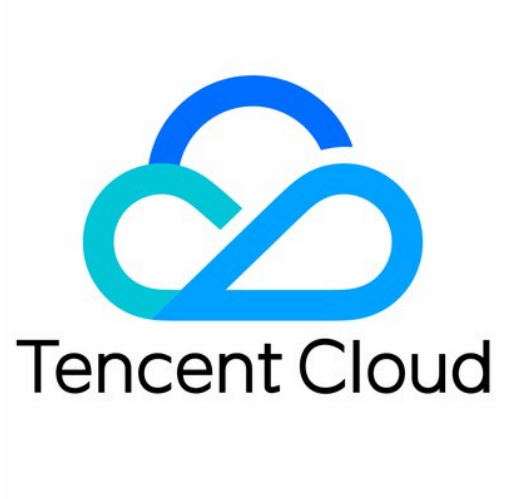
Cloud Load Balancer

FAQ

제품 문서



목록:

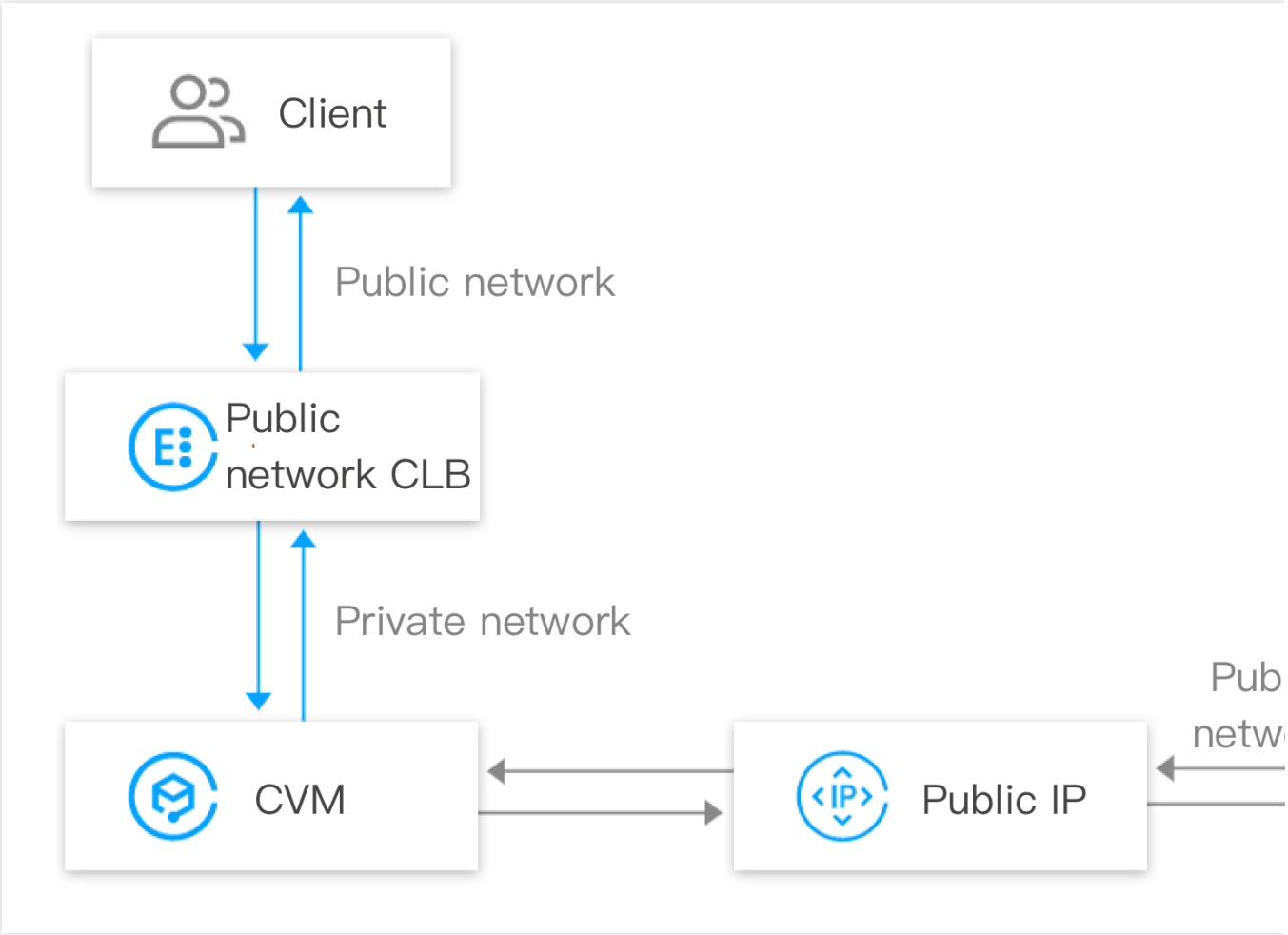
FAQ
과금 관련

최종 업데이트 날짜: : 2024-01-04 20:21:51

과
금 관련 문제

CLB 인스턴스와 백엔드 CVM 인스턴스 간의 통신은 공중망 또는 사설망을 통해 이루어집니까?

CLB와 CVM 인스턴스 간의 통신은 계정 유형이 IP별 청구인지 CVM별 청구인지에 관계없이 사설망 트래픽을 생성합니다. 두 가지 유형의 트래픽 경로는 다음과 같습니다.
클라이언트는 공중망을 통해 CLB 인스턴스에 액세스하고, CLB 인스턴스는 사설망을 통해 트래픽을 CVM 인스턴스로 포워딩하고, CVM 인스턴스는 사설망을 통해 CLB 인스턴스에 응답하고, 마지막으로 CLB 인스턴스는 클라이언트에 응답합니다.
CVM 인스턴스가 공중망에 액세스하거나 공중망 IP를 통해 액세스하면 CVM 인스턴스는 공중망 IP 또는 EIP를 통해 클라이언트와 인터랙션합니다.



[상단으로 이동]

CLB는 어떻게 과금되나요?

CLB 청구 정책은 계정 유형에 따라 다릅니다. 자세한 내용은 Billing Overview를 참고하십시오. IP별 청구와 CVM별 청구 계정 간의 주요 차이점은 과금 기준이며 서비스 액세스 및 모니터링과 같은 다른 측면은 동일합니다. 계정 유형 간의 차이점에 대한 자세한 내용은 Checking Account Type을 참고하십시오.

IP별 청구 계정의 공중망 요금: CLB 인스턴스 또는 공중망 IP에 액세스하는 공중망 트래픽에 대해 공중망 요금은 CLB 인스턴스 또는 공중망 IP에 각각 부과됩니다.

CVM별 청구 계정의 공중망 요금: CLB 인스턴스 또는 공중망 IP에 액세스하는 공중망 트래픽의 경우 CVM 인스턴스에 공중망 요금이 부과됩니다.

[상단으로 이동]

내 계정 유형을 IP별 청구와 CVM별 청구 간에 전환할 수 있습니까?

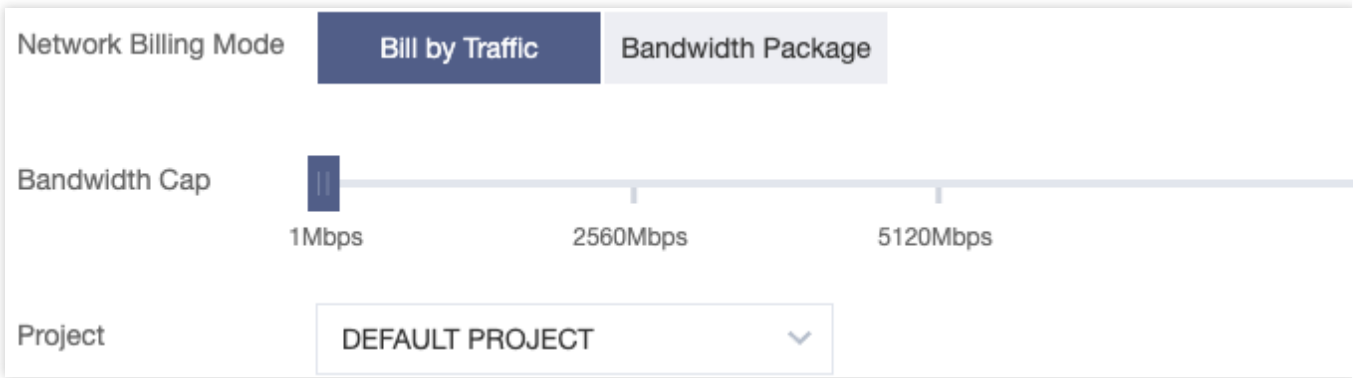
계정 유형을 CVM별 청구에서 IP별 청구로 업그레이드할 수 있습니다.
IP별 청구 계정은 CVM별 청구 계정으로 되돌릴 수 없습니다.
[상단으로 이동]

리전 간 바인딩 요금은 어떻게 청구되나요?

리전 간 바인딩 요금은 CLB 리전 간 바인딩 기능을 사용하는 경우에만 부과됩니다. 자세한 내용은 Cloud Connect Network를 참고하십시오.
크로스 리전1.0: 리전 간 요금은 CLB 인스턴스에 부과됩니다.
크로스 리전2.0: 리전 간 요금은 CLB 인스턴스가 아닌 CCN 인스턴스에 부과됩니다.
[상단으로 이동]

CLB 인스턴스의 대역폭 한도는 얼마입니까?

IP별 청구 계정: CLB 인스턴스를 구매할 때 CLB 대역폭 한도를 선택해야 합니다. 비즈니스 대역폭이 상한을 초과하면 CLB 인스턴스는 자동으로 패킷을 잃게 됩니다.



CVM별 청구 계정: CLB 인스턴스를 구매할 때 CLB 대역폭 한도를 선택할 필요가 없습니다. CLB 대역폭은 백엔드 CVM 인스턴스의 총 공중망 대역폭에 의해 제한됩니다.
[상단으로 이동]

CLB 구성

최종 업데이트 날짜: : 2024-01-04 20:22:05

개념

레이어 4와 레이어 7 로드 밸런싱의 차이점은 무엇입니까?

UDP와 TCP의 차이점은 무엇입니까?

CLB는 어떻게 Cookies를 기반으로 세션 지속성을 구현합니까?

리얼 서버 가중치란 무엇입니까?

가중치를 0으로 재설정하는 것과 RS 바인딩을 해제하는 것의 차이점은 무엇입니까?

상태 확인

상태 확인 중에 예외가 발생하면 어떻게 해야 합니까?

상태 확인 빈도가 과도히 높은 이유는 무엇입니까?

액세스

로드 포워딩의 HTTP 리디렉션

로드 밸런싱에 사용할 수 있는 TCP 포트는 무엇입니까?

포트 843에서 policy 요청(즉, flash server 요청)이 전송된 후 정책 파일이 반환되지 않고 연결이 중단됩니다.

CLB 인스턴스가 Client IP를 직접 가져올 수 있습니까?

포트 A에서 동일한 서버의 다른 포트로 트래픽을 포워딩하도록 CVM 인스턴스에 대한 사설망 CLB를 구성할 수 있습니까?

백엔드 CVM 인스턴스에 공중망 대역폭이 필요합니까? 대역폭이 CLB 서비스에 영향을 미치나요?

클라이언트와 서버의 HTTP 버전이 다른 경우 호환 버전에 대한 참고 사항

Gzip 호환성

CLB 리얼 서버의 보안 그룹은 어떻게 설정하나요? 액세스 블록리스트를 구성하는 방법은 무엇입니까?

액세스 블록리스트 설정

CLB 인스턴스는 사설망 또는 공중망를 통해 리얼 서버와 통신합니까?

CLB VIP Ping

Telnet 명령을 실행하여 CLB 수신 포트 연결

사설망 루프백

클라이언트가 중간 노드를 통해 리얼 서버의 동일한 포트에 액세스하는 경우, 이러한 노드를 구체적으로 확인할 수 없습니다

공중망의 액세스 트래픽을 차단하고 CLB 인스턴스의 액세스만 허용하도록 보안 그룹이 있는 백엔드 CVM 인스턴스를 구성했습니다. 그러나 적용되지 않습니다

리스너로 CLB 인스턴스를 구성하고 리스너를 백엔드 CVM에 바인딩했으며 도메인 이름을 백엔드 CVM의 IP로 확인했습니다. 그러나 도메인 이름에 액세스하면 모니터 데이터가 표시되지 않습니다

843 리스너를 생성하지 않았지만 Telnet 명령을 실행하여 연결할 수 있는 이유는 무엇입니까?

CLB 액세스 로그에 기록된 9/11 IP 범위의 주소가 Tencent Cloud 사설망 IP 범위입니까?

레이어 4 로드 밸런싱과 레이어 7 로드 밸런싱의 차이점은 무엇입니까?

레이어 4 로드 밸런싱은 IP + 포트를 기반으로 합니다.
레이어 7 로드 밸런싱은 HTTP 헤더 및 URL과 같은 애플리케이션 레이어 정보를 기반으로 합니다.
레이어 4 인스턴스와 레이어 7 인스턴스의 차이점은 리얼 서버에서 로드 밸런싱을 위해 트래픽을 포워딩하는 방법을 결정하는 기준으로 레이어 4 또는 레이어 7 정보를 사용하는지 여부입니다.
예를 들어 레이어 4 CLB 인스턴스는 레이어 3 IP 주소(VIP) 및 레이어 4 포트 번호를 기반으로 로드 밸런싱이 필요한 트래픽을 결정합니다. 처리할 트래픽에 대해 NAT(Network Address Translation)를 수행한 다음 리얼 서버로 전달합니다. 또한 TCP 또는 UDP 트래픽을 처리한 서버를 기록하고 이 연결의 모든 후속 트래픽을 처리를 위해 동일한 서버로 전달합니다.
레이어 7 CLB는 애플리케이션 레이어 기능과 결합된 레이어 4 CLB 인스턴스입니다.
예를 들어 동일한 Web 서버의 CLB 인스턴스는 VIP 및 포트 80 외에도 레이어 7 URL, 브라우저 유형 및 언어를 기반으로 처리해야 하는 트래픽을 식별할 수 있습니다.
레이어 7 로드 밸런싱은 '콘텐츠 교환'이라고도 하며, 메시지의 의미 있는 애플리케이션 레이어 콘텐츠와 CLB 인스턴스에 구성된 서버 선택 방법을 기반으로 내부 서버가 선택됩니다.
실제 애플리케이션 레이어 콘텐츠를 기반으로 서버를 선택하려면 레이어 7 CLB 인스턴스가 클라이언트로부터 실제 애플리케이션 레이어 콘텐츠가 포함된 메시지를 수신하기 위해 최종 서버의 프록시로서 클라이언트와 연결(3방향 핸드셰이크)을 설정해야 합니다. 그런 다음 메시지의 특정 필드와 CLB 인스턴스에 구성된 서버 선택 방법에 따라 내부 서버를 선택합니다. 이 경우 CLB 인스턴스는 프록시 서버에 가깝고 각각 프런트엔드 클라이언트 및 리얼 서버와 TCP 연결을 설정합니다.

[맨 위로]

UDP와 TCP 프로토콜의 차이점은 무엇입니까?

TCP는 연결 지향 프로토콜입니다. TCP는 데이터를 수신 및 전송하기 전에 상대방과 신뢰할 수 있는 연결을 설정해야 합니다. UDP는 메시지 지향(연결 없는) 프로토콜입니다. 상대방과 3방향 핸드셰이크를 수행하지 않고 데이터 패킷을 직접 전송합니다. UDP는 화상 채팅, 금융 시장 정보의 실시간 푸시, DNS 및 IoT와 같이 신뢰성보다 실시간성에 중점을 둔 시나리오에 적합합니다.

[맨 위로]

CLB는 어떻게 Cookies를 기반으로 세션 지속성을 구현합니까?

Cookie 삽입 모드에서는 CLB 인스턴스가 Cookie를 삽입하므로 리얼 서버는 수정할 필요가 없습니다. 첫 번째 HTTP 요청을 하면 (Cookie 없이) CLB 인스턴스에 들어가고 로드 밸런싱 알고리즘 정책에 따라 리얼 서버를 선택하고 서버로 요청을 보냅니다. 그런 다음 리얼 서버는 CLB 인스턴스로 다시 전송되는 HTTP 응답(Cookie 제외)을 보내고, CLB 인스턴스는 Cookie를 삽입하고 HTTP 응답(Cookie 포함)을 클라이언트에 반환합니다.

두 번째 HTTP 요청(CLB 인스턴스가 마지막으로 삽입한 Cookie 사용)을 하면 CLB 인스턴스에 들어가 Cookie의 세션 지속성 값을 읽고(위와 동일한 Cookie 포함) 지정된 리얼 서버로 요청을 보냅니다. 서버는 HTTP 응답을 제공합니다. 서버가 Cookie를 작성하지 않기 때문에 응답에 Cookie가 포함되지 않습니다. 응답 트래픽이 CLB 인스턴스에 다시 입력되면 CLB는 업데이트된 세션 지속성 Cookie를 응답에 기록합니다.

[맨 위로]

리얼 서버 가중치란 무엇입니까?

리얼 서버 풀의 각 CVM 인스턴스에 대한 포워딩 가중치를 지정할 수 있으며 가중치가 높은 인스턴스에 더 많은 액세스 요청이 할당됩니다. 서비스 기능 및 상태에 따라 백엔드 CVM 인스턴스의 가중치를 구성할 수 있습니다.
세션 지속성도 활성화한 경우 동일한 액세스 요청이 다른 리얼 서버로 전달될 수 있습니다. 세션 지속성을 일시적으로 비활성화한 다음 문제가 지속되는지 확인하는 것이 좋습니다.

[맨 위로]

가중치를 0으로 재설정하는 것과 RS 바인딩을 해제하는 것의 차이점은 무엇입니까?

가중치를 0으로 재설정: TCP 리스너는 기존 연결을 계속 포워딩하고 UDP 리스너는 동일한 5배 연결을 포워딩하며 HTTP/HTTPS 리스너는 기존 연결을 계속 포워딩합니다.
RS 바인딩 해제: TCP/UDP 리스너는 기존 연결 포워딩을 중지하고 HTTP/HTTPS 리스너는 기존 연결을 계속 포워딩합니다.

[맨 위로]

상태 확인 중에 예외가 발생하면 어떻게 해야 합니까?

다음 단계에 따라 문제를 해결하십시오.
리얼 서버를 통해 직접 애플리케이션 서비스에 액세스해야 합니다.
리얼 서버에서 해당 포트가 열려 있는지 확인하십시오.
리얼 서버에 방화벽과 같은 보안 소프트웨어가 있는지 확인하십시오. 이로 인해 CLB 인스턴스가 리얼 서버와 통신하지 못할 수 있습니다.
CLB 인스턴스의 상태 확인 매개변수가 올바르게 구성되었는지 확인합니다.
상태 확인을 위해 정적 페이지를 사용하는 것이 좋습니다.
응답이 느려지는 CVM 인스턴스의 부하가 높은지 확인하십시오.
CVM 인스턴스에 IP 제한(iptables)이 없는지 확인하십시오.

[맨 위로]

상태 확인 빈도가 과도히 높은 이유는 무엇입니까?

콘솔에서 5초마다 상태 확인 패킷을 보내도록 구성했다고 가정합니다. 그러나 리얼 서버는 1초에 하나 이상의 상태 확인 요청을 받습니다.
자주 발생하는 상태 확인은 CLB 상태 확인의 구현 메커니즘과 관련이 있습니다. client의 100만 요청이 리얼 서버로 전송되기 전에 4개의 CLB 인스턴스에 분산되고 각 CLB 리얼 서버에서 개별적으로 상태 확인을 수행한다고 가정합니다. CLB 인스턴스가 5초마다 상태 확인 요청을 보내도록 구성된 경우 각 CLB 인스턴스는 5s마다 상태 확인 요청을 보냅니다. 이것이 리얼 서버가 여러 상태 확인 요청을 수신하는 이유입니다. 예를 들어 클러스터에 8개의 CLB 인스턴스가 있고 각각 5s마다 요청을 보내는 경우 리얼 서버는 5s 동안 8개의 상태 확인 요청을 수신할 수 있습니다.
이 구현 방식의 장점은 고효율, 정확한 검사, 잘못된 제거 방지입니다. 예를 들어 클러스터의 CLB 서버 8개 중 하나에 장애가 발생하더라도 나머지 7개 서버는 정상적으로 트래픽을 전달할 수 있습니다.
따라서 리얼 서버 확인 빈도가 너무 높은 경우 더 긴 확인 간격(예시: 15s)을 구성할 수 있습니다.

[맨 위로]

로드 포워딩의 HTTP 리디렉션

브라우저를 통해 `http://example.com` 웹사이트를 방문할 때 서버에 대한 루트 디렉터리로의 리디렉션이 필요합니다. 브라우저를 통해 `http://example.com/` 웹사이트를 방문하면 서버는 웹사이트 루트 디렉터리의 기본 페이지를 직접 반환합니다. 마찬가지로 `http://cloud.tencent.com/movie` 가 URL 재작성을 통해 `http://cloud.tencent.com/movie/` 로 리디렉션되는 경우 `http://cloud.tencent.com/movie` 를 입력하면 추가 URL 재작성 프로세스로 인해 약간의 성능 저하 및 시간 소모가 발생합니다. 다만, URL 재작성을 통해 `http://cloud.tencent.com/product` 가 `http://cloud.tencent.com/product/` 이외의 페이지로 리디렉션되는 경우 보조 URL 뒤에 `/` 를 추가할지 고려해야 합니다.
Tencent Cloud CLB에서 프런트엔드와 백엔드 포트 번호가 다른 경우, HTTP 리디렉션 후 포트 번호 변경을 방지하고 정상적인 페이지 액세스를 보장하기 위해 보조 페이지 방문 시 보조 URL 뒤에 `/` 를 추가해야 합니다.
레이어 7 포워딩에서 CLB 인스턴스의 포트 80과 리얼 서버의 포트 8081이 수신된다고 가정합니다. 클라이언트가 `http://www.example.com/movie` 에 액세스하면 액세스 요청은 CLB 인스턴스를 통해 리얼 서버로 포워딩되고, 서버는 `http://www.example.com:8081/movie/` (수신 포트는 8081)로 리다이렉트 합니다. 이 경우 클라이언트 액세스가 실패합니다(포트 오류).
따라서 `http://www.example.com/movie/` 와 같이 `/` 를 사용하여 보조 URL에 대한 액세스 요청을 다시 작성하는 것이 좋습니다. 이렇게 하면 HTTP 리디렉션을 방지하고 불필요한 판단을 제거하며 원치 않는 로드를 줄일 수 있습니다. HTTP 리디렉션이 필요한 경우 CLB 수신 포트가 리얼 서버와 동일한지 확인하십시오.

[맨 위로]

로드 밸런싱에 사용할 수 있는 TCP 포트는 무엇입니까?

21(FTP), 25(SMTP), 80(HTTP), 443(HTTPS), 1024 – 65535 등의 TCP 포트에 대해 로드 밸런싱을 수행할 수 있습니다.

[맨 위로]

policy 파일이 반환되지 않고 포트 843에서 정책 요청(즉, flash server 요청)이 전송된 후 연결이 중단되면 어떻게 해야 합니까?

CLB 인스턴스가 포트 843에서 policy 요청을 수신하면 일반 crossdomain 정책 구성 파일을 반환합니다. 정책 파일이 반환되지 않고 연결이 직접 닫히면 flash server 요청이 올바르지 않을 수 있습니다.
올바른 flash server 요청이 전송되었는지 확인하십시오: \\0.
주의사항:
\\0으로 끝나야 하고 23바이트를 포함해야 합니다. \\0은 ASCII 코드가 0이고 1바이트만 차지하는 문자를 나타냅니다.
포트 843에서 반환되는 정상적인 결과는 다음과 같습니다.

```
VM_02_sles10_64:/ # perl -e 'printf "<policy-file-request/>%c",0' | netcat -i 1 101.226.62.63 8
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM "/xml/dtds/cross-domain-policy.dtd">

<!-- Policy file for xmlsocket://socks.example.com -->
<cross-domain-policy>

   <!-- This is a master socket policy file -->
   <!-- No other socket policies on the host will be permitted -->
   <site-control permitted-cross-domain-policies="master-only"/>

   <!-- Instead of setting to-ports="*", administrator's can use ranges and commas -->
   <!-- This will allow access to ports 123, 456, 457 and 458 -->
   <allow-access-from domain="*" to-ports="*" />

</cross-domain-policy>
```

[맨 위로]

CLB 인스턴스가 Client IP를 직접 가져올 수 있습니까?

IPv6 NAT64 CLB 인스턴스는 Client IP 가져오기를 지원하지 않습니다.
공중망 레이어 7 IPv4 및 IPv6 CLB 인스턴스는 X-Forwarded-For 메소드를 사용하여 실제 클라이언트 IP를 가져옵니다. Client IP 가져오기는 기본적으로 CLB 인스턴스에서 활성화되지만 리얼 서버에서 구성해야 합니다. 자세한 내용은 Obtaining Real Client IPs Over IPv4 CLBs를 참고하십시오.
공중망 레이어 4 IPv4 및 IPv6 CLB 인스턴스(TCP를 통해)는 백엔드 CVM 인스턴스에서 실제 클라이언트 IP를 직접 가져올 수 있으며 추가 구성이 필요하지 않습니다. 2016년 10월 24일 이후 구매한 사설망 레이어 4 CLB 인스턴스의 경우 SNAT(Source Network Address Translation)가 수행되지 않습니다. 추가 구성 없이 server에서 실제 client IP를 직접 가져올 수 있습니다.

[맨 위로]

포트 A에서 동일한 서버의 다른 포트로 트래픽을 포워딩하도록 CVM 인스턴스에 대한 사설망 CLB를 구성할 수 있습니까?

아니요. 서버 A(10.66..*101)의 포트 a에 액세스하려면 사설망 CLB 인스턴스를 통해 요청을 서버 B(10.66.*..102)의 포트 b로 포워딩할 수 있습니다. 그러나 동일한 서버 A(10.66.* .101)의 포트 b로 포워딩할 수 없습니다.

[맨 위로]

백엔드 CVM 인스턴스에 공중망 대역폭이 필요합니까? 대역폭이 CLB 서비스에 영향을 미치나요?

IP별 청구 계정의 CLB 인스턴스에 바인딩된 백엔드 CVM 인스턴스에는 공중망 대역폭이 필요하지 않습니다.
CVM별 청구 계정의 CLB 인스턴스에는 트래픽 또는 대역폭 요금이 부과되지 않습니다. CLB 서비스에서 생성된 모든 공중망 트래픽 요금은 바인딩된 백엔드 CVM 인스턴스에 부과됩니다. 총 CLB 송신 트래픽의 변동을 추적할 필요가 없도록 CVM 인스턴스를 구매하고 합리적인 피크 대역폭 임계값을 구성할 때 공중망 대역폭에 대해 트래픽별 청구를 선택하는 것이 좋습니다. 인터넷 Web 비즈니스의 트래픽은 변동이 심하여 정확하게 예측할 수 없습니다. 대역폭별 청구를 선택하면 과도한 대역폭을 구입하는 것이 비용 효율적이지 않지만 대역폭이 충분하지 않은 경우 비즈니스 피크 시 패킷 손실이 발생할 수 있습니다.

[맨 위로]

클라이언트와 서버의 HTTP 버전이 다른 경우 호환 버전에 대한 참고 사항

포워딩 호환성

프런트엔드(client)에서는 HTTP/1.0 및 HTTP/1.1 이하 버전이 지원됩니다.
백엔드(server)에서 Tencent Cloud는 HTTP/1.0을 사용합니다. HTTP/1.0 및 HTTP/1.1 이하 버전이 지원됩니다.
주의사항:
HTTP/2는 HTTPS에서만 지원되지만 HTTP에서는 지원되지 않으며 client와 server 모두에서 이전 버전과의 호환성이 허용됩니다.

Gzip 호환성

프런트엔드(client)에서 Gzip은 HTTP/1.0, HTTP/1.1 이하 버전에서 지원됩니다. 메인 스트림 브라우저는 모두 Gzip을 지원하므로 추가 구성이 필요하지 않습니다.
백엔드(server)에서는 Tencent Cloud 사설망을 통해 CVM 인스턴스에서 HTTP/1.1을 지원하므로 구성할 필요가 없으며 기본적으로 Nginx에 구성된 HTTP/1.1을 직접 사용하여 호환성을 얻을 수 있습니다.
주의사항:

HTTP/2는 HTTPS에서만 지원되지만 Gzip은 Tencent Cloud에서 지원하는 모든 HTTP 버전에서 사용할 수 있습니다.

[맨 위로]

CLB 리얼 서버의 보안 그룹은 어떻게 설정하나요? 액세스 블록리스트를 구성하는 방법은 무엇입니까?

CLB 보안 그룹 구성

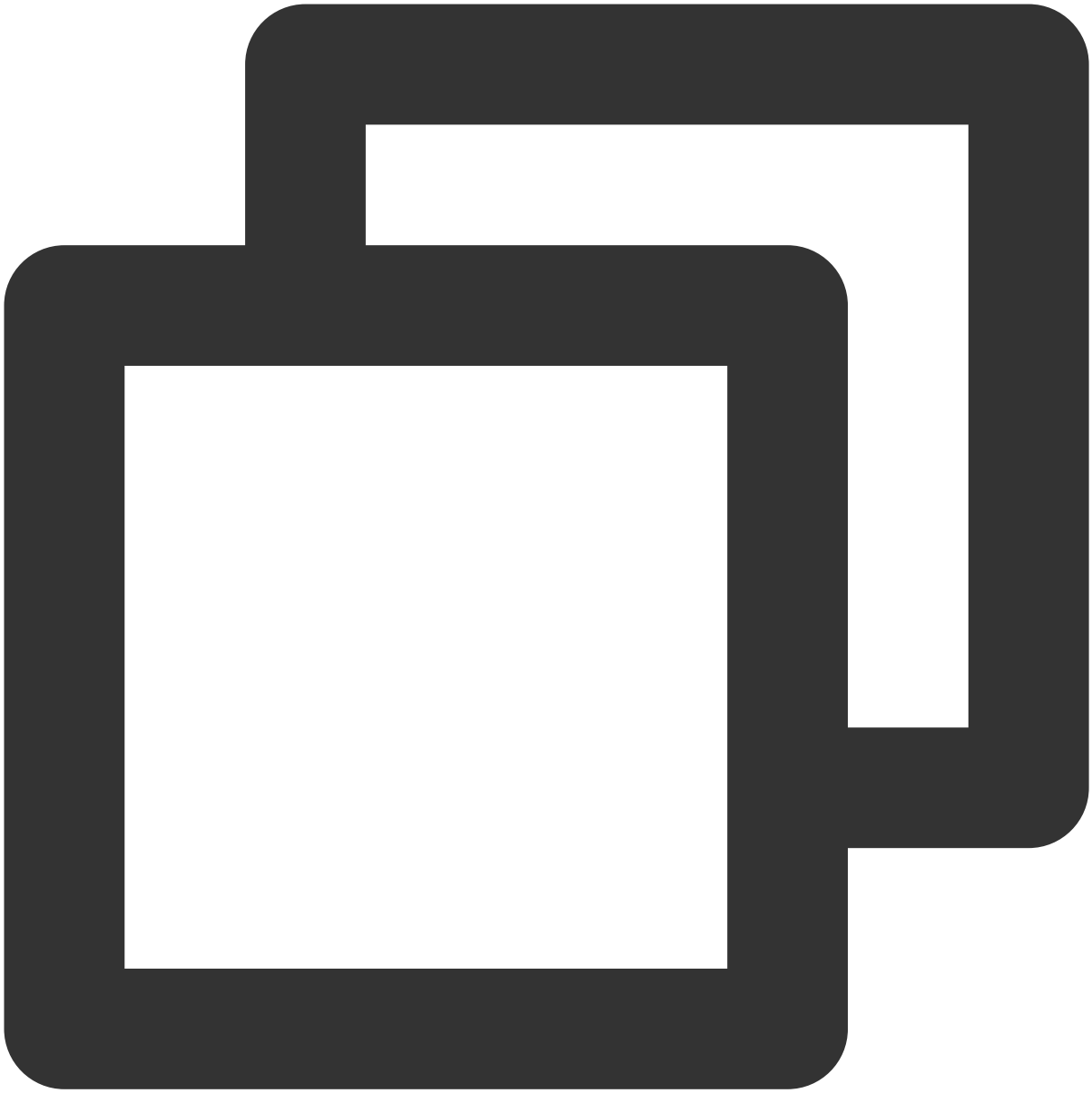
리얼 서버에 대해 보안 그룹 규칙이 구성된 경우 CLB 인스턴스가 서버와 통신하지 못할 수 있습니다. 따라서 레이어 4 및 레이어 7 포워딩 시 리얼 서버의 보안 그룹을 모든 액세스 요청을 허용하도록 설정하는 것을 권장합니다. 보안 그룹이 활성화되어 있고 기본적으로 모든 프로토콜 또는 IP 세그먼트에서 액세스가 허용되는 경우 모든 클라이언트의 IP를 서버 IP의 보안 그룹 규칙에 맞게 구성해야 합니다.
일부 악성 IP의 경우 보안 그룹의 최상위 규칙에 추가하여 리얼 서버에 액세스하지 못하도록 할 수 있습니다. 그런 다음 모든 IP(0.0.0.0)에서 로컬 서비스 포트로의 액세스 요청을 허용할 수 있으므로 일반 클라이언트가 서버에 액세스할 수 있습니다. 보안 그룹 규칙은 우선 순위에 따라 정렬되고 위에서 아래로 매칭됩니다.
VPC에서 레이어 7 CLB 포워딩에 대해 상태 확인이 구성된 경우 리얼 서버 보안 규칙에서 CLB VIP를 허용해야 합니다. 그렇지 않으면 상태 확인이 실패할 수 있습니다.

액세스 블록리스트 설정

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.

주의사항

아래 단계를 주어진 순서대로 엄격하게 따르십시오. 그렇지 않으면 블록리스트 구성이 실패할 수 있습니다.
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
```

보안 그룹에 대한 자세한 내용은 Configuring CVM Security Groups를 참고하십시오.

[맨 위로]

CLB 인스턴스는 사설망 또는 공중망을 통해 리얼 서버와 통신합니까?

바인딩된 CVM 인스턴스에 공중망 IP가 있는 경우에도 CLB 인스턴스는 항상 사설망을 통해 리얼 서버와 통신합니다.

[맨 위로]

CLB VIP Ping

CLB VIP에 대한 Ping 요청은 CLB 클러스터에서 응답하며 리얼 서버로 포워딩되지 않습니다.
공중망 CLB VIP를 Ping할 수 있습니다.
사설망 CLB의 VIP는 해당 VPC에서 오는 클라이언트 Ping만 지원하며, 다른 VPC나 로컬 IDC에서 오는 클라이언트 Ping은 대답이며 실제 링크를 반영할 수 없기 때문에 Ping을 보장할 수 없습니다. (예: CCN, 피어링 연결 등으로 VPC에 액세스하는 경우, Telnet을 사용하여 테스트하는 것이 좋습니다)

[맨 위로]

Telnet 명령을 실행하여 CLB 수신 포트 연결

레이어 4 리스너(TCP, UDP, TCP SSL)가 생성된 후 리얼 서버와 바인딩되지 않으면 Telnet 명령을 실행하여 수신 포트에 연결하는 데 실패합니다. 리얼 서버와 바인딩되면 성공합니다.
레이어 7 리스너(HTTP 및 HTTPS)를 생성한 후, 리얼 서버에 바인딩하지 않아도 Telnet 명령을 실행하여 수신 포트에 연결하면 CLB 인스턴스가 대신 응답합니다.

[맨 위로]

사설망 루프백

사설망 CLB 인스턴스의 경우 CVM은 클라이언트와 서버가 될 수 없습니다. CLB 인스턴스가 동일한 Client IP 및 Server IP를 읽으면 액세스가 실패합니다.
클라이언트를 서버로 사용해야 하는 경우 최소 2개의 리얼 서버를 바인딩하십시오. CLB에는 자동 루프백을 방지하기 위한 관련 정책이 있습니다. Client A가 CLB 인스턴스에 액세스하면 CLB 인스턴스는 Client A가 아닌 리얼 서버에 요청을 자동으로 스케줄링합니다.

[맨 위로]

클라이언트가 다른 중간 노드를 통해 리얼 서버의 동일한 포트에 액세스하는 경우 이러한 노드를 구체적으로 확인할 수 없습니다.

문제

클라이언트가 다른 중간 노드를 통해 동시에 리얼 서버의 동일한 포트에 액세스하는 경우 이러한 노드를 구체적으로

결정할 수 없습니다. 시나리오는 아래에 자세히 설명되어 있습니다.
클라이언트는 동일한 CLB 인스턴스의 레이어 4 및 레이어 7 리스너를 통해 동시에 리얼 서버의 동일한 포트에 액세스합니다.
클라이언트는 동시에 다른 CLB 인스턴스의 다른 리스너를 통해 리얼 서버의 동일한 포트에 액세스합니다.
리얼 서버의 공중망 CLB 인스턴스에 액세스하는 여러 클라이언트보다 리얼 서버의 사설망 CLB 인스턴스에 액세스하는 클라이언트에 대한 중간 노드를 결정하는 것이 더 복잡합니다.

문제 원인

CLB 인스턴스는 클라이언트 IP를 리얼 서버에 전달하고 `client_ip:client_port -> vip:vport -> rs_ip:rs_port` 는 `client_ip:client_port --> rs_ip:rs_port` 로 변경됩니다.

솔루션

분산 클라이언트: 액세스를 시작하는 데 여러 클라이언트가 사용됩니다.
더 적은 수의 CLB 인스턴스: 비즈니스 기능 및 재해 복구 요구 사항을 충족한다는 전제 하에 CLB 인스턴스 및 리스너의 수를 줄입니다.
분산 리얼 서버 포트: 리얼 서버의 여러 포트는 혼잡을 피하기 위해 서비스를 제공하는 데 사용됩니다.
분산 배포: 다른 CLB 인스턴스는 리얼 서버의 다른 포트에 바인딩됩니다. 예를 들어, 한 CVM 인스턴스 세트에 바인딩된 CLB 인스턴스 1과 다른 세트에 바인딩된 CLB 인스턴스 2에 동시에 액세스할 수 있습니다.

[맨 위로]

공중망의 액세스 트래픽을 차단하고 CLB 인스턴스의 액세스만 허용하도록 보안 그룹이 있는 백엔드 CVM 인스턴스를 구성했습니다. 그러나 적용되지 않습니다.

트래픽이 CLB 인스턴스를 통과하는 백엔드 CVM 인스턴스에 액세스할 수 있도록 하려면 백엔드 CVM 및 CLB 보안 그룹 모두에서 공중망의 트래픽을 허용해야 합니다. 먼저 백엔드 CVM 보안 그룹의 공중망을 통한 CLB VIP의 액세스 트래픽만 허용한 다음 필요에 따라 CLB 보안 그룹의 공중망 액세스 IP를 허용하는 것이 좋습니다.

[맨 위로]

리스너가 있는 CLB 인스턴스를 구성하고 리스너를 백엔드 CVM에 바인딩하고 도메인 이름을 백엔드 CVM의 IP로 확인했습니다. 그러나 도메인 이름에 액세스하면 모니터 데이터가 표시되지 않습니다.

CLB를 통과하는 트래픽만 모니터링됩니다. 도메인 이름을 CLB 인스턴스의 VIP로 확인하고 도메인 이름에 액세스하여 CLB 모니터링 정보를 볼 수 있습니다.

[맨 위로]

843 리스너를 생성하지 않았지만 Telnet 명령을 실행하여 연결할 수 있는 이유는 무엇입니까?

포트 843은 기본적으로 사용자가 Flash 액세스를 위해 포트를 재설정할 수 있도록 열려 있습니다. 닫고 싶다면 TCP:843 리스너를 설정한 후 리얼 서버를 바인딩하지 않으면 됩니다.

[맨 위로]

CLB 액세스 로그에 기록된 9/11 IP 범위의 주소가 Tencent Cloud 사설망 IP 범위입니까?

예. Tencent Cloud CLB 제품은 9/11 IP 범위의 주소를 사설망 IP 범위 주소로 사용합니다.

[맨 위로]

상태 확인 문제 해결

최종 업데이트 날짜: : 2024-01-04 20:22:15

Tencent Cloud CLB는 상태 확인을 통해 리얼 서버의 가용성을 확인할 수 있습니다. 상태 확인 예외가 발생하면 다음과 같이 문제를 해결할 수 있습니다.

설명:

상태 확인 중에 예외가 감지되면 CLB는 더 이상 예외적인 리얼 서버로 트래픽을 포워딩하지 않습니다.
상태 확인 중에 모든 리얼 서버에서 예외가 감지되면 요청이 모든 리얼 서버로 포워딩됩니다.
상태 확인 작동 방식에 대한 자세한 내용은 상태 확인을 참고하십시오.

리얼 서버의 공중망 대역폭 확인

기존 계정의 경우 계정의 대역폭 속성이 CLB가 아닌 CVM에 있으므로 CLB에 바인딩된 백엔드 CVM 인스턴스에 대해 공중망 대역폭을 구성해야 합니다. 그렇지 않으면 상태 확인 예외가 발생합니다.
표준 계정의 경우 CLB에 바인딩된 백엔드 CVM 인스턴스에 대해 공중망 대역폭을 구성할 필요가 없으며 CLB 서비스는 영향을 받지 않습니다.

설명

계정 유형을 확인하려면 Checking Account Type을 참고하십시오.
기존 계정에는 CLB 트래픽 또는 대역폭 요금이 부과되지 않습니다. CLB 서비스에서 발생하는 공중망 트래픽 요금은 바인딩된 백엔드 CVM 인스턴스에 의해 과금됩니다.
공중망 IP를 할당하지 않고 CVM 인스턴스에 대한 공중망 대역폭을 구입할 수 있습니다.

보안 그룹 구성 확인

CLB 인스턴스에서 보안 그룹에서 기본적으로 트래픽 허용 기능이 활성화되어 있는지 확인하고, 그렇지 않은 경우 CVM 인스턴스의 보안 그룹에서 원본 IP를 열어야 합니다. CLB 서비스가 모든 IP에서 액세스를 허용하도록 하려면 보안 그룹의 인바운드 규칙에서 원본 IP를 0.0.0.0/0으로 구성합니다. 자세한 내용은 Configuring CLB Security Group을 참고하십시오.

레이어 4 리스너 확인

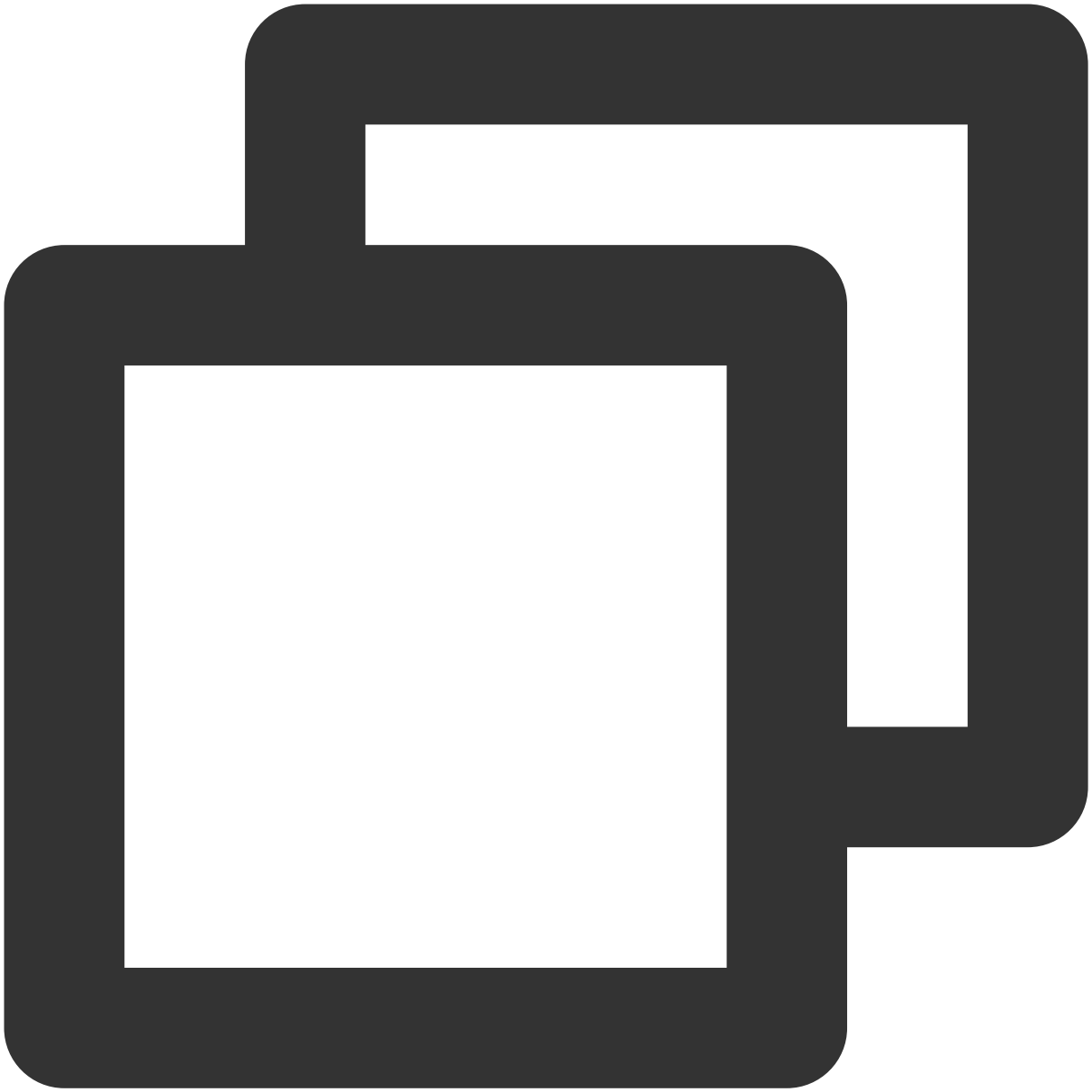
설명

TCP 프로토콜에서 CLB는 확인을 위해 SYN 패킷을 사용합니다.
UDP 프로토콜에서 CLB는 확인을 위해 `ping` 명령을 사용합니다.
페이지에 표시된 대로 CLB 리얼 서버 포트의 상태가 예외적인 경우 다음 단계에 따라 문제를 해결하십시오.

CLB 리얼 서버가 서비스에 영향을 미치는 보안 그룹으로 구성되어 있는지 확인하십시오. 리얼 서버는 보안 그룹을 통해 액세스를 제어하여 서비스의 정상적인 실행을 보장할 수 있습니다. 자세한 내용은 Configuring CVM Security Groups를 참고하십시오.
`netstat` 명령을 실행하여 리얼 서버 포트에서 수신 대기하는 프로세스가 있는지 확인합니다. 그러한 프로세스가 없으면 서비스를 다시 시작합니다.

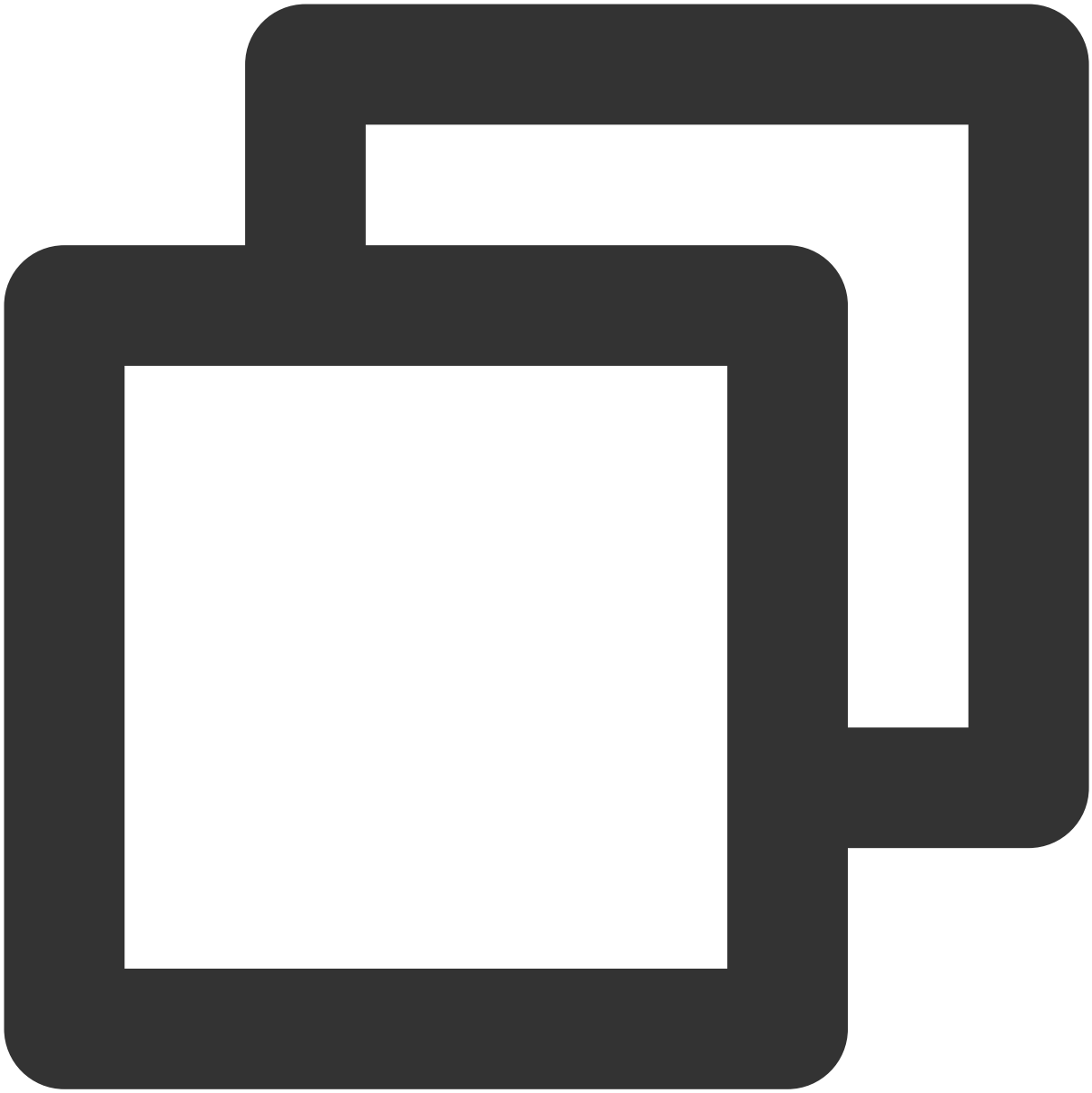
레이어 7 프로토콜 확인

레이어 7(HTTP 프로토콜) 서비스의 경우 상태 확인 중 리스너에 '예외'가 발생하면 다음 단계에 따라 문제를 해결할 수 있습니다.
CLB의 레이어 7 상태 확인 서비스는 사설망을 통해 백엔드 CVM 인스턴스와 통신하기 때문에 해당 사설망 주소에서 애플리케이션 서버 포트가 정상적으로 수신되는지 확인하기 위해서는 서버에 로그인이 필요하며, 그렇지 않은 경우 애플리케이션 서버 포트의 리스너를 사설망으로 이동하여 CLB와 백엔드 CVM 인스턴스 간의 정상적인 통신을 보장합니다.
CLB의 프런트엔드 포트와 CVM의 백엔드 포트가 모두 80이고 CVM의 사설망 IP가 `1.1.1.10` 이라고 가정합니다. Windows의 서버의 경우 다음 명령을 사용합니다.



```
netstat -ano | findstr :80
```

Linux의 서버의 경우 다음 명령을 사용합니다.



```
netstat -anp | grep :80
```

`1.1.1.10:80` 또는 `0.0.0.0:80` 에서 수신을 볼 수 있다면 구성이 정상입니다.

CLB 리스너에 구성된 백엔드 포트가 리얼 서버에서 활성화되었는지 확인하십시오.

레이어 4 CLB의 경우 백엔드 포트에 대한 `telnet` 이 응답하는 한 정상으로 간주됩니다. 테스트를 위해 `telnet 1.1.1.10 80` 을 사용할 수 있습니다.

레이어 7 CLB의 경우 200과 같은 HTTP 상태 코드가 반환되면 정상으로 간주됩니다. 확인 방법은 다음과 같습니다.

Windows에서는 CVM 인스턴스의 브라우저에 사설망 IP를 직접 입력하여 정상인지 테스트할 수 있습니다. 이 예시에서는 `http://1.1.1.10` 을 사용합니다.

Linux에서는 `curl -I` 명령을 실행하여 상태가 HTTP/1.1 200 OK인지 확인할 수 있습니다. 이 예시에서는 `curl -I 1.1.1.10` 명령을 사용합니다.
백엔드 CVM에 CLB의 로컬 IP 주소를 차단할 가능성이 있는 방화벽 또는 기타 보안 소프트웨어가 있는지 확인하십시오. 이로 인해 CLB가 리얼 서버와 통신할 수 없습니다.
서버의 사설망 방화벽이 포트 80의 통과를 허용하는지 확인하십시오. 테스트를 위해 방화벽을 일시적으로 비활성화할 수 있습니다.
Windows의 경우 'firewall.cpl' 명령을 실행하여 방화벽을 비활성화합니다.
Linux의 경우 `/etc/init.d/iptables stop` 명령을 실행하여 방화벽을 비활성화합니다(CentOS 7.x의 경우 `systemctl stop firewalld` 실행).
CLB의 상태 확인 매개변수가 올바르게 구성되었는지 확인합니다. Health Check Overview에 설명된 대로 기본 상태 확인 매개변수 값을 사용하는 것이 좋습니다.
상태 확인을 위해 지정한 테스트 파일은 반환된 결과만 확인하는 HTML 형식의 단순 페이지를 사용하는 것이 좋습니다. PHP와 같은 동적 프로그래밍 언어는 권장되지 않습니다.
백엔드 CVM 인스턴스의 부하가 높아 응답이 느린지 확인합니다.
HTTP 요청 방법을 확인합니다.
HEAD를 사용하는 경우 리얼 서버는 HEAD를 지원해야 합니다.
GET을 사용하는 경우 리얼 서버는 GET을 지원해야 합니다.
TCP 고속 재활용(tcp_tw_recycle)과 타임스탬프(tcp_timestamps)가 모두 활성화된 경우 상태 확인이 예외적일 수 있습니다. tcp_tw_recycle을 비활성화하는 것이 좋습니다. 자세한 내용은 Cause Analysis를 참고하십시오.

높은 상태 확인 빈도

상태 확인 패킷은 콘솔에 구성된 대로 5s마다 전송되지만 리얼 서버는 1s 이내에 하나 또는 여러 개의 상태 확인 요청이 수신되는 것을 찾습니다. 이 문제는 주로 CLB 리얼 서버 상태 확인의 구현 메커니즘과 관련이 있습니다.
Client의 100만 요청이 리얼 서버로 전송되기 전에 4개의 CLB 리얼 서버에 배포된다고 가정합니다. 각 CLB 리얼 서버는 개별적으로 상태 확인을 수행합니다. CLB 인스턴스가 5s마다 상태 확인 요청을 보내도록 구성된 경우 각 CLB 리얼 서버는 5s마다 상태 확인 요청을 보냅니다. 따라서 리얼 서버는 5s 동안 4개의 상태 확인 요청을 수신할 수 있습니다.

이 방식의 장점은 높은 효율, 정확한 검사, 잘못된 삭제 방지입니다. 예를 들어, CLB 인스턴스 클러스터에 있는 8개의 물리적 서버 중 하나가 실패하더라도 나머지 7개의 서버는 여전히 정상적으로 트래픽을 포워딩할 수 있습니다.

귀하의 비즈니스가 부하에 민감한 경우 매우 빈번한 상태 확인이 정상적인 비즈니스 액세스에 영향을 미칠 수 있습니다. 이 경우 확인 간격을 늘려 영향을 줄일 수 있습니다(예: 15s에 한 번 상태 확인 수행).

리얼 서버가 여러 CLB 인스턴스에 바인딩된 경우 각 CLB 인스턴스는 서버의 정상 여부를 감지하기 위해 상태 감지 메시지를 전송하므로 상태 감지 빈도가 높아집니다.

HTTPS

최종 업데이트 날짜: : 2024-01-04 20:22:28

HTTP 정보

인증서 정보

HTTPS는 어떤 암호 제품군을 지원합니까?

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-CHACHA20-POLY1305:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128:AES256:AES:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK

[상단으로 이동]

HTTPS는 어떤 버전의 SSL/TLS 보안 프로토콜을 지원합니까?

CLB HTTPS에서 지원하는 ssl_protocols에는 TLSv1, TLSv1.1, TLSv1.2 및 TLSv1.3이 있습니다.

[상단으로 이동]

HTTPS 수신에 사용할 수 있는 포트는 무엇입니까?

포트 443을 권장합니다. 필수 사항은 아닙니다.
[상단으로 이동]

HTTPS 양방향 인증이 필요한 이유는 무엇입니까?

금융 서비스 제공 업체와 같은 일부 사용자는 데이터 보안에 대해 더 높은 요구 사항을 가지고 있습니다. 서버와 클라이언트 모두에서 HTTPS 인증이 필요합니다. 그들의 요구를 충족시키기 위해 HTTPS 양방향 인증이 제공됩니다.
[상단으로 이동]

HTTPS가 실제로 청구된 트래픽보다 더 많은 트래픽을 생성하는 이유는 무엇입니까?

HTTPS 프로토콜을 사용하는 경우 일부 트래픽이 프로토콜 핸드셰이크에 사용되기 때문에 실제로 청구된 트래픽보다 더 많은 트래픽이 생성됩니다.
[상단으로 이동]

HTTPS 리스너가 추가된 후에도 CLB 인스턴스에서 리얼 서버로의 요청이 HTTP를 통해 계속 전송됩니까?

예. HTTPS 리스너가 추가된 후 클라이언트에서 CLB 인스턴스로의 요청은 HTTPS를 통해 암호화되지만 CLB 인스턴스에서 리얼 서버로의 요청은 여전히 HTTP를 통해 전송됩니다. 따라서 리얼 서버에서 SSL을 구성할 필요가 없습니다.
[상단으로 이동]

CLB는 현재 어떤 유형의 인증서를 지원합니까?

CLB는 서버 인증서 및 CA 인증서 업로드를 지원합니다. 서버 인증서의 경우 인증서 내용과 개인 키를 업로드해야 합니다. CA 인증서의 경우 인증서 내용만 업로드하면 됩니다. 두 인증서 모두 PEM 인코딩 형식으로만 업로드할 수 있습니다.
[상단으로 이동]

리스너가 바인딩할 수 있는 HTTPS 인증서는 몇 개입니까?

HTTPS 단방향 인증을 사용하는 경우 하나의 서버 인증서만 리스너에 바인딩할 수 있습니다. HTTPS 양방향 인증을 사용하는 경우 하나의 서버 인증서와 하나의 CA 인증서를 수신기에 바인딩해야 합니다.
[상단으로 이동]

인증서 하나를 적용할 수 있는 클라우드 로드 밸런서 및 리스너는 몇 개입니까?

인증서는 하나 이상의 클라우드 로드 밸런서 또는 여러 리스너에 적용할 수 있습니다.
[상단으로 이동]

인증서를 어떻게 업로드합니까?

API를 호출하거나 CLB 콘솔을 통해 업로드할 수 있습니다.
[상단으로 이동]

인증서는 리전에 따라 달라지나요?

아니요. 인증서를 구매하여 발급한 후에는 설치 및 배포가 리전별로 제한되지 않습니다.
[상단으로 이동]

백엔드 CVM 인스턴스에 인증서를 업로드해야 합니까?

아니요. CLB HTTPS는 사용자 인증서를 관리하고 저장하기 위한 인증서 관리 시스템을 제공합니다. 백엔드 CVM 인스턴스에 인증서를 업로드할 필요가 없으며 인증서 관리 시스템에 업로드된 모든 개인 키는 암호화된 방식으로 저장됩니다.
[상단으로 이동]

인증서가 만료된 후에는 어떻게 해야 합니까?

인증서를 수동으로 업데이트해야 합니다.
[상단으로 이동]

인증서 오류가 발생하면 어떻게 해야 합니까?

잘못된 개인 키 때문에 오류가 발생할 수 있습니다. 인증서를 비즈니스 요구 사항을 충족하는 새 인증서로 교체해야 합니다.
[상단으로 이동]

WS/WSS 프로토콜 지원

최종 업데이트 날짜: : 2024-01-04 20:22:43

제품 소개

제품 구매

제품 구현

WS/WSS란 무엇입니까?

WebSocket(WS)은 단일 TCP 연결을 통해 전이중(full-duplex) 통신 채널을 제공하는 프로토콜입니다.
WebSocket은 클라이언트와 서버 간의 데이터 교환을 용이하게 하고 서버에서 클라이언트로 능동적인 데이터 푸시를 허용합니다. WebSocket API에서는 브라우저와 서버 간에 한 번의 핸드셰이크만 있으면 영구 연결을 생성하고 양방향 데이터 전송을 수행할 수 있습니다.
[상단으로 이동]

왜 WS/WSS를 사용해야 하나요?

WebSocket이 없으면 클라이언트는 폴링을 통해 서버에서 데이터를 가져와야(Pull) 합니다.
이 데이터 교환 방법에는 두 가지 단점이 있습니다.
1. 효율이 낮습니다. 실시간 데이터를 가져오려면 클라이언트가 Ajax 요청을 자주 시작해야 합니다.
2. 서버는 데이터를 사전에 푸시(Push)할 수 없습니다.
WebSocket은 이러한 문제를 해결하기 위해 설계되었습니다. HTML5 출시와 함께 출시된 새로운 프로토콜인 WebSocket은 브라우저와 서버 간의 전이중(full-duplex) 통신을 구현합니다. 메시지 기반 텍스트 및 이진법 데이터를 전송하여 프로토콜 레벨에서 HTTP 문제를 해결할 수 있습니다.
WebSocket의 주요 이점:
1. 오버헤드가 적습니다. 연결이 설정된 후 제어에 사용되는 패킷 헤더는 작습니다. 완전한 헤더가 필요한 HTTP 요청에 비해 WebSocket은 오버헤드를 줄이는 데 도움이 됩니다.
2. 실시간성이 높습니다. 전이중 프로토콜로서 WebSocket은 서버에서 클라이언트로 실시간 데이터 푸시를 달성할 수 있습니다.
3. 연결이 지속적입니다.

[상단으로 이동]

WS/WSS는 어떻게 과금되나요?

CLB는 기본적으로 WS/WSS를 지원하며 추가 비용을 청구하지 않습니다.

[상단으로 이동]

CLB용 WS/WSS를 어떻게 활성화합니까?

CLB는 기본적으로 WS/WSS가 활성화되어 있습니다. 연결이 60s 이상 유휴 상태인 경우 `proxy_read_timeout` 매개변수를 사용자 지정해야 합니다. 이 매개변수는 900s 미만인 것이 좋습니다. 자세한 내용은 레이어 7 사용자 정의 구성을 참고하십시오.

리스너가 HTTP를 수신하는 경우 기본적으로 WS가 지원됩니다. HTTPS를 수신하는 경우 기본적으로 WSS가 지원됩니다.

WSS를 사용하는 경우 CLB는 SSL 오프로딩을 수행합니다.

[상단으로 이동]

WS/WSS를 지원하는 리전은 어디인가요?

현재 WS/WSS 프로토콜은 **모든 리전**에서 지원됩니다.

[상단으로 이동]

HTTP/2 프로토콜 지원

최종 업데이트 날짜: : 2024-01-04 20:22:54

제품 내용물

HTTP/2란 무엇입니까?

HTTP/2(Hypertext Transfer Protocol 버전2)는 웹 서비스에서 사용되는 HTTP 프로토콜의 주요 버전입니다.
HTTP/2는 HTTP1.X의 성능 문제를 해결하도록 설계되어 네트워크 리소스를 더 잘 활용하고 네트워크 어플리케이션의 지연 시간을 줄일 수 있습니다.
HTTP/2는 HTTP1.X와 역호환됩니다.

HTTP/2를 사용해야 하는 이유

HTTP/2는 HTTP1.X보다 더 빠른 응답성과 효율성을 제공하며 다음과 같은 이점을 제공합니다.
멀티플렉싱: 동시 처리가 더 빠른 응답성을 제공합니다.
서버 푸시: 서버가 클라이언트에 필요한 자원을 적극적으로 푸시하여 요청 수를 줄입니다.
흐름 제어, 요청 우선 순위, 헤더 압축, 이진 프레임 등의 다양한 기능이 있습니다.

제품 구매

CLB는 어떻게 유료인가요?

CLB는 기본적으로 추가 비용 없이 HTTP/2 프로토콜을 지원합니다.

제품 구현

CLB에서 HTTP/2를 활성화하려면 어떻게 해야 합니까?

기본적으로 리스너는 추가 구성 없이 HTTPS에서 HTTP/2를 지원합니다..
HTTPS 핸드셰이크 중에 프로토콜 버전을 협상해야 합니다. 클라이언트는 프로토콜 목록에 따라 HTTP/2 또는 HTTP1.X를 선택하고 추가 구성 없이도 ALPN(Application Layer Protocol Collaboration)을 사용하여 서버에서 지원하는 프로토콜 목록을 통지합니다.

> **참고:**

1. 일반 HTTP/2는 지원되지 않습니다. 메인스트림(Mainstream) 브라우저 및 웹 서버는 TLS 기반 HTTP/2 프로토콜만 지원합니다.
2. CLB와 실제 서버 간에는 여전히 HTTP1.X 프로토콜을 사용합니다.

어떤 영역이 HTTP/2를 지원합니까?

베이징, 상하이, 광저우, 홍콩(중국), 실리콘 밸리 및 프랑크푸르트 지역에서 HTTP/2를 지원합니다.