스턴스를 동시에 바인딩해야 합니다. IPv6 인스턴스가 IPv6 리얼 서버에 바인딩되면 리전 간 바인딩 2.0 및 하이브리드 클라우드 배포는 지원되지 않습니다.

리전 간 바인딩 2.0 및 하이브리드 클라우드 배포는 리얼 서버에서 Client IP 및 서비스 포트를 허용해야 하는 [보안 그룹 기본 허용 활성화](#)를 지원하지 않습니다.

리전 간 바인딩 2.0 및 하이브리드 클라우드 배포 시나리오에서 다른 CLB 인스턴스를 바인딩할 수 없습니다(CLB에 CLB 바인딩 불가).

이 기능은 광저우, 상하이, 지난, 항저우, 허페이, 베이징, 텐진, 청두, 충칭, 중국홍콩, 싱가포르 및 실리콘밸리에서만 사용할 수 있습니다.

TCP 및 TCP SSL 리스너는 RS에서 TOA를 사용하여 소스 IP를 가져와야 합니다. 자세한 내용은 [하이브리드 클라우드 배포에서 TOA를 통해 리얼 클라이언트 IP 가져오기](#)를 참고하십시오.

HTTP 및 HTTPS 리스너는 X-Forwarded-For(XFF)를 사용하여 소스 IP를 가져와야 합니다.

UDP 리스너는 소스 IP를 가져올 수 없습니다.

전제 조건

1. 베타 테스트 신청서를 제출했습니다. 중국 본토 내의 리전 간 바인딩의 경우 [베타 신청](#)을 통해, 중국 본토 외의 리전 간 바인딩의 경우 [Tencent Cloud 담당자에게 문의](#)하여 신청하십시오.
2. CLB 인스턴스를 생성했습니다. 자세한 내용은 [CLB 인스턴스 생성](#)을 참고하십시오.
3. CCN 인스턴스를 생성했습니다. 자세한 내용은 [CCN 인스턴스 생성](#)을 참고하십시오.
4. IDC 및 대상 VPC와 연결된 직접 연결 게이트웨이를 생성된 CCN 인스턴스에 바인딩했습니다. 자세한 내용은 [네트워크 인스턴스 연결](#)을 참고하십시오.

작업 단계

1. [CLB 콘솔](#)에 로그인합니다.
2. '인스턴스 관리' 페이지에서 대상 CLB 인스턴스의 ID를 클릭합니다.
3. '리얼 서버' 섹션의 '기본 정보' 탭에서 구성을 클릭하여 다른 VPC의 사설망 IP를 바인딩합니다.

The screenshot shows the 'Basic Info' tab of a CLB instance. The instance name is 'lb-kyqjxnhg'. The status is 'Normal'. The instance type is 'Public Network'. The region is 'Guangzhou' and the availability zone is 'Guangzhou Zone 4'. The ISP is 'BGP'. The network is also shown. On the right, there is an 'Access Log' section with a note about the 'Store Logs in COS' feature being deactivated in all regions. Below that, there is a 'Real Server' section with a brief description of CLB's capabilities.

4. '본 VPC 외부의 IP 열기 및 사용' 팝업 창에서 제출을 클릭합니다.

The dialog box has a title 'Enable Binding IP of Other VPCs' and a close button (X). The text inside says: 'After enabling it, a CLB instance can be bound with private IPs of other VPCs.' At the bottom, there are two buttons: 'Submit' (highlighted with a red border) and 'Close'.

5. '리얼 서버' 섹션의 '기본 정보' 탭에서 SNAT IP 추가를 클릭합니다.

The 'Real Server' section shows a description of CLB's capabilities for cross-region connection. It lists two policies: 'Cross-region Binding' and 'Binding IPs of other VPCs'. The 'Binding IPs of other VPCs' policy is currently selected. Below the description, there is a toggle switch for 'Binding IP of Other VPCs' which is turned on. At the bottom, there is a button 'Add SNAT IP' (highlighted with a red border).

6. 'SNAT IP 추가' 팝업 창에서 '서브넷'을 선택하고 추가를 클릭하여 IP를 할당한 후 저장을 클릭합니다.

설명 :

SNAT IP는 주로 요청이 IDC 서버로 전달되는 하이브리드 클라우드 배포에 사용됩니다. CLB와 상호 연결된 IDC의 IP에 CLB 인스턴스를 바인딩할 때 할당해야 하며 VPC의 사설망 IP 역할을 합니다.

각 CLB 인스턴스에 대해 최대 10개의 SNAT IP를 구성할 수 있습니다.

각 CLB 인스턴스는 하나의 포워딩 규칙에서 하나의 SNAT IP를 구성하고 하나의 리얼 서버에 바인딩된 후 최대 5.5만 개의 연결을 지원합니다. 더 많은 SNAT IP 또는 리얼 서버를 구성하면 연결 수가 비례하여 증가합니다. CLB 1개의 인스턴스에 대해 2개의 SNAT IP를 구성하고 리얼 서버에 10개의 포트를 바인딩하여 최대 110만개 연결($2 \times 10 \times 5.5\text{만} = 110\text{만개}$)을 생성한다고 가정합니다. 연결 수에 따라 할당할 SNAT IP 수를 계산할 수 있습니다.

SNAT IP를 삭제하면 IP의 모든 연결이 끊어집니다. 유의하시기 바랍니다.

7. 인스턴스 세부 정보 페이지에서 '리스너 관리' 탭을 열고 리스너 구성 섹션에서 리얼 서버를 CLB 인스턴스에 바인딩합니다. 자세한 내용은 [CLB에 리얼 서버 추가](#)를 참고하십시오.

8. 팝업 창에서 '기타 사설망 IP'를 선택하고 사설망 IP 추가를 클릭한 후 대상 IDC 사설 IP, 포트 및 가중치를 입력합니다. 그 다음 확인을 클릭합니다. 포트에 대한 자세한 내용은 [서버 상용 포트](#)를 참고하십시오.

9. 이제 '바인딩된 리얼 서버' 섹션에서 바인딩된 IDC 사설망 IP를 볼 수 있습니다.

관련 문서

[Cross-Region Binding 2.0 \(New\)](#)

CVM 보안 그룹 구성

최종 업데이트 날짜: : 2024-01-04 19:56:56

CVM 보안 그룹 개요

CLB의 백엔드 CVM 인스턴스는 방화벽 역할을 하는 [보안 그룹](#)을 통해 액세스 제어를 수행할 수 있습니다.

하나 이상의 보안 그룹을 백엔드 CVM과 연결하고 각 보안 그룹에 하나 이상의 규칙을 추가하여 서로 다른 서버의 트래픽 액세스 권한을 제어할 수 있습니다. 보안 그룹에 대한 규칙은 언제든지 수정할 수 있으며 새 규칙은 해당 보안 그룹과 연결된 모든 인스턴스에 자동으로 적용됩니다. 자세한 내용은 [보안 그룹](#)을 참고하십시오. [VPC](#) 환경에서 [Network ACLs](#)를 사용하여 액세스를 제어할 수도 있습니다.

CVM 보안 그룹 구성

Client IP를 허용하고 CVM 보안 그룹에서 서비스 포트를 열어야 합니다.

CLB 인스턴스를 사용하여 비즈니스 트래픽을 CVM 인스턴스로 포워딩하려는 경우 효과적인 상태 확인을 위해 CVM 보안 그룹을 다음과 같이 구성해야 합니다.

1. 공중망 CLB: CLB 인스턴스가 VIP를 사용하여 백엔드 CVM의 상태를 확인할 수 있도록 백엔드 CVM의 보안 그룹에서 CLB VIP를 허용해야 합니다.

2. 사설망 CLB:

사설망 CLB(이전의 '애플리케이션 사설망 CLB')의 경우 CLB 인스턴스가 VPC에 있는 경우 상태 확인을 위해 백엔드 CVM의 보안 그룹에서 CLB VIP를 허용해야 합니다. CLB 인스턴스가 기본 네트워크에 있는 경우 기본적으로 상태 확인 IP가 허용되므로 추가 구성이 필요하지 않습니다.

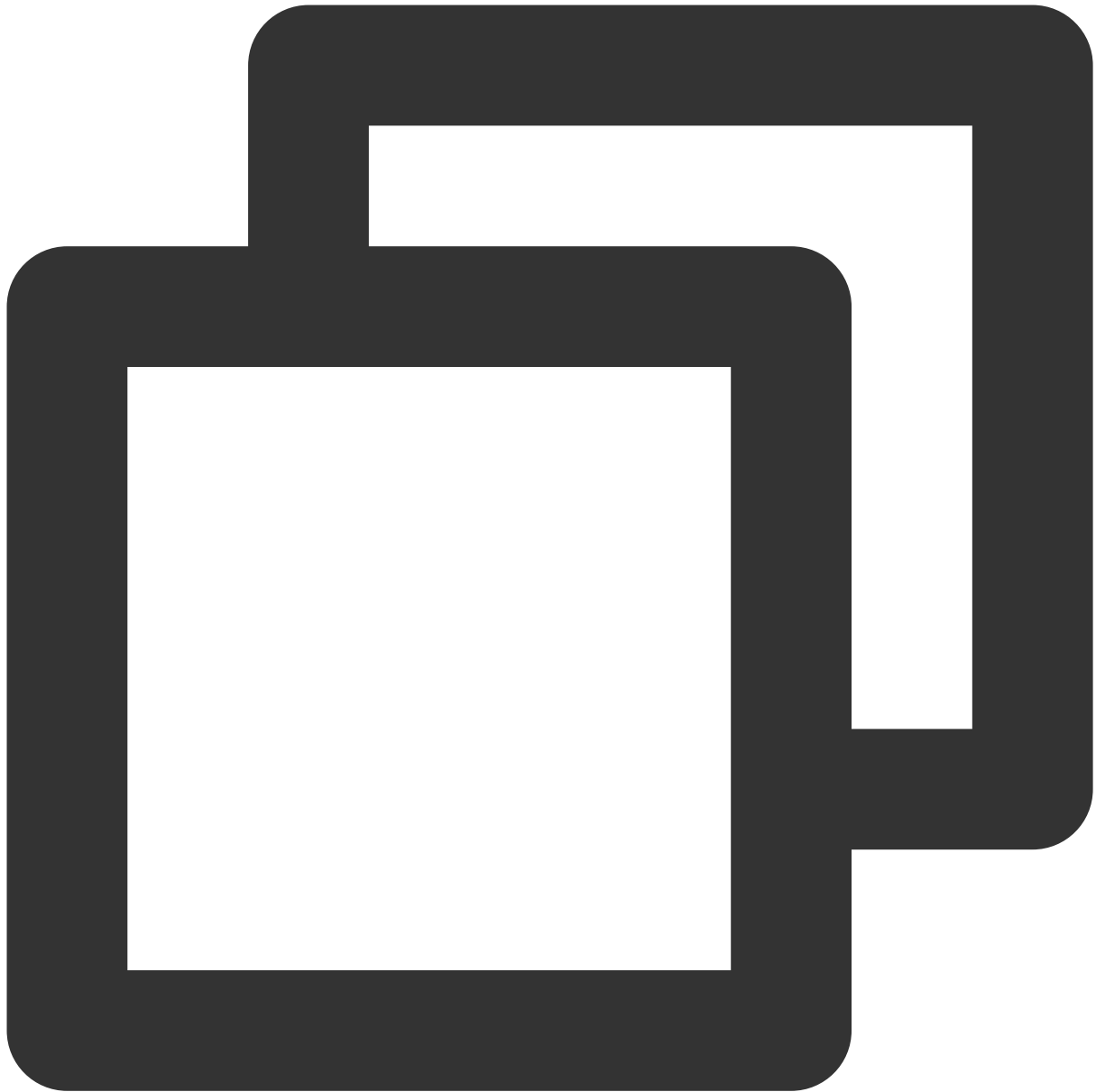
CVM 보안 그룹 구성 예시

이 예시는 CLB를 통해 CVM에 액세스할 때 CVM 보안 그룹을 구성하는 예시를 보여줍니다. [Configuring CLB Security Group](#)

을 참고하여 CLB 보안 그룹의 규칙을 구성합니다.

적용 시나리오1:

TCP:80 리스너 및 백엔드 서비스 포트 8080으로 구성된 공중망 CLB의 경우 Client IP(ClientA IP 및 ClientB IP)만 CLB에 액세스하도록 허용하려면 백엔드 CVM 보안 그룹의 인바운드 규칙을 다음과 같이 구성해야 합니다.



```
ClientA IP + 8080 allow
ClientB IP + 8080 allow
CLB VIP    + 8080 allow
0.0.0.0/0  + 8080 drop
```

적용 시나리오2:

HTTP:80 리스너 및 백엔드 서비스 포트 8080으로 구성된 공중망 CLB의 경우 모든 Client IP가 CLB에 액세스하도록 허용하려면 백엔드 CVM 보안 그룹의 인바운드 규칙을 다음과 같이 구성해야 합니다.

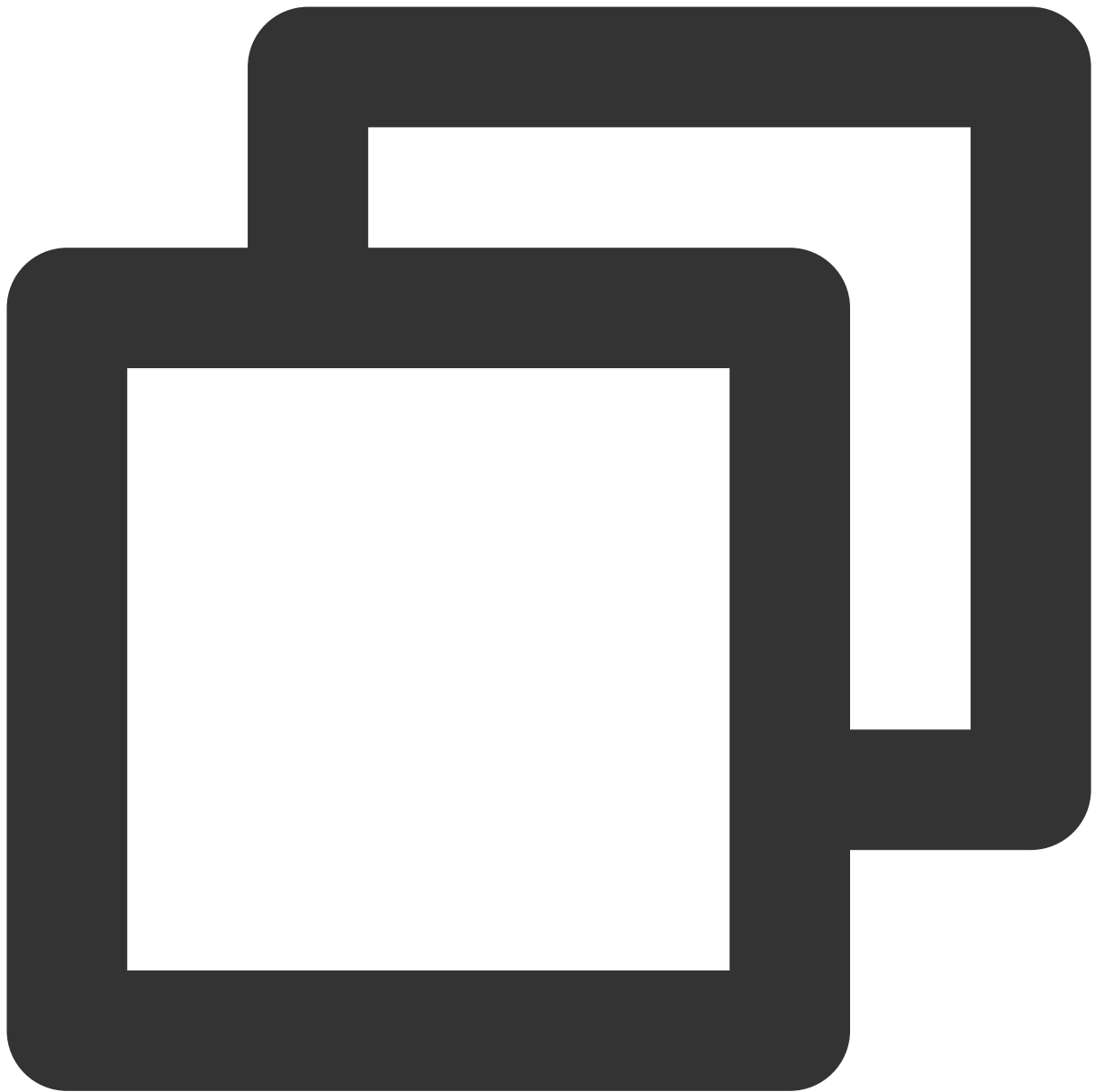


```
0.0.0.0/0 + 8080 allow
```

적용 시나리오3:

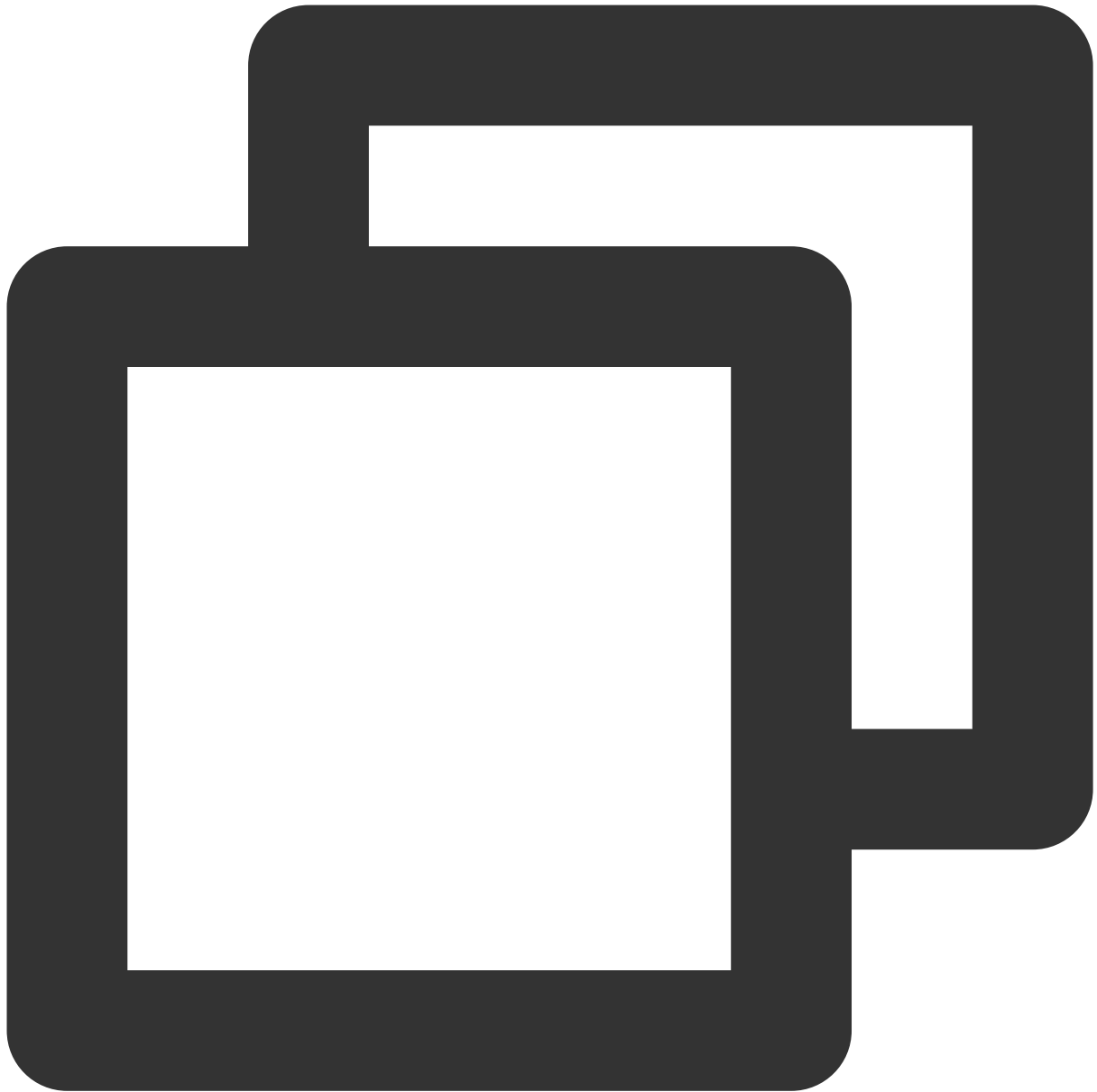
CVM 보안 그룹의 CLB VIP가 상태 확인을 수행하도록 허용합니다. VPC를 사용하고 TCP:80 리스너와 리얼 서버 포트 8080으로 구성된 사설망 CLB(이전의 '애플리케이션 사설망 CLB')의 경우, Client IP(ClientA IP 및 ClientB IP)만 CLB에 액세스하도록 허용하고 VIP 및 CLB에 바인딩된 백엔드 CVM에만 액세스하도록 Client IP를 제한하려면,

- 리얼 서버에 대한 보안 그룹 인바운드 규칙을 다음과 같이 구성합니다.



```
ClientA IP + 8080 allow
ClientB IP + 8080 allow
CLB VIP    + 8080 allow
0.0.0.0/0  + 8080 drop
```

b. Client로 사용되는 서버에 대한 보안 그룹 아웃바운드 규칙을 다음과 같이 구성합니다.



```
CLB VIP      + 8080 allow
0.0.0.0/0    + 8080 drop
```

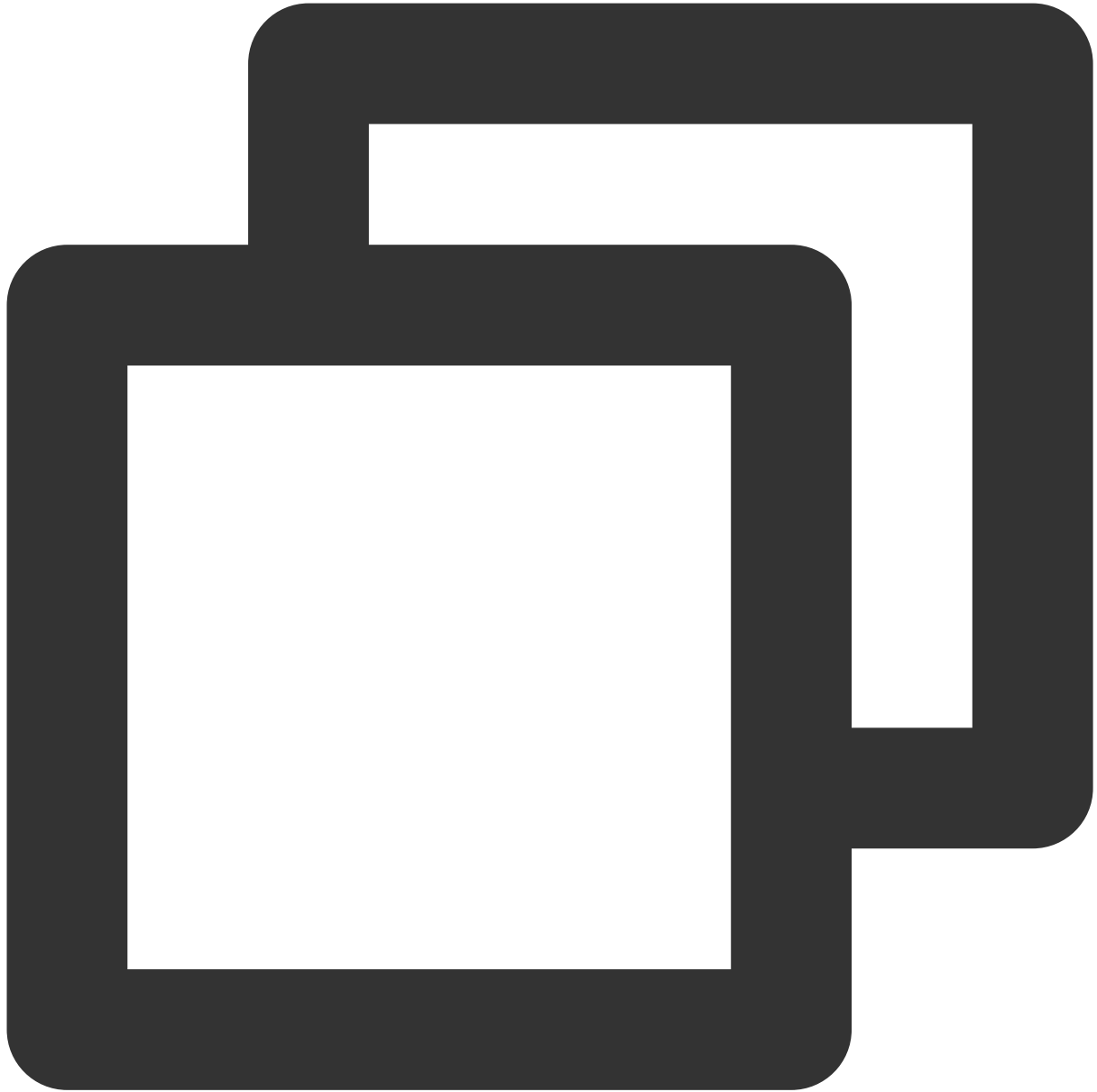
적용 시나리오4: 블록리스트

일부 Client IP가 액세스 요청을 거부하도록 블록리스트를 구성해야 하는 경우 클라우드 서비스와 연결된 보안 그룹을 구성할 수 있습니다. 보안 그룹 규칙은 다음과 같이 구성해야 합니다.

거부할 Client IP + 포트를 보안 그룹에 추가하고 정책 열에서 이 IP의 액세스를 거부하는 옵션을 선택합니다.

기본적으로 모든 IP에서 포트에 대한 액세스 요청을 허용하도록 위의 구성을 완료한 후 다른 보안 그룹 규칙을 추가합니다.

구성이 완료되면 보안 그룹 규칙은 다음과 같습니다.



```
clientA IP + port drop  
clientB IP + port drop  
0.0.0.0/0 + port accept
```

주의 :

상기 단계를 **지정된 순서대로 엄격하게** 따르십시오. 그렇지 않으면 블록리스트 구성이 실패할 수 있습니다.
보안 그룹은 상태를 저장합니다. 위의 구성은 모두 **인바운드 규칙**의 구성입니다.

CVM 보안 그룹 운영 가이드

콘솔을 사용하여 백엔드 CVM 보안 그룹 관리

1. [CLB 콘솔](#)에 로그인하고 해당 CLB 인스턴스 ID를 클릭하여 CLB 세부 정보 페이지로 이동합니다.
2. CLB에 바인딩된 CVM 페이지에서 대상 백엔드 CVM ID를 클릭하여 CVM 세부 정보 페이지로 이동합니다.
3. **보안 그룹** 탭을 클릭합니다. 탭에서 보안 그룹을 바인딩/바인딩 해제합니다.

Tencent Cloud API를 사용하여 백엔드 CVM 보안 그룹 관리

[AssociateSecurityGroups](#) 및 [DisassociateSecurityGroups](#)를 참고하십시오.

상태 확인

상태 확인 개요

최종 업데이트 날짜: : 2024-01-04 19:57:15

CLB 인스턴스는 상태 확인을 통해 리얼 서버의 가용성을 결정하여 프런트엔드 비즈니스가 리얼 서버 예외의 영향을 받는 것을 방지하고 비즈니스의 전반적인 가용성을 향상시킵니다.

상태 확인이 활성화되면 백엔드 CVM 인스턴스의 가중치(0 포함)에 관계없이 CLB 인스턴스는 항상 상태 확인을 수행합니다. 인스턴스 목록 페이지 또는 리스너의 바인딩된 리얼 서버 세부 정보 페이지의 상태 열에서 '상태 확인' 상태를 확인할 수 있습니다.

백엔드 CVM 인스턴스가 비정상인 경우 CLB 인스턴스는 새 요청을 비정상 인스턴스가 아닌 다른 일반 CVM 인스턴스에 자동으로 포워딩합니다.

비정상적인 CVM 인스턴스가 복구되면 CLB 서비스에서 다시 사용되며 새로운 요청을 받습니다.

모든 리얼 서버가 비정상으로 확인되면 요청이 모든 백엔드 CVM 인스턴스로 포워딩됩니다.

상태 확인이 비활성화된 경우 CLB 인스턴스는 비정상적인 서버를 포함한 모든 리얼 서버로 트래픽을 포워딩합니다. 따라서 CLB 인스턴스의 상태 확인을 활성화하여 리얼 서버를 자동으로 확인하고 비정상적인 서버를 제거하는 것이 좋습니다.

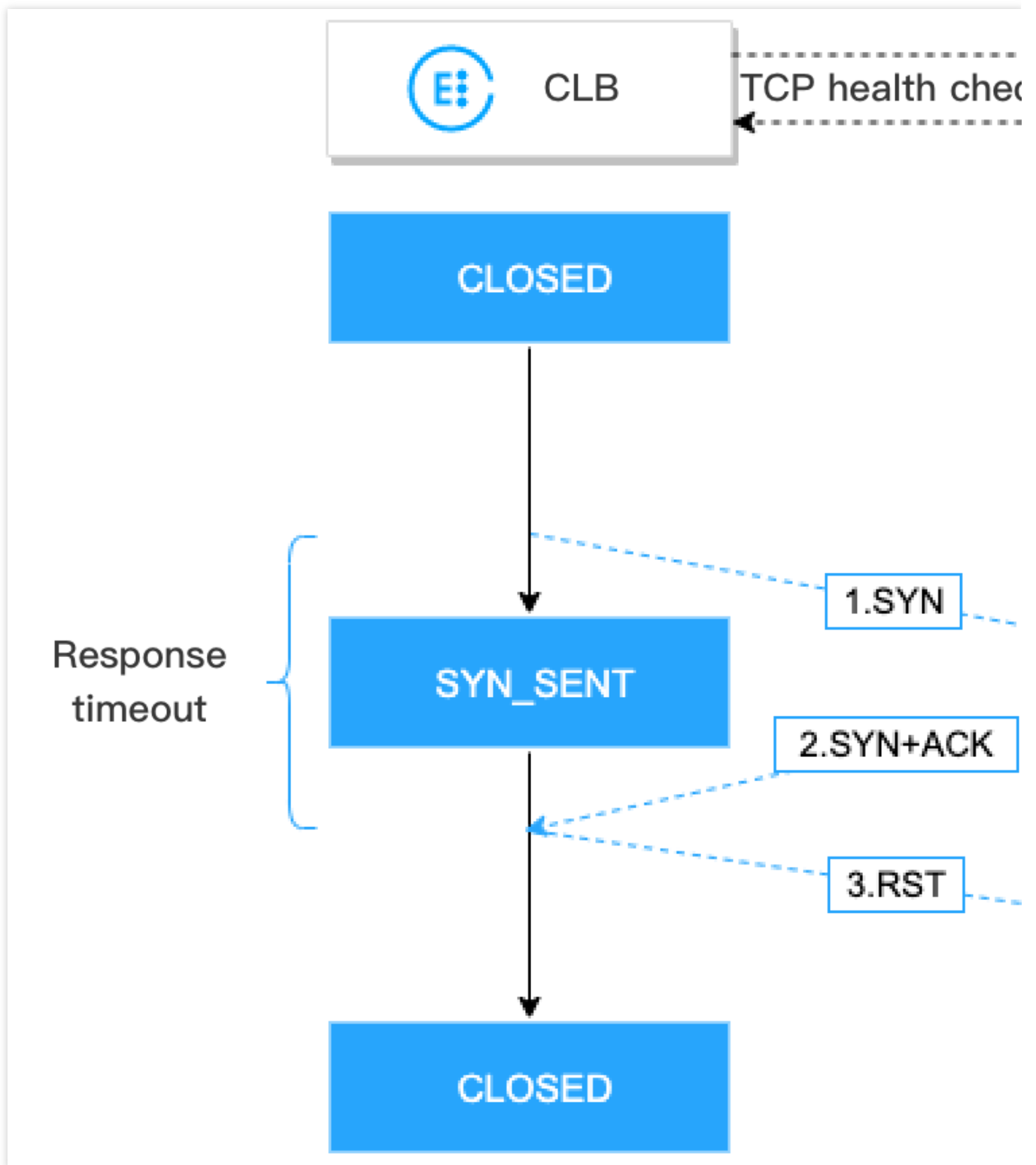
상태 확인 상태

백엔드 CVM 인스턴스의 상태 확인 상태 설명은 다음과 같습니다.

상태	설명	트래픽 포워딩 여부
감지 중	확인 간격 × 정상 임계값 기간 동안의 새 백엔드 CVM 인스턴스의 상태입니다. 예를 들어 확인 간격이 2s이고 정상 임계값이 3회라고 가정하면 백엔드 CVM 인스턴스는 6s 동안 이 상태를 유지합니다.	CLB는 '감지 중'인 백엔드 서비스로 트래픽을 포워딩하지 않습니다.
정상	리얼 서버 정상	CLB는 트래픽을 '정상' 백엔드 서비스로 포워딩합니다.
비정상	리얼 서버 비정상	CLB는 '비정상' 백엔드 서비스로 트래픽을 포워딩하지 않습니다. 레이어 4 리스너 또는 레이어 7 URL 규칙에 따라 CLB 인스턴스가 모든 리얼 서버가 비정상임을 감지하면 모든 리얼 서버로 요청을 포워딩합니다.
비활성화됨	상태 확인 비활성화	CLB는 트래픽을 백엔드 서비스로 포워딩합니다.

TCP 상태 확인

레이어 4 TCP 리스너의 경우 SYN 패킷, 즉 TCP 3방향 핸드셰이크를 통해 백엔드 CVM 인스턴스의 상태를 가져오도록 TCP 상태 확인을 구성할 수 있습니다. 또한 이를 위해 프로토콜의 요청 및 반환 내용을 사용자 지정할 수 있습니다.



TCP 상태 확인 메커니즘은 다음과 같습니다.

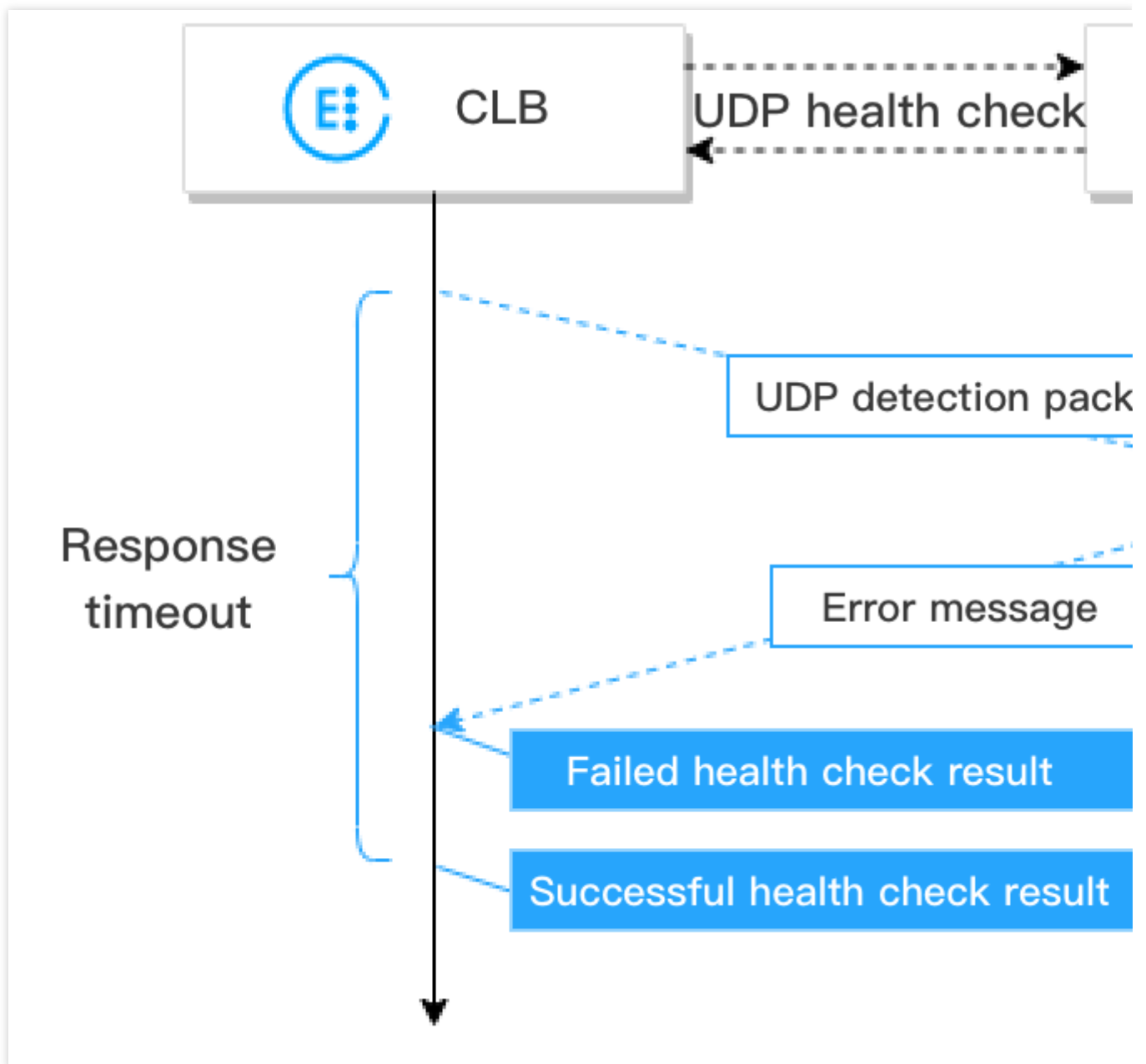
1. CLB 인스턴스는 백엔드 CVM 인스턴스(사실망 IP+상태 확인 포트)에 SYN 연결 요청 패킷을 보냅니다.
2. SYN 요청 패킷을 수신한 후 백엔드 CVM 인스턴스는 포트가 정상적으로 수신 중이면 SYN+ACK 응답 패킷을 반환합니다.
3. CLB 인스턴스가 응답 제한 시간 내에 반환된 SYN+ACK 응답 패킷을 받으면 리얼 서버가 정상이고 상태 확인 결과가 성공적임을 나타냅니다. 그런 다음 CLB 인스턴스는 백엔드 CVM 인스턴스에 TCP 재설정(RST) 패킷을 보내 TCP

연결을 끊습니다.

4. CLB 인스턴스가 응답 제한 시간 내에 반환된 SYN+ACK 응답 패킷을 수신하지 못하면 리얼 서버가 비정상적이며 상태 확인 결과가 실패한 것입니다. 그런 다음 CLB 인스턴스는 백엔드 CVM 인스턴스에 TCP 재설정(RST) 패킷을 보내 TCP 연결을 끊습니다.

UDP 상태 확인

레이어 4 UDP 리스너의 경우 `Ping` 명령을 실행하고 UDP 감지 패킷을 상태 확인 포트에 전송하여 백엔드 CVM 인스턴스의 상태를 가져오도록 UDP 상태 확인을 구성할 수 있습니다. 또한 이를 위해 프로토콜의 요청 및 반환 내용을 사용자 지정할 수 있습니다.



UDP 상태 확인 메커니즘은 다음과 같습니다.

1. CLB 인스턴스는 백엔드 CVM 인스턴스의 사설망 IP에 `Ping` 명령을 보냅니다.
2. 그런 다음 CLB 인스턴스는 UDP 감지 패킷을 (사설망 IP+상태 확인 포트) 백엔드 CVM 인스턴스로 보냅니다.
3. `Ping` 명령이 성공하고 백엔드 CVM 인스턴스가 응답 제한 시간 내에 `port XX unreachable` 오류를 반환하지 않으면 리얼 서버가 정상이고 상태 확인 결과가 성공임을 나타냅니다.
4. `Ping` 명령이 실패하거나 백엔드 CVM 인스턴스가 응답 제한 시간 내에 `port XX unreachable` 오류를 반환하는 경우 리얼 서버가 비정상적이며 상태 확인 결과가 실패임을 나타냅니다.

주의 :

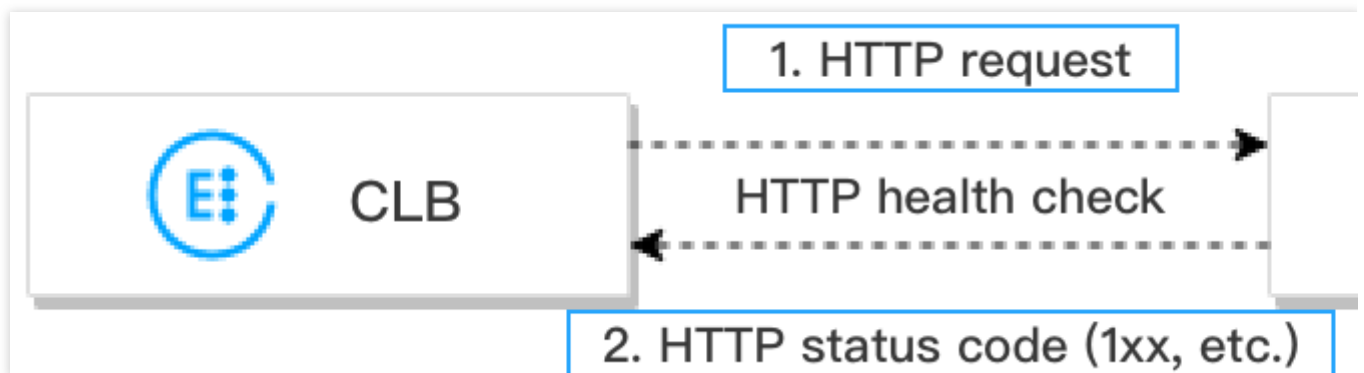
1. UDP 상태 확인은 ICMP를 기반으로 하므로 백엔드 CVM 인스턴스가 ICMP 패킷(즉, `Ping` 명령이 지원됨) 및 ICMP 포트에 연결할 수 없는 패킷(즉, 포트를 감지할 수 있음)에 응답하도록 허용되어야 합니다.

2. Linux 서버가 백엔드 CVM 인스턴스로 사용되는 경우 Linux 서버는 ICMP 공격으로부터 자신을 방어하는 메커니즘이 있으므로 높은 동시성 동안 ICMP 패킷을 보내는 서버의 속도가 제한됩니다. 이 경우 리얼 서버가 비정상이더라도 `port XX unreachable` 오류를 CLB 인스턴스에 반환할 수 없습니다. 그러면 CLB 인스턴스는 상태 확인 결과가 성공적이라고 판단하므로 리얼 서버의 실제 상태를 반환할 수 없습니다.

솔루션: 사용자 지정 입력 및 출력 문자열을 사용하여 UDP 상태 확인을 구성할 수 있습니다. 그래서 상태 확인에서 사용자 지정 입력 문자열은 리얼 서버로 보내지고, 그 결과는 CLB 인스턴스가 사용자 지정 응답 문자열을 받은 후에야 성공으로 판단됩니다. 이 메소드는 상태 확인 입력 문자열을 처리하고 사용자 지정 출력 문자열을 반환해야 하는 리얼 서버를 기반으로 합니다.

HTTP 상태 확인

레이어 4 TCP 리스너 및 레이어 7 HTTP/HTTPS 리스너의 경우 HTTP 요청을 전송하여 백엔드 CVM 인스턴스의 상태를 가져오도록 HTTP 상태 확인을 구성할 수 있습니다.



HTTP 상태 확인 메커니즘은 다음과 같습니다.

1. 상태 확인 구성에 따라 CLB 인스턴스는 HTTP 요청(대상 도메인 이름이 지정됨)을 백엔드 CVM 인스턴스(사설망 IP+상태 확인 포트+확인 경로)로 보낼 수 있습니다.
2. 요청을 수신한 후 백엔드 CVM 인스턴스는 해당 HTTP 상태 코드를 반환합니다.
3. CLB 인스턴스가 응답 제한 시간 내에 반환된 HTTP 상태 코드를 수신하고 HTTP 상태 코드가 설정된 값과 일치하면 상태 확인 결과가 성공했음을 나타내며, 그렇지 않으면 실패했음을 나타냅니다.
4. CLB 인스턴스가 응답 제한 시간 내에 백엔드 CVM 인스턴스로부터 응답을 받지 못하면 상태 확인 결과가 실패했음을 나타냅니다.

설명 :

레이어 7 HTTPS 리스너의 경우 HTTPS 리스너 포워딩 규칙의 백엔드 프로토콜로 HTTP를 선택하면 HTTP 상태 확인이 수행됩니다. HTTPS를 선택하면 HTTPS 상태 확인이 수행됩니다.

HTTPS 상태 확인은 기본적으로 **HTTP 상태 확인**과 동일합니다. 차이점은 HTTPS 상태 확인에서 HTTPS 요청이 전송되고 백엔드 CVM 인스턴스 상태가 반환된 HTTPS 상태 코드에 의해 결정된다는 것입니다.

상태 확인 시간 창

CLB 상태 확인 메커니즘은 비즈니스 가용성을 향상시키지만 빈번한 상태 확인 오류는 불필요한 서버 전환을 유발하여 시스템 가용성을 손상시킬 수 있습니다. 따라서 상태 확인 시간 창에서 결과가 여러 번 동일한 경우에만 상태 확인 상태를 정상과 비정상으로 전환할 수 있습니다. 상태 확인 시간 창은 아래 요소를 기반으로 합니다.

상태 확인 구성	설명	기본값
응답 시간 초과	상태 확인에 대한 최대 응답 시간 초과입니다. 리얼 서버가 제한 시간 내에 응답하지 않으면 비정상으로 간주됩니다. 값 범위: 2 - 60초.	2 - 60초
확인 간격	두 상태 확인 사이의 간격입니다. 값 범위: 5 - 300초.	5초
비정상 임계값	상태 확인 결과가 n회(n은 사용자 지정 가능한 값) 동안 실패하면 백엔드 CVM 인스턴스가 비정상으로 간주되어 콘솔에 예외로 표시됩니다. 값 범위: 2 - 10회.	3회
정상 임계값	상태 확인 결과가 n회(n은 사용자 지정 가능한 값) 동안 성공하면 백엔드 CVM 인스턴스가 정상으로 간주되고 콘솔에 표시되는 상태가 정상입니다. 값 범위: 2 - 10회.	3회

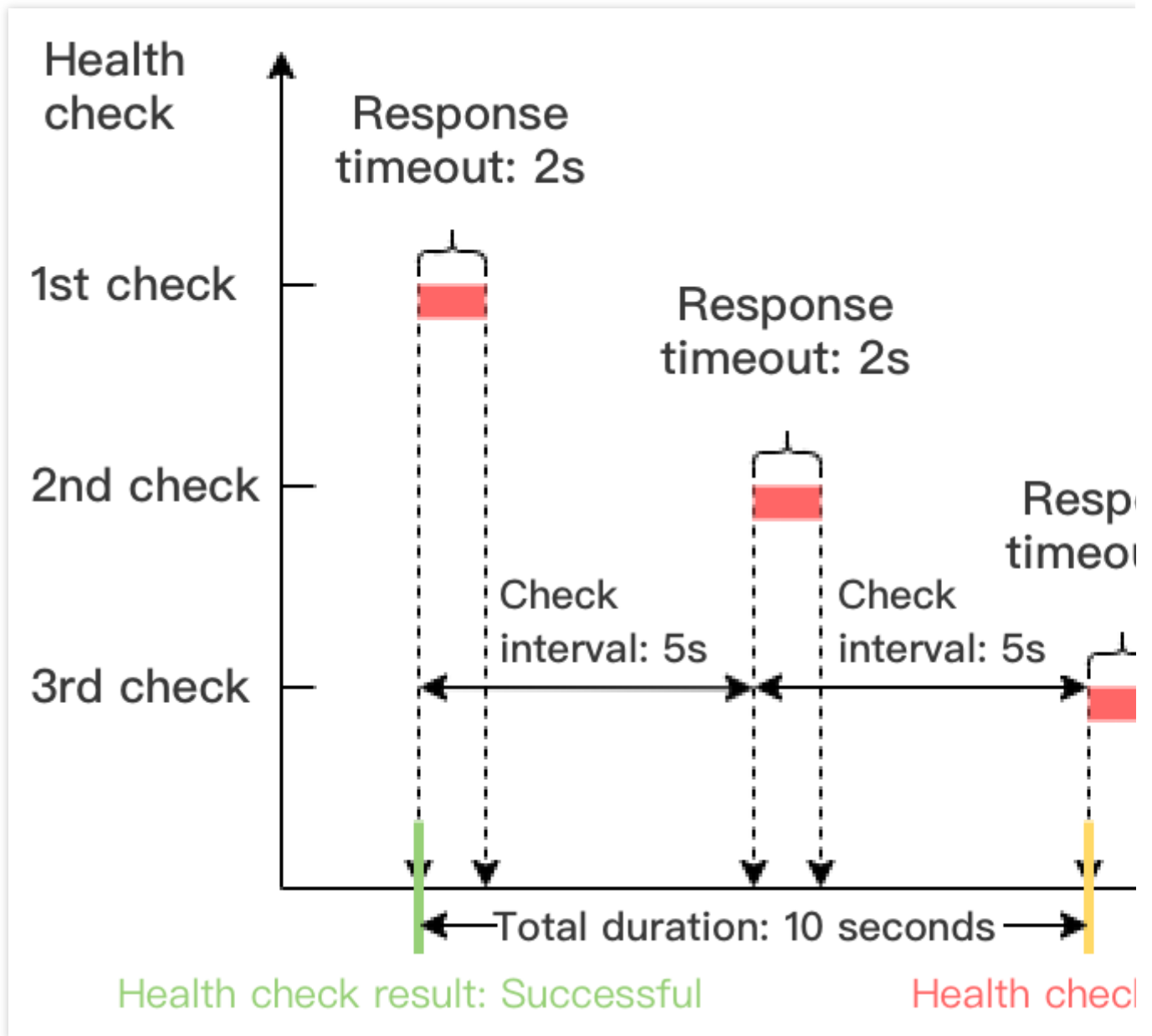
레이어 4 상태 확인 시간 창의 계산은 다음과 같습니다.

설명 :

레이어 4 상태 확인, 즉 TCP 상태 확인 또는 UDP 상태 확인, 두 확인 사이의 시간 간격은 결과가 성공하거나 응답 시간이 초과되는지 여부에 관계없이 설정된 값입니다.

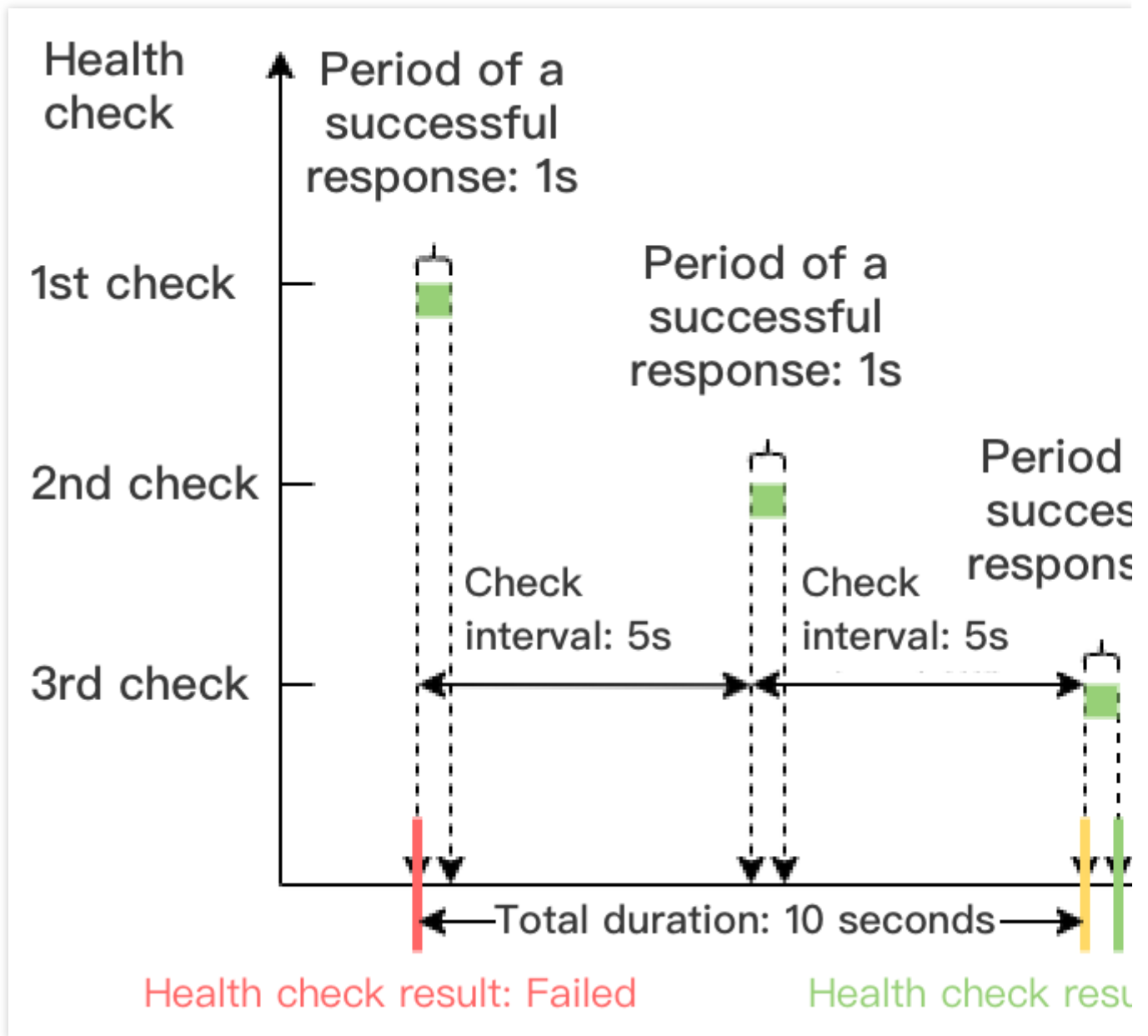
실패한 결과가 있는 상태 확인의 시간 창 = 확인 간격 × (비정상 임계값 - 1)

아래 예시에서 상태 확인 응답 시간 초과는 2s, 확인 간격은 5s, 비정상 임계값은 3회이므로, 결과가 실패한 상태 확인의 시간 창 = 5 × (3-1) = 10s.



성공적인 결과가 있는 상태 확인의 시간 창 = 확인 간격 × (정상 임계값 - 1)

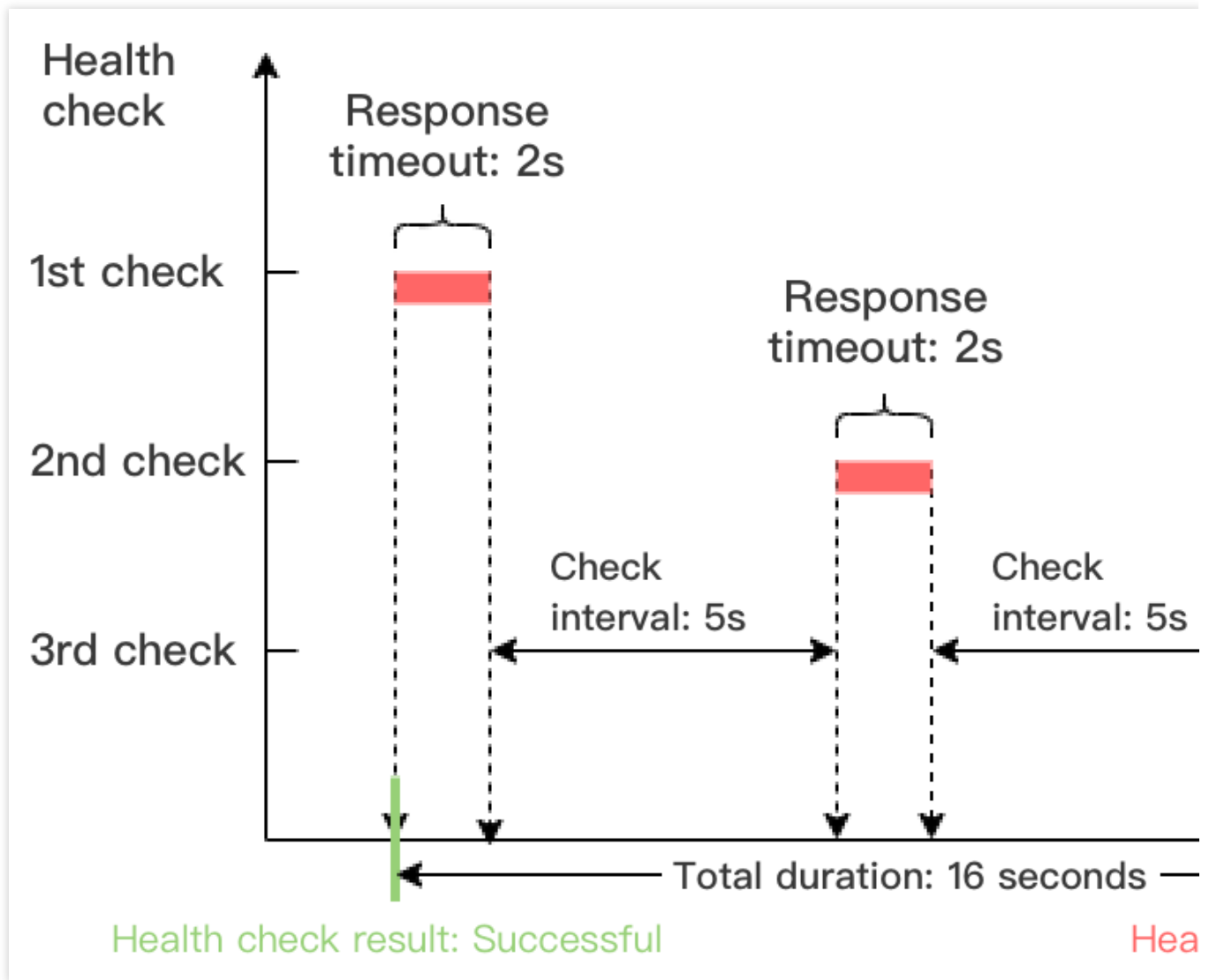
아래 예시에서 성공적인 상태 확인 응답의 기간은 1s, 확인 간격은 5s, 정상 임계값은 3회이므로 성공적인 결과가 있는 상태 확인의 시간 창 = 5 × (3-1) = 10s.



레이어 7 상태 확인 시간 창 계산은 다음과 같습니다.

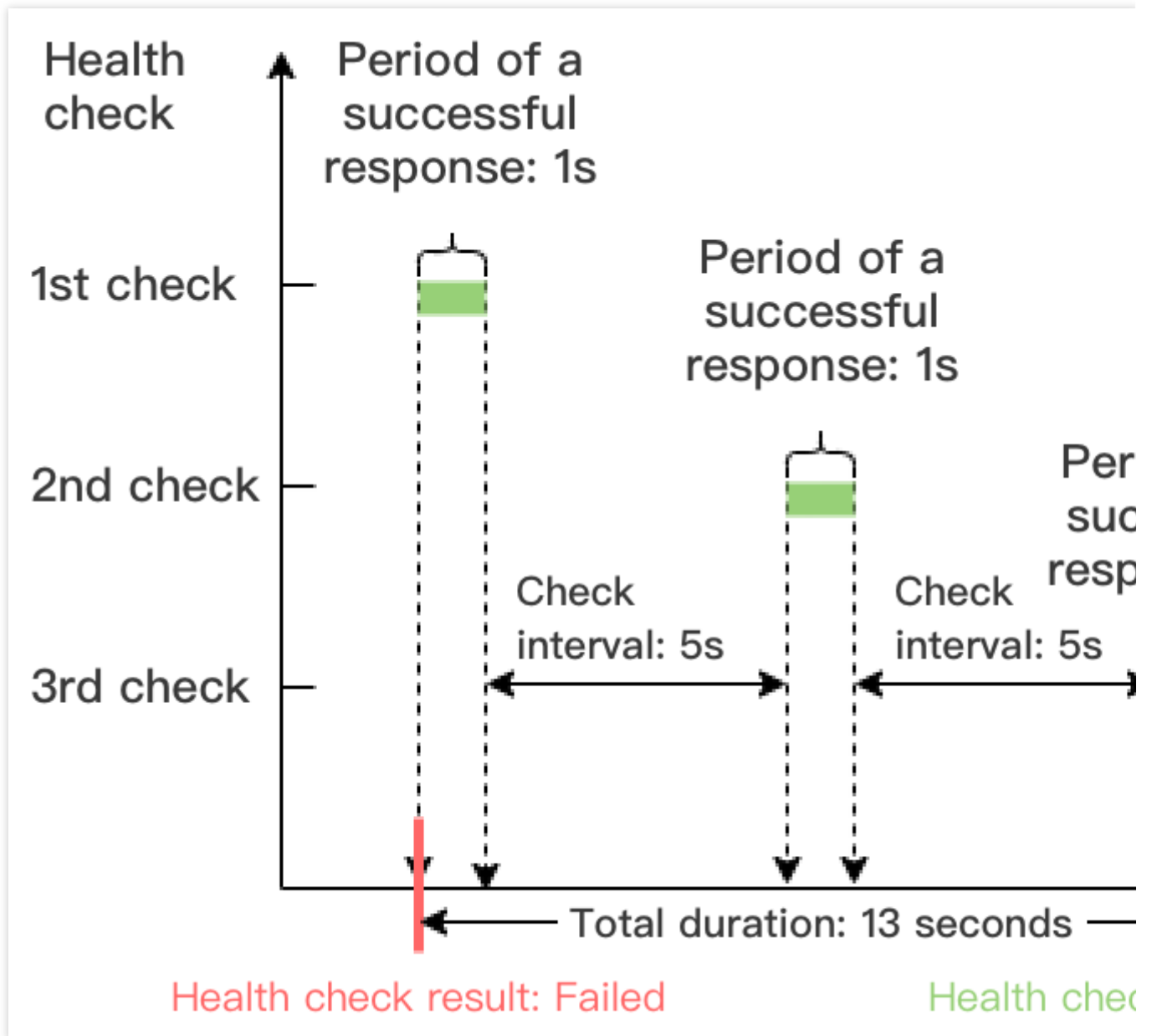
실패한 결과가 있는 상태 확인의 시간 창 = 응답 시간 초과 × 비정상 임계값 + 확인 간격 × (비정상 임계값 - 1)

아래 예시에서 상태 확인 응답 시간 초과는 2s, 점검 간격은 5s, 비정상 임계값은 3회이므로 실패한 결과가 있는 상태 점검의 시간 창 = $2 \times 3 + 5 \times (3 - 1) = 16s$.



성공적인 결과가 있는 상태 확인의 시간 창 = 성공적인 상태 확인 응답 기간 × 정상 임계값 + 확인 간격 × (건강 임계값 - 1)

아래 예시에서 성공적인 상태 확인 응답의 주기는 1s, 확인 간격은 5s, 정상 임계값은 3회이므로 성공적인 결과가 있는 상태 확인의 시간 창 = $1 \times 3 + 5 \times (3-1) = 13s$.



상태 확인 식별자

CLB 상태 확인이 시작된 후 리얼 서버는 일반 비즈니스 요청 외에 상태 확인 요청을 수신합니다. 상태 확인 요청에는 다음 속성이 있을 수 있습니다.

상태 확인 소스 IP는 CLB VIP 또는 100.64 IP 대역입니다.

레이어 4 리스너(TCP, UDP 및 TCP SSL)의 상태 확인 요청은 'HEALTH CHECK'으로 표시됩니다.

레이어 7 리스너(HTTP 및 HTTPS)의 상태 확인 요청의 경우 Header의 user-agent는 'clb-healthcheck'입니다.

관련 문서

[Configuring Health Check](#)

[Configuring Alarm Policy](#)

상태 확인 구성

최종 업데이트 날짜: : 2024-01-04 19:57:35

리스너를 구성할 때 상태 확인을 활성화하여 리얼 서버의 가용성 정보를 얻을 수 있습니다. 상태 확인에 대한 자세한 내용은 [Health Check Overview](#)를 참고하십시오.

제한 설명

IPv6 CLB(Cloud Load Balancer) 인스턴스용 TCP 리스너는 HTTP 상태 확인 또는 사용자 지정 프로토콜 상태 확인을 지원하지 않습니다.

IPv6 CLB 인스턴스용 UDP 리스너는 포트 기반 상태 확인을 지원하지 않습니다.

전제 조건

1. CLB 인스턴스 생성을 완료합니다. 자세한 내용은 [Creating CLB Instances](#)를 참고하십시오.
2. CLB 리스너 생성을 완료합니다.

TCP 리스너 생성하려면 [Configuring TCP Listener](#)에서 자세한 정보를 참고하십시오.

UDP 리스너를 생성하려면 [Configuring a UDP Listener](#)에서 자세한 정보를 참고하십시오.

TCP SSL 리스너를 생성하려면 [Configuring TCP SSL Listener](#)에서 자세한 정보를 참고하십시오.

HTTP 리스너를 생성하려면 [Configuring HTTP Listener](#)에서 자세한 정보를 참고하십시오.

HTTPS 리스너를 생성하려면 [Configuring HTTPS Listener](#)에서 자세한 정보를 참고하십시오.

TCP 리스너

레이어 4 TCP 리스너는 레이어 4 TCP, 레이어 7 HTTP 및 사용자 지정 프로토콜의 세 가지 상태 확인을 지원합니다. TCP 상태 확인은 SYN 패킷으로 수행됩니다. 즉, TCP 3 방향 핸드셰이크가 시작되어 리얼 서버의 상태 정보를 얻습니다.

HTTP 상태 확인은 리얼 서버의 상태 정보를 얻기 위해 HTTP 요청을 전송하여 수행됩니다.

사용자 지정 프로토콜 상태 확인은 리얼 서버의 상태 정보를 얻기 위해 응용 레이어 프로토콜의 입력 및 출력 내용을 사용자 지정하여 수행됩니다.

TCP 상태 확인 구성

1. [전제 조건](#)을 참고하여 '상태 확인' 탭으로 이동합니다.
2. '상태 확인' 탭에서 프로토콜로 'TCP'를 선택합니다.

매개변수	설명
상태 확인	활성화되거나 비활성화 될 수 있습니다. 리얼 서버에 대한 자동 확인 및 비정상 포트 제거를 활성화 하는 것이 좋습니다.
상태 확인 소스 IP	상태 확인 패킷의 소스 IP입니다. 기본값은 CLB VIP입니다. Tencent Kubernetes Engine(TKE) 시나리오에서 컨테이너 루프백 문제를 해결하려면 100.64 IP 범위를 선택합니다.
프로토콜 확인	'TCP'를 선택하면 TCP 상태 확인이 수행됩니다.
포트 확인	선택 사항입니다. 특정 포트를 확인해야 하는 경우가 아니면 포트를 지정하지 않는 것이 좋습니다. 여기서 포트를 지정하지 않으면 리얼 서버 포트가 확인됩니다.
고급 옵션 표시	자세한 내용은 고급 옵션 을 참고하십시오.

HTTP 상태 확인 구성

1. [전제 조건](#)을 참고하여 '상태 확인' 탭으로 이동합니다.
2. '상태 확인' 탭에서 'HTTP'를 프로토콜로 선택합니다.

매개변수	설명
상태 확인	활성화되거나 비활성화 될 수 있습니다. 리얼 서버에 대한 자동 확인 및 비정상 포트 제거를 활성화 하는 것이 좋습니다.
상태 확인 소스 IP	상태 확인 패킷의 소스 IP 주소입니다. 기본값은 CLB VIP입니다. Tencent Kubernetes Engine(TKE) 시나리오에서 컨테이너 루프백 문제를 해결하려면 100.64 IP 범위를 선택합니다.
프로토콜	'HTTP'를 선택하면 HTTP 상태 확인이 수행됩니다.
포트 확인	선택 사항입니다. 특정 포트를 확인해야 하는 경우가 아니면 포트를 지정하지 않는 것이 좋습니다. 여기서 포트를 지정하지 않으면 리얼 서버 포트가 확인됩니다.
도메인 확인	상태 확인 도메인 이름에 대한 요구 사항: 길이: 1 - 80자. 기본 값: 포워딩 도메인 이름.

	<p>정규식은 지원되지 않습니다. 포워딩 도메인 이름이 와일드카드 이름인 경우 고정(비정규) 도메인 이름을 상태 확인 도메인 이름으로 지정해야 합니다.</p> <p>지원되는 문자: 영어 소문자(a-z), 숫자(0-9), 소수점(.), 하이픈(-).</p>
경로	<p>상태 확인 경로에 대한 요구 사항:</p> <p>길이: 1 - 200자.</p> <p>/는 기본값이며, 첫 번째 문자여야 합니다.</p> <p>정규식은 지원되지 않습니다. 상태 확인을 위해 고정 URL(정적 웹 페이지)을 지정하는 것이 좋습니다.</p> <p>지원되는 문자: 영어 소문자(a-z), 영어 대문자(A-Z), 숫자(0-9), 소수점(.), 하이픈(-), 밑줄(_), 슬래시(/), 등호(=) 및 물음표(?).</p>
HTTP 요청 방법	<p>상태 확인의 HTTP 요청 방법입니다. 옵션: GET(기본 방법) 및 HEAD.</p> <p>HEAD를 선택하면 서버는 HTTP 헤더 정보만 반환하므로 백엔드 오버헤드를 줄이고 요청 효율성을 높일 수 있습니다. 리얼 서버는 HEAD를 지원해야 합니다.</p> <p>GET을 선택하면 리얼 서버가 GET을 지원해야 합니다.</p>
HTTP 버전	<p>리얼 서버의 HTTP 버전입니다.</p> <p>리얼 서버에서 지원하는 버전이 HTTP 1.0이면 요청의 Host 필드는 인증이 필요하지 않습니다. 즉, 확인 도메인을 구성할 필요가 없습니다.</p> <p>리얼 서버에서 지원하는 버전이 HTTP 1.1인 경우 요청의 Host 필드에 인증이 필요합니다. 즉, 확인 도메인을 구성해야 합니다.</p> <p>HTTP/1.1 버전을 선택한 경우, 이 때 도메인 이름 확인이 구성되지 않은 경우 HTTP 표준 프로토콜에 따라 리얼 서버는 상태 확인이 비정상임을 나타내는 오류 코드 400을 반환합니다. 정상 상태 코드 http_4xx을(를) 선택하는 것이 좋습니다.</p>
정상 상태 코드	<p>리얼 서버의 반환 코드가 선택된 상태 코드이면 상태 확인이 정상으로 간주되고 트래픽이 해당 리얼 서버로 계속 전달됩니다. 사용 가능한 옵션: http_1xx, http_2xx, http_3xx, http_4xx 및 http_5xx.</p>
고급 옵션	<p>자세한 내용은 고급 옵션을 참고하십시오.</p>

표시

사용자 지정 프로토콜 상태 확인 구성

1. [전제 조건](#)을 참고하여 '상태 확인' 탭으로 이동합니다.
2. '상태 확인' 탭에서 '사용자 지정 프로토콜'을 프로토콜로 선택합니다.

매개변수	설명
상태 확인	활성화되거나 비활성화 될 수 있습니다. 리얼 서버에 대한 자동 확인 및 비정상 포트 제거를 활성화하는 것이 좋습니다.
상태 확인 소스 IP	상태 확인 패킷의 소스 IP 주소입니다. 기본값은 CLB VIP입니다. Tencent Kubernetes Engine(TKE) 시나리오에서 컨테이너 루프백 문제를 해결하려면 100.64 IP 범위를 선택합니다.
프로토콜 확인	'사용자 지정 프로토콜'을 선택한 경우 사용자 지정 프로토콜 상태 확인이 수행됩니다. 이것은 TCP의 비 HTTP 프로토콜에 적용할 수 있습니다.
포트 확인	선택 사항입니다. 특정 포트를 확인해야 하는 경우가 아니면 포트를 지정하지 않는 것이 좋습니다. 여기서 포트를 지정하지 않으면 리얼 서버 포트가 확인됩니다.
입력 형식	텍스트 및 16진법 문자열이 지원됩니다. 텍스트를 선택하면 요청을 보내고 반환된 결과를 비교하기 위해 텍스트가 이진법 문자열로 변환됩니다. 16진법을 선택하면 요청을 보내고 반환된 결과를 비교하기 위해 16진법 문자열이 이진법 문자열로 변환됩니다.
요청	DNS 서비스 상태 확인을 위한, F13E0100000100000000000000377777047465737403636F6D0774656E63656E7403636F6D000001000

확 인	와 같이 필수로 필요한 사용자 지정 상태 확인 요청 콘텐츠입니다.
반 환 된 확 인 결 과	상태 확인 요청을 사용자 지정할 때 DNS 서비스 상태 확인의 경우 F13E와 같이 반환된 상태 확인 결과를 입력해야 합니다.
고 급 옵 션 표 시	자세한 내용은 고급 옵션 을 참고하십시오.

UDP 리스너

UDP 리스너는 포트를 확인하고 PING 명령을 실행하여 수행할 수 있는 UDP 상태 확인을 지원합니다.

UDP 상태 확인 구성 - 포트 확인

1. [전제 조건](#)을 참고하여 '상태 확인' 탭으로 이동합니다.
2. '상태 확인' 탭에서 '포트'를 프로토콜로 선택합니다.

매 개 변 수	설명
상 태 확 인	활성화되거나 비활성화 될 수 있습니다. 리얼 서버에 대한 자동 확인 및 비정상 포트 제거를 활성화하는 것이 좋습니다.
상 태 확 인 소 스 IP	상태 확인 패킷의 소스 IP 주소입니다. 기본값은 CLB VIP입니다. Tencent Kubernetes Engine(TKE) 시나리오에서 컨테이너 루프백 문제를 해결하려면 100.64 IP 범위를 선택합니다.

프로토콜 확인	'포트 확인'을 선택하면 상태 프로브의 소스 IP가 백엔드 서버의 상태 정보를 얻기 위해 백엔드 서버에 UDP 프로브 메시지를 보냅니다.
포트 확인	선택 사항입니다. 특정 포트를 확인해야 하는 경우가 아니면 포트를 지정하지 않는 것이 좋습니다. 여기서 포트를 지정하지 않으면 리얼 서버 포트가 확인됩니다.
입력 형식	텍스트 및 16진법 문자열이 지원됩니다. 텍스트를 선택하면 요청을 보내고 반환된 결과를 비교하기 위해 텍스트가 이진법 문자열로 변환됩니다. 16진법을 선택하면 요청을 보내고 반환된 결과를 비교하기 위해 16진법 문자열이 이진법 문자열로 변환됩니다.
요청 확인	DNS 서비스 상태 확인을 위한, F13E01000001000000000000003777777047465737403636F6D0774656E63656E7403636F6D000001000· 와 같은 사용자 지정 상태 확인 요청 콘텐츠입니다.
반환된 확인 결과	상태 확인 요청을 사용자 지정할 때 DNS 서비스 상태 확인의 경우 F13E와 같이 반환된 상태 확인 결과를 구성해야 합니다.
고급 옵션 표시	자세한 내용은 고급 옵션 을 참고하십시오.

UDP 상태 확인 구성 - PING 명령

1. [전제 조건](#)을 참고하여 '상태 확인' 탭으로 이동합니다.
2. '상태 확인' 탭에서 프로토콜로 'PING'을 선택합니다.

매개변	설명
-----	----

수	
상태 확인	활성화되거나 비활성화 될 수 있습니다. 리얼 서버에 대한 자동 확인 및 비정상 포트 제거를 활성화 하는 것이 좋습니다.
상태 확인 소스 IP	상태 확인 패킷의 소스 IP 주소입니다. 기본값은 CLB VIP입니다. Tencent Kubernetes Engine(TKE) 시나리오에서 컨테이너 루프백 문제를 해결하려면 100.64 IP 범위를 선택합니다.
프로토콜 확인	'PING'을 선택하면 리얼 서버의 IP가 Ping되어 리얼 서버 상태 정보를 얻습니다.
고급 옵션 표시	자세한 내용은 고급 옵션 을 참고하십시오.

TCP SSL 리스너

TCP 상태 확인 구성

1. [전제 조건](#)을 참고하여 '상태 확인' 탭으로 이동합니다.
2. '상태 확인' 탭에서 프로토콜로 'TCP'를 선택합니다.

매개변수	설명
상태 확인	활성화되거나 비활성화 될 수 있습니다. 리얼 서버에 대한 자동 확인 및 비정상 포트 제거를 활성화 하는 것이 좋습니다.
상태 확인 소스 IP	상태 확인 패킷의 소스 IP 주소입니다. 기본값은 CLB VIP입니다. Tencent Kubernetes Engine(TKE) 시나리오에서 컨테이너 루프백 문제를 해결하려면 100.64 IP 범위를 선택합니다.
프로토콜 확인	'TCP'를 선택하면 TCP 상태 확인이 수행됩니다.
포트 확인	TCP SSL 리스너의 상태 확인 포트와 수신 포트는 동일합니다.
고급 옵션 표시	자세한 내용은 고급 옵션 을 참고하십시오.

HTTP 상태 확인 구성

1. [전제 조건](#)을 참고하여 '상태 확인' 탭으로 이동합니다.
2. '상태 확인' 탭에서 'HTTP'를 프로토콜로 선택합니다.

--	--

매개 변수	설명
상태 확인	활성화되거나 비활성화 될 수 있습니다. 리얼 서버에 대한 자동 확인 및 비정상 포트 제거를 활성화하는 것이 좋습니다.
상태 확인 소스 IP	상태 확인 패킷의 소스 IP 주소입니다. 기본값은 CLB VIP입니다. Tencent Kubernetes Engine(TKE) 시나리오에서 컨테이너 루프백 문제를 해결하려면 100.64 IP 범위를 선택합니다.
프로토콜	'HTTP'를 선택하면 HTTP 상태 확인이 수행됩니다.
포트 확인	TCP SSL 리스너의 상태 확인 포트와 수신 포트는 동일합니다.
도메인 확인	<p>상태 확인 도메인 이름에 대한 요구 사항:</p> <p>길이: 1 - 80자.</p> <p>기본 값: 포워딩 도메인 이름.</p> <p>정규식은 지원되지 않습니다. 포워딩 도메인 이름이 와일드카드 이름인 경우 고정(비정규) 도메인 이름을 상태 확인 도메인 이름으로 지정해야 합니다.</p> <p>지원되는 문자: 영어 소문자(a-z), 숫자(0-9), 소수점(.), 하이픈(-).</p>
경로 확인	<p>상태 확인 경로에 대한 요구 사항:</p> <p>길이: 1 - 200자.</p> <p>/는 기본값이며, 첫 번째 문자여야 합니다.</p> <p>정규식은 지원되지 않습니다. 상태 확인을 위해 고정 URL(정적 웹 페이지)을 지정하는 것이 좋습니다.</p> <p>지원되는 문자: 영어 소문자(a-z), 영어 대문자(A-Z), 숫자(0-9), 소수점(.), 하이픈(-), 밑줄(_), 슬래시(/), 등호(=) 및 물음표(?).</p>
HTTP 요청 방법	<p>상태 확인의 HTTP 요청 방법입니다. 옵션: GET(기본 방법) 및 HEAD.</p> <p>HEAD를 선택하면 서버는 HTTP 헤더 정보만 반환하므로 백엔드 오버헤드를 줄이고 요청 효율성을 높일 수 있습니다. 리얼 서버는 HEAD를 지원해야 합니다.</p>

	GET을 선택하면 리얼 서버가 GET을 지원해야 합니다.
HTTP 버전	리얼 서버의 HTTP 버전입니다. HTTP 1.1만 지원됩니다. 리얼 서버는 요청의 Host 필드를 인증해야 합니다. 즉, 확인 도메인을 구성해야 합니다. 도메인 이름 확인이 구성되지 않은 경우 HTTP 표준 프로토콜에 따라 백엔드 서버는 상태 확인이 비정상임을 나타내는 오류 코드 400을 반환합니다. 정상 상태 코드 http_4xx을(를) 선택하는 것이 좋습니다.
정상 상태 코드	리얼 서버의 반환 코드가 선택된 상태 코드이면 상태 확인이 정상으로 간주되고 트래픽이 해당 리얼 서버로 계속 전달됩니다. 사용 가능한 옵션: http_1xx, http_2xx, http_3xx, http_4xx 및 http_5xx.
고급 옵션 표시	자세한 내용은 고급 옵션 을 참고하십시오.

HTTP 리스너

HTTP 상태 확인 구성

1. [전제 조건](#)을 참고하여 '상태 확인' 탭으로 이동합니다.

매개변수	설명
상태 확인	활성화되거나 비활성화 될 수 있습니다. 리얼 서버에 대한 자동 확인 및 비정상 포트 제거를 활성화하는 것이 좋습니다.
상태 확인 소스 IP	상태 확인 패킷의 소스 IP 주소입니다. 기본값은 CLB VIP입니다. Tencent Kubernetes Engine(TKE) 시나리오에서 컨테이너 루프백 문제를 해결하려면 100.64 IP 범위를 선택합니다.
도메인 확인	상태 확인 도메인 이름에 대한 요구 사항: 길이: 1 - 80자. 기본 값: 포워딩 도메인 이름. 정규식은 지원되지 않습니다. 포워딩 도메인 이름이 와일드카드 이름인 경우 고정(비정규) 도메인 이름을 상태 확인 도메인 이름으로 지정해야 합니다.

	지원되는 문자: 영어 소문자(a-z), 숫자(0-9), 소수점(.), 하이픈(-).
경로 확인	<p>상태 확인 경로는 리얼 서버의 루트 디렉터리 또는 지정된 URL로 설정할 수 있습니다. 요구 사항은 다음과 같습니다.</p> <p>길이: 1 - 200자.</p> <p>/는 기본값이며, 첫 번째 문자여야 합니다.</p> <p>정규식은 지원되지 않습니다. 상태 확인을 위해 고정 URL(정적 웹 페이지)을 지정하는 것이 좋습니다.</p> <p>지원되는 문자: 영어 소문자(a-z), 영어 대문자(A-Z), 숫자(0-9), 소수점(.), 하이픈(-), 밑줄(_), 슬래시(/), 등호(=) 및 물음표(?).</p>
응답 시간 초과	<p>상태 확인에 대한 최대 응답 시간 초과입니다.</p> <p>리얼 서버가 제한 시간 내에 응답하지 않으면 상태 확인이 비정상으로 간주됩니다.</p> <p>값 범위: 2 - 60초.</p>
확인 간격	<p>두 상태 확인 사이의 간격입니다.</p> <p>값 범위: 2 - 300초.</p>
비정상 임계값	<p>상태 확인 결과가 n회(n은 사용자 지정 가능한 값) 동안 실패하면 백엔드 CVM 인스턴스가 비정상적으로 간주되어 콘솔에 표시되는 상태가 비정상입니다.</p> <p>값 범위: 2 - 10회.</p>
상태 임계값	<p>상태 확인 결과가 n회(n은 사용자 지정 가능한 값) 동안 성공하면 백엔드 CVM 인스턴스가 정상으로 간주되고 콘솔에 표시되는 상태가 정상입니다.</p> <p>값 범위: 2 - 10회.</p>
HTTP 요청 방법	<p>상태 확인의 HTTP 요청 방법입니다. 옵션: GET(기본 방법) 및 HEAD.</p> <p>HEAD를 선택하면 서버는 HTTP 헤더 정보만 반환하므로 백엔드 오버헤드를 줄이고 요청 효율성을 높일 수 있습니다. 리얼 서버는 HEAD를 지원해야 합니다.</p> <p>GET을 선택하면 리얼 서버가 GET을 지원해야 합니다.</p>
정상 상태 코드	<p>리얼 서버의 반환 코드가 선택된 상태 코드이면 상태 확인이 정상으로 간주되고 트래픽이 해당 리얼 서버로 계속 전달됩니다. 사용 가능한 옵션: http_1xx, http_2xx, http_3xx, http_4xx 및 http_5xx.</p>

TCP 상태 확인 구성

1. [전제 조건](#)을 참고하여 '상태 확인' 탭으로 이동합니다.
2. '상태 확인' 탭에서 프로토콜로 'TCP'를 선택합니다.

매개변수	설명
상태 확인	활성화되거나 비활성화 될 수 있습니다. 리얼 서버에 대한 자동 확인 및 비정상 포트 제거를 활성화 하는 것이 좋습니다.
상태 확인 소스 IP	상태 확인 패킷의 소스 IP 주소입니다. 기본값은 CLB VIP입니다. Tencent Kubernetes Engine(TKE) 시나리오에서 컨테이너 루프백 문제를 해결하려면 100.64 IP 범위를 선택합니다.
프로토콜 확인	'TCP'를 선택하면 TCP 상태 확인이 수행됩니다.
고급 옵션 표시	자세한 내용은 고급 옵션 을 참고하십시오.

HTTPS 리스너

설명 :

HTTPS 리스너 포워딩 규칙의 백엔드 프로토콜로 HTTP를 선택하면 HTTP 상태 확인이 수행됩니다. HTTPS를 선택 하면 HTTPS 상태 확인이 수행됩니다.

HTTPS 리스너의 상태 확인 구성은 [#http](#) HTTP 리스너를 참고하십시오.

고급 옵션

상태 확인 구성	설명	기본 값
응답 시간 초과	<ul style="list-style-type: none">상태 확인에 대한 최대 응답 시간 초과입니다. 리얼 서버가 제한 시간 내에 응답 하지 않으면 비정상으로 간주됩니다. 값 범위: 2 - 60초.	2 초
확인 간격	<ul style="list-style-type: none">두 상태 확인 사이의 간격입니다. 값 범위: 2 - 300초.	5 초

비정상 임계값	<ul style="list-style-type: none">상태 확인 결과가 n회(n은 사용자 지정 가능한 값) 동안 실패하면 백엔드 CVM 인스턴스가 비정상으로 간주되어 콘솔에 표시되는 상태가 비정상입니다. 값 범위: 2 - 10회.	3회
정상 임계값	<ul style="list-style-type: none">상태 확인 결과가 n회(n은 사용자 지정 가능한 값) 동안 성공하면 백엔드 CVM 인스턴스가 정상으로 간주되고 콘솔에 표시되는 상태가 정상입니다. 값 범위: 2 - 10회.	3회

관련 문서

[Health Check Overview](#)

[Configuring Alarm Policy](#)

인증서 관리

인증서 관리

최종 업데이트 날짜: : 2024-01-04 19:58:11

CLB(Cloud Load Balancer) 인스턴스의 HTTPS 리스너를 구성할 때 SSL 인증서 서비스에서 인증서를 직접 사용하거나 타사 CA에서 발급한 서버 인증서와 [SSL Certificate](#) 를 CLB에 업로드할 수 있습니다.

인증서 요구 사항

CLB는 PEM 형식의 인증서만 지원합니다. 인증서를 업로드하기 전에 인증서, 인증서 체인 및 개인 키가 형식 요구 사항을 충족하는지 확인하십시오. 인증서 요구 사항은 [Certificate Requirements and Certificate Format Conversion](#)을 참고하십시오.

인증서 구성

HTTPS 리스너에 대한 인증서 구성은 다음 두 가지 유형으로 나뉩니다.

SNI가 활성화되지 않은 경우 모든 도메인 이름이 동일한 인증서를 사용하는 리스너 레벨에서 인증서를 구성할 수 있습니다. 자세한 내용은 [Configuring HTTPS Listener](#)를 참고하십시오.

SNI가 활성화된 경우 도메인 이름 레벨에서 인증서를 구성할 수 있으며 리스너 아래의 다른 도메인 이름에 대해 다른 인증서를 구성할 수 있습니다. 자세한 내용은 [SNI Support for Binding Multiple Certificates to a CLB Instance](#)를 참고하십시오.

인증서 일괄 업데이트

인증서 만료가 서비스에 영향을 미치지 않도록 하려면 만료되기 전에 인증서를 업데이트하십시오.

설명 :

인증서가 업데이트된 후 시스템은 레거시 인증서를 삭제하지 않습니다. 대신 새 인증서를 생성합니다. 인증서를 사용하는 모든 CLB 인스턴스에 대해 인증서가 자동으로 업데이트됩니다.

1. [CLB 콘솔](#)에 로그인합니다.
2. 왼쪽 사이드바에서 [인증서 관리]를 클릭합니다.
3. '인증서 관리' 페이지의 인증서 목록에서 대상 인증서 오른쪽의 '작업' 열에서 [업데이트]를 클릭합니다.
4. 팝업되는 '인증서 생성' 대화 상자에서 새 인증서의 인증서 내용과 주요 내용을 입력하고 [제출]을 클릭합니다.

Create a new certificate

Certificate Name

cert

Cannot exceed 80 characters, only English letters, numbers, underscores, and hyphens are supported "-", ".", ".".

Certificate Type

☒ Server Certificate ☐ Client CA Certificate

Certificate Content

-----BEGIN CERTIFICATE-----
[Blurred Content]

[View Examples](#)

Key Content

-----BEGIN RSA PRIVATE KEY-----
[Blurred Content]

[View Examples](#)

Submit

Close

인증서와 연결된 CLB 인스턴스 보기

1. [CLB 콘솔](#)에 로그인합니다.
2. 왼쪽 사이드바에서 [인증서 관리]를 클릭합니다.
3. '인증서 관리' 페이지의 인증서 목록에서 대상 인증서의 ID를 클릭합니다.
4. '기본 정보' 페이지에서 인증서와 연결된 CLB 인스턴스를 확인합니다.

Basic Info

Name manuel-test

ID ha2qQzkD

Certificate Type Server Certificate

Certificate Content

-----BEGIN CERTIFICATE-----

[Blurred certificate content]

[Copy](#)

Load Balancer Bound

[Blurred load balancer bound information]

Primary Domain Name

[Blurred primary domain name]

Alternate Domain

-

Upload Time 2020-10-29 12:06:20

Start Time 2020-07-03 18:05:58

Expiry Time 2021-07-03 18:05:58

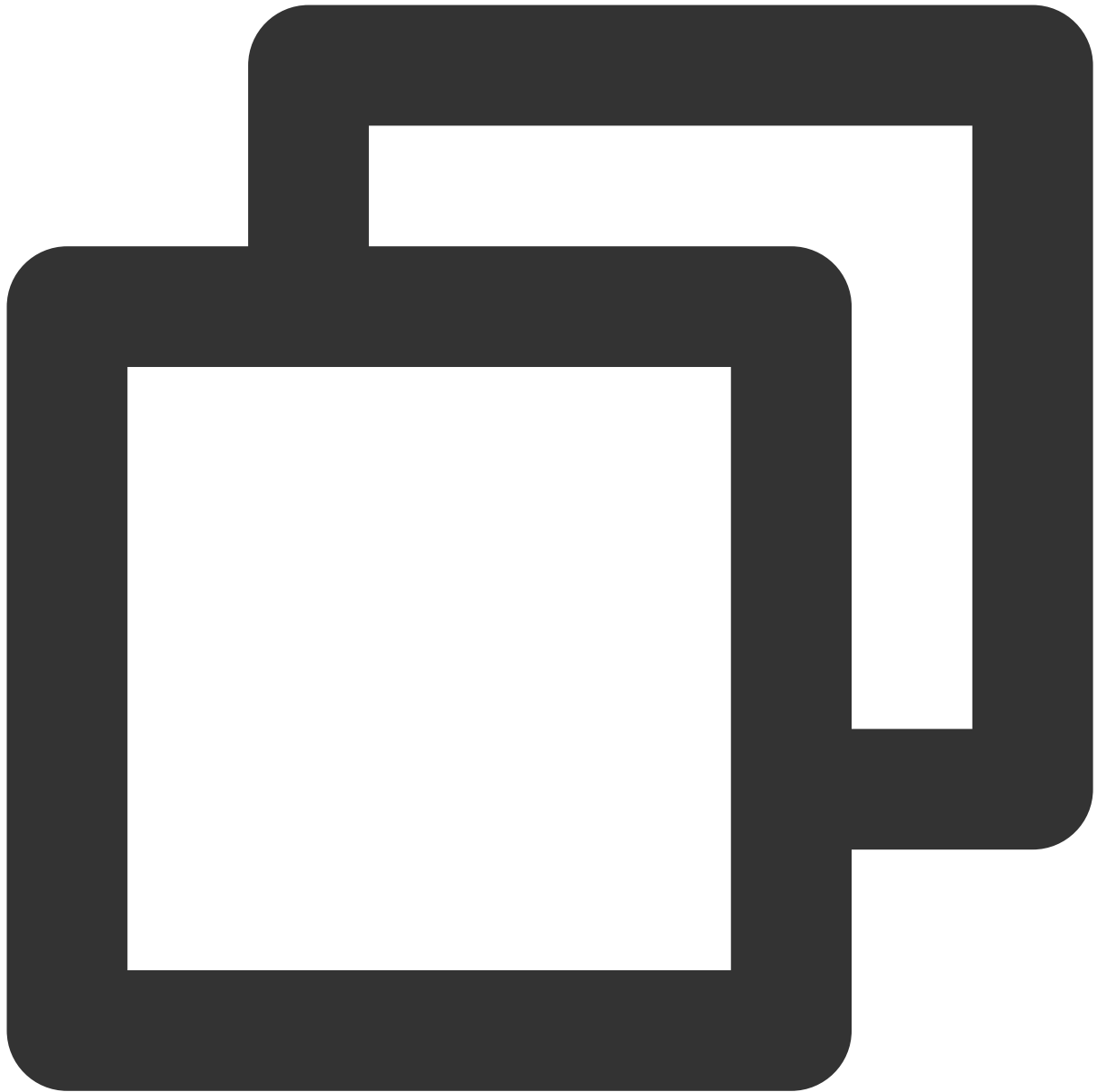
인증서 요구 사항 및 인증서 형식 변환

최종 업데이트 날짜: : 2024-01-04 19:58:32

본문은 SSL 인증서 요구 사항과 인증서 형식 변환 방법을 설명합니다.

인증서 신청 절차

1. OpenSSL을 사용하여 개인 키 파일(예: `privateKey.pem`)을 로컬로 생성합니다. 비공개로 유지하십시오.



```
openssl genrsa -out privateKey.pem 2048
```

2. OpenSSL을 사용하여 인증서 요청 파일(예: `server.csr`)을 생성합니다. 인증서 신청에 사용할 수 있습니다.



```
openssl req -new -key privateKey.pem -out server.csr
```

3. 인증서 요청 파일의 내용을 얻고 CA 사이트를 방문하여 인증서를 신청합니다.

인증서 형식 요구 사항

사용자가 신청해야 하는 인증서는 Linux에서 PEM 형식이어야 합니다. CLB는 다른 형식의 인증서를 지원하지 않습니다. 자세한 내용은 [인증서를 PEM 형식으로 변환](#)을 참고하십시오.

연결 규칙은 다음과 같습니다. 서버 인증서를 중간 인증서 앞에 빈 줄 없이 배치합니다.

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

인증서 체인 규칙:

인증서 사이에 빈 줄이 없어야 합니다.

모든 인증서는 위와 같은 요구 사항을 충족해야 합니다.

RSA 개인 키 형식 요구 사항

다음은 예시입니다.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAzSSChH67bmT8mFykAxQ1tKCYukwBiWZwk0StFEbTWHy8K
tTHSFD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A
Xw95grqFJMJC Lva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ
/fD0XXyuWoqaIePZtK9Qnjn957ZEPhtUpVZuhS3409DDM/tJ3Tl8aaNYWhrPBc0
jNcz0Z6XQGf1rZG/Ve520GX6rb5dUYpdcfXzN5MM6xYg8a1L7UHDHHPI4AYsatdG
z5TMPnmEf8yZPUYudTLxgMVAovJr09Dq+5Dm3QIDAQABAOIBAGl68Z/nnFyRHRFi
LaF6+Wen8ZvNqkm0hAMQwIjH1Vp1fL74//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35
cgQ93Tx424WGPcwUshSfxewfbAYGF3ur8WOxq0uU07BAxaKHNcmNG7dGyo1UowRu
S+yXLrpVzH1YkuH8TT5udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2
06W/zH24YAxwkTYLKGHjoieYs111ah1AJvICVgTc3+LzG2pIpM7I+K0nHCSeswvM
i5x9h/OT/ujZsyX9P0PaAyE2bqy0t080tGexM076Ssv0KVhKFvWjLUnhf6WcqFCD
xqhhxkECgYEA+PftNb6eyX1+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhagHu0edU
ZXIHRJ9u6B1XE1arpjVs/WHmFhYSTm6DbdD7S1tLy0BY4cPTRhziFTKt8AkIXMK
605u0UiWsq0Z8hn1X14lox2cW9ZQa/HC9udeyQotP4NsMJWgpBV7tC0CgYEAwwNF
0f+/jUjt0HoyCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzFEG8/AR3Md2rhmZi
GnJ5fdfe7uY+JsQfX2Q5JjwTad1BW4led0Sa/uKRa04UzVgnYp2aJKxtuWffvVbU
+kf728ZJRA6azSLvGm8hu/GL6bgfU3fkSkw03ECgYBpYK7TT7JvvnAERmtJf2yS
ICRkbQaB3gPSe/lCgy1nhtaF0UbNxGeuowLAZR0wrz7X3TZqHEDcYoJ7mK346of
QhGLITyoeHkbYkAUTaQ038Y04EKH6S/IzMzB0frXiPKg9s8UKQzkU+GSE7ootli+a
R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUHKIKcP/+xn
R3kVl06MZCFAdqirAjiQWapkh9Bxbp2eHCrB8lMFAWLRQSl0k79b/jVmTzMC3upd
EJ/iSWjZKPbw7hCFAeRtPhxyNTJ5idEiu9U8EQid81l1giPgn0p3sE0HpDI89qZX
aaiMEQKBgQDK2bsnZ9y0ZWhGTeu94vziKmFrSkJMGH8pLaTiliw1iRhRYWJysZ9
B0IDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcv0Bh5Hx0yy23m9hFRzfDeQ7z
NTKh193HHF1joNM81LHFyGRFEWWrroW5gfBudR6USRnR/6iQ11xZXw==
-----END RSA PRIVATE KEY-----
```

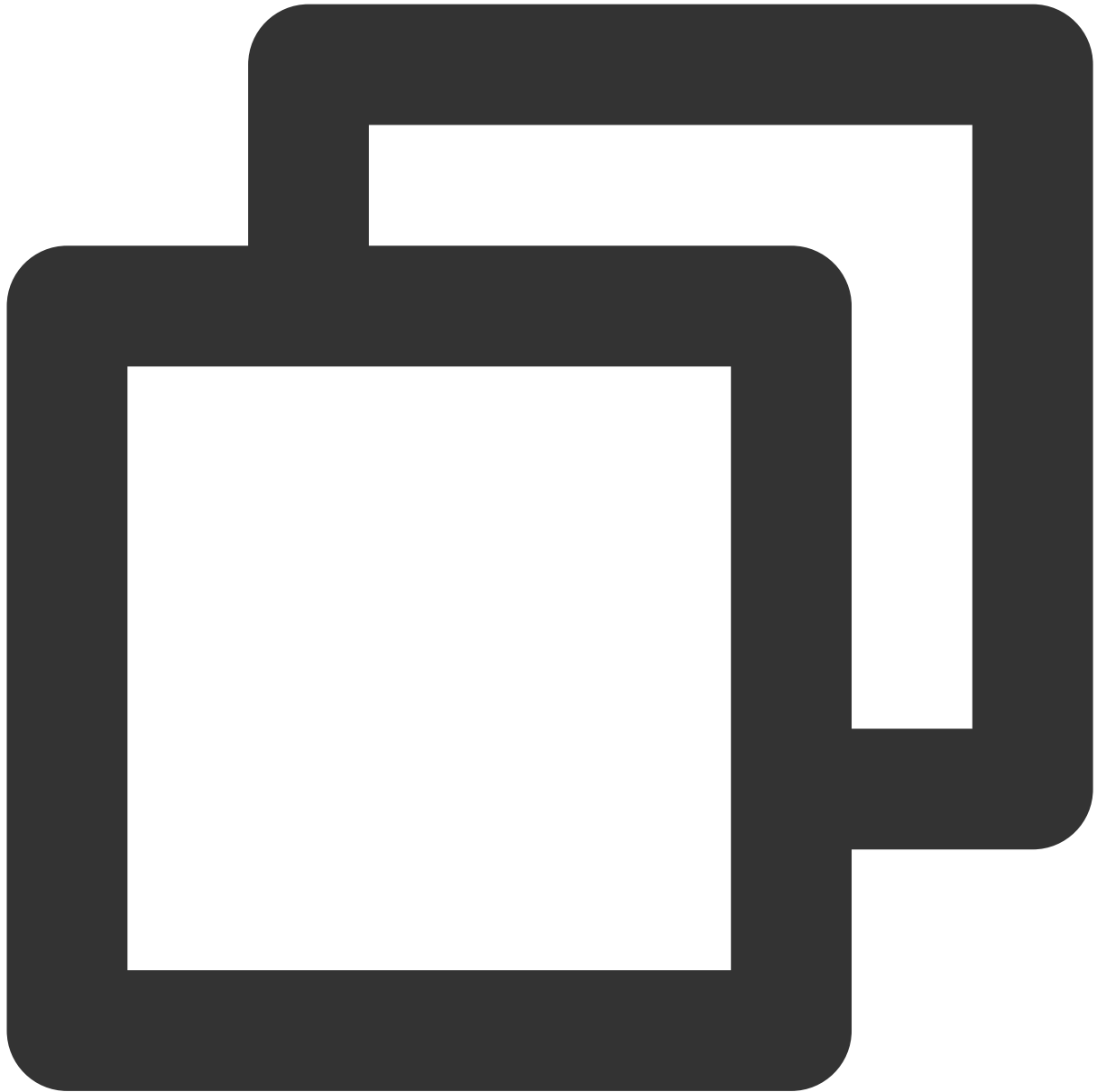
RSA 개인 키는 모든 개인 키(RSA 및 DSA), 공개 키(RSA 및 DSA) 및 (x509) 인증서를 포함할 수 있습니다. Base64로 인코딩된 DER 형식으로 데이터를 저장하고 ASCII 헤더로 래핑하여 시스템 간의 텍스트 모드 전송에 적합합니다.

RSA 개인 키 규칙:

인증서는 [-----BEGIN RSA PRIVATE KEY-----, -----END RSA PRIVATE KEY-----] 시작과 끝을 함께 업로드해야 합니다.

각 줄은 64자를 포함해야 하며 마지막 줄은 64자 미만이어야 합니다.

위의 방식에 따라 [-----BEGIN PRIVATE KEY-----, -----END PRIVATE KEY-----] 형식으로 사용 가능한 개인 키를 생성하지 않으면 다음과 같이 사용 가능한 개인 키로 변환할 수 있습니다.



```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

그런 다음 인증서와 함께 new_server_key.pem 콘텐츠를 업로드할 수 있습니다.

인증서를 PEM 형식으로 변환

현재 CLB는 PEM 형식의 인증서만 지원합니다. 다른 형식의 인증서는 CLB에 업로드하기 전에 먼저 openssl을 사용하여 PEM 형식으로 변환해야 합니다. 다음은 몇 가지 일반적인 형식을 PEM 형식으로 변환하는 방법을 보여줍니다.

DER 에서 PEM 으로 변환

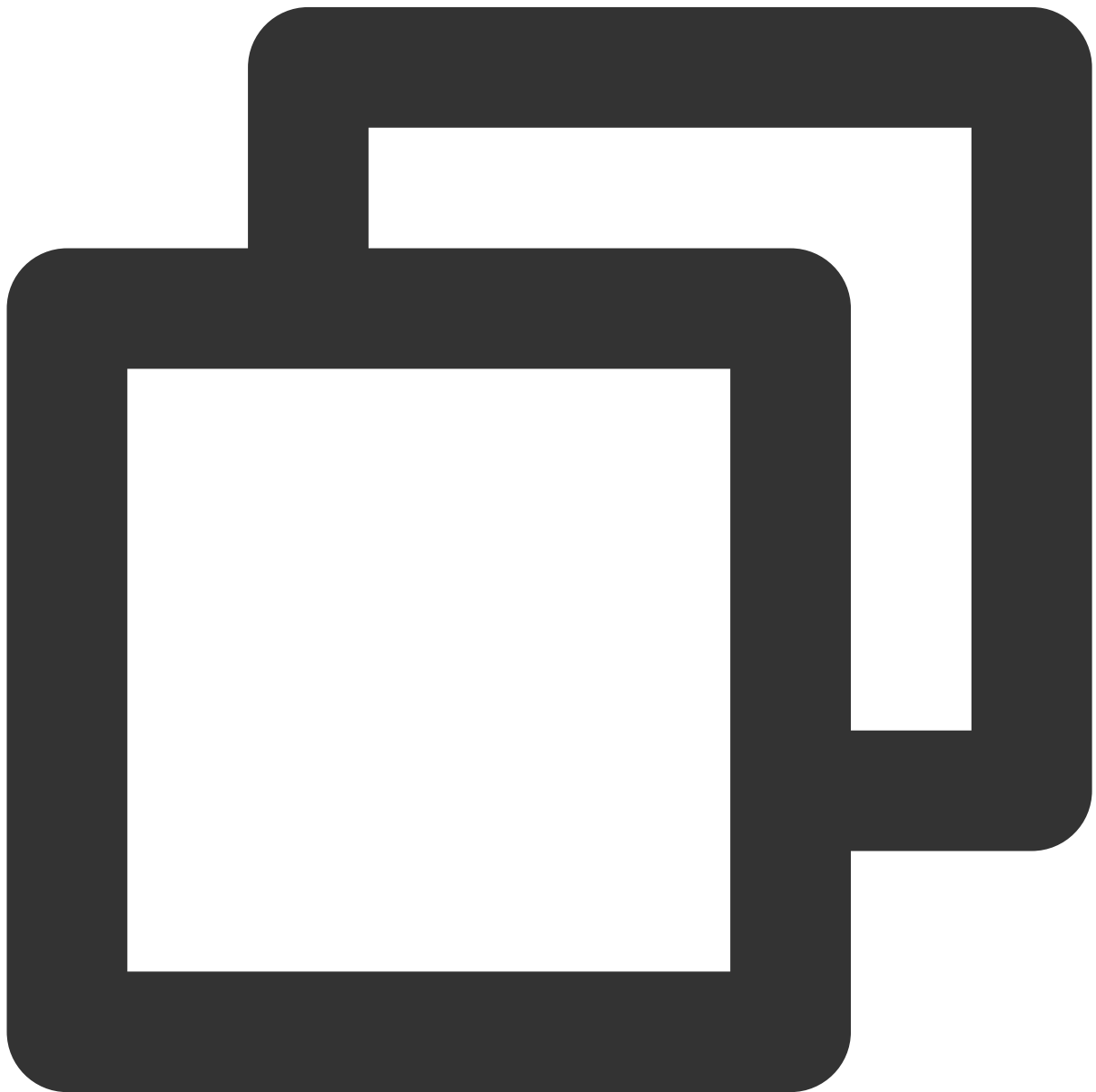
P7B 에서 PEM 으로 변환

PFX 에서 PEM 으로 변환

CER/CRT 에서 PEM 으로 변환

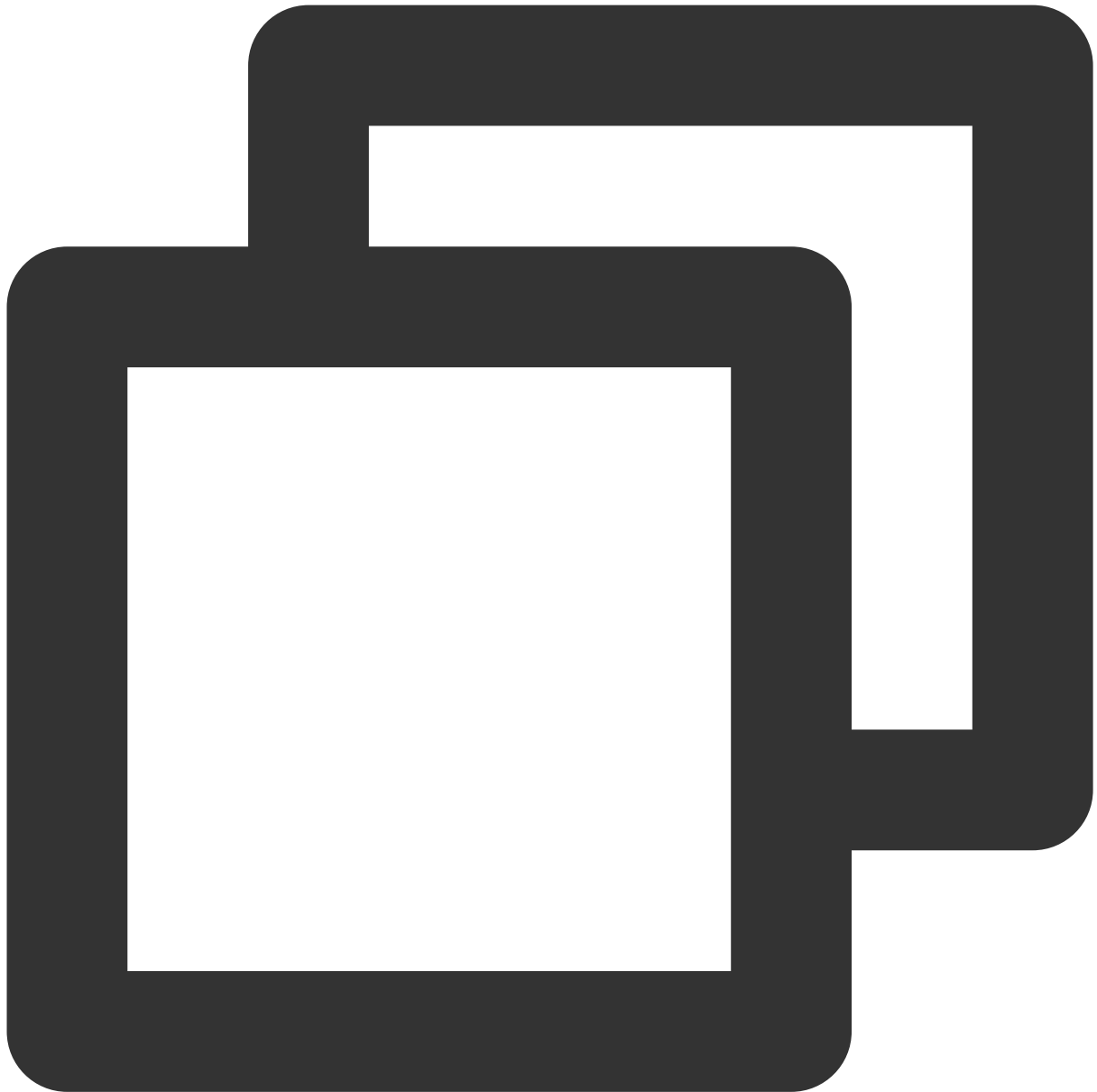
DER 형식은 일반적으로 Java 플랫폼에서 사용됩니다.

인증서 변환:



```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

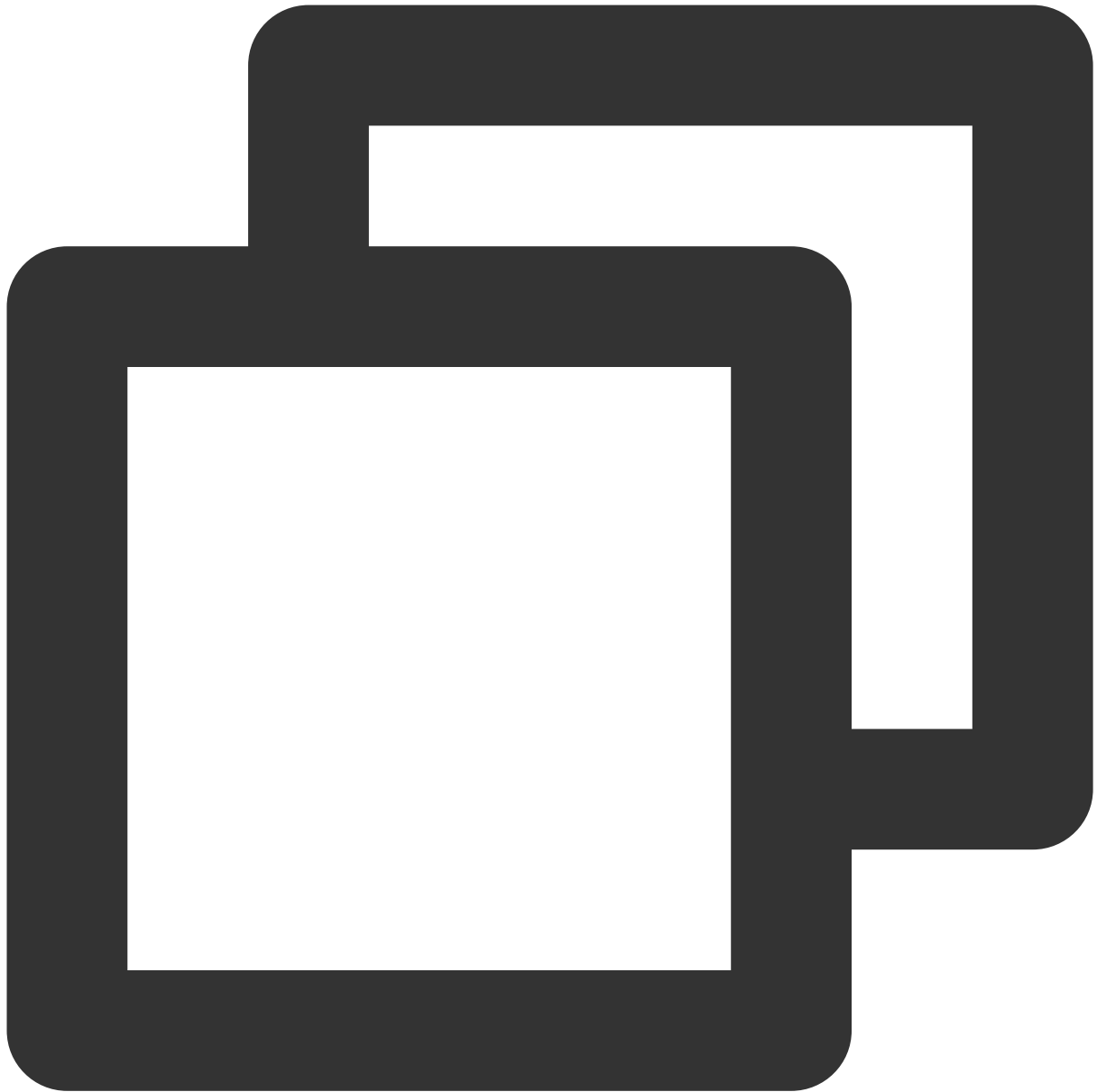
개인키 변환:



```
openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
```

P7B 형식은 일반적으로 Windows Server와 tomcat에서 사용됩니다.

인증서 변환:



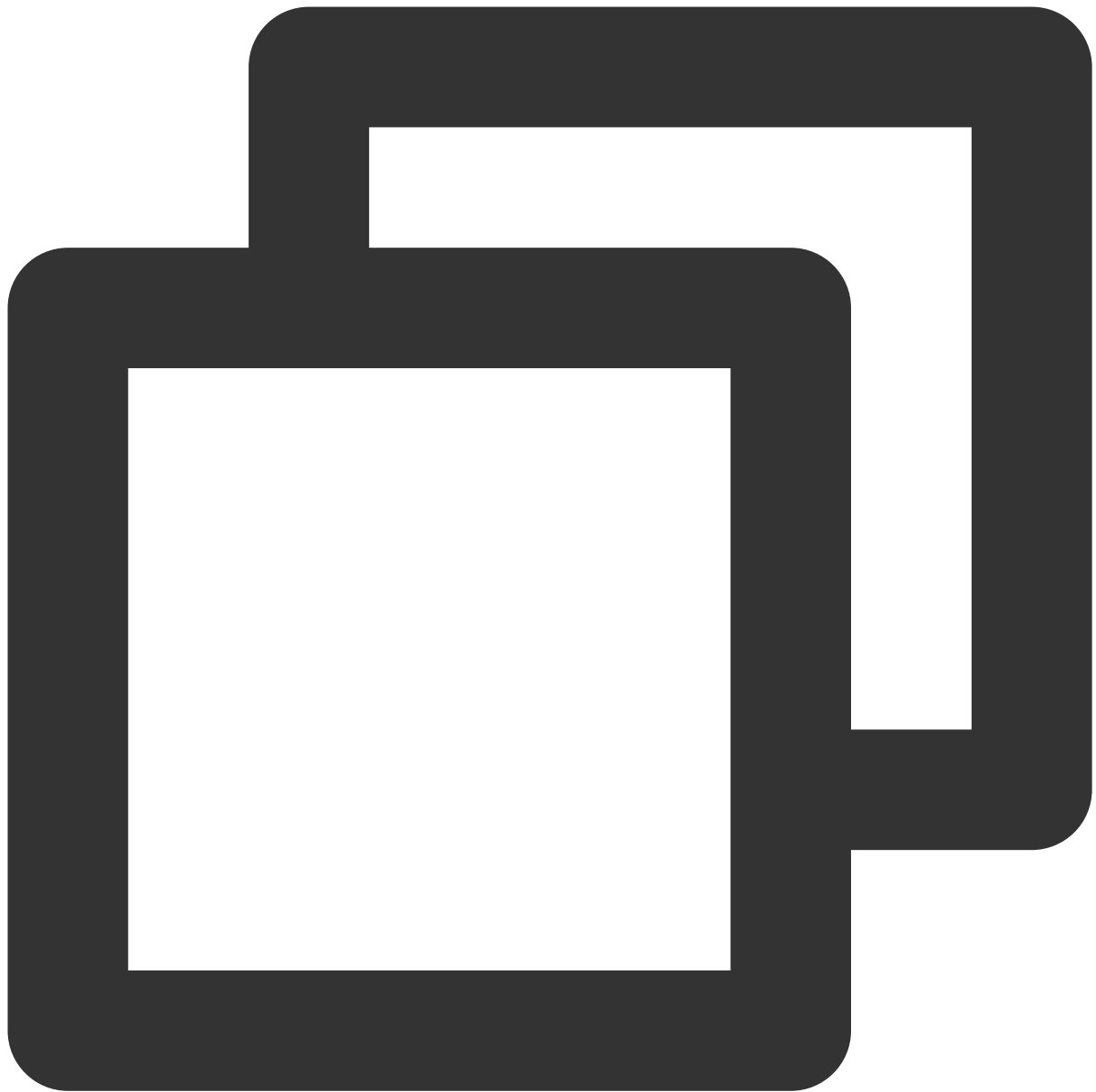
```
openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer
```

인증서로 업로드하려면 outcertificat.cer에서 [—BEGIN CERTIFICATE—, —END CERTIFICATE—]의 콘텐츠를 가져와야 합니다.

개인키 변환: 개인키는 일반적으로 IIS 서버에서 내보낼 수 있습니다.

PFX 형식은 일반적으로 Windows Server에서 사용됩니다.

인증서 변환:



```
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
```

개인키 변환:



```
openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes  
````
```

파일 확장자 이름을 직접 수정하여 CER/CRT 형식의 인증서를 PEM으로 변환할 수 있습니다. 예를 들어 'servertest.crt' 인증서 파일의 이름을 'servertest.pem'으로 직접 바꿀 수 있습니다.

# SSL 단방향 인증 및 양방향 인증

최종 업데이트 날짜: : 2024-01-04 19:59:08

SSL(Secure Sockets Layer, 보안 소켓 레이어)은 인터넷 통신을 위한 보안 및 데이터 무결성을 보장하도록 설계된 보안 프로토콜입니다. 본문은 SSL 단방향 인증과 양방향 인증을 소개합니다.

## 설명 :

CLB 인스턴스에 대한 TCP SSL 리스너 또는 HTTPS 리스너를 생성할 때 SSL 구문 분석 방법으로 단방향 인증 또는 양방향 인증을 선택할 수 있습니다. 자세한 내용은 [Configuring TCP SSL Listener](#) 및 [Configuring HTTPS Listener](#)를 참고하십시오.

## SSL 단방향 인증과 양방향 인증의 차이점

[SSL 단방향 인증](#)의 경우 인증서는 서버에만 필요하고 클라이언트에는 필요하지 않습니다. [SSL 양방향 인증](#)의 경우 서버와 클라이언트 모두에 인증서가 필요합니다.

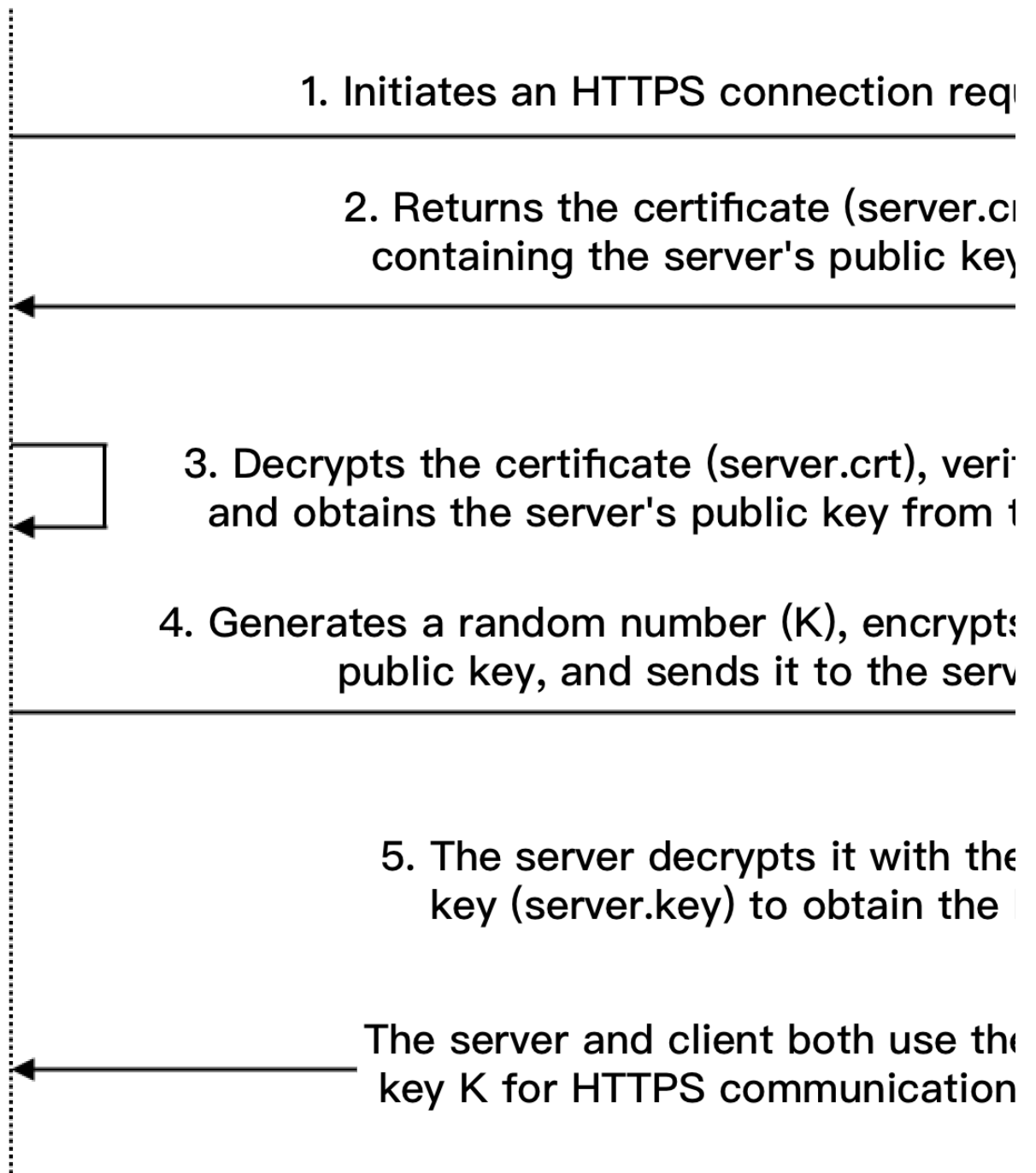
SSL 양방향 인증과 비교하여 단방향 인증은 서버에서 클라이언트 인증서 확인 및 암호화 스키마 협상을 포함하지 않습니다. 서버가 클라이언트에게 보내는 암호화 스키마는 암호화되지 않지만 SSL 인증의 보안은 손상되지 않습니다. Web 애플리케이션은 일반적으로 많은 수의 사용자를 가지고 있으며 SSL 단방향 인증을 사용할 수 있는 통신 레이어에서 사용자 신원 확인이 필요하지 않습니다. 그러나 금융 애플리케이션에 연결하는 클라이언트의 경우 신원 확인이 필요할 수 있으므로 SSL 양방향 인증을 사용해야 합니다.

## SSL 단방향 인증

SSL 단방향 인증에서는 클라이언트 ID가 아닌 서버 ID만 확인하면 됩니다. SSL 단방향 인증 프로세스는 다음과 같습니다.



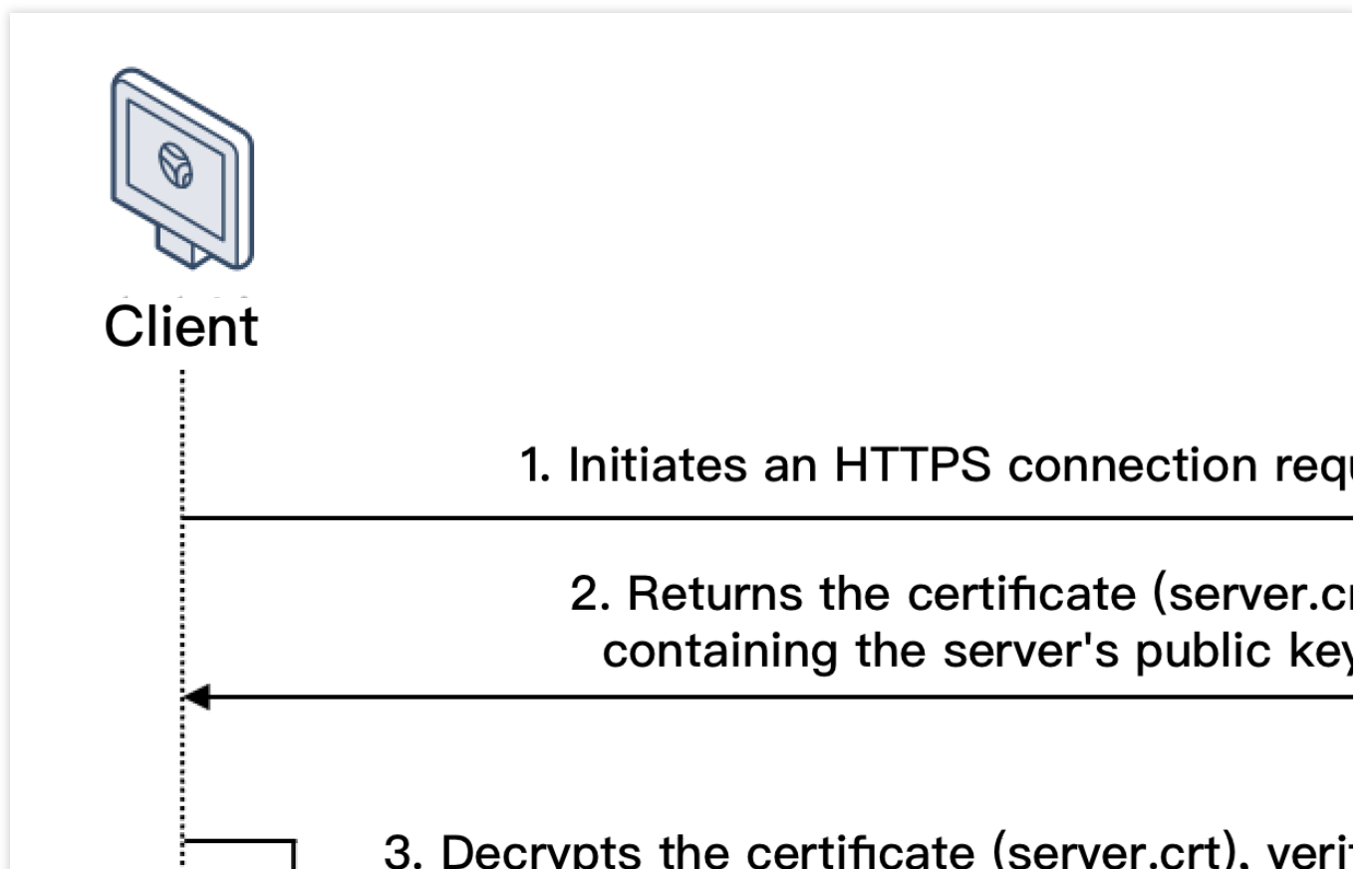
Client

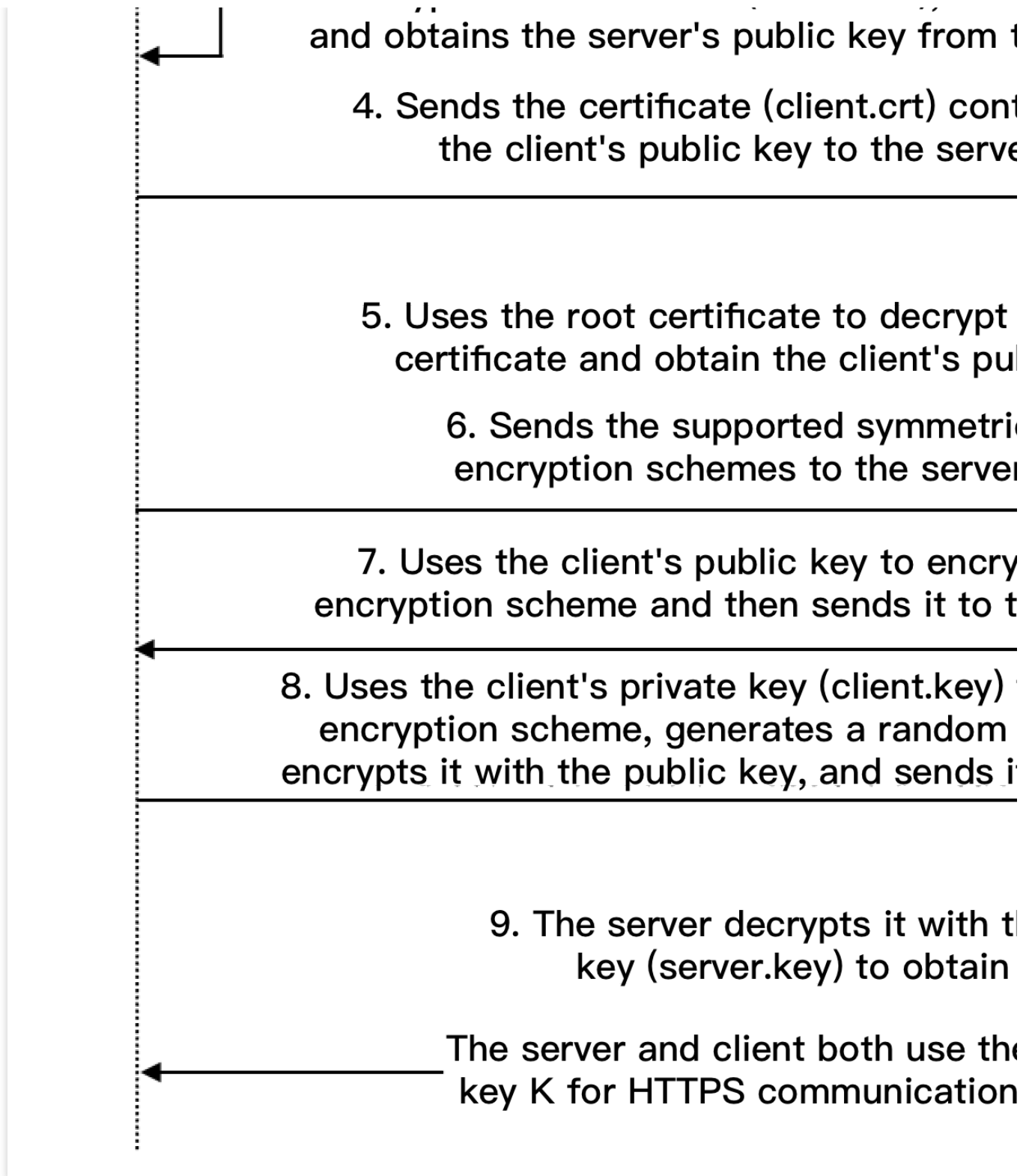


1. 클라이언트는 지원되는 SSL 프로토콜 버전, 암호화 알고리즘, 생성된 랜덤 수 및 기타 정보와 함께 서버에 대한 HTTPS 연결 요청을 시작합니다.
2. 서버는 SSL 프로토콜 버전, 암호화 알고리즘, 생성된 랜덤 수, 서버 인증서(server.crt) 및 기타 정보를 클라이언트에 반환합니다.
3. 클라이언트는 아래 요인에 대한 인증서(server.crt)의 유효성을 확인하고 인증서에서 서버의 공개 키를 얻습니다.  
인증서 만료 여부입니다.  
인증서 해지 여부입니다.  
인증서 신뢰 가능 여부입니다.  
요청한 도메인 이름이 수신된 인증서의 도메인 이름과 동일한지 여부입니다.
4. 인증서가 검증된 후 클라이언트는 랜덤 수(통신을 위한 대칭 암호화 키로 사용되는 키 K)를 생성하고 서버 인증서에서 얻은 공개 키로 암호화한 다음 서버로 보냅니다.
5. 암호화된 정보를 수신한 후 서버는 개인 키(server.key)를 사용하여 대칭 암호화 키(키 K)를 얻기 위해 암호를 해독합니다.  
대칭 암호화 키(키 K)는 정보 보안을 보장하기 위해 서버와 클라이언트에서 통신에 사용됩니다.

## SSL 양방향 인증

SSL 양방향 인증에서는 서버 ID와 클라이언트 ID를 모두 확인해야 합니다. SSL 양방향 인증 과정은 다음과 같습니다.





- 클라이언트는 지원되는 SSL 프로토콜 버전, 암호화 알고리즘, 생성된 랜덤 수 및 기타 정보와 함께 서버에 대한 HTTPS 연결 요청을 시작합니다.
- 서버는 SSL 프로토콜 버전, 암호화 알고리즘, 생성된 랜덤 수, 서버 인증서(server.crt) 및 기타 정보를 클라이언트에 반환합니다.
- 클라이언트는 아래 요인에 대한 인증서(server.crt)의 유효성을 확인하고 인증서에서 서버의 공개 키를 얻습니다. 인증서 만료 여부입니다.

인증서 해지 여부입니다.

인증서 신뢰 가능 여부입니다.

요청한 도메인 이름이 수신된 인증서의 도메인 이름과 동일한지 여부입니다.

4. 서버는 클라이언트가 클라이언트 인증서(client.crt)를 보내도록 요구하고 클라이언트는 필요에 따라 보냅니다.
5. 서버는 클라이언트 인증서(client.crt)를 확인합니다. 확인된 후 서버는 루트 인증서(root.crt)를 사용하여 클라이언트 인증서를 해독하고 클라이언트의 공개 키를 얻습니다.
6. 클라이언트는 지원되는 대칭 암호화 스키마를 서버로 보냅니다.
7. 서버는 클라이언트가 보낸 스키마 중에서 암호화 수준이 가장 높은 암호화 스키마를 선택하고 클라이언트의 공개 키를 사용하여 암호화한 후 클라이언트에게 반환합니다.
8. 클라이언트는 개인 키(client.key)를 사용하여 암호화 스키마를 해독하고 랜덤 수(통신을 위한 대칭 암호화 키로 사용되는 키 K)를 생성하고 서버 인증서에서 얻은 공개 키로 암호화한 다음 서버로 보냅니다.
9. 암호화된 정보를 수신한 후 서버는 개인 키(server.key)를 사용하여 대칭 암호화 키(키 K)를 얻기 위해 암호를 해독합니다.

대칭 암호화 키(키 K)는 정보 보안을 보장하기 위해 서버와 클라이언트에서 통신에 사용됩니다.

## 관련 문서

[Certificate Requirements and Certificate Format Conversion](#)



# 로그 관리

## 액세스 로그 개요

최종 업데이트 날짜: : 2024-01-04 20:00:50

CLB(Cloud Load Balancer) 액세스 로그는 요청 시간, 요청 경로, 클라이언트 IP 및 포트, 반환 코드, 응답 시간과 같은 각 클라이언트 요청의 세부 정보를 수집하고 기록합니다. 이 기능은 클라이언트 요청을 더 잘 이해하고, 문제를 해결하고, 사용자 행동을 분석하는 데 도움이 될 수 있습니다.

### 설명 :

레이어 7 CLB만 액세스 로그 구성을 지원합니다.

현재 일부 리전에서만 액세스 로그 구성을 지원합니다. 자세한 내용은 CLS의 [가용 리전](#)을 참고하십시오.

## 스토리지 메소드

CLB 액세스 로그는 [Cloud Log Service\(CLS\)](#)에 저장 가능: CLS는 로그 수집, 저장, 검색, 분석, 실시간 내보내기, 배송 등 다양한 로그 서비스를 제공하는 원스톱 로그 서비스 플랫폼입니다. 비즈니스 운영, 보안 모니터링, 로그 감사 및 로그 분석을 구현하는 데 도움이 됩니다.

| 기능               | CLS에 액세스 로그 저장                                                         |
|------------------|------------------------------------------------------------------------|
| 로그 획득을 위한 시간 세분성 | 분                                                                      |
| 온라인 검색           | 지원                                                                     |
| 검색 구문            | 전체 텍스트 검색, 키-값 검색, 퍼지 키워드 검색 등 자세한 내용은 <a href="#">검색 규칙</a> 을 참고하십시오. |
| 지원 리전            | CLS 사용 가능한 리전에 대한 자세한 내용은 <a href="#">가용 리전</a> 을 참고하십시오.              |
| 지원되는 CLB 유형      | 공중망/사설망 CLB                                                            |
| 업스트림/다운스트림 링크    | CLS 로그는 COS로 배송되고 추가 처리를 위해 CKafka로 내보낼 수 있습니다.                        |
| 로그 저장            | Tencent Cloud는 기본적으로 액세스 로그를 저장하지 않습니다. 필요에 따라 스토리지 기능을 구성할 수 있습니다.    |

## 관련 작업

## Storing CLB access logs to CLS

# 작업 로그 보기

최종 업데이트 날짜: : 2024-01-04 20:01:04

Cloud Audit 콘솔에서 CLB(Cloud Load Balancer)의 작업 내역을 조회하고 다운로드할 수 있습니다.

Cloud Audit을 사용하면 Tencent Cloud 계정에 대한 감독, 규정 준수 확인, 운영 검토 및 위험 검토를 수행할 수 있습니다. Tencent Cloud 콘솔, API, 명령줄 도구 및 기타 Tencent Cloud 서비스를 통해 수행된 작업을 포함하여 Tencent Cloud 계정 활동의 이벤트 기록을 제공하여 보안 분석, 리소스 변경 추적 및 문제 해결을 간소화합니다.

## 작업 단계

1. CA 콘솔 에 로그인합니다.
2. 왼쪽 사이드바에서 **작업 기록**을 클릭하여 '작업 기록' 페이지로 이동합니다. CLB 콘솔에 로그인하고 오른쪽 상단 모서리에 있는 CA를 선택할 수도 있습니다.
3. 작업 기록 페이지에서 사용자 이름, 리소스 유형, 리소스 이름, 이벤트 소스, 이벤트 ID 등으로 작업을 쿼리합니다. 기본적으로 일부 데이터만 표시되며, 페이지 하단의 **자세히 보기**를 클릭하여 더 많은 결과를 가져올 수 있습니다.

| EventName             | CreateListener |                | Nearly 7 days | 2020-02-09 00:00:00 ~ 2020-03-09 23:59:59 |  |
|-----------------------|----------------|----------------|---------------|-------------------------------------------|--|
| Event time            | User name      | Event name     | Resource type | Resource name                             |  |
| ▶ 2020-02-27 11:51:28 |                | CreateListener | clb           | clb/1                                     |  |
| ▶ 2020-02-11 20:28:03 |                | CreateListener | clb           | clb/1                                     |  |

4. 작업 왼쪽을 클릭하면



액세스 키, 오류 코드 및 이벤트 ID와 같은 세부 정보를 볼 수 있습니다. 이벤트 세부 정보를 보려면 **이벤트 보기**를 클릭합니다.

[View event](#)

# 액세스 로그 구성

최종 업데이트 날짜: : 2024-01-04 20:01:32

CLB(Cloud Load Balancer)는 클라이언트 요청을 더 잘 이해하고, 문제를 해결하고, 사용자 행동을 분석하는 데 도움이 될 수 있는 레이어 7(HTTP/HTTPS) 액세스 로그(Access Log) 구성을 지원합니다. 현재 액세스 로그는 CLS에 저장되고, 미세한 단위로 보고되며, 여러 규칙에 따라 온라인으로 검색할 수 있습니다.

CLB의 액세스 로그는 주로 문제를 빠르게 찾고 해결하는 데 사용됩니다. 액세스 로그 기능에는 로그 리포트, 저장 및 검색이 포함됩니다.

로그 리포트는 최선의 서비스(Best-Effort Service)를 제공합니다. 즉, 로그 리포트보다 서비스 포워딩을 우선시합니다.

로그 스토리지 및 검색은 현재 사용 중인 스토리지 서비스를 기반으로 SLA를 제공합니다.

## 설명:

현재 액세스 로그는 레이어 7 프로토콜(HTTP/HTTPS)에 대해서만 CLS에 저장할 수 있으며, 레이어 4 프로토콜(TCP/UDP/TCP SSL)에는 저장할 수 없습니다.

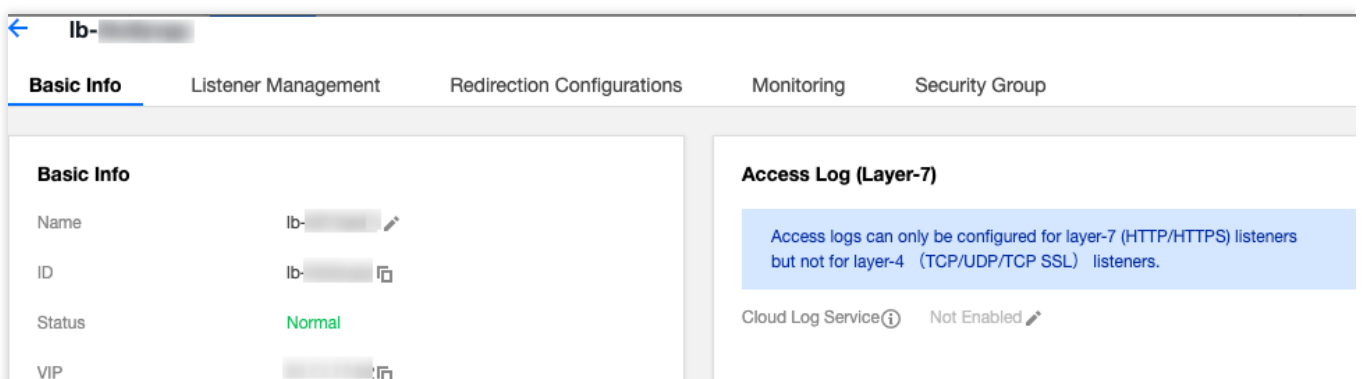
CLS에 대한 CLB 액세스 로그 저장은 무료입니다. CLS 서비스에 대한 요금만 지불하면 됩니다.

이 기능은 CLS 사용 가능 리전에서만 지원됩니다. 사용 가능한 리전을 참고하십시오.

## 방법1: 단일 인스턴스 액세스 로그

### 1단계: CLS에서 액세스 로그 스토리지 활성화

1. CLB 콘솔에 로그인하고 왼쪽 사이드바에서 **인스턴스 관리**를 클릭합니다.
2. 인스턴스 관리 페이지에서 CLB 인스턴스 ID를 클릭합니다.
3. 기본 정보 페이지의 '액세스 로그(레이어 7)' 모듈에서 연필 아이콘을 클릭합니다.



4. CLS 로그 스토리지 위치 수정 팝업 창에서 **로그를 활성화**하고 액세스 로그 스토리지에 대한 대상 로그셋 및 로그 테마를 선택한 다음 **제출**을 클릭합니다. 아직 로그셋 또는 로그 테마를 생성하지 않은 경우 **관련 리소스 생성** 후 다음 저장 위치로 선택하십시오.

**설명:**

clb\_logset 로그셋에서 CLB로 표시된 로그 테마를 사용하는 것이 좋습니다. CLB로 표시된 로그 테마와 일반 테마의 차이점은 다음과 같습니다.

**CLB** 로그 테마는 자동으로 인덱스를 생성할 수 있지만 일반적인 로그 테마는 수동 인덱스 생성이 필요합니다.

기본적으로 **CLB** 로그 테마에 대한 대시보드가 제공되지만 일반적인 로그 테마에 대해서는 수동으로 구성해야 합니다.

5. 로그셋 또는 로그 테마를 클릭하여 CLS의 로그 검색 분석 페이지로 리디렉션합니다.

6. (옵션) 로그를 비활성화하려면 연필 아이콘을 클릭하여 **CLS 로그 저장 위치 수정** 창을 열고 비활성화합니다.

**2단계: 로그 테마 인덱스 구성****설명:**

단일 인스턴스에 대해 액세스 로그가 구성된 경우 로그 테마에 대한 인덱스를 구성해야 합니다. 그렇지 않으면 로그를 찾을 수 없습니다.

권장 인덱스는 다음과 같습니다.

| 키-값 인덱스     | 필드 유형 | 구분 기호            |
|-------------|-------|------------------|
| server_addr | text  | 구분 기호가 필요하지 않습니다 |
| server_name | text  | 구분 기호가 필요하지 않습니다 |
| http_host   | text  | 구분 기호가 필요하지 않습니다 |
| status      | long  | -                |
| vip_vpcid   | long  | -                |

단계는 다음과 같습니다.

1. **CLS 콘솔**에 로그인하고 왼쪽 사이드바에서 **로그 테마**를 클릭합니다.
2. **로그 테마** 페이지에서 대상 로그 테마 ID를 클릭합니다.

3. 로그 테마 세부 정보 페이지에서 **인덱스 구성** 탭을 선택하고 **편집**을 클릭하여 인덱스를 추가합니다. 인덱스 구성에 대한 자세한 내용은 [Configuring Index](#)를 참고하십시오.

1. The modified index configuration is only effective for newly written data, and have no impact on the index of the existed data.

2. Delimiter cannot be letters, numbers or Chinese characters. For whitespace characters, such as "\t" "\n" "\r", escaping is required. For other characters, escaping is not required.

### Index Configuration

Index Status ☒

Full-Text Index ☒ ☒ Case-sensitive

Full-text delimiter

Key-Value Index ☒ ☐ Case-sensitive

| Key-Value Index                          | Field Type                        | Delimiter                                                                  | Operation              |
|------------------------------------------|-----------------------------------|----------------------------------------------------------------------------|------------------------|
| <input type="text" value="remote_addr"/> | <input type="text" value="text"/> | <input '&lt;&gt;="" ?\ ;\n\t\""="" type="text" value="!@#%^&amp;*()-_=\"/> | <a href="#">Delete</a> |
| <input type="text" value="remote_port"/> | <input type="text" value="text"/> | <input '&lt;&gt;="" ?\ ;\n\t\""="" type="text" value="!@#%^&amp;*()-_=\"/> | <a href="#">Delete</a> |
| <input type="text" value="status"/>      | <input type="text" value="long"/> | -                                                                          | <a href="#">Delete</a> |

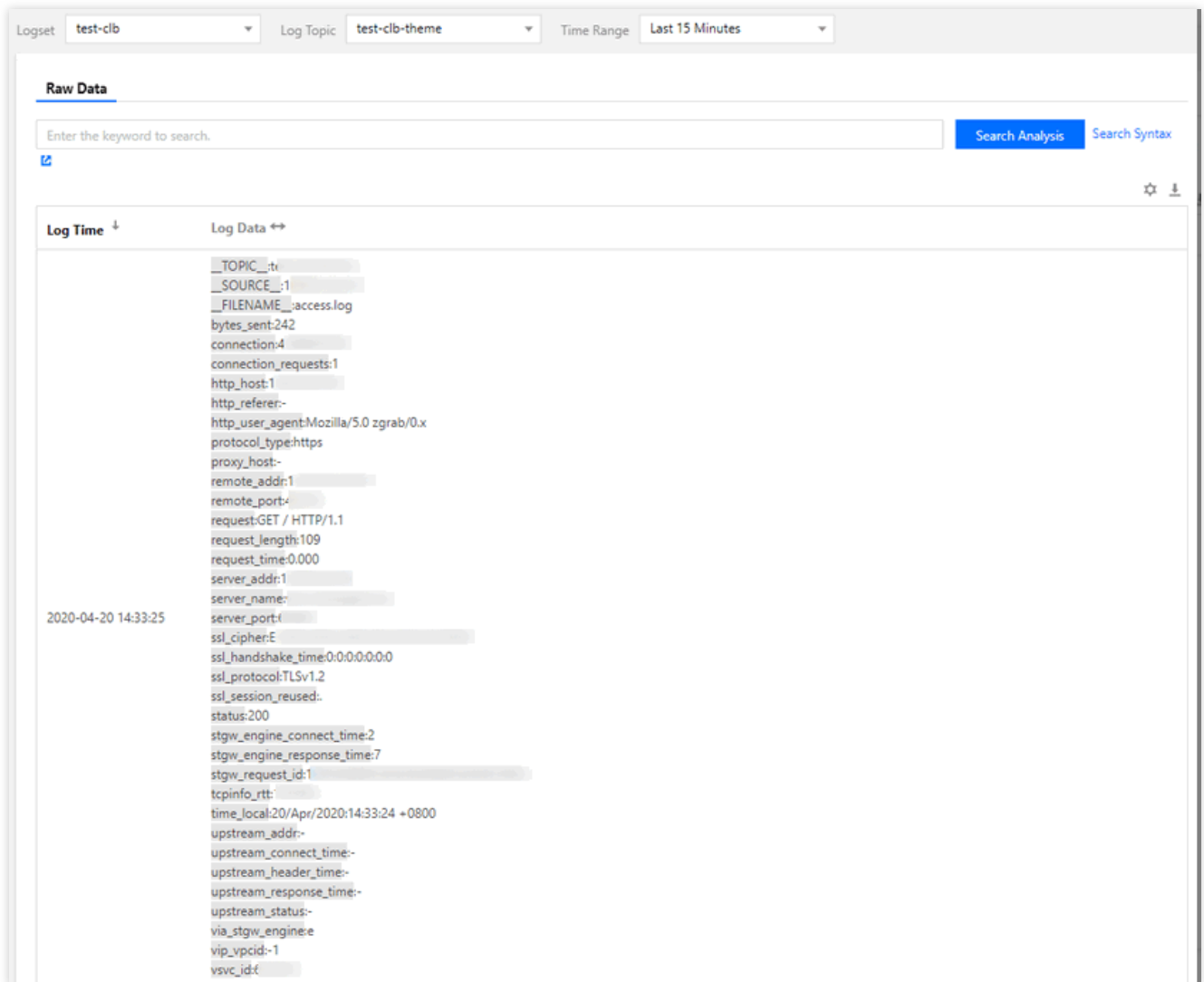
4. 인덱스 구성 결과는 다음과 같습니다.

| Index Configuration |                                  |                                  | Edit |
|---------------------|----------------------------------|----------------------------------|------|
| Index Status        | Enabled                          |                                  |      |
| Full-Text Index     | Enabled                          | Case-sensitive                   |      |
| Full-text delimiter | !@#%^&*()_="', <>/?\ ;\n\t\r[]{} |                                  |      |
| Key-Value Index     | Enabled                          |                                  |      |
| Key-Value Index     | Field Type                       | Delimiter                        |      |
| remote_addr         | text                             | !@#%^&*()_="', <>/?\ ;\n\t\r[]{} |      |
| remote_port         | text                             | !@#%^&*()_="', <>/?\ ;\n\t\r[]{} |      |
| status              | long                             | None                             |      |
| server_addr         | text                             | !@#%^&*()_="', <>/?\ ;\n\t\r[]{} |      |
| server_name         | text                             | !@#%^&*()_="', <>/?\ ;\n\t\r[]{} |      |
| http_host           | text                             | !@#%^&*()_="', <>/?\ ;\n\t\r[]{} |      |
| request_time        | double                           | None                             |      |

### 3단계: 액세스 로그 보기

1. [CLS 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **검색 및 분석**을 클릭합니다.
2. **검색 분석** 페이지에서 로그셋, 로그 테마 및 시간 범위를 선택하고 **검색 분석**을 클릭하여 CLB에서 CLS에 보고한 액세스 로그를 검색합니다. 검색 구문에 대한 자세한 내용은 [Legacy CLS Search Syntax](#)를 참고하십시오.





## 방법2: 액세스 로그 일괄 구성

### 1단계: 로그셋 및 로그 테마 생성

CLS에서 액세스 로그를 구성하려면 먼저 로그셋 및 로그 테마를 생성해야 합니다.

로그셋과 로그 테마를 생성했다면 바로 **2단계**로 이동할 수 있습니다.

1. **CLB 콘솔**에 로그인하고 왼쪽 사이드바에서 **액세스 로그**를 선택합니다.
2. **액세스 로그** 페이지에서 로그 집합에 대한 영역을 선택한 다음 **로그셋 정보** 섹션에서 **로그셋 생성**을 클릭합니다.
3. **로그셋 생성** 팝업 창에서 저장 기간을 설정하고 **저장**을 클릭합니다.

#### 설명:

각 리전에서 'clb\_logset'이라는 단일 로그셋만 생성할 수 있습니다.

4. **액세스 로그** 페이지의 **로그 테마** 섹션에서 **로그 테마 생성**을 클릭합니다.
5. **로그 테마 추가** 팝업 창에서 스토리지 유형 및 로그 저장 시간을 선택한 후, 오른쪽 목록에 추가할 CLB 인스턴스를 선택하고 **저장**을 클릭합니다.

#### 설명:

스토리지 유형은 STANDARD, STANDARD\_IA로 구분됩니다. 자세한 내용은 [Storage Class Overview](#)를 참고하십시오.

로그는 영구적으로 또는 지정된 기간 동안 보관할 수 있습니다.

로그 테마를 생성할 때 필요에 따라 CLB 인스턴스를 추가할 수 있습니다. 추가하려면 목록에서 로그 테마를 선택하고 **작업** 열에서 **관리**를 클릭합니다. 각 CLB 인스턴스는 하나의 로그 테마에만 추가할 수 있습니다.

로그셋에는 여러 로그 테마(Topic)가 포함될 수 있습니다. CLB 로그를 **CLB**로 표시되는 다양한 로그 테마로 분류할 수 있습니다.

6. (옵션) 액세스 로그를 닫으려면 로그 테마 우측의 **작업** 열에서 **중지**를 클릭하기만 하면 됩니다.

## 2단계: 액세스 로그 보기

수동 구성 없이 CLB는 액세스 로그 값으로 인덱스 검색으로 자동 구성되었습니다. 검색 분석을 통해 접속 로그를 직접 조회할 수 있습니다.

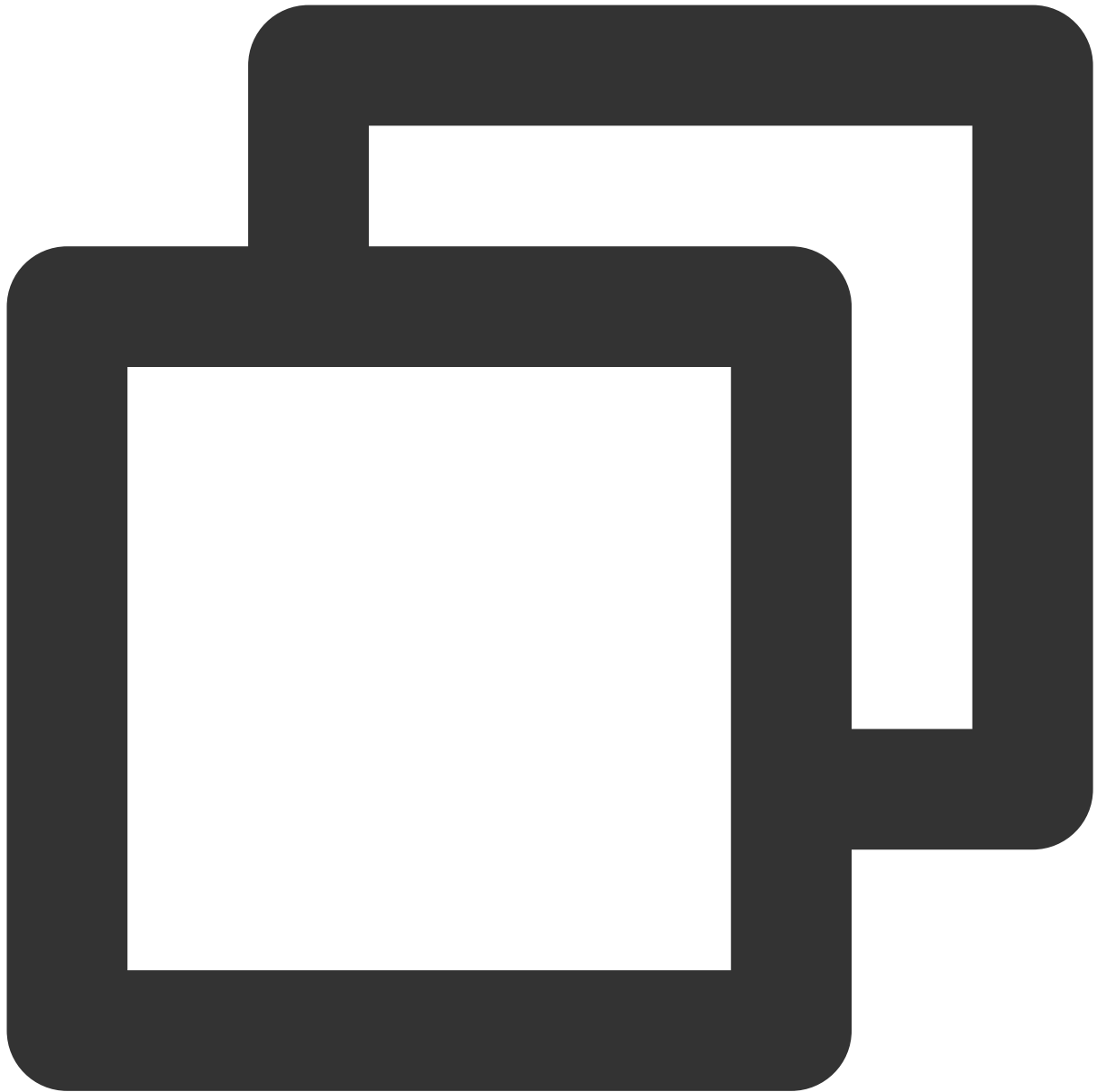
1. **CLB 콘솔**에 로그인하고 왼쪽 사이드바에서 **액세스 로그**를 선택합니다.
2. 로그 테마를 선택하고 **작업** 열에서 **검색**을 클릭하면 **CLS 콘솔**의 '검색 분석' 페이지로 리디렉션됩니다.
3. **검색 분석** 페이지에서 입력 상자에 검색 구문을 입력하고 시간 범위를 선택한 다음 **검색 분석**을 클릭하여 CLB에서 CLS에 리포트한 액세스 로그를 검색합니다.

### 설명:

검색 구문에 대한 자세한 내용은 [Overview and Syntax Rules](#)를 참고하십시오.

## 로그 형식 및 변수 설명

### 로그 형식



```
[$stgw_request_id] [$time_local] [$protocol_type] [$server_addr:$server_port] [$se
```

## 필드 유형

현재 CLS는 다음 세 가지 필드 유형을 지원합니다.

| 이름   | 유형 설명         |
|------|---------------|
| text | 텍스트 유형        |
| long | 정수 유형(Int 64) |

|        |                   |
|--------|-------------------|
| double | 부동 소수점 유형(64 bit) |
|--------|-------------------|

## 로그 변수 설명

| 변수 이름              | 설명                                                                                                        | 필드 유형  |
|--------------------|-----------------------------------------------------------------------------------------------------------|--------|
| stgw_request_id    | 요청 ID.                                                                                                    | text   |
| time_local         | 액세스 시간 및 시간대(예시: '01/Jul/2019:11:11:00 +0800', 여기서 '+0800'은 UTC+8, 즉 베이징 시간을 나타냄).                        | text   |
| protocol_type      | 프로토콜 유형(HTTP/HTTPS/SPDY/HTTP2/WS/WSS).                                                                    | text   |
| server_addr        | CLB VIP.                                                                                                  | text   |
| server_port        | CLB VPort, 즉 수신 포트입니다.                                                                                    | long   |
| server_name        | 규칙의 server_name, 즉 CLB 리스너에 구성된 도메인 이름입니다.                                                                | text   |
| remote_addr        | 클라이언트 IP.                                                                                                 | text   |
| remote_port        | 클라이언트 포트.                                                                                                 | long   |
| status             | CLB에서 클라이언트로 반환된 상태 코드입니다.                                                                                | long   |
| upstream_addr      | RS 주소.                                                                                                    | text   |
| upstream_status    | RS에서 CLB로 반환된 상태 코드입니다.                                                                                   | text   |
| proxy_host         | stream ID.                                                                                                | text   |
| request            | 요청 라인.                                                                                                    | text   |
| request_length     | 클라이언트에서 받은 요청의 바이트 수입니다.                                                                                  | long   |
| bytes_sent         | 클라이언트에 보낸 바이트 수입니다.                                                                                       | long   |
| http_host          | HTTP 헤더의 Host인 도메인 이름을 요청합니다.                                                                             | text   |
| http_user_agent    | HTTP 헤더의 user_agent 필드입니다.                                                                                | text   |
| http_referer       | HTTP 요청 소스입니다.                                                                                            | text   |
| http_x_forward_for | HTTP 요청에 있는 x-forward-for header의 콘텐츠입니다.                                                                 | text   |
| request_time       | 요청 처리 시간: 타이밍은 클라이언트로부터 첫 번째 바이트를 수신한 시점부터 클라이언트에게 마지막 바이트가 전송된 시점까지를 의미합니다. 이는 클라이언트 요청이 CLB 인스턴스에 도달하고, | double |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |        |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
|                        | CLB 인스턴스가 요청을 RS로 전달하고, RS가 응답을 보내고 CLB 인스턴스가 데이터를 클라이언트로 전달하는 전체 프로세스에 대한 총 시간을 의미합니다. 단위: 초.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |        |
| upstream_response_time | 전체 백엔드 요청 프로세스 소요 시간: CLB 인스턴스가 CONNECT RS될 때부터 RS가 요청을 수신하고 응답할 때까지. 단위: 초.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | double |
| upstream_connect_time  | RS와 TCP의 연결 설정 소요 시간: CLB 인스턴스가 CONNECT RS될 때부터 HTTP 요청을 보낼 때까지.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | double |
| upstream_header_time   | RS에서 HTTP 헤더 수신 소요 시간: CLB 인스턴스가 CONNECT RS될 때부터 RS로부터 HTTP 응답 헤더가 수신될 때까지.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | double |
| tcpinfo_rtt            | TCP 연결 RTT.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | long   |
| connection             | 연결 ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | long   |
| connection_requests    | 연결 요청 수입입니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | long   |
| ssl_handshake_time     | <p>x:x:x:x:x형식의 각 SSL 핸드셰이크 단계에 소요된 시간입니다. 이 중 콜론으로 구분된 문자열은 단위는 ms이며, 각 단계에 소요된 시간이 1ms 미만이면 0으로 표시됩니다.</p> <p>첫 번째 필드는 SSL 세션 재사용 여부를 나타냅니다.</p> <p>2번째 필드는 전체 핸드셰이크 시간을 나타냅니다.</p> <p>3번째~7번째 필드는 각 SSL 핸드셰이크 단계에 소요되는 시간을 나타냅니다.</p> <p>3번째 필드는 CLB가 client hello를 수신한 시점부터 server hello done을 전송한 시점까지의 시간을 나타냅니다.</p> <p>4번째 필드는 CLB가 server 인증서 전송을 시작한 시점부터 server 인증서 전송을 완료한 시점까지의 시간을 나타냅니다.</p> <p>5번째 필드는 CLB가 서명을 계산한 시점부터 server key exchange 전송을 완료한 시점까지의 시간을 나타냅니다.</p> <p>6번째 필드는 CLB가 client key exchange 수신을 시작한 시점부터 client key exchange 수신을 완료할 때까지의 시간을 나타냅니다.</p> <p>7번째 필드는 CLB가 client key exchange 수신을 시작한 시점부터 server finished를 보낸 시점까지의 시간을 나타냅니다.</p> | text   |
| ssl_cipher             | SSL 암호화 제품군.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | text   |
| ssl_protocol           | SSL 프로토콜 버전.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | text   |
| vip_vpcid              | CLB 인스턴스의 VPC ID이며 공중망 CLB의 값은 -1입니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | long   |
| request_method         | 요청 방법. POST 및 GET 요청만 지원됩니다.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | text   |
| uri                    | 리소스 식별자.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | text   |
| server_protocol        | CLB에 사용되는 프로토콜.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | text   |

## 기본 검색 로그 값

다음 필드는 기본적으로 'CLB'가 있는 로그셋에서 찾을 수 있습니다.

| 인덱스 필드                 | 설명                                                                                                                                                                                                       | 필드 유형  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| time_local             | 액세스 시간 및 시간대(예시: '01/Jul/2019:11:11:00 +0800', 여기서 '+0800'은 UTC+8, 즉 베이징 시간을 나타냄).                                                                                                                       | text   |
| protocol_type          | 프로토콜 유형(HTTP/HTTPS/SPDY/HTTP2/WS/WSS).                                                                                                                                                                   | text   |
| server_addr            | CLB VIP.                                                                                                                                                                                                 | text   |
| server_name            | 규칙의 server_name, 즉 CLB 리스너에 구성된 도메인 이름입니다.                                                                                                                                                               | text   |
| remote_addr            | 클라이언트 IP.                                                                                                                                                                                                | text   |
| status                 | CLB에서 클라이언트로 반환된 상태 코드입니다.                                                                                                                                                                               | long   |
| upstream_addr          | RS 주소.                                                                                                                                                                                                   | text   |
| upstream_status        | RS에서 CLB로 반환된 상태 코드입니다.                                                                                                                                                                                  | text   |
| request_length         | 클라이언트에서 받은 요청의 바이트 수입니다.                                                                                                                                                                                 | long   |
| bytes_sent             | 클라이언트에 보낸 바이트 수입니다.                                                                                                                                                                                      | long   |
| http_host              | HTTP 헤더의 Host인 도메인 이름을 요청합니다.                                                                                                                                                                            | text   |
| request_time           | 요청 처리 시간: 타이밍은 클라이언트로부터 첫 번째 바이트를 수신한 시점부터 클라이언트에게 마지막 바이트가 전송된 시점까지를 의미합니다. 이는 클라이언트 요청이 CLB 인스턴스에 도달하고, CLB 인스턴스가 요청을 RS로 전달하고, RS가 응답을 보내고 CLB 인스턴스가 데이터를 클라이언트로 전달하는 전체 프로세스에 대한 총 시간을 의미합니다. 단위: 초. | double |
| upstream_response_time | 전체 백엔드 요청 프로세스 소요 시간: CLB 인스턴스가 CONNECT RS될 때부터 RS가 요청을 수신하고 응답할 때까지.                                                                                                                                    | double |

# 로그 샘플링 및 수집

최종 업데이트 날짜: : 2024-01-04 20:01:52

레이어 7 액세스 로그 또는 상태 확인 로그를 활성화한 후 많은 양의 로그가 있는 일부 시나리오의 경우 전체 로그 양을 리포트하면 더 높은 로그 비용이 발생할 수 있습니다. CLB는 일부 로그의 샘플 수집을 지원하여 데이터 리포트 양을 줄여 로그 비용을 줄입니다.

## 설명:

CLB는 로그 데이터의 검색, 분석, 시각화 및 알람을 실현하기 위해 로그 서비스 CLS에 대한 액세스 로그 및 상태 확인 로그의 구성을 지원합니다. Tencent Cloud CLS는 개별 과금 제품입니다. 과금 기준은 [CLS 과금 세부 정보](#)를 참고하십시오.

## 전제 조건

액세스 로그에 대한 로그셋 및 로그 토픽을 생성합니다. 자세한 내용은 [액세스 로그 구성](#)을 참고하십시오.  
상태 확인 로그의 로그 셋과 로그 토픽을 생성합니다. 자세한 내용은 [상태 확인 로그 구성](#)을 참고하십시오.

## 레이어 7 액세스 로그 샘플링 및 수집

1. [CLB 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **액세스 로그 > 로그 목록**을 선택합니다.
2. **액세스 로그** 세부 정보 페이지의 왼쪽 상단에서 리전을 선택하고 로그 토픽 목록에서 대상 로그 토픽을 찾은 다음 작업 열에서 **자세히 > 샘플링 및 수집**을 선택합니다.
3. 팝업된 **CLB 로그 샘플링 및 수집 관리** 창에서 샘플링 및 수집 스위치를 활성화하고 필요에 따라 매개변수를 구성합니다.

| 매개변수         | 설명                                                                                                     |
|--------------|--------------------------------------------------------------------------------------------------------|
| 샘플링 및 수집 스위치 | 활성화 후, 샘플링 및 수집 로그가 지원됩니다.<br>비활성화 후 모든 로그가 수집되며 샘플링 및 수집은 더 이상 진행되지 않습니다.                             |
| 기본 샘플링 비율    | 샘플링 및 수집 로그에 대한 샘플링 규칙을 구성한 후 샘플링 규칙과 일치하지 않는 로그는 기본 샘플링 비율에 따라 수집됩니다. 1-100의 정수 입력 지원.                |
| 샘플링 필드       | 샘플링 및 수집을 지원하는 현재 로그 필드의 상태 코드는 <b>status</b> 입니다.                                                     |
| 샘플링 규칙       | 샘플링 규칙은 정규식을 지원합니다. 예를 들어 <b>status</b> 상태 코드가 400 또는 500인 로그를 샘플링하려는 경우 샘플링 규칙을 400 500으로 설정할 수 있습니다. |
| 샘플링 비율       | 샘플링 및 수집 비율을 정의하는데 사용되며 1-100의 정수 입력을 지원합니다.                                                           |
| 작업           | 샘플링 및 수집 규칙을 삭제하도록 선택할 수 있습니다.                                                                         |

|    |                                                                                              |
|----|----------------------------------------------------------------------------------------------|
| 추가 | 현재 샘플링 규칙이 요구 사항을 충족할 수 없는 경우 샘플링 규칙을 계속 추가하도록 선택할 수 있습니다. 각 로그 토픽은 최대 5개의 샘플링 규칙 구성을 지원합니다. |
|----|----------------------------------------------------------------------------------------------|

### Sample CLB logs

Sample ☒

Default ratio ⓘ  %

Logs are sampled based on the sampling rule and sampling ratio. The sampling rule supports regular expressions, and the an integer between 1-100. [Learn more](#)

| Sampling field                      | Sampling rule                        | Sampling ratio                    | Operation |
|-------------------------------------|--------------------------------------|-----------------------------------|-----------|
| <input type="text" value="status"/> | <input type="text" value="400 500"/> | <input type="text" value="20"/> % | Delete    |

Add

Submit Cancel

4. 구성 완료 후 **제출** 버튼을 클릭하면 로그 토픽 목록 페이지로 돌아가며, 샘플링 및 수집이 활성화된 로그 토픽에 **샘플링** 플래그가 추가됩니다.

test **Sampling**

Shipping

30

## 상태 확인 로그 샘플링 및 수집

1. CLB 콘솔에 로그인하고 왼쪽 사이드바에서 **상태 확인 로그**를 선택합니다.
2. 나머지 단계는 상기 **레이어 7 액세스 로그 샘플링 및 수집**을 참고하십시오.

## 관련 문서

[액세스 로그 구성](#)



상태 확인 로그 구성

# 상태 확인 로그 구성

최종 업데이트 날짜: : 2024-01-04 20:02:07

CLB는 상태 확인 로그를 CLS에 저장하여 로그를 보고, 분 단위로 리포트하고, 여러 규칙에 따라 온라인으로 쿼리하여 상태 확인 실패의 원인을 진단할 수 있도록 지원합니다.

## 설명:

상태 확인 로그는 현재 베타 사용자가 사용할 수 있습니다. 이 서비스를 이용하시려면 [티켓 제출](#)하십시오.

상태 확인 로그에는 로그 리포트, 저장 및 쿼리가 포함됩니다.

로그 리포트: 서비스 포워딩을 먼저 처리한 후 로그 리포트를 처리합니다.

로그 스토리지 및 쿼리: 현재 사용 중인 스토리지 서비스를 기반으로 SLA 지원을 제공합니다.

## 제한 설명

CLB 레이어 4 및 레이어 7 프로토콜은 상태 확인 로그를 CLS에 저장하는 데 사용할 수 있습니다.

CLB 상태 확인 로그를 CLS에 저장하는 것은 무료입니다. CLS 서비스에 대한 요금만 지불하면 됩니다.

이 기능은 애플리케이션 CLB에서만 사용할 수 있습니다.

IPv4 및 IPv6 NAT64 CLB 인스턴스만 이 기능이 지원됩니다.

이 기능은 CLS 사용 가능 리전에서만 지원됩니다. 사용 가능한 리전을 참고하십시오.

## 1단계: 역할 권한 추가

역할 권한을 추가하려면 CLS 서비스를 활성화했는지 확인하십시오.

1. [CLB 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **상태 확인 로그**를 선택합니다.
2. '상태 확인 로그' 페이지에서 **지금 활성화**를 클릭합니다. 팝업 창에서 **인증 및 활성화**를 클릭합니다.
3. [CAM 콘솔](#)에서 '역할 관리' 페이지로 이동하고 **권한 부여 동의**를 클릭하십시오.

## 2단계: 로그셋 및 로그 테마 생성

상태 확인 로그를 CLS에 저장하려면 먼저 로그셋 및 로그 테마를 생성해야 합니다.

로그셋 및 로그 테마를 생성한 경우 [3단계](#)로 바로 이동할 수 있습니다.

1. [CLB 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **상태 확인 로그**를 선택합니다.
2. **상태 확인 로그** 페이지에서 로그셋에 대한 리전을 선택한 다음 **로그셋 정보** 섹션에서 **로그셋 생성**을 클릭합니다.
3. **로그셋 생성** 팝업 창에서 저장 기간을 설정하고 **저장**을 클릭합니다.
4. **상태 확인 로그** 페이지의 **로그 테마** 섹션에서 **로그 테마 생성**을 클릭합니다.

5. **로그 테마 추가** 팝업 창에서 스토리지 유형 및 로그 저장 시간을 선택한 후, 오른쪽 목록에 추가할 CLB 인스턴스를 선택하고 **저장**을 클릭합니다.

**설명:**

스토리지 유형은 STANDARD, STANDARD\_IA로 구분됩니다. 자세한 내용은 [스토리지 유형 개요](#)를 참고하십시오.

로그는 영구적으로 또는 지정된 기간 동안 보관할 수 있습니다.

로그 테마를 생성할 때 필요에 따라 CLB 인스턴스를 추가할 수 있습니다. 추가하려면 목록에서 로그 테마를 선택하고 **작업** 열에서 **관리**를 클릭합니다. 각 CLB 인스턴스는 하나의 로그 테마에만 추가할 수 있습니다.

로그셋에는 여러 로그 테마(Topic)가 포함될 수 있습니다. CLB 로그를 'CLB'로 표시되는 다양한 로그 테마로 분류할 수 있습니다.

6. (옵션) 상태 확인 로그를 비활성화하려면 로그 테마 우측의 **작업** 열에서 **중지**를 클릭하기만 하면 됩니다.

## 3단계: 상태 확인 로그 보기

수동 구성 없이 CLB는 상태 확인 로그 값으로 인덱스 검색으로 자동 구성되었습니다. 검색 및 분석을 통해 상태 확인 로그를 직접 쿼리할 수 있습니다.

1. [CLB 콘솔](#)에 로그인하고 왼쪽 사이드바에서 **상태 확인 로그**를 선택합니다.

2. '상태 확인 로그' 페이지에서 보려는 로그셋의 리전을 선택합니다. '로그 테마' 섹션에서 선택한 로그 테마의 오른쪽의 '작업' 열에서 **검색**을 클릭하면 [CLS 콘솔](#)로 리디렉션됩니다.

3. CLS 콘솔에서 왼쪽 사이드바의 **검색 분석**을 클릭합니다.

4. **검색 분석** 페이지에서 입력 상자에 검색 구문을 입력하고 시간 범위를 선택한 다음 **검색 분석**을 클릭하여 CLB에서 CLS에 리포트한 상태 확인 로그를 검색합니다.

**설명:**

검색 구문에 대한 자세한 내용은 [Overview and Syntax Rules](#)를 참고하십시오.

## 상태 확인 로그 형식 및 변수

### 로그 형식



```
[${protocol}] [${rsport}] [${rs_vpcid}] [${vport}] [${vpcid}] [${time}] [${vip}] [${rsip}] [${status}] [${domain}]
```

## 로그 변수 설명

| 변수 이름    | 설명                                     | 필드 유형 |
|----------|----------------------------------------|-------|
| protocol | 프로토콜 유형(HTTP/HTTPS/SPDY/HTTP2/WS/WSS). | text  |
| rsport   | RS 포트.                                 | long  |

|          |                                                                                    |      |
|----------|------------------------------------------------------------------------------------|------|
| rs_vpcid | 리얼 서버의 VPC ID 공중망 CLB 인스턴스의 vip_vpcid는 -1입니다.                                      | long |
| vport    | CLB VPort, 즉 수신 포트입니다.                                                             | long |
| vpcid    | CLB VIP의 VPC ID 공중망 CLB 인스턴스의 vip_vpcid는 -1입니다.                                    | long |
| time     | 액세스 시간 및 시간대(예시: '01/Jul/2019:11:11:00 +0800', 여기서 '+0800'은 UTC+8, 즉 베이징 시간을 나타냄). | text |
| vip      | CLB VIP.                                                                           | text |
| rsip     | RS IP.                                                                             | text |
| status   | 상태 확인 상태입니다.<br>true: 정상<br>false: 비정상                                             | text |
| domain   | 확인할 도메인 이름입니다. 레이어 4 리스너가 사용되는 경우 이 매개변수는 비어 있습니다.                                 | text |
| url      | 확인할 URL입니다. 레이어 4 리스너가 사용되는 경우 이 매개변수는 비어 있습니다.                                    | text |

## 관련 문서

[Getting Started in Five Minutes](#)

# 모니터링 및 알람

## 모니터링 데이터 가져오기

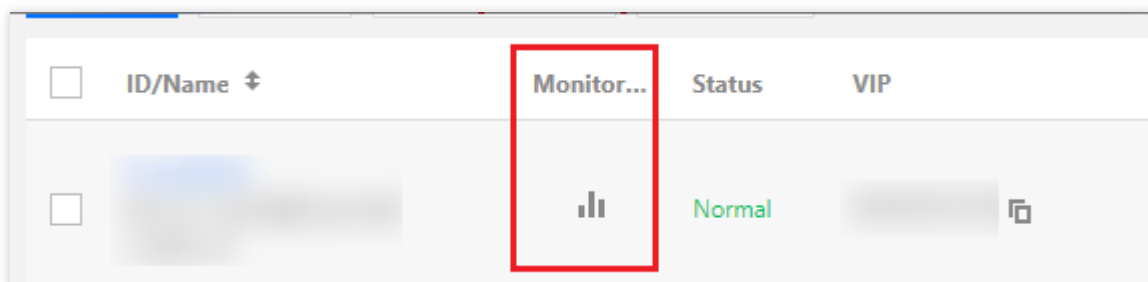
최종 업데이트 날짜: : 2024-01-04 20:02:32

Tencent Cloud Monitor는 CLB 인스턴스 및 리얼 서버에 대한 데이터를 수집 및 표시하여 CLB 통계를 얻고 시스템이 정상적으로 실행되고 있는지 확인하고 알람을 생성하도록 돕습니다. Tencent Cloud Monitor에 대한 자세한 내용은 [Cloud Monitor](#) 문서를 참고하십시오.

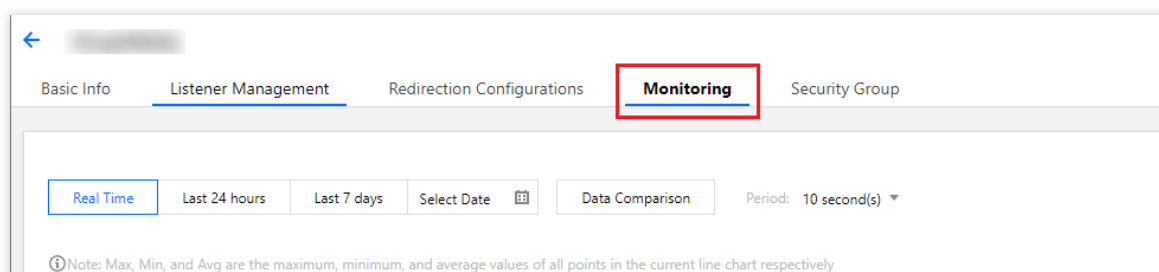
Tencent Cloud는 기본적으로 모든 사용자에게 Tencent Cloud Monitor 기능을 제공하며 수동 활성화가 필요하지 않습니다. Tencent Cloud Monitor를 사용하여 CLB 인스턴스의 모니터링 데이터를 수집하고 다음 방식을 사용하여 데이터를 볼 수 있습니다.

## CLB 콘솔 방식

1. [CLB 콘솔](#)에 로그인하고 CLB 인스턴스 ID 옆에 모니터링 아이콘을 클릭 한 다음 플로팅 창에서 인스턴스의 성능 데이터를 찾아보십시오.



2. CLB 인스턴스의 ID/이름을 클릭하여 세부 정보 페이지로 이동합니다. [모니터링](#)을 클릭하여 모니터링 데이터를 봅니다.



## Tencent Cloud Monitor 콘솔

CLB 모니터링 데이터를 보려면 [Tencent Cloud Monitor 콘솔](#)에 로그인합니다. 왼쪽 사이드 바에서 **CLB**를 클릭 한 다음 CLB 인스턴스의 ID/이름을 클릭하여 모니터링 세부 정보 페이지로 이동하면 CLB 인스턴스의 모니터링 데이터를 보고 드롭다운 목록을 펼쳐 리스너 및 리얼 서버 모니터링 정보를 볼 수 있습니다.

## API 방식

GetMonitorData API를 사용하여 모든 제품의 모니터링 데이터를 가져옵니다. 자세한 내용은 [GetMonitorData](#), [공중망 CLB 모니터링 메트릭](#), [사설망 CLB](#)를 참고하십시오.

# 모니터링 지표

최종 업데이트 날짜: : 2024-01-04 20:02:51

클라우드 모니터는 실행 중인 CLB 인스턴스에서 원시 데이터를 수집하고 직관적인 그래프에 데이터 항목을 표시합니다. 통계 데이터는 기본적으로 한 달 동안 유지됩니다. 해당 월의 애플리케이션 서비스 상태에 대한 정보를 유지하기 위해 인스턴스 운영을 관찰할 수 있습니다.

[클라우드 모니터 콘솔](#)로 이동하여 CLB 모니터링 데이터를 볼 수 있습니다. 클라우드 제품 모니터링 > [CLB](#) 선택 후 CLB 인스턴스 ID를 클릭하여 모니터링 세부 정보 페이지로 이동합니다. CLB 인스턴스의 모니터링 데이터를 보고, 펼쳐 리스너 및 리얼 서버 모니터링 정보를 볼 수 있습니다.

## 설명 :

CLB 고급 메트릭에는 인스턴스 레벨에서 최대 연결 사용률(ConcurConnVipRatio) 및 새 연결 사용률(NewConnVipRatio)이 포함됩니다.

현재 LCU 지원 CLB 인스턴스의 ConcurConnVipRatio 및 NewConnVipRatio 메트릭만 활성화되면 데이터를 리포트하는 반면 공유 CLB 인스턴스는 당분간 데이터를 보고하지 않습니다.

## CLB 인스턴스 레벨

| 매개변수               | 메트릭 이름              | 설명                                                   | 단위 | 통계 기간 (초)   |
|--------------------|---------------------|------------------------------------------------------|----|-------------|
| ClientConnum       | 클라이언트에서 LB로의 활성 연결  | 통계 세분성 내에서 주어진 시간에 클라이언트에서 로드 밸런서 또는 리스너로의 활성 연결 수.  | 개  | 10, 60, 300 |
| ClientInactiveConn | 클라이언트에서 LB로의 비활성 연결 | 통계 세분성 내에서 주어진 시간에 클라이언트에서 로드 밸런서 또는 리스너로의 비활성 연결 수. | 개  | 10, 60, 300 |



|                    |                       |                                                     |     |             |
|--------------------|-----------------------|-----------------------------------------------------|-----|-------------|
| ClientConcurConn   | 클라이언트에서 LB로의 동시 접속    | 통계 세분성 내에서 주어진 시간에 클라이언트에서 로드 밸런서 또는 리스너로의 동시 접속 수. | 개   | 10, 60, 300 |
| ClientNewConn      | 클라이언트에서 LB로의 새로운 연결   | 통계 세분성 내에서 클라이언트에서 로드 밸런서 또는 리스너의 초당 새로운 연결 수.      | 개/초 | 10, 60, 300 |
| ClientInpkg        | 클라이언트에서 LB로의 인바운드 패킷  | 통계 세분성 내에서 클라이언트에서 로드 밸런서로 전송된 초당 데이터 패킷 수.         | 개/초 | 10, 60, 300 |
| ClientOutpkg       | 클라이언트에서 LB로의 아웃바운드 패킷 | 통계 세분성 내에서 로드 밸런서에서 클라이언트로 전송된 초당 데이터 패킷 수.         | 개/초 | 10, 60, 300 |
| ClientAccIntraffic | 클라이언트에서 LB로의 인바운드 트래픽 | 통계 세분성 내에서 클라이언트에서 로드 밸런서로 유입되는 트래픽.                | MB  | 10, 60, 300 |
|                    |                       |                                                     |     |             |

|                     |                        |                                           |      |             |
|---------------------|------------------------|-------------------------------------------|------|-------------|
| ClientAccOuttraffic | 클라이언트에서 LB로의 아웃바운드 트래픽 | 통계 세분성 내에서 로드 밸런서에서 클라이언트로 유출되는 트래픽.      | MB   | 10, 60, 300 |
| ClientOuttraffic    | 클라이언트에서 LB로의 아웃바운드 대역폭 | 통계적 세분성 내에서 로드 밸런서에서 클라이언트로 유출에 사용하는 대역폭. | Mbps | 10, 60, 300 |
| ClientIntraffic     | 클라이언트에서 LB로의 인바운드 대역폭  | 통계 세분성 내에서 클라이언트에서 로드 밸런서로 유입에 사용하는 대역폭.  | Mbps | 10, 60, 300 |
| OutTraffic          | LB에서 리얼 서버의 아웃바운드 대역폭  | 통계 세분성 내에서 리얼 서버에서 로드 밸런서로 유출에 사용하는 대역폭.  | Mbps | 60, 300     |
| InTraffic           | LB에서 리얼 서버의 인바운드       | 통계 세분성 내에서 로드 밸런서에서 리얼 서버로 유입에 사용하는 대역폭.  | Mbps | 60, 300     |

|                | 드 대역폭                  |                                                                                                                                                                          |     |                   |
|----------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-------------------|
| AccOuttraffic  | LB에서 리얼 서버로의 아웃바운드 트래픽 | 통계 세분성 내에서 로드 밸런서에서 리얼 서버로 유입되는 트래픽. 이 메트릭은 공중망 CLB 인스턴스에서만 지원됩니다.                                                                                                       | MB  | 10, 60, 300, 3600 |
| DropTotalConns | 드롭된 연결 수               | 통계 세분성 내에서 LB 또는 리스너에 의해 드롭된 연결 수. 이 메트릭은 IP별 청구 계정에서만 지원되며 CVM별 청구 계정에서는 지원되지 않습니다. 계정 유형에 대한 자세한 내용은 <a href="#">Checking Account Type</a> 을 참고하십시오.                   | 개   | 10, 60, 300       |
| InDropBits     | 드롭된 인바운드 대역폭           | 통계 세분성 내에서 공중망을 통해 로드 밸런서에 액세스할 때 클라이언트에 의해 드롭된 대역폭. 이 메트릭은 IP별 청구 계정에서만 지원되며 CVM별 청구 계정에서는 지원되지 않습니다. 계정 유형에 대한 자세한 내용은 <a href="#">Checking Account Type</a> 을 참고하십시오. | 바이트 | 10, 60, 300       |
| OutDropBits    | 드롭된 아웃바운드 대역폭          | 통계 세분성 내에서 공중망에 액세스할 때 로드 밸런서에 의해 드롭된 대역폭. 이 메트릭은 IP별 청구 계정에서만 지원되며 CVM별 청구 계정에서는 지원되지 않습니다. 계정 유형에 대한 자세한 내용은 <a href="#">Checking Account Type</a> 을 참고하십시오.           | 바이트 | 10, 60, 300       |
| InDropPkts     | 드롭된 인바운드 패킷            | 통계 세분성 내에서 공중망을 통해 로드 밸런서에 액세스할 때 클라이언트에 의해 드롭된 패킷. 이 메트릭은 IP별 청구 계정에서만 지원되며 CVM별 청구 계정에서는 지원되지 않습니다. 계정 유형에 대한 자세한 내용은 <a href="#">Checking Account Type</a> 을 참고하십시오.  | 개/초 | 10, 60, 300       |
| OutDropPkts    | 드롭된 아웃바운드 패킷           | 통계 세분성 내에서 공중망에 액세스할 때 로드 밸런서에 의해 드롭된 패킷. 이 메트릭은 IP별 청구 계정에서만 지원되며 CVM별 청구 계정에서는 지원되지 않습니다. 계정 유형에 대한 자세한 내용은 <a href="#">Checking Account Type</a> 을 참고하십시오.            | 개/초 | 10, 60, 300       |
| DropQps        | 드롭된 QPS                | 통계 세분성 내에서 로드 밸런서 또는 리스너에 의해 드롭된 요청. 이 메트릭은 레이어 7 리스너 전용입니다. IP별 청구 계정에서만 지원되며 CVM별 청구 계정에서는 지원되지                                                                        | 개   | 60, 300           |

|                      |               |                                                                                                                                                                                                                                        |     |             |
|----------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-------------|
|                      |               | 지 않습니다. 계정 유형에 대한 자세한 내용은 <a href="#">Checking Account Type</a> 을 참고하십시오.                                                                                                                                                              |     |             |
| IntraTrafficVipRatio | 인바운드 대역폭 사용률  | 클라이언트가 통계 단위 내에서 공중망을 통해 로드 밸런서에 액세스하는 데 사용하는 대역폭의 사용률입니다. 이 메트릭은 IP별 청구 계정에서만 지원되며 CVM별 청구 계정에서는 지원되지 않습니다. 계정 유형에 대한 자세한 내용은 <a href="#">Checking Account Type</a> 을 참고하십시오. 이 메트릭은 현재 베타 버전입니다. 사용해 보려면 <a href="#">티켓 제출</a> 하십시오. | %   | 10, 60, 300 |
| OutTrafficVipRatio   | 아웃바운드 대역폭 사용률 | 로드 밸런서가 통계 단위 내에서 공중망에 액세스하는 데 사용하는 대역폭의 사용률입니다. 이 메트릭은 IP별 청구 계정에서만 지원되며 CVM별 청구 계정에서는 지원되지 않습니다. 계정 유형에 대한 자세한 내용은 <a href="#">Checking Account Type</a> 을 참고하십시오. 이 메트릭은 현재 베타 버전입니다. 사용해 보려면 <a href="#">티켓 제출</a> 하십시오.           | %   | 10, 60, 300 |
| ReqAvg               | 평균 요청 시간      | 통계 세분성 내에서 로드 밸런서의 평균 요청 시간. 이 메트릭은 레이어 7 리스너 전용입니다.                                                                                                                                                                                   | 밀리초 | 60, 300     |
| ReqMax               | 최대 요청 시간      | 통계 세분성 내에서 로드 밸런서의 최대 요청 시간. 이 메트릭은 레이어 7 리스너 전용입니다.                                                                                                                                                                                   | 밀리초 | 60, 300     |
| RspAvg               | 평균 응답 시간      | 통계 세분성 내에서 로드 밸런서의 평균 응답 시간. 이 메트릭은 레이어 7 리스너 전용입니다.                                                                                                                                                                                   | 밀리초 | 60, 300     |
| RspMax               | 최대 응답 시간      | 통계 세분성 내에서 로드 밸런서의 최대 응답 시간. 이 메트릭은 레이어 7 리스너 전용입니다.                                                                                                                                                                                   | 밀리초 | 60, 300     |
| RspTimeout           | 응답 시간 초과 횟수   | 통계 세분성 내에서 로드 밸런서 응답 시간 초과 횟수. 이 메트릭은 레이어 7 리스너 전용입니다.                                                                                                                                                                                 | 개/분 | 60, 300     |
| SuccReq              | 분당 성공한 요청 수   | 통계 세분성 내에서 로드 밸런서의 분당 성공한 요청 수. 이 메트릭은 레이어 7 리스너 전용입니다.                                                                                                                                                                                | 개/분 | 60, 300     |
| TotalReq             | 초당 요청 수       | 통계 세분성 내에서 초당 로드 밸런서의 요청 수. 이 메트릭은 레이어 7 리스너 전용입니다.                                                                                                                                                                                    | 개   | 60, 300     |

|            |                                         |                                                                                 |     |            |
|------------|-----------------------------------------|---------------------------------------------------------------------------------|-----|------------|
| ClbHttp3xx | CLB<br>에서<br>반환<br>된<br>3xx<br>상태<br>코드 | 통계 세분성 내에서 CLB에서 반환된 3xx 상태 코드 수 (CLB와 리얼 서버 반환 코드의 합계).이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60,<br>300 |
| ClbHttp4xx | CLB<br>에서<br>반환<br>된<br>4xx<br>상태<br>코드 | 통계 세분성 내에서 CLB에서 반환된 4xx 상태 코드 수 (CLB와 리얼 서버 반환 코드의 합계).이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60,<br>300 |
| ClbHttp5xx | CLB<br>에서<br>반환<br>된<br>5xx<br>상태<br>코드 | 통계 세분성 내에서 CLB에서 반환된 5xx 상태 코드 수 (CLB와 리얼 서버 반환 코드의 합계).이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60,<br>300 |
| ClbHttp404 | CLB<br>에서<br>반환<br>된<br>404<br>상태<br>코드 | 통계 세분성 내에서 CLB에서 반환된 404 상태 코드 수 (CLB와 리얼 서버 반환 코드의 합계).이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60,<br>300 |
| ClbHttp499 | CLB<br>에서<br>반환<br>된<br>499<br>상태<br>코드 | 통계 세분성 내에서 CLB에서 반환된 499 상태 코드 수 (CLB와 리얼 서버 반환 코드의 합계).이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60,<br>300 |
| ClbHttp502 | CLB<br>에서<br>반환<br>된<br>502             | 통계 세분성 내에서 CLB에서 반환된 502 상태 코드 수 (CLB와 리얼 서버 반환 코드의 합계).이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60,<br>300 |

|            | 상태 코드               |                                                                                 |     |        |
|------------|---------------------|---------------------------------------------------------------------------------|-----|--------|
| ClbHttp503 | CLB에서 반환된 503 상태 코드 | 통계 세분성 내에서 CLB에서 반환된 503 상태 코드 수 (CLB와 리얼 서버 반환 코드의 합계).이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60,300 |
| ClbHttp504 | CLB에서 반환된 504 상태 코드 | 통계 세분성 내에서 CLB에서 반환된 504 상태 코드 수 (CLB와 리얼 서버 반환 코드의 합계).이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60,300 |
| Http2xx    | 2xx 상태 코드           | 통계 세분성 내에서 리얼 서버에서 반환된 2xx 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다.                     | 개/분 | 60,300 |
| Http3xx    | 3xx 상태 코드           | 통계 세분성 내에서 리얼 서버에서 반환된 3xx 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다.                     | 개/분 | 60,300 |
| Http4xx    | 4xx 상태 코드           | 통계 세분성 내에서 리얼 서버에서 반환된 4xx 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다.                     | 개/분 | 60,300 |
| Http5xx    | 5xx 상태 코드           | 통계 세분성 내에서 리얼 서버에서 반환된 5xx 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다.                     | 개/분 | 60,300 |
| Http404    | 404 상태 코드           | 통계 세분성 내에서 리얼 서버에서 반환된 404 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다.                     | 개/분 | 60,300 |
| Http499    | 499 상태 코드           | 통계 세분성 내에서 리얼 서버에서 반환된 499 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다.                     | 개/분 | 60,300 |
| Http502    | 502 상태 코드           | 통계 세분성 내에서 리얼 서버에서 반환된 502 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다.                     | 개/분 | 60,300 |
|            |                     |                                                                                 |     |        |

|                 |                                       |                                                                                                                                                      |     |            |
|-----------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|-----|------------|
| Http503         | 503<br>상태<br>코드                       | 통계 세분성 내에서 리얼 서버에서 반환된 503 상태 코드의 수. 이 메트릭은 레이어 7 리스너 전용입니다.                                                                                         | 개/분 | 60,<br>300 |
| Http504         | 504<br>상태<br>코드                       | 통계 세분성 내에서 리얼 서버에서 반환된 504 상태 코드의 수. 이 메트릭은 레이어 7 리스너 전용입니다.                                                                                         | 개/분 | 60,<br>300 |
| OverloadCurConn | SNAT<br>동시<br>접속<br>수                 | 통계 단위 내에서 분당 로드 밸런서의 SNAT IP 동시 접속 수입니다. 이 메트릭은 현재 베타 버전입니다. 사용해 보려면 <a href="#">티켓 제출</a> 하십시오.                                                     | 개/분 | 60         |
| ConnRatio       | SNAT<br>포트<br>사용<br>률                 | 통계 단위 내에서 로드 밸런서의 SNAT IP의 포트 사용률입니다. 포트 사용률 = SNAT 동시 접속 수 / (SNAT IP 수 × 55000 × 리얼 서버 수). 이 메트릭은 현재 베타 버전입니다. 사용해 보려면 <a href="#">티켓 제출</a> 하십시오. | %   | 60         |
| SnatFail        | SNAT<br>연결<br>실패<br>수                 | 통계 단위 내에서 로드 밸런서의 SNAT IP와 리얼 서버 간의 분당 실패한 연결 수입니다. 이 메트릭은 현재 베타 버전입니다. 사용해 보려면 <a href="#">티켓 제출</a> 하십시오.                                          | 개/분 | 60         |
| UnhealthRsCount | 비정<br>상<br>상<br>태<br>확<br>인<br>횟<br>수 | 통계 세분성 내에서 로드 밸런서의 비정상 상태 확인 횟수.                                                                                                                     | 개   | 60,<br>300 |

## 레이어 4 리스너(TCP/UDP) 레벨

레이어 4 리스너를 사용하면 세 가지 레벨에서 모니터링 메트릭을 볼 수 있습니다.

리스너 레벨.

리얼 서버 레벨.

리얼 서버의 포트 레벨.

| 매개변수          | 메트릭 이름               | 설명                                                  | 단위 | 통계<br>기간<br>(초) |
|---------------|----------------------|-----------------------------------------------------|----|-----------------|
| ClientConnnum | 클라이언트에서<br>LB로의 활성 연 | 통계 세분성 내에서 주어진 시간에 클라이언트에서 로드 밸런서 또는 리스너로의 활성 연결 수. | 개  | 10,<br>60,      |

|                     |                         |                                                       |      |             |
|---------------------|-------------------------|-------------------------------------------------------|------|-------------|
|                     | 결                       |                                                       |      | 300         |
| ClientNewConn       | 클라이언트에서 LB 로의 새로운 연결    | 통계 세분성 내에서 클라이언트에서 로드 밸런서 또는 리스너의 초당 새로운 연결 수.        | 개/초  | 10, 60, 300 |
| ClientInpkg         | 클라이언트에서 LB로의 인바운드 패킷    | 통계 세분성 내에서 클라이언트에서 로드 밸런서로 전송된 초당 데이터 패킷 수.           | 개/초  | 10, 60, 300 |
| ClientOutpkg        | 클라이언트에서 LB 로의 아웃바운드 패킷  | 통계 세분성 내에서 로드 밸런서에서 클라이언트로 전송된 초당 데이터 패킷 수.           | 개/초  | 10, 60, 300 |
| ClientAccIntraffic  | 클라이언트에서 LB로의 인바운드 트래픽   | 통계 세분성 내에서 클라이언트에서 로드 밸런서로 유입되는 트래픽.                  | MB   | 10, 60, 300 |
| ClientAccOuttraffic | 클라이언트에서 LB로의 아웃바운드 트래픽  | 통계 세분성 내에서 로드 밸런서에서 클라이언트로 유출되는 트래픽.                  | MB   | 10, 60, 300 |
| ClientOuttraffic    | 클라이언트에서 LB 로의 아웃바운드 대역폭 | 통계적 세분성 내에서 로드 밸런서에서 클라이언트로 유출에 사용하는 대역폭.             | Mbps | 10, 60, 300 |
| ClientIntraffic     | 클라이언트에서 LB로의 인바운드 대역폭   | 통계 세분성 내에서 클라이언트에서 로드 밸런서로 유입되는 트래픽.                  | Mbps | 10, 60, 300 |
| OutTraffic          | LB에서 리얼 서버로의 아웃바운드 대역폭  | 통계 세분성 내에서 리얼 서버에서 로드 밸런서로 유출에 사용하는 대역폭.              | Mbps | 60, 300     |
| InTraffic           | LB에서 리얼 서버로의 인바운드 대역폭   | 통계 세분성 내에서 로드 밸런서에서 리얼 서버로 유입에 사용하는 대역폭.              | Mbps | 60, 300     |
| OutPkg              | LB에서 리얼 서버로의 아웃바운드 패킷   | 통계 세분성 내에서 리얼 서버에서 로드 밸런서로 보낸 초당 패킷 수.                | 개/초  | 60, 300     |
| InPkg               | LB에서 리얼 서버로의 인바운드 패킷    | 통계 세분성 내에서 로드 밸런서에서 리얼 서버로 보낸 초당 패킷 수.                | 개/초  | 60, 300     |
| AccOuttraffic       | LB에서 리얼 서버로의 아웃바        | 통계 세분성 내에서 로드 밸런서에서 리얼 서버로 유입되는 트래픽. 이 메트릭은 공중망 CLB 인 | MB   | 10, 60,     |



|                 |                   |                                     |     |              |
|-----------------|-------------------|-------------------------------------|-----|--------------|
|                 | 운드 트래픽            | 스턴스에서만 지원됩니다.                       |     | 300,<br>3600 |
| ConNum          | LB에서 리얼 서버로의 연결   | 통계 세분성 내에서 로드 밸런서에서 리얼 서버로의 연결 수.   | 개   | 60,<br>300   |
| NewConn         | LB에서 리얼 서버로의 새 연결 | 통계 세분성 내에서 로드 밸런서에서 리얼 서버로의 새 연결 수. | 개/분 | 60,<br>300   |
| UnhealthRsCount | 비정상 상태 확인 횟수      | 통계 세분성 내에서 로드 밸런서의 비정상 상태 확인 횟수.    | 개   | 60,<br>300   |

## 레이어 7 리스너(HTTP/HTTPS) 레벨

레이어 7 리스너를 사용하면 3가지 레벨에서 모니터링 메트릭을 볼 수 있습니다.

리스너 레벨.

리얼 서버 레벨.

리얼 서버의 포트 레벨.

| 매개변수               | 메트릭 이름                 | 설명                                                  | 단위  | 통계<br>기간<br>(초)   |
|--------------------|------------------------|-----------------------------------------------------|-----|-------------------|
| ClientConnum       | 클라이언트에서 LB로의 활성 연결     | 통계 세분성 내에서 주어진 시간에 클라이언트에서 로드 밸런서 또는 리스너로의 활성 연결 수. | 개   | 10,<br>60,<br>300 |
| ClientNewConn      | 클라이언트에서 LB 로의 새로운 연결   | 통계 세분성 내에서 클라이언트에서 로드 밸런서 또는 리스너의 초당 새로운 연결 수.      | 개/초 | 10,<br>60,<br>300 |
| ClientInpkg        | 클라이언트에서 LB로의 인바운드 패킷   | 통계 세분성 내에서 클라이언트에서 로드 밸런서로 전송된 초당 데이터 패킷 수.         | 개/초 | 10,<br>60,<br>300 |
| ClientOutpkg       | 클라이언트에서 LB 로의 아웃바운드 패킷 | 통계 세분성 내에서 로드 밸런서에서 클라이언트로 전송된 초당 데이터 패킷 수.         | 개/초 | 10,<br>60,<br>300 |
| ClientAccIntraffic | 클라이언트에서 LB로의 인바운드 트래픽  | 통계 세분성 내에서 클라이언트에서 로드 밸런서로 유입되는 트래픽.                | MB  | 10,<br>60,<br>300 |

|                     |                        |                                                                    |      |                   |
|---------------------|------------------------|--------------------------------------------------------------------|------|-------------------|
| ClientAccOuttraffic | 클라이언트에서 LB로의 아웃바운드 트래픽 | 통계 세분성 내에서 로드 밸런서에서 클라이언트로 유출되는 트래픽.                               | MB   | 10, 60, 300       |
| ClientOuttraffic    | 클라이언트에서 LB로의 아웃바운드 대역폭 | 통계적 세분성 내에서 로드 밸런서에서 클라이언트로 유출에 사용하는 대역폭.                          | Mbps | 10, 60, 300       |
| ClientIntraffic     | 클라이언트에서 LB로의 인바운드 대역폭  | 통계 세분성 내에서 클라이언트에서 로드 밸런서로 유입되는 트래픽.                               | Mbps | 10, 60, 300       |
| OutTraffic          | LB에서 리얼 서버로의 아웃바운드 대역폭 | 통계 세분성 내에서 리얼 서버에서 로드 밸런서로 유출에 사용하는 대역폭.                           | Mbps | 60, 300           |
| InTraffic           | LB에서 리얼 서버로의 인바운드 대역폭  | 통계 세분성 내에서 로드 밸런서에서 리얼 서버로 유입에 사용하는 대역폭.                           | Mbps | 60, 300           |
| OutPkg              | LB에서 리얼 서버로의 아웃바운드 패킷  | 통계 세분성 내에서 리얼 서버에서 로드 밸런서로 보낸 초당 패킷 수.                             | 개/초  | 60, 300           |
| InPkg               | LB에서 리얼 서버로의 인바운드 패킷   | 통계 세분성 내에서 로드 밸런서에서 리얼 서버로 보낸 초당 패킷 수.                             | 개/초  | 60, 300           |
| AccOuttraffic       | LB에서 리얼 서버로의 아웃바운드 트래픽 | 통계 세분성 내에서 로드 밸런서에서 리얼 서버로 유입되는 트래픽. 이 메트릭은 공중망 CLB 인스턴스에서만 지원됩니다. | MB   | 10, 60, 300, 3600 |
| ConNum              | LB에서 리얼 서버로의 연결        | 통계 세분성 내에서 로드 밸런서에서 리얼 서버로의 연결 수.                                  | 개    | 60, 300           |
| NewConn             | LB에서 리얼 서버로의 새 연결      | 통계 세분성 내에서 로드 밸런서에서 리얼 서버로의 새 연결 수.                                | 개/분  | 60, 300           |
| ReqAvg              | 평균 요청 시간               | 통계 세분성 내에서 로드 밸런서의 평균 요청 시간. 이 메트릭은 레이어 7 리스너 전용입니다.               | 밀리초  | 60, 300           |
| ReqMax              | 최대 요청 시간               | 통계 세분성 내에서 로드 밸런서의 최대 요청 시간. 이 메트릭은 레이어 7 리스너 전용입니다.               | 밀리초  | 60, 300           |

|            |                     |                                                                                 |     |         |
|------------|---------------------|---------------------------------------------------------------------------------|-----|---------|
| RspAvg     | 평균 응답 시간            | 통계 세분성 내에서 로드 밸런서의 평균 응답 시간. 이 메트릭은 레이어 7 리스너 전용입니다.                            | 밀리초 | 60, 300 |
| RspMax     | 최대 응답 시간            | 통계 세분성 내에서 로드 밸런서의 최대 응답 시간. 이 메트릭은 레이어 7 리스너 전용입니다.                            | 밀리초 | 60, 300 |
| RspTimeout | 응답 시간 초과 횟수         | 통계 세분성 내에서 로드 밸런서 응답 시간 초과 횟수. 이 메트릭은 레이어 7 리스너 전용입니다.                          | 개/분 | 60, 300 |
| SuccReq    | 분당 성공한 요청 수         | 통계 세분성 내에서 로드 밸런서의 분당 성공한 요청 수. 이 메트릭은 레이어 7 리스너 전용입니다.                         | 개/분 | 60, 300 |
| TotalReq   | 초당 요청 수             | 통계 세분성 내에서 초당 로드 밸런서의 요청 수. 이 메트릭은 레이어 7 리스너 전용입니다.                             | 개   | 60, 300 |
| ClbHttp3xx | CLB에서 반환된 3xx 상태 코드 | 통계 세분성 내에서 CLB에서 반환된 3xx 상태 코드 수(CLB와 리얼 서버 반환 코드의 합계). 이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| ClbHttp4xx | CLB에서 반환된 4xx 상태 코드 | 통계 세분성 내에서 CLB에서 반환된 4xx 상태 코드 수(CLB와 리얼 서버 반환 코드의 합계). 이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| ClbHttp5xx | CLB에서 반환된 5xx 상태 코드 | 통계 세분성 내에서 CLB에서 반환된 5xx 상태 코드 수(CLB와 리얼 서버 반환 코드의 합계). 이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| ClbHttp404 | CLB에서 반환된 404 상태 코드 | 통계 세분성 내에서 CLB에서 반환된 404 상태 코드 수(CLB와 리얼 서버 반환 코드의 합계). 이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| ClbHttp499 | CLB에서 반환된 499 상태 코드 | 통계 세분성 내에서 CLB에서 반환된 499 상태 코드 수(CLB와 리얼 서버 반환 코드의 합계). 이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| ClbHttp502 | CLB에서 반환된 502 상태 코드 | 통계 세분성 내에서 CLB에서 반환된 502 상태 코드 수(CLB와 리얼 서버 반환 코드의 합계). 이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| ClbHttp503 | CLB에서 반환된 503 상태 코드 | 통계 세분성 내에서 CLB에서 반환된 503 상태 코드 수(CLB와 리얼 서버 반환 코드의 합계). 이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| ClbHttp504 | CLB에서 반환된 504 상태 코드 | 통계 세분성 내에서 CLB에서 반환된 504 상태 코드 수(CLB와 리얼 서버 반환 코드의 합계). 이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| Http2xx    | 2xx 상태 코드           | 통계 세분성 내에서 리얼 서버에서 반환된 2xx 상                                                    | 개/분 | 60,     |

|                 |              |                                                             |     |         |
|-----------------|--------------|-------------------------------------------------------------|-----|---------|
|                 |              | 태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다.                             |     | 300     |
| Http3xx         | 3xx 상태 코드    | 통계 세분성 내에서 리얼 서버에서 반환된 3xx 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| Http4xx         | 4xx 상태 코드    | 통계 세분성 내에서 리얼 서버에서 반환된 4xx 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| Http5xx         | 5xx 상태 코드    | 통계 세분성 내에서 리얼 서버에서 반환된 5xx 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| Http404         | 404 상태 코드    | 통계 세분성 내에서 리얼 서버에서 반환된 404 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| Http499         | 499 상태 코드    | 통계 세분성 내에서 리얼 서버에서 반환된 499 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| Http502         | 502 상태 코드    | 통계 세분성 내에서 리얼 서버에서 반환된 502 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| Http503         | 503 상태 코드    | 통계 세분성 내에서 리얼 서버에서 반환된 503 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| Http504         | 504 상태 코드    | 통계 세분성 내에서 리얼 서버에서 반환된 504 상태 코드의 수.이 메트릭은 레이어 7 리스너 전용입니다. | 개/분 | 60, 300 |
| UnhealthRsCount | 비정상 상태 확인 횟수 | 통계 세분성 내에서 로드 밸런서의 비정상 상태 확인 횟수.                            | 개   | 60, 300 |

### 설명 :

리스너 아래에 있는 리얼 서버의 모니터링 데이터를 보고 싶다면 [CLB 콘솔](#)에 로그인하여 CLB 인스턴스 ID 옆에 있는 모니터링 바 아이콘을 클릭한 후 플로팅 창에서 각 인스턴스의 성능 데이터를 찾아보십시오.

## 관련 문서

Public Network CLB

# 알람 정책 구성

최종 업데이트 날짜: : 2024-01-04 20:06:13

본문은 알람 정책을 생성하는 방법을 설명합니다.

## 응용 시나리오

클라우드 모니터에서 지원하는 모니터 유형의 성능 소비 메트릭에 대한 임계값 알람을 설정할 수 있습니다. Tencent Cloud 서비스 인스턴스 또는 기본 플랫폼 인프라의 서비스 상태에 대한 이벤트 알람을 설정할 수도 있습니다. 이렇게 하면 예외가 발생했을 때 즉시 알람을 받게 되어 적절한 조치를 취할 수 있습니다. 알람 정책은 이름, 정책 유형, 알람 트리거 조건, 알람 객체 및 알람 통지 템플릿의 5가지 필수 매개변수로 구성됩니다. 아래 가이드에 따라 알람 정책을 생성할 수 있습니다.

## 기본 개념

| 용어        | 정의                                                                                                              |
|-----------|-----------------------------------------------------------------------------------------------------------------|
| 알람 정책     | 알람 이름, 알람 정책 유형, 알람 발생 조건, 알람 객체, 알람 템플릿으로 구성                                                                   |
| 알람 정책 유형  | 알람 정책 유형은 정책 범주를 식별하고 특정 Tencent Cloud 제품에 해당하며, 예를 들어 CVM 정책을 선택하면 CPU 사용률, 디스크 사용률 등에 대한 메트릭 알람을 사용자 지정할 수 있음 |
| 알람 트리거 조건 | 알람 트리거 조건은 메트릭, 비교, 임계값, 통계 기간 및 N개의 연속 모니터링 데이터 포인트로 구성된 semantics 조건                                          |
| 모니터링 유형   | 유형에는 Tencent Cloud 서비스 모니터링, 애플리케이션 성능 모니터링, 프런트엔드 성능 모니터링 및 클라우드 자동화 테스트 포함                                    |
| 알림 템플릿    | 알림 템플릿은 여러 정책에 빠르게 재사용할 수 있으므로 다양한 사용 사례에서 경보 수신에 적합하며, 자세한 내용은 <a href="#">알림 템플릿 생성</a> 을 참고하십시오              |

## 작업 단계

1. [Tencent Cloud Observability Platform](#)에 로그인합니다.

2. **알람 설정 > 알람 정책**을 클릭하여 알람 정책 설정 페이지로 들어갑니다.

3. **추가**를 클릭하고 아래와 같이 새 알람 정책을 설정합니다.

| 유형 설정 | 설정 항목         | 설명                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 기본 정보 | 정책 이름         | 사용자 지정 정책 이름                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|       | 비고            | 사용자 지정 정책 비고                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|       | 모니터링 유형       | 유형에는 Tencent Cloud 서비스 모니터링, 애플리케이션 성능 모니터링, 프런트엔드 성능 모니터링 및 클라우드 자동화 테스트 포함                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|       | 정책 유형         | 모니터링할 클라우드 서비스 정책 유형 선택                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|       | 프로젝트          | 이 구성 항목의 두 가지 기능:<br>알람 정책을 관리합니다. 서브 프로젝트를 설정하면 알람 정책 리스트에서 해당 프로젝트의 알람 정책을 빠르게 필터링할 수 있습니다.<br>인스턴스를 관리합니다. 필요에 따라 프로젝트를 선택하면 알람 객체 중 해당 프로젝트의 인스턴스를 빠르게 선택할 수 있습니다. 비즈니스 유형에 따라 클라우드 서비스를 각 프로젝트에 할당할 수 있습니다. 프로젝트를 생성해야 할 경우 <a href="#">프로젝트 관리</a> 를 참고하여, 프로젝트 생성 후 각 클라우드 서비스 콘솔을 사용하여 프로젝트를 리소스에 할당할 수 있습니다. TencentDB for MySQL과 같은 일부 Tencent Cloud 서비스는 프로젝트 할당을 지원하지 않습니다. 이 경우 <a href="#">인스턴스에 프로젝트 지정</a> 을 참고하여 해당 인스턴스에 프로젝트를 할당할 수 있습니다. 프로젝트 권한이 없는 경우 <a href="#">CAM</a> 을 참고하여 권한을 얻으십시오.                                      |
| 알람 정책 | 알람 객체         | 인스턴스 ID를 선택하면 알람 정책이 선택한 인스턴스와 연결됩니다.<br>인스턴스 그룹을 선택하면 알람 정책이 선택한 인스턴스 그룹과 연결됩니다.<br>전체 객체를 선택하면 알람 정책을 현재 계정의 모든 인스턴스와 연결합니다 (권한 필요).                                                                                                                                                                                                                                                                                                                                                                                                                 |
|       | 수동 설정(메트릭 알람) | 알람 트리거 조건은 메트릭, 비교, 임계값, 측정 기간 및 N 모니터링 데이터 포인트로 구성된 <b>semantics</b> 조건입니다. 차트의 메트릭 변경 추세에 따라 알람 임계값을 설정할 수 있습니다. 예를 들어 메트릭이 CPU 사용률인 경우 비교는 >, 임계값은 80%, 측정 기간은 5분, 연속 모니터링 데이터 포인트는 2 데이터 포인트입니다. 그런 다음 CVM 인스턴스의 CPU 사용률에 대한 데이터는 5분마다 한 번씩 수집되며, CPU 사용률이 두 기간 연속으로 80%를 초과하면 알람이 트리거됩니다.<br><br>알람 빈도: 모든 알람 규칙에 반복 알람 정책을 설정할 수 있습니다. 이렇게 하면 알람이 트리거될 때 지정된 빈도로 알람이 반복적으로 전송됩니다.<br>빈도 옵션: 반복하지 않음, 5분마다 한 번, 10분마다 한 번, 기하급수적으로 증가하는 간격 및 기타 빈도 옵션.<br>기하급수적으로 증가하는 간격은 알람이 첫 번째, 두 번째, 네 번째, 여덟 번째... 등으로 트리거될 때 알람이 전송됨을 의미합니다. 즉, 반복되는 알람으로 |

|          |               |                                                                                                                                                                  |
|----------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          |               | <p>인한 방해 줄이기 위해 시간이 지남에 따라 알람 알람이 전송되는 빈도가 점점 줄어듭니다.</p> <p>반복 알람 기본 로직: 설정된 반복 알람 빈도에 따라 알람 생성 후 24시간 내에 알람이 반복 전송됩니다. 알람 생성 후 24시간이 지나면 알람이 하루에 한 번 전송됩니다.</p> |
|          | 수동 설정(이벤트 알람) | 클라우드 서비스 리소스나 인프라 서비스에 이상이 발생했을 경우 이벤트 알람을 생성해 즉시 조치를 취하도록 알릴 수 있습니다.                                                                                            |
|          | 템플릿 선택        | <p>템플릿 버튼을 클릭하여 드롭다운 리스트에서 구성된 템플릿을 선택합니다.</p> <p>자세한 구성은 <a href="#">트리거 조건 템플릿 구성</a>을 참고하십시오. 새로 생성된 템플릿이 표시되지 않으면 오른쪽의 <b>**새로고침**</b>을 클릭합니다.</p>           |
| 알람 전송 구성 | 알람 전송         | 시스템 사전 설정 알람 템플릿 및 사용자 정의 알람 템플릿을 선택할 수 있으며 알람 정책마다 최대 3개의 알람 템플릿을 바인딩할 수 있습니다. 상세 내용은 <a href="#">알람 템플릿 생성</a> 을 참고하십시오.                                       |
| 고급 설정    | 오토 스케일링       | 이 옵션을 활성화하고 성공적으로 구성한 후 알람 조건이 충족되면 조정을 위해 Auto Scaling 정책이 트리거됨                                                                                                 |

4. 상기 정보를 설정한 후 **저장**을 클릭합니다.

#### 설명 :

CVM 알람은 [모니터링 에이전트](#)가 CVM 인스턴스에 설치되고, 모니터링 메트릭 데이터를 리포트한 후에만 정상적으로 전송될 수 있습니다. 클라우드 모니터링 페이지에서 agent가 설치되지 않은 CVM 인스턴스를 확인하고 IP 주소 목록을 다운로드할 수 있습니다.



# 알람 지표 설명

최종 업데이트 날짜: : 2024-01-04 20:06:36

## 알람 설명

실행 상태가 특정 조건을 충족할 때 CLB 인스턴스가 대상 사용자 그룹에 알람 정보를 보내도록 지정된 인스턴스 지표에 대한 알람을 생성할 수 있습니다. 이렇게 하면 적시에 예외를 감지하고 적절한 조치를 취하여 시스템 안정성과 신뢰성을 유지할 수 있습니다. CLB 알람 정책에는 다음이 포함됩니다.

공중망 리스너

사설망 리스너

서버 포트(기타)

리스너 레벨

서버 포트 레벨

서버 포트(사설망 클래식 유형)

레이어 7 프로토콜 모니터링

## 공중망/사설망 리스너

현재 공중망 CLB와 사설망 CLB는 모두 다음 메트릭을 사용하여 리스너 수준에서 알람을 지원합니다.

| 메트릭           | 단위   | 설명                                                |
|---------------|------|---------------------------------------------------|
| Inbound 대역폭   | Mbps | 클라이언트가 통계 기간 내에 공중망을 통해 CLB에 액세스하는 데 사용하는 대역폭입니다. |
| Outbound 대역폭  | Mbps | 통계 기간 내에 공중망에 액세스하기 위해 CLB에서 사용하는 대역폭입니다.         |
| Inbound 패킷 수  | 개/s  | 통계 기간 내에 CLB가 초당 수신한 요청 데이터 패킷 수입니다.              |
| Outbound 패킷 수 | 개/s  | 통계 기간 내에서 초당 CLB에서 보낸 데이터 패킷 수입니다.                |

## 서버 포트(기타)

사설망 클래식 인스턴스를 제외한 모든 CLB 인스턴스는 다음 두 가지 레벨에서 알람을 지원합니다.

1. 리스너 레벨

리스너 아래에 바인딩된 모든 서버 포트의 예외 통계에 대해 리스너의 리얼 서버 예외 포트 수를 구성할 수 있으며, 구성된 임계값에 따라 알람이 트리거됩니다. 아래와 같이 선택된 리스너 아래에 있는 모든 리얼 서버의 예외 포트 수는 1분에 한 번씩 수집되며, 비정상 포트 수가 2회 연속으로 10개/초 이상인 경우 알람이 발생합니다. 알람은 하루에 한 번 트리거됩니다.

설명 :

리스너 레벨 알람을 활성화하려면 [티켓 제출](#)을 통해 신청할 수 있습니다.

알람 객체 구성:

Alarm Object

☐ All Objects

☒ Select some objects(2 selected)

☐ Select instance group [Create instance group](#)

Region: Guangzhou Project: DEFAULT PROJECT

| ID | VIP |
|----|-----|
| 1  | 1   |
| 1  | 1   |

트리거 조건 구성:

Trigger Condition

☐ Trigger Condition Template [Add Trigger Condition Template](#)

☒ Configure trigger conditions

☒ Indicator alarm

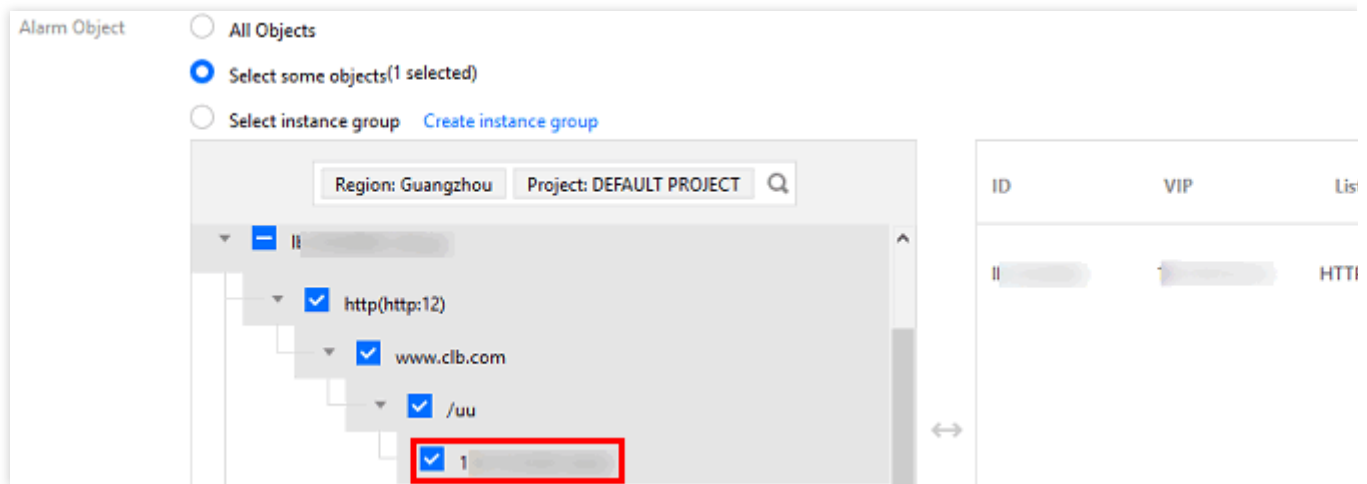
RS\_UNHEALTH\_NUM Measurement Period > 10 Continuous1

[Add](#)

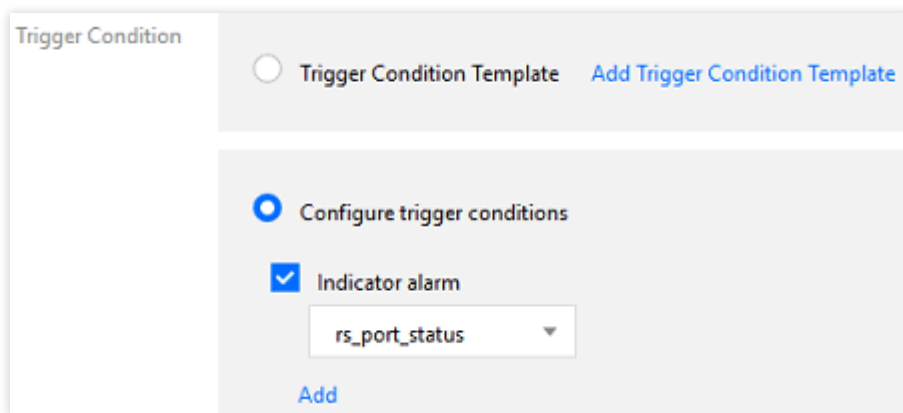
## 2. 서버 포트 레벨

리스너에 바인딩된 리얼 서버의 지정된 포트에 대해 예외 알람을 구성하여 포트 예외 발생 시 알람이 전송되도록 할 수 있습니다.

알람 객체 구성:



트리거 조건 구성:



주의 :

리얼 서버 포트 예외: CLB가 리얼 서버의 포트를 사용할 수 없음을 발견했음을 의미합니다. 경우에 따라 네트워크 지터도 포트 예외를 유발할 수 있습니다.

리스너 레벨의 통계에는 단일 알람 수렴에서 임계값 알람에 이르기까지 리스너 아래의 모든 리얼 서버의 포트 상태가 포함됩니다. 네트워크 지터의 영향을 방지하려면 리스너 레벨 알람을 사용하는 것이 좋습니다.

## 서버 포트(사설망 클래식 유형)

‘서버 포트(기타)-서버 포트 레벨’에 설명된 대로 사설망 클래식 CLB에 대한 서버 포트 예외 알람을 구성할 수 있습니다.

리스너에 바인딩된 리얼 서버의 지정된 포트에 대해 예외 알람을 구성하여 포트 예외 발생 시 알람이 전송되도록 할 수 있습니다.

## 레이어 7 프로토콜 모니터링

모든 레이어 7(HTTP/HTTPS) 리스너에 대해 고유한 모니터링 지표 알람 정책을 구성할 수 있습니다. 구체적인 메트릭은 다음과 같습니다.

| 메트릭                 | 단위   | 설명                                                |
|---------------------|------|---------------------------------------------------|
| Inbound 대역폭         | Mbps | 클라이언트가 통계 기간 내에 공중망을 통해 CLB에 액세스하는 데 사용하는 대역폭입니다. |
| Outbound 대역폭        | Mbps | 통계 기간 내에 공중망에 액세스하기 위해 CLB에서 사용하는 대역폭입니다.         |
| Inbound 패킷 수        | 개/s  | 통계 기간 내에 CLB가 초당 수신한 요청 데이터 패킷 수입니다.              |
| Outbound 패킷 수       | 개/s  | 통계 기간 내에서 초당 CLB에서 보낸 데이터 패킷 수입니다.                |
| 새 연결 수              | 개    | 통계 기간 내에 분당 설정된 새 연결 수입니다.                        |
| 활성 연결 수             | 개    | 통계 기간 내 분당 활성 연결 수입니다.                            |
| 평균 응답 시간            | ms   | 통계 기간 내 CLB의 평균 응답 시간입니다.                         |
| 최대 응답 시간            | ms   | 통계 기간 내 CLB의 최대 응답 시간입니다.                         |
| 2xx 상태 코드           | 개    | 통계 기간 내에 리얼 서버에서 반환된 2xx 상태 코드의 수입니다.             |
| 3xx 상태 코드           | 개    | 통계 기간 내에 리얼 서버에서 반환된 3xx 상태 코드의 수입니다.             |
| 4xx 상태 코드           | 개    | 통계 기간 내에 리얼 서버에서 반환된 4xx 상태 코드의 수입니다.             |
| 5xx 상태 코드           | 개    | 통계 기간 내에 리얼 서버에서 반환된 5xx 상태 코드의 수입니다.             |
| 404 상태 코드           | 개    | 통계 기간 내에 리얼 서버에서 반환된 404 상태 코드의 수입니다.             |
| 502 상태 코드           | 개    | 통계 기간 내에 리얼 서버에서 반환된 502 상태 코드의 수입니다.             |
| CLB에서 반환한 3xx 상태 코드 | 개    | 통계 기간 내에 CLB에서 반환한 3xx 상태 코드의 수입니다.               |
| CLB에서 반환한 4xx 상태 코드 | 개    | 통계 기간 내에 CLB에서 반환한 4xx 상태 코드의 수입니다.               |

|                     |   |                                     |
|---------------------|---|-------------------------------------|
| 태 코드                |   |                                     |
| CLB에서 반환한 5xx 상태 코드 | 개 | 통계 기간 내에 CLB에서 반환한 5xx 상태 코드의 수입니다. |
| CLB에서 반환한 404 상태 코드 | 개 | 통계 기간 내에 CLB에서 반환한 404 상태 코드의 수입니다. |
| CLB에서 반환한 502 상태 코드 | 개 | 통계 기간 내에 CLB에서 반환한 502 상태 코드의 수입니다. |

# 액세스 관리

## 개요

최종 업데이트 날짜: : 2024-01-04 20:06:54

Tencent Cloud 계정 키를 공유하는 다른 사용자가 관리하는 CLB, CVM, TencentDB와 같은 여러 Tencent Cloud 서비스를 사용하는 경우 다음과 같은 문제가 발생할 수 있습니다.

사용자의 키를 여러 사람과 공유할수록 유출 위험도 높아집니다.

다른 사람의 액세스 권한을 제한할 수 없으므로 오작동 및 보안 위험이 발생할 가능성이 높아집니다.

**CAM(Cloud Access Management)**은 Tencent Cloud 리소스에 대한 액세스 권한을 관리하는 데 사용됩니다. CAM을 사용하면 ID 관리 및 정책 관리 기능을 사용하여 어떤 Tencent Cloud 리소스에 어떤 서브 계정이 액세스할 수 있는지 제어할 수 있습니다.

예를 들어, 계정 아래에 서로 다른 프로젝트에 배포된 여러 CLB 인스턴스가 있는 경우 액세스 권한을 관리하고 리소스를 승인하기 위해 이 관리자만 프로젝트 A에서 CLB 리소스를 사용할 수 있다는 권한 정책을 사용하여 프로젝트 A의 관리자를 바인딩할 수 있습니다.

서브 계정에 대한 CLB 리소스에 대한 액세스 권한을 관리할 필요가 없다면 이 섹션을 건너뛸 수 있습니다. 이 섹션을 건너뛰더라도 문서의 나머지 섹션을 이해하고 사용하는 데 영향을 미치지 않습니다.

## CAM의 기본 개념

루트 계정은 정책을 바인딩하여 서브 계정에 권한을 부여합니다. 정책 설정은 **[API, 리소스, 사용자/사용자 그룹, 허용/거부 및 조건]** 레벨에 따라 다를 수 있습니다.

### 1. 계정

#### 루트 계정

루트 계정은 Tencent Cloud 리소스의 기본 소유자로서 리소스 사용 요금 계산 및 과금의 주체이며 Tencent Cloud 서비스에 로그인하는 데 사용할 수 있습니다.

#### 서브 계정

서브 계정은 루트 계정에 의해 생성되며 Tencent Cloud 콘솔에 로그인하는 데 사용할 수 있는 특정 ID 및 ID 자격 증명이 있습니다. 루트 계정은 여러 서브 계정(사용자)을 만들 수 있습니다. **서브 계정은 기본적으로 리소스를 소유하지 않습니다. 루트 계정을 통해 권한을 부여 받아야 합니다.**

#### 신원 자격 증명

여기에는 로그인 자격 증명 및 액세스 인증서가 포함됩니다. **로그인 자격 증명**은 사용자 이름과 비밀번호를 나타냅니다. **액세스 인증서**는 TencentCloud API 키(SecretId 및 SecretKey)를 나타냅니다.

### 2. 리소스 및 권한

#### 리소스

리소스는 CVM 인스턴스 및 VPC 인스턴스와 같이 Tencent Cloud 서비스에서 운영되는 객체입니다.

## 권한

권한은 특정 사용자가 특정 작업을 수행하도록 허용 또는 거부하는 권한입니다. 기본적으로 루트 계정은 그 아래의 모든 리소스에 대한 전체 액세스 권한을 가집니다. 반면 서브 계정은 루트 계정의 리소스에 대한 액세스 권한이 없습니다.

## 정책

정책은 하나 이상의 권한을 정의하고 설명하는 데 사용되는 구문 규칙입니다. 루트 계정은 사용자/사용자 그룹과 정책을 연결하여 권한 부여를 수행합니다.

자세한 내용은 [CAM Overview](#)를 참고하십시오.

## 관련 문서

| 문서 설명             | 링크                                   |
|-------------------|--------------------------------------|
| 정책과 사용자의 관계       | <a href="#">Policy</a>               |
| 기본 정책 구조          | <a href="#">Element Reference</a>    |
| CAM을 지원하는 더 많은 제품 | <a href="#">CAM-Enabled Products</a> |

# 권한 정의

최종 업데이트 날짜: : 2024-01-04 20:08:12

## CAM에서 권한 부여 가능한 CLB 리소스 유형

| 리소스 유형    | 권한 부여 정책 중 리소스 메소드 설명                                             |
|-----------|-------------------------------------------------------------------|
| CLB 인스턴스  | <code>qcs::clb:\$region::clb/\$loadbalancerid</code>              |
| CLB 리얼 서버 | <code>qcs::cvm:\$region:\$account:instance/\$cvminstanceid</code> |

이 중,

`$region` 은 항상 region의 ID여야 하며 비워 둘 수 있습니다.

`$account` 는 항상 리소스 소유자의 AccountId 또는 '\*'여야 합니다.

`$loadbalancerid` 는 항상 loadbalancer 인스턴스의 ID 또는 '\*'여야 합니다.

등등.

## CAM의 CLB에 대해 권한 부여가 가능한 API

CAM에서 CLB 리소스에 대해 다음 Action을 권한 부여할 수 있습니다.

### 인스턴스

| API 작업                       | 리소스 설명         | API 설명                                                        |
|------------------------------|----------------|---------------------------------------------------------------|
| DescribeLoadBalancers        | CLB 인스턴스 목록 쿼리 | * API만 인증함을 나타냄                                               |
| CreateLoadBalancer           | CLB 인스턴스 구매    | <code>qcs:\$projectid:clb:\$region:\$account:clb/*</code>     |
| DeleteLoadBalancers          | CLB 인스턴스 삭제    | <code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code> |
| ModifyLoadBalancerAttributes | CLB 인          | <code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code> |



|                     |                           |                                                               |
|---------------------|---------------------------|---------------------------------------------------------------|
|                     | 스턴스<br>속성 수<br>정          |                                                               |
| ModifyForwardLBName | CLB 인<br>스턴스<br>이름 수<br>정 | <code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code> |

## 리스너

| API 작업                        | 리스<br>스<br>설명                                | API 설명                                                      |
|-------------------------------|----------------------------------------------|-------------------------------------------------------------|
| DeleteLoadBalancerListeners   | CLB<br>리스<br>너<br>삭제                         | <code>qcs::clb:\$region:\$account:clb/\$loadbalancer</code> |
| DescribeLoadBalancerListeners | CLB<br>리스<br>너<br>목록<br>가져<br>오기             | <code>qcs::clb:\$region:\$account:clb/\$loadbalancer</code> |
| ModifyLoadBalancerListener    | CLB<br>리스<br>너의<br>속성<br>수정                  | <code>qcs::clb:\$region:\$account:clb/\$loadbalancer</code> |
| CreateLoadBalancerListeners   | CLB<br>리스<br>너<br>생성                         | <code>qcs::clb:\$region:\$account:clb/\$loadbalancer</code> |
| DeleteForwardLBListener       | CLB<br>리스<br>너<br>(레<br>이어<br>4 및<br>레이<br>어 | <code>qcs::clb:\$region:\$account:clb/\$loadbalancer</code> |

|                                      |                                         |                                                             |
|--------------------------------------|-----------------------------------------|-------------------------------------------------------------|
|                                      | 7)<br>삭제                                |                                                             |
| ModifyForwardLBSeventhListener       | CLB<br>레이<br>어 7<br>리스<br>너<br>속성<br>수정 | <code>qcs::clb:\$region:\$account:clb/\$loadbalancer</code> |
| ModifyForwardLBFourthListener        | CLB<br>레이<br>어 4<br>리스<br>너<br>속성<br>수정 | <code>qcs::clb:\$region:\$account:clb/\$loadbalancer</code> |
| DescribeForwardLBLListeners          | CLB<br>리스<br>너<br>목록<br>쿼리              | <code>qcs::clb:\$region:\$account:clb/\$loadbalancer</code> |
| CreateForwardLBSeventhLayerListeners | 레이<br>어 7<br>CLB<br>리스<br>너<br>생성       | <code>qcs::clb:\$region:\$account:clb/\$loadbalancer</code> |
| CreateForwardLBFourthLayerListeners  | 레이<br>어 4<br>CLB<br>리스<br>너<br>생성       | <code>qcs::clb:\$region:\$account:clb/\$loadbalancer</code> |

## CLB 도메인 이름 + URL

| API 작업                     | 리소스<br>설명  | API 설명                                                        |
|----------------------------|------------|---------------------------------------------------------------|
| ModifyForwardLBRulesDomain | CLB<br>리스너 | <code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code> |

|                              |                                 |                                                               |
|------------------------------|---------------------------------|---------------------------------------------------------------|
|                              | 의 포워딩 규칙의 도메인 이름 수정             |                                                               |
| CreateForwardLBListenerRules | CLB 리스너 포워딩 규칙 생성               | <code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code> |
| DeleteForwardLBListenerRules | 레이어 7 CLB 리스너 규칙 삭제             | <code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code> |
| DeleteRewrite                | CLB 인스턴스의 포워딩 규칙의 리디렉션 관계 삭제    | <code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code> |
| ManualRewrite                | CLB 인스턴스의 포워딩 규칙의 리디렉션 관계 수동 추가 | <code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code> |
| AutoRewrite                  | CLB 인스턴스의 포워딩 규칙의 리디렉션          | <code>qcs::clb:\$region:\$account:clb/\$loadbalancerid</code> |

선  
관  
계  
자  
동  
생  
성

## 리얼 서버

| API 작업                              | 리소스 설명                        | API 설명                                              |
|-------------------------------------|-------------------------------|-----------------------------------------------------|
| ModifyLoadBalancerBackends          | CLB 인스턴스의 리얼 서버 가중치 수정        | <code>qcs::clb:\$region:\$account:clb/\$load</code> |
| DescribeLoadBalancerBackends        | CLB 인스턴스에 바인딩된 리얼 서버 목록 가져 오기 | <code>qcs::clb:\$region:\$account:clb/\$load</code> |
| DeregisterInstancesFromLoadBalancer | 리얼 서버 바인딩 해제                  | <code>qcs::clb:\$region:\$account:clb/\$load</code> |
| RegisterInstancesWithLoadBalancer   | 리얼 서버를 CLB 인스턴스에              | <code>qcs::clb:\$region:\$account:clb/\$load</code> |

|                                               |                                     |                                                     |
|-----------------------------------------------|-------------------------------------|-----------------------------------------------------|
|                                               | 바인딩                                 |                                                     |
| DescribeLBHealthStatus                        | CLB 상태 쿼리                           | <code>qcs::clb:\$region:\$account:clb/\$load</code> |
| ModifyForwardFourthBackendsPort               | 레이어 4 리스너의 포워딩 규칙에서 CVM 인스턴스 포트 수정  | <code>qcs::clb:\$region:\$account:clb/\$load</code> |
| ModifyForwardFourthBackendsWeight             | 레이어 4 리스너의 포워딩 규칙에서 CVM 인스턴스 가중치 수정 | <code>qcs::clb:\$region:\$account:clb/\$load</code> |
| RegisterInstancesWithForwardLBSeventhListener | CLB 레이어 7 리스너의 포워딩 규칙에 CVM          | <code>qcs::clb:\$region:\$account:clb/\$load</code> |

|                                                |                                         |                                                     |
|------------------------------------------------|-----------------------------------------|-----------------------------------------------------|
|                                                | 인스턴스 바인딩                                |                                                     |
| RegisterInstancesWithForwardLBFourthListener   | CLB 레이어 4 리스너의 포워딩 규칙에 CVM 인스턴스 바인딩     | <code>qcs::clb:\$region:\$account:clb/\$load</code> |
| DeregisterInstancesFromForwardLBFourthListener | CLB 레이어 4 리스너의 포워딩 규칙에서 CVM 인스턴스 바인딩 해제 | <code>qcs::clb:\$region:\$account:clb/\$load</code> |
| DeregisterInstancesFromForwardLB               | CLB 레이어 7 리스너의 포워딩 규칙에서 CVM             | <code>qcs::clb:\$region:\$account:clb/\$load</code> |

|                                  |                                     |                                                     |
|----------------------------------|-------------------------------------|-----------------------------------------------------|
|                                  | 인스턴스 바인딩 해제                         |                                                     |
| ModifyForwardSeventhBackends     | 레이어 7 리스너의 포워딩 규칙에서 CVM 인스턴스 가중치 수정 | <code>qcs::clb:\$region:\$account:clb/\$load</code> |
| ModifyForwardSeventhBackendsPort | 레이어 7 리스너의 포워딩 규칙에서 CVM 인스턴스 포트 수정  | <code>qcs::clb:\$region:\$account:clb/\$load</code> |
| DescribeForwardLBBackends        | CLB 인스턴스의 CVM 인스턴스 목록 쿼리            | <code>qcs::clb:\$region:\$account:clb/\$load</code> |
| DescribeForwardLBHealthStatus    | CLB                                 | <code>qcs::clb:\$region:\$account:clb/*</code>      |

|                              |                                                                          |                                                      |
|------------------------------|--------------------------------------------------------------------------|------------------------------------------------------|
|                              | 상태<br>확인<br>상태<br>쿼리                                                     |                                                      |
| ModifyLoadBalancerRulesProbe | CLB<br>리스<br>너의<br>포워<br>딩<br>규칙<br>상태<br>확인<br>및<br>포워<br>딩<br>경로<br>수정 | <code>qcs::clb:\$region:\$account:clb/\$loadl</code> |



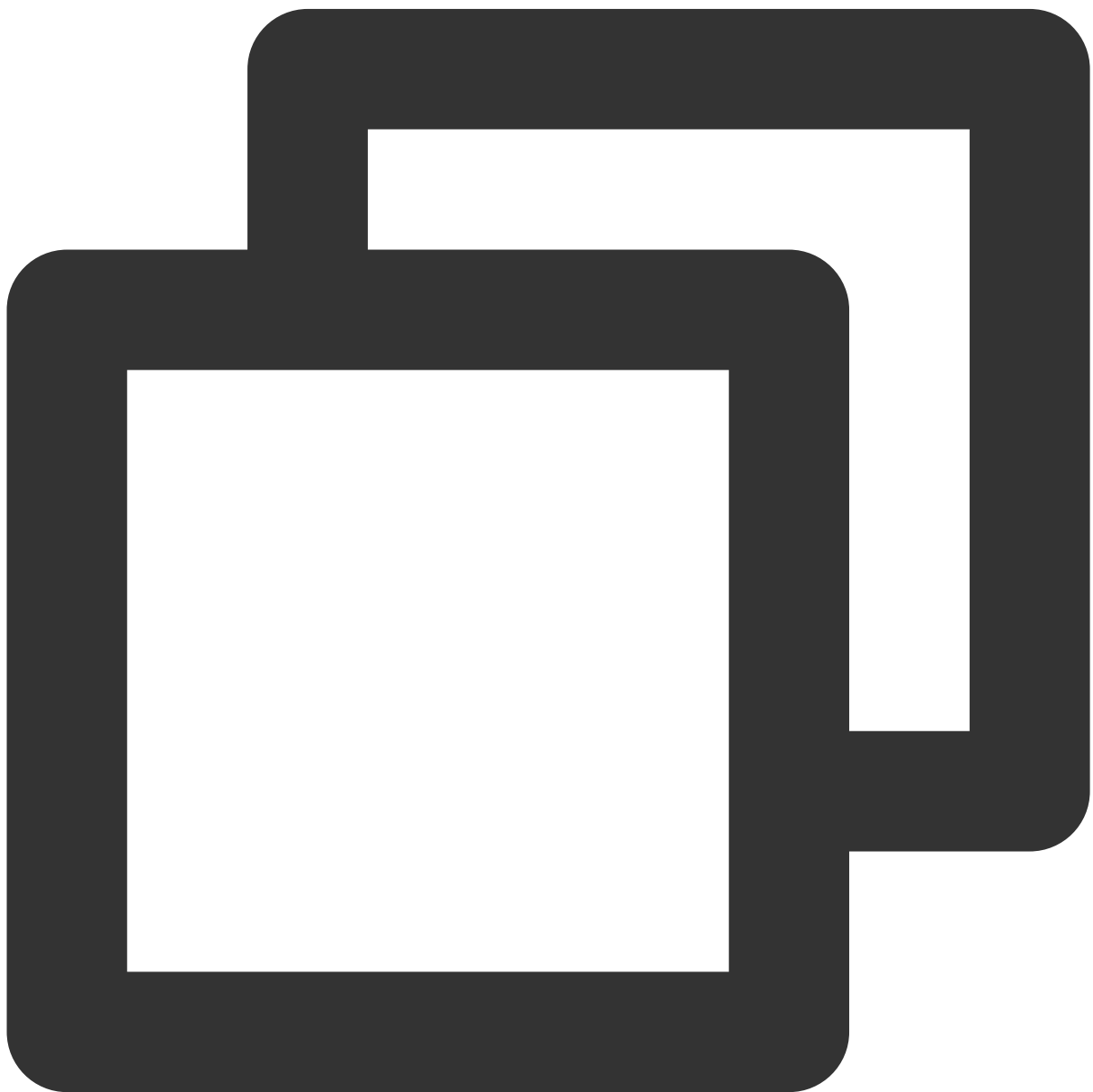
# 정책 예시

최종 업데이트 날짜: : 2024-01-04 20:08:29

## 모든 CLB 인스턴스에 대한 전체 액세스 정책

CLB 서비스(생성, 관리 등)에 대한 전체 액세스 권한을 서브 계정에 부여합니다.

정책 이름: CLBResourceFullAccess

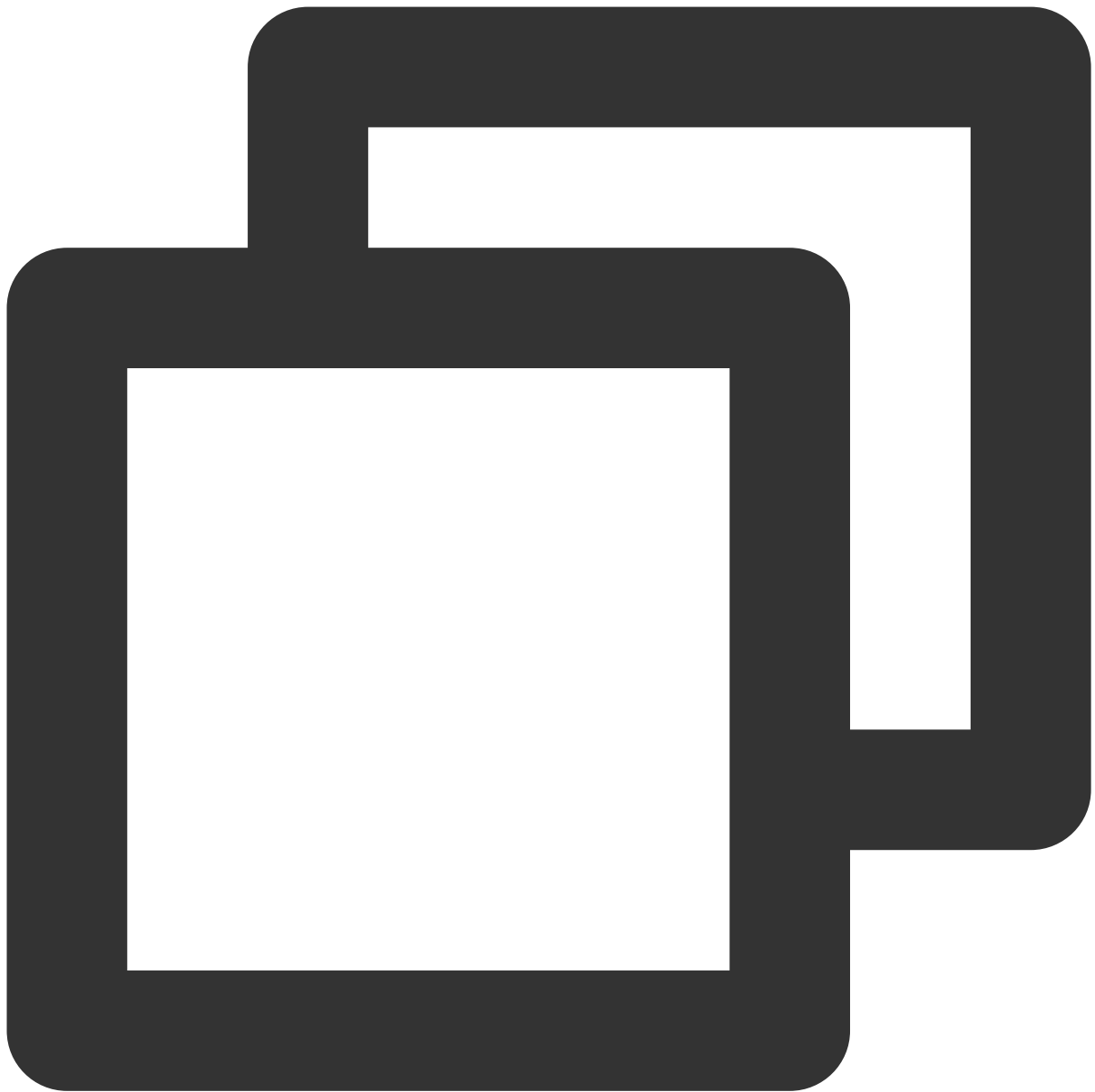


```
{
 "version": "2.0",
 "statement": [{
 "action": [
 "name/clb:*"
],
 "resource": "*",
 "effect": "allow"
 }]
}
```

## 모든 CLB 인스턴스에 대한 읽기 전용 정책

서브 계정에 CLB에 대한 읽기 전용 액세스 권한을 부여합니다(즉, 모든 CLB 리소스를 생성, 업데이트 또는 삭제할 수는 없지만 볼 수 있는 권한). 콘솔에서 리소스를 조작하기 위한 전제 조건은 리소스를 볼 수 있는 기능입니다. 따라서 서브 계정에 CLB에 대한 전체 읽기 액세스 권한을 부여하는 것이 좋습니다.

정책 이름: CLBResourceReadOnlyAccess

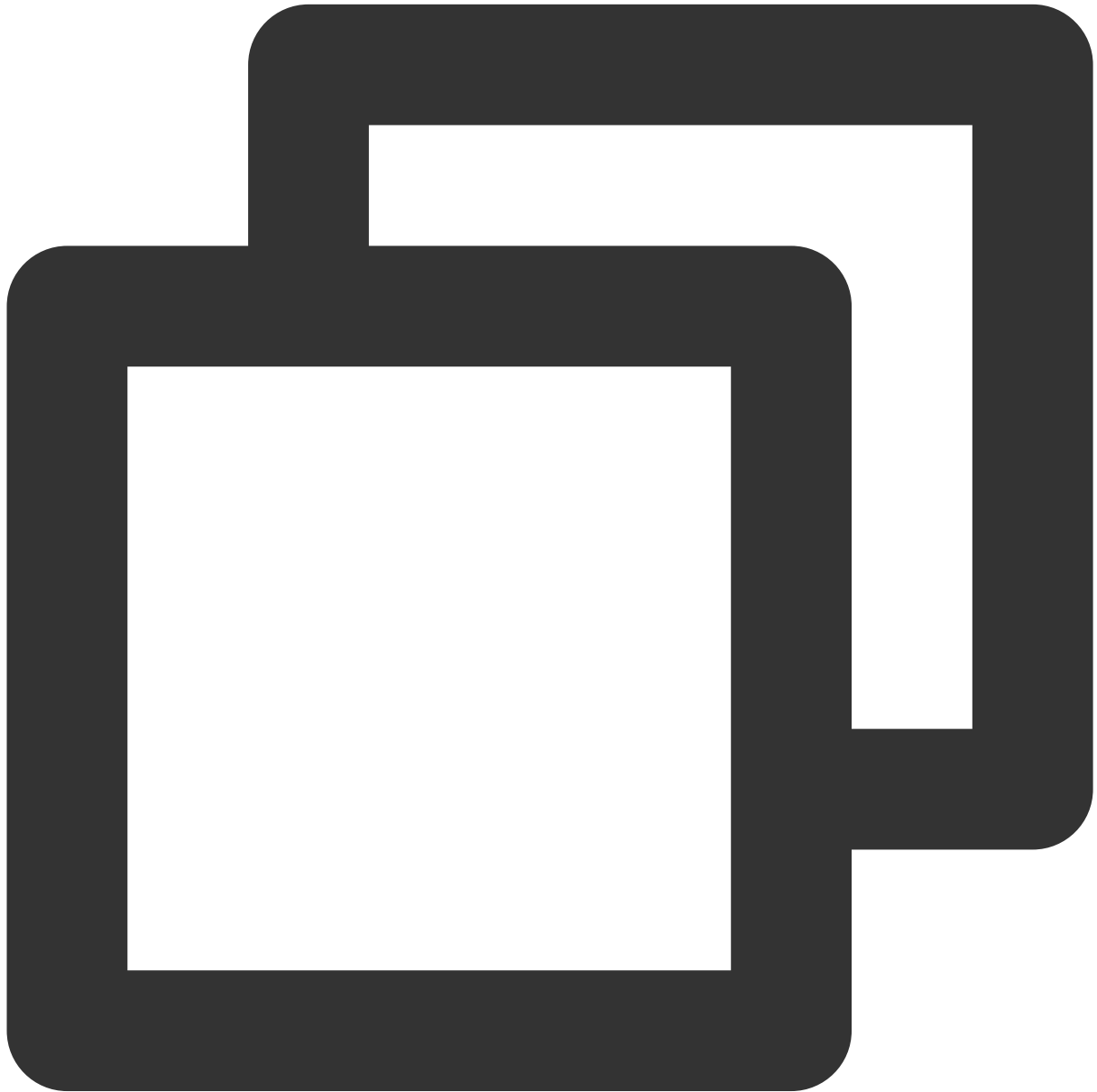


```
{
 "version": "2.0",
 "statement": [{
 "action": [
 "name/clb:Describe*"
],
 "resource": "*",
 "effect": "allow"
 }]
}
```

## 지정된 태그의 CLB 서비스에 대한 전체 액세스 정책

서브 계정에 지정된 태그(태그 키: tagkey, 태그 값: tagvalue)에서 CLB 서비스(인스턴스 생성, 리스너 관리 등)에 대한 전체 액세스 권한을 부여합니다.

CLB 인스턴스는 태그 구성 및 인증을 위한 태그 사용을 지원합니다.



```
{
 "version": "2.0",
 "statement": [
 {
```

```
 "effect": "allow",
 "action": "*",
 "resource": "*",
 "condition": {
 "for_any_value: string_equal": {
 "qcs:tag": [
 "tagkey&tagvalue"
]
 }
 }
]
}
```