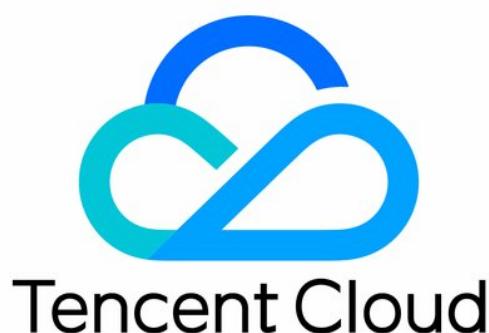


TDSQL for MySQL

운영 가이드 (InnoDB)

제품 문서



저작권 고지

©2013-2025 Tencent Cloud. 모든 권리 보유.

본 문서의 저작권은 텐센트 클라우드(Tencent Cloud)에 단독으로 귀속됩니다. 텐센트 클라우드의 사전 서면 승인 없이는 어떠한 주체도 본 문서 내용의 전부 또는 일부를 복제·수정·표절·전송하는 등 어떠한 형태로도 이용할 수 없습니다.

상표 고지



텐센트 클라우드(Tencent Cloud) 및 관련 서비스의 모든 상표는 텐센트(Tencent) 그룹 산하 법인들(모회사, 자회사 및 계열사 포함)이 소유합니다. 본 문서에 언급된 제3자 상표는 해당 법적 권리자가 소유합니다.

서비스 고지

본 문서는 고객에게 텐센트 클라우드(Tencent Cloud) 제품 및 서비스 전부 또는 일부에 대한 현재적 개괄적 정보를 제공하기 위한 것으로, 특정 제품·서비스의 내용은 수시로 변경될 수 있습니다. 고객이 실제 구매한 제품·서비스의 적용 기준은 고객과 텐센트 클라우드간 체결된 상업계약에 명시된 내용이 우선하며, 별도 서면 합의가 없는 한 텐센트 클라우드는 본 문서 내용에 대해 법적 효력이 있는 명시적·묵시적 진술이나 보증을 일체 하지 않습니다.

목록:

운영 가이드 (InnoDB)

인스턴스 관리

인스턴스 격리, 복원 및 종료

인스턴스 재시작

재해 복구/읽기 전용 인스턴스

네트워크 수정

계정 관리

계정 생성

계정 권한 수정

계정 클론

읽기/쓰기 분리 설정

계정 비밀번호 재설정

계정 삭제

보안 관리

액세스 관리

개요

정책 구조

리소스 수준 권한 지원

콘솔 예시

CAM 지원 작업

보안 그룹 설정

TDE 데이터 암호화

슬로우 쿼리 분석

백업과 룰백

백업 방식

백업 파일 다운로드

백업 암호화

데이터베이스 룰백

데이터 마이그레이션

데이터베이스 감사

데이터베이스 감사 활성화

감사 로그 조회

로그 저장 기간 수정

운영 가이드 (InnoDB)

인스턴스 관리

인스턴스 격리, 복원 및 종료

최종 업데이트 날짜: 2024-01-06 15:18:59

인스턴스 격리

더 이상 사용하지 않을 때 인스턴스를 격리할 수 있습니다. 일단 격리되면 인스턴스를 사용하거나 액세스할 수 없으며(아직 제거되지는 않음) 휴지통으로 이동되어 복구하거나 제거할 수 있습니다. 그렇지 않으면 만료되면 자동으로 제거됩니다. 인스턴스가 격리되더라도 해당 리소스가 차지하는 공간은 해제되지 않으며 여전히 가장 기본적인 데이터 복제본이 있습니다.

- 종량제 인스턴스: [콘솔](#)에 로그인하고 인스턴스 목록에서 종량제 인스턴스를 선택한 다음 **폐기/반환**을 클릭하여 수동으로 반환할 수 있습니다. 인스턴스가 반환된 후에는 **격리됨** 상태가 되며 액세스할 수 없는 3일 동안 유지됩니다. 복구하려면 휴지통 목록에서 복구할 수 있습니다.

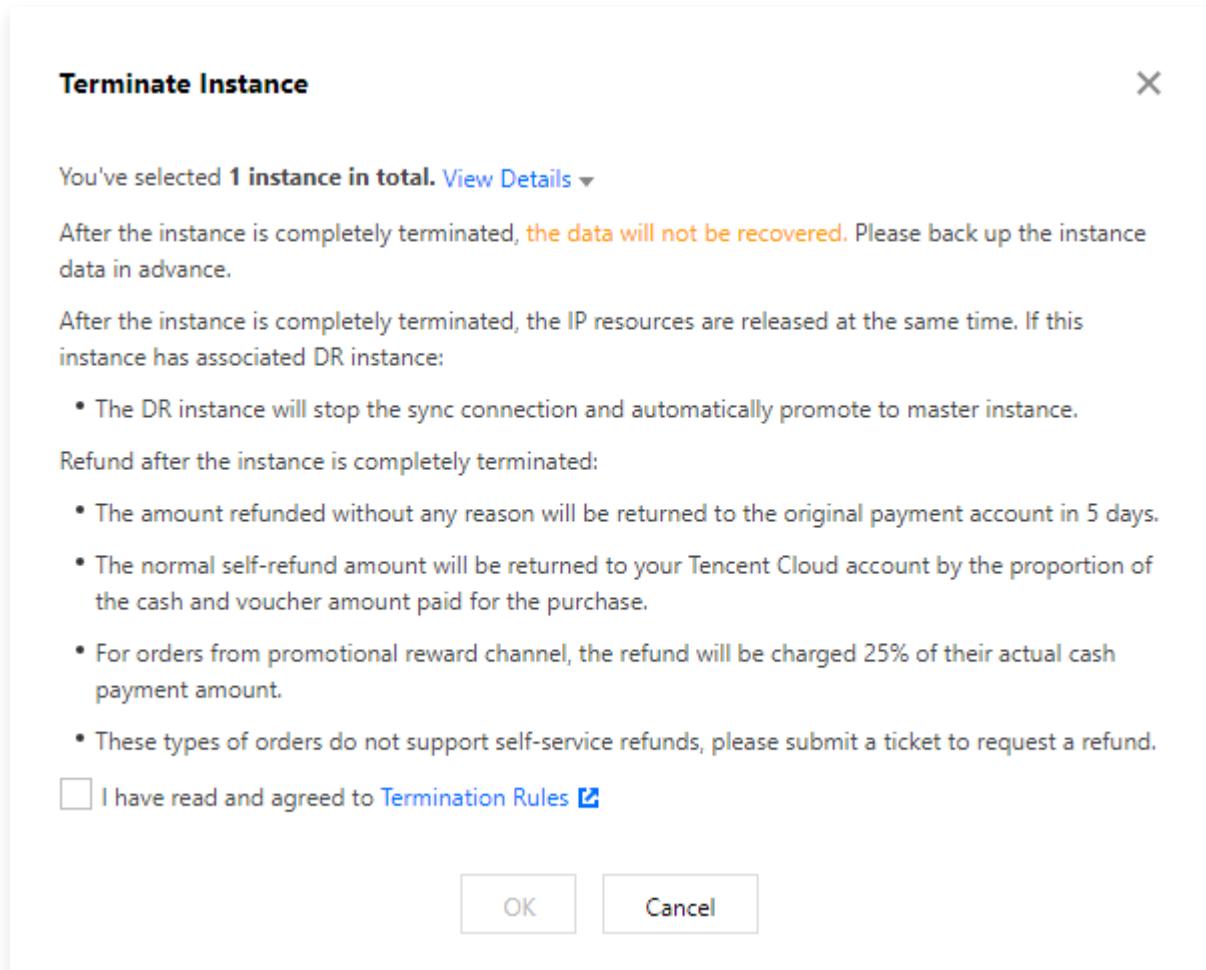
인스턴스가 반환된 후 상태가 **격리됨**으로 변경되면 관련 요금이 발생하지 않습니다.

⚠ 주의 사항:

- 인스턴스가 격리되면 해당 IP가 해제되며 인스턴스가 복구된 후에는 원래 IP를 되찾지 못할 수 있습니다.
- 인스턴스가 격리된 후에는 업그레이드, 매개변수 수정, 계정 생성 또는 수정, 롤백 또는 이름 변경이 불가능합니다.

작업 단계

- [TDSQL for MySQL 콘솔](#)에 로그인합니다. 인스턴스 목록에서 인스턴스를 선택하고 상단의 **더보기>폐기/반환**을 클릭합니다.
- 팝업 창에서 동의를 선택한 뒤, **확인**을 클릭합니다.



휴지통으로 이동하면 인스턴스가 **격리됨** 상태인 것을 확인할 수 있습니다.

인스턴스 복구

격리된 인스턴스는 정상 실행 상태로 복구할 수 있습니다. 복구까지 몇 분 정도 소요될 수 있습니다. 복구된 인스턴스는 격리 전의 원래 IP가 아닌 새 IP를 가질 수 있습니다.

작업 단계

1. [TDSQL for MySQL 콘솔](#)에 로그인하고 휴지통 목록에서 인스턴스를 찾은 다음 **복구/시작**을 클릭합니다.
2. 팝업 창에서 **확인**을 클릭합니다.

인스턴스 폐기

더 이상 인스턴스가 필요하지 않으면 반환할 수 있습니다. 반환되면 **격리됨** 상태가 되며 휴지통으로 이동되어 만료되면 자동으로 제거됩니다. 또는 **지금 완전 삭제**를 클릭하여 완전히 종료할 수 있습니다.

주의 사항

- 인스턴스가 제거된 후에는 해당 데이터를 복구할 수 없습니다. 데이터를 미리 백업하십시오.
- 인스턴스가 제거되면 해당 IP 리소스가 동시에 해제되고 재해 복구 인스턴스는 동기화 연결을 중지하고 기본

인스턴스로 자동 승격됩니다.

인스턴스 재시작

최종 업데이트 날짜: 2024-01-06 15:18:59

본문은 콘솔에서 인스턴스를 재시작하는 방법을 설명합니다.

작업 시나리오

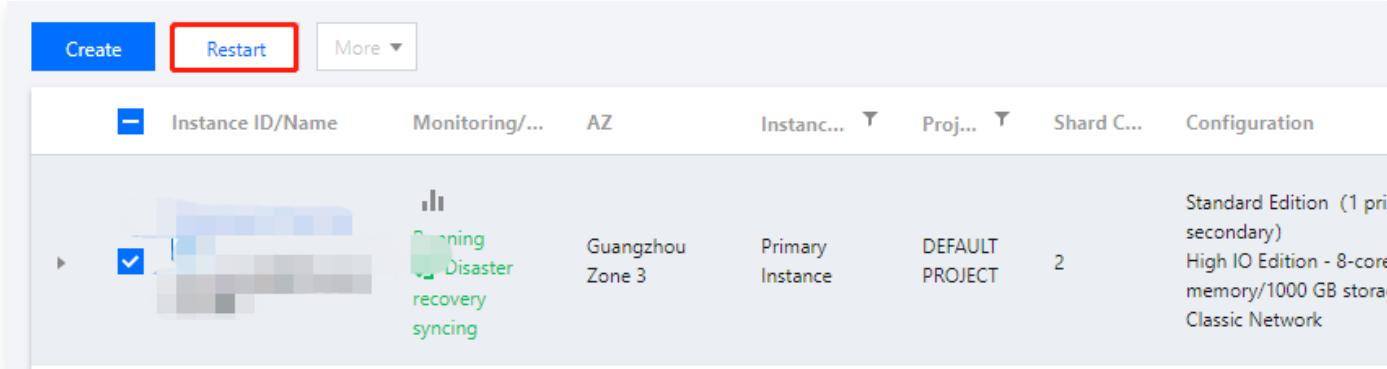
인스턴스 재시작은 TDSQL for MySQL의 일반적인 유지 관리 방법이며 로컬 데이터베이스를 재시작하는 것과 유사합니다.

주의 사항

- 재시작 준비:** 재시작하는 동안 인스턴스는 서비스를 제공할 수 없습니다. 따라서 재시작하기 전에 TDSQL for MySQL이 비즈니스 요청 수락을 중지했는지 확인하십시오. 다시 시작하는 동안 비즈니스 쓰기 볼륨이 높으면 더티 페이지가 생성됩니다. 이 경우 업무 중단을 줄이기 위해 재시작에 실패할 수 있습니다.
- 재시작 방법:** 인스턴스에서 재시작 명령을 실행하는 대신 Tencent Cloud에서 제공하는 단계에 따라 인스턴스를 다시 시작하는 것이 좋습니다.
- 재시작 시간:** 일반적으로 인스턴스를 다시 시작하는 데 몇 분 밖에 걸리지 않습니다.
- 물리적 인스턴스 기능:** 인스턴스를 재시작해도 물리적 기능이나 사설 IP는 변경되지 않습니다.

작업 단계

- TDSQL for MySQL 콘솔에 로그인하고 인스턴스 목록에서 하나 이상의 인스턴스를 선택하고 상단에서 **재시작**을 클릭합니다.



- 팝업 창에서 모든 정보가 올바른지 확인하고 **확인**을 클릭하여 단일 인스턴스 또는 여러 인스턴스를 일괄 재시작합니다.

재해 복구/읽기 전용 인스턴스

최종 업데이트 날짜: 2024-01-06 15:18:59

본 문서에서는 콘솔에서 재해 복구/읽기 전용 인스턴스를 만들고 관리하는 방법을 설명합니다.

작업 시나리오

TDSQL for MySQL은 가용존/리전 간 재해 복구 읽기 전용 인스턴스를 제공하여 서비스 연속성, 데이터 안정성 및 규정 준수 요구 사항이 더 높은 애플리케이션에 대한 데이터 안정성을 개선하는 동시에 저렴한 비용으로 지속적인 서비스를 제공할 수 있도록 지원합니다.

설명:

재해 복구/읽기 전용 인스턴스 요금은 원본 인스턴스와 동일합니다. [제품 가격](#)을 참고하십시오.

적용 시나리오

- 원격 재해 복구: 데이터 보안을 보장하기 위해 재해 복구 인스턴스를 사용하여 여러 리전의 비즈니스 및 데이터를 백업할 수 있습니다. 가용존/리전 장애로 인해 인스턴스를 사용할 수 없게 된 경우 가용존/리전 간 재해 복구 인스턴스로 신속하게 전환하여 비즈니스에 미치는 영향을 최소화할 수 있습니다.
- 근거리 액세스: 특정 가용존의 인스턴스를 원본 인스턴스로 사용하고 다른 가용존/리전의 인스턴스를 읽기 전용 인스턴스로 사용할 수 있어 사용자에게 근거리 액세스, 원격 읽기 기능 및 향상된 액세스 속도를 제공합니다.
- 다중 리전 배포: TDSQL for MySQL 인스턴스는 여러 지역에 배포할 수 있습니다. 인스턴스가 가용존/리전에서 네트워크 변동 또는 가용성이 없는 경우 비즈니스 요구 사항에 따라 다른 가용존/리전으로 전환할 수 있습니다.

기능

- 재해 복구/읽기 전용 인스턴스는 읽기 전용 액세스를 위해 별도의 데이터베이스 연결 주소를 제공합니다. 더 낮은 비용의 장치 이종화로 근거리 액세스 및 데이터 분석에 사용할 수 있습니다.
- 원본 인스턴스는 다른 리전 및 가용존에 배포할 수 있는 재해 복구 읽기 전용 인스턴스 하나를 생성할 수 있습니다.
- 재해 복구/읽기 전용 인스턴스는 고가용성(1-원본-1-복제본 및 1-원본-2-복제본) 아키텍처를 지원하여 데이터베이스에 대한 단일 장애점을 방지합니다.
- 원본 인스턴스가 실패하면 재해 복구/읽기 전용 인스턴스가 몇 초 만에 활성화되어 전체 읽기/쓰기 기능을 제공할 수 있습니다.
- 재해 복구/읽기 전용 인스턴스의 데이터는 공용 네트워크보다 대기 시간이 짧고 안정성이 뛰어난 사설망을 통해 동기화됩니다.
- 현재는 프로모션 기간으로 전용 회선 트래픽을 무상으로 이용할 수 있습니다. 상용화 후 요금 부과 시 별도로

공지합니다.

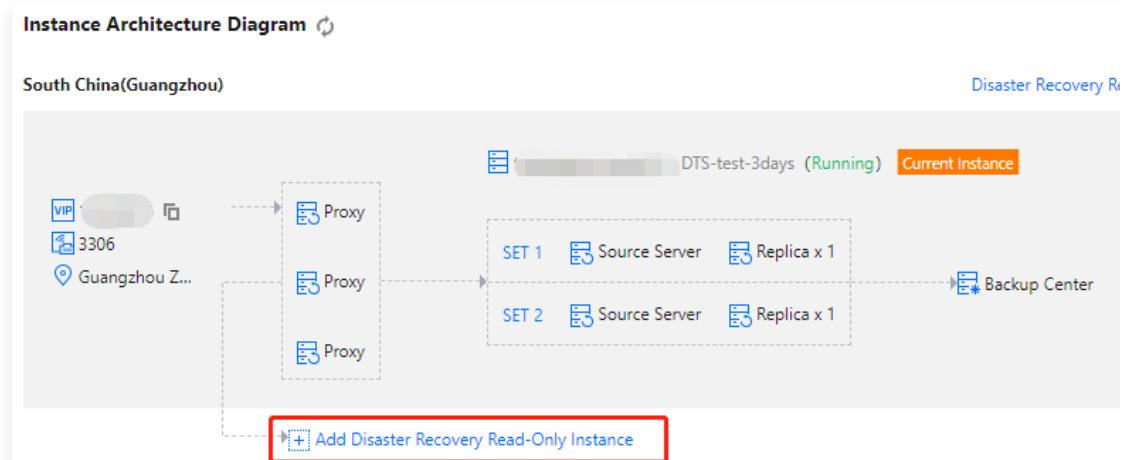
기능 제한

- 재해 복구/읽기 전용 인스턴스는 매개변수 설정 및 계정 관리 기능을 지원하지 않습니다.
- 재해 복구/읽기 전용 인스턴스의 데이터베이스 버전은 기본적으로 원본 인스턴스와 동일합니다. 인스턴스 사양 및 디스크 크기는 원본 인스턴스보다 크거나 같아야 합니다.

작업 단계

재해 복구/읽기 전용 인스턴스 생성

1. [TDSQL for MySQL 콘솔](#)에 로그인한 후, 인스턴스 목록에서 인스턴스 ID를 클릭하여 인스턴스 관리 페이지로 이동합니다.
2. 인스턴스 세부 정보 페이지의 인스턴스 아키텍처 다이어그램에서 **재해 복구/읽기 전용 인스턴스 추가**를 클릭합니다.



3. 구매 페이지에서 재해 복구/읽기 전용 인스턴스의 청구 모드, 리전 및 기타 기본 정보를 선택하고 **구매하기**를 클릭합니다.

설명:

- 생성을 완료하는 데 필요한 시간은 데이터 양에 따라 다르며 생성 중에는 콘솔의 원본 인스턴스에 대해 어떤 작업도 수행할 수 없습니다. 적절한 시기에 하는 것이 좋습니다.
- 현재 전체 인스턴스 데이터 동기화만 지원합니다. 디스크 용량이 충분한지 확인하십시오.
- 원본 인스턴스가 실행 중 상태이고 실행 중인 작업이 없는지 확인합니다. 그렇지 않으면 동기화 작업이 실패할 수 있습니다.

4. 결제 후 인스턴스 목록으로 돌아가 인스턴스를 초기화하면 다음 작업을 진행할 수 있습니다.

재해 복구/읽기 전용 인스턴스 관리

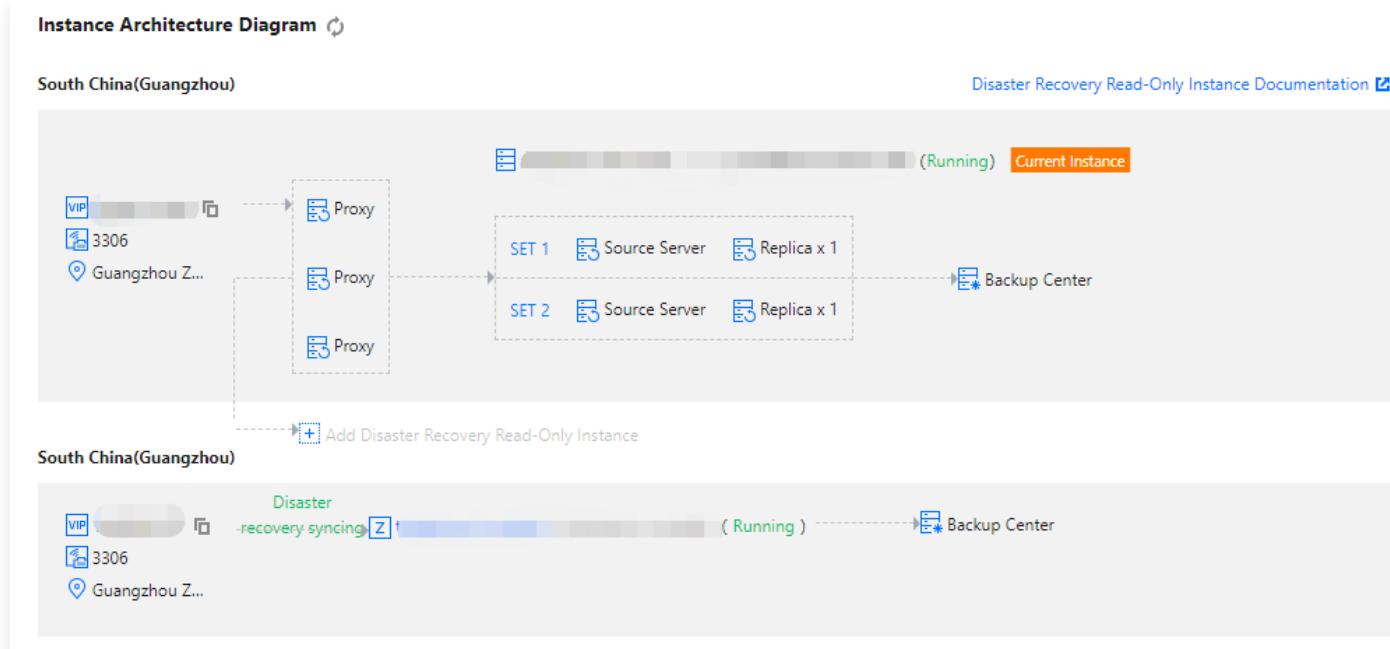
• 재해 복구/읽기 전용 인스턴스 보기

재해 복구/읽기 전용 인스턴스가 있는 리전에서 보고, 인스턴스 목록에서 필터링할 수 있습니다.

<input type="checkbox"/> Instance ID/Name	Monitoring/St...	AZ	Instance ...	Project	Shard Qua...	C
<input type="checkbox"/> [REDACTED]	Running	Guangzhou Zone 6	<input type="checkbox"/> All	<input type="checkbox"/> Source (Dedicated Cluster)	<input type="checkbox"/> Source Instance	<input type="checkbox"/> Disaster Recovery Read-Only Instance
<input type="checkbox"/> [REDACTED]	Disaster	Guangzhou Zone 3	<input type="checkbox"/> Disaster Recovery Read-Only Instance (Dedicated)	<input type="button" value="OK"/>	<input type="button" value="Reset"/>	

• 원본 인스턴스와 재해 복구 읽기 전용 인스턴스 간의 관계 보기

인스턴스 세부 정보 페이지의 인스턴스 아키텍처 다이어그램에서 원본 인스턴스와 재해 복구 읽기 전용 인스턴스 간의 관계를 볼 수 있습니다.



- **재해 복구 읽기 전용 인스턴스 기능**

재해 복구/읽기 전용 인스턴스는 인스턴스 세부 정보, 샤프 관리, 모니터링 및 알람, 매개변수 설정, 데이터 보안, 백업 및 복원, 성능 최적화 기능을 제공합니다.

재해 복구/읽기 전용 인스턴스를 원본 인스턴스로 업그레이드

필요에 따라 재해 복구/읽기 전용 인스턴스를 콘솔에서 원본 인스턴스로 전환할 수 있습니다.

1. [TDSQL for MySQL 콘솔](#)에 로그인하여 인스턴스 목록에서 타깃 재해 복구/읽기 전용 인스턴스를 선택한 후 인스턴스 ID를 클릭하여 인스턴스 관리 페이지로 들어갑니다.
2. 오른쪽 상단 모서리에 있는 **원본 인스턴스로 전환**을 클릭하여 재해 복구/읽기 전용 인스턴스를 원본 인스턴스로 업그레이드합니다. 전환 후에는 원본 인스턴스와의 동기화 링크가 연결 해제되어 업그레이드된 인스턴스가 데이터 쓰기 기능과 전체 TDSQL for MySQL 기능을 사용할 수 있습니다.

⚠ 주의 사항:

동기화 연결이 끊어지면 재연결할 수 없습니다. 작업 시 주의하십시오.

네트워크 설정

최종 업데이트 날짜: 2024-01-06 15:18:59

본문은 인스턴스 네트워크 유형을 변경하고 인스턴스 액세스 주소를 수정하는 방법을 설명합니다.

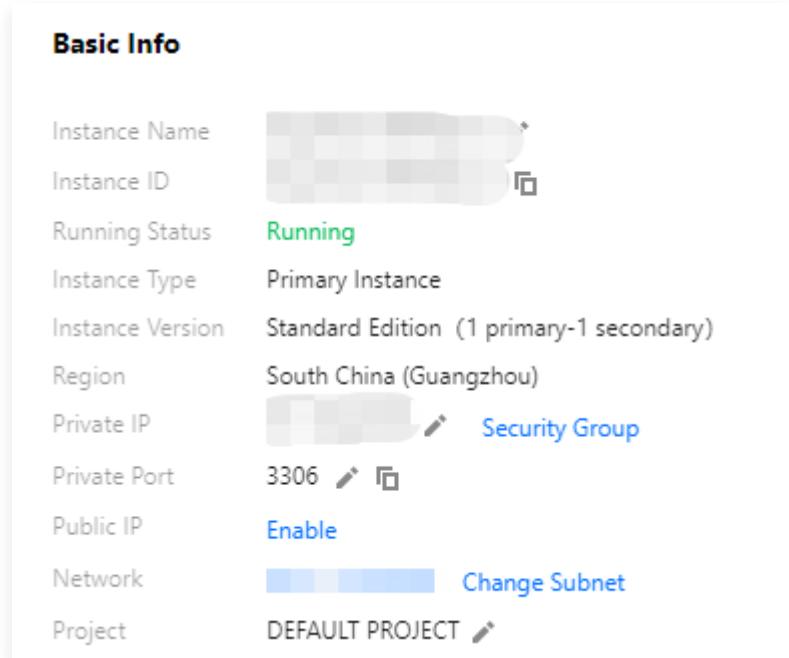
⚠ 주의 사항:

인스턴스의 네트워크 구성을 수정하는 것은 매우 위험합니다. 사용량이 적은 시간에만 수행하십시오. 수정 후, 기존 IP를 다른 서비스에 할당하거나 사용자 지정 IP 회수 시간을 설정하지 않는 한, 기본적으로 기존 IP는 24시간 동안 유효합니다. 가능한 빨리 비즈니스 구성을 적절하게 수정하는 것이 좋습니다.

사설망 주소 수정

VPC에서 TencentDB 인스턴스의 사설망 주소를 수정할 수 있습니다.

1. [TDSQL for MySQL 콘솔](#)에 로그인하고 인스턴스 리스트에서 인스턴스 ID를 클릭하여 인스턴스 세부 정보 페이지로 들어갑니다.
2. 인스턴스 세부 정보 페이지에서 **사설망 주소** 옆에 있는 을(를) 클릭하여 수정합니다. 현재 서브넷에 사용 가능한 IP가 있는 경우에만 그렇게 할 수 있습니다.



3. 팝업 창에서 사설망 주소를 수정하고 **확인**을 클릭합니다.

VPC 서브넷 간 전환

VPC 서브넷 간에 TDSQL for MySQL 인스턴스의 네트워크를 전환할 수 있습니다.

1. [TDSQL for MySQL 콘솔](#)에 로그인하고 인스턴스 리스트에서 인스턴스 ID를 클릭하여 인스턴스 세부 정보 페이지로 들어갑니다.

2. 인스턴스 세부 정보 페이지의 **네트워크** 섹션에서 **네트워크 변경**을 클릭합니다.
3. 팝업 창에서 VPC 아래 전환할 서브넷을 선택하고 **IP 자동 할당** 또는 IP 지정을 선택하고 기존 IP의 유효 시간을 설정한 후 **확인**을 클릭합니다.

! 설명:

- 기존 IP 주소는 네트워크가 변경된 후 기본적으로 다른 24시간 동안 유효합니다. 24시간 이내에 비즈니스 IP 주소를 변경하십시오.
- **기존 IP의 유효 시간**을 0 – 168시간으로 설정할 수 있습니다. 0시간으로 설정하면 네트워크 변경 직후 IP가 해제됩니다. 귀하의 비즈니스에 영향을 미칠 수 있습니다.
- 제품이 지역 내 Active–Active 아키텍처를 지원하므로 비즈니스 서버 또는 원본 노드와 동일한 리전에서 VPC 서브넷을 선택하는 것이 좋습니다.

Change Subnet

Changing subnet may cause the change of the instance IP. The original IP will become invalid after 24 hours. Modify the instance IP on the client in time.

Select a subnet



CID

253 subnet IPs in total, 242 subnet IPs in total,

To change the network, please go to the console to [Create VPC](#) or [Create Subnet](#)

In the current network environment, only devices in the VPC1 VPC can access this database instance.

It is recommended to select the same subnet as that of the business server or database instance primary node.

Auto-assign IP

Specify IP

OK

Cancel

VPC 간 전환

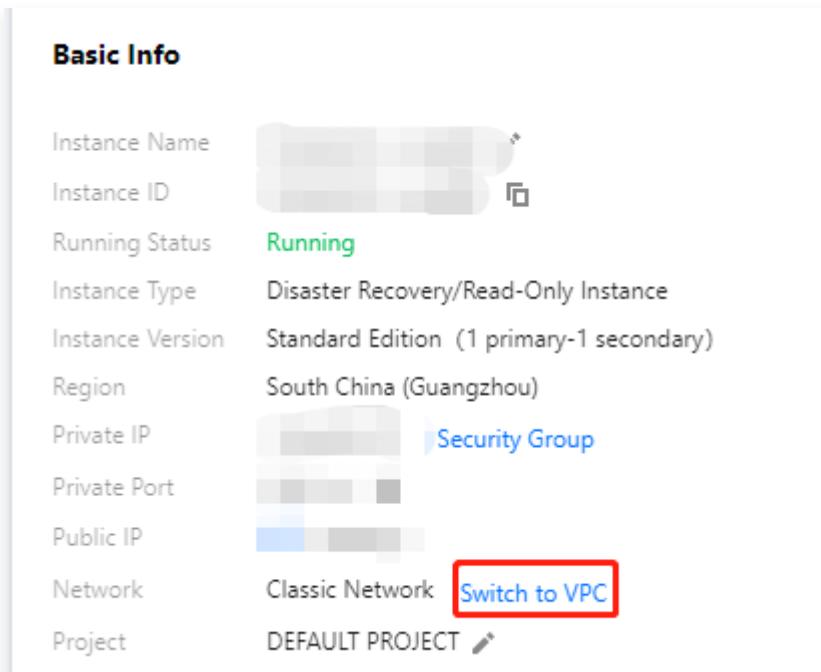
1. [TDSQL for MySQL 콘솔](#)에 로그인하고 인스턴스 리스트에서 인스턴스 ID를 클릭하여 인스턴스 세부 정보 페이지로 들어갑니다.
2. 인스턴스 세부 정보 페이지의 **네트워크** 섹션에서 **네트워크 변경**을 클릭합니다.
3. 팝업 창에서 전환할 VPC를 선택하고 **IP 자동 할당** 또는 IP 지정을 선택하고 기존 IP의 유효 시간을 설정한 후 **확인**을 클릭합니다.

설명:

- 기존 VIP 주소는 네트워크가 변경된 후 기본적으로 다른 24시간 동안 유효합니다. 24시간 이내에 비즈니스 IP 주소를 변경하십시오.
- 기존 IP의 유효 시간**을 0 – 168시간으로 설정할 수도 있습니다. 0시간으로 설정하면 네트워크 변경 직후 IP가 해제됩니다. 귀하의 비즈니스에 영향을 미칠 수 있습니다.
- 제품이 지역 내 Active–Active 아키텍처를 지원하므로 비즈니스 서버 또는 원본 노드와 동일한 리전에서 VPC 서브넷을 선택하는 것이 좋습니다.

클래식 네트워크에서 VPC로 전환

1. [TDSQL for MySQL 콘솔](#)에 로그인하고 인스턴스 리스트에서 인스턴스 ID를 클릭하여 인스턴스 세부 정보 페이지로 들어갑니다.
2. 인스턴스 세부 정보 페이지에서 **네트워크** 옆에 있는 **VPC로 전환**을 클릭합니다.



3. 팝업 창에서 VPC를 선택하고 **IP 자동 할당** 또는 IP 지정을 선택한 후 **확인**을 클릭합니다.

주의 사항:

- 클래식 네트워크에서 VPC로의 전환은 되돌릴 수 없습니다.
- 전환 후 VPC 액세스는 즉시 적용됩니다. 원래의 클래식 네트워크 액세스는 24시간 동안 유지됩니다. 따라서 인스턴스와 연결된 다른 인스턴스는 중단 없는 액세스를 보장하기 위해 24시간 이내에 VPC로 마이그레이션해야 합니다.
- 제품이 지역 내 Active–Active 아키텍처를 지원하므로 비즈니스 서버 또는 원본 노드와 동일한 리전에서 VPC 서브넷을 선택하는 것이 좋습니다.

계정 관리

계정 생성

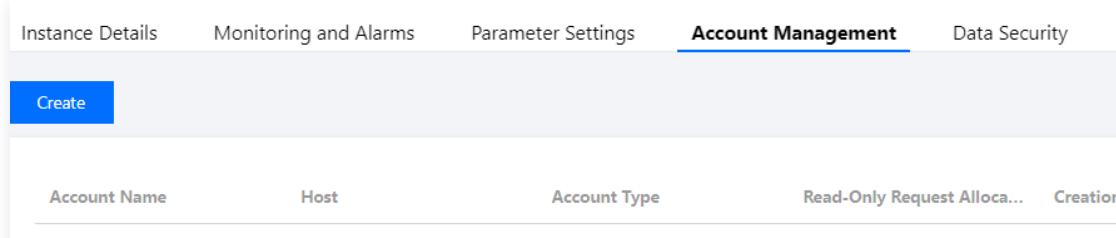
최종 업데이트 날짜: 2024-01-06 15:18:59

개요

본문은 데이터베이스 인스턴스를 관리하고 연결하기 위해 콘솔에서 TencentDB for MySQL 계정을 생성하는 방법을 설명합니다.

작업 단계

1. [TDSQL 콘솔](#)에 로그인합니다. **인스턴스 목록**에서 인스턴스 ID를 클릭하거나 **작업** 열의 **관리**를 클릭하여 인스턴스 관리 페이지로 이동합니다.
2. 인스턴스 관리 페이지에서 **계정 관리** 탭을 선택하고 **계정 생성**을 클릭합니다.



3. 팝업 대화 상자에서 계정 이름, 호스트, 비밀번호 등을 입력합니다. 모든 항목이 올바른지 확인한 후 **확인**, 다음 단계를 클릭합니다.
 - 계정 ID: 1 – 32자의 알파벳, 숫자 또는 기호를 포함하고 알파벳으로 시작해야 합니다.
 - 호스트: IP 형식으로 % 포함 가능합니다.
 - 비밀번호: 8 – 32자의 소문자, 대문자, 숫자, 기호 `() ~ ! @ # $ % ^ & * - + = _ | { } [] : < > , . ? /`를 포함해야 하며, '/'(슬래시)로 시작할 수 없습니다.
 - 최대 연결 수: 비어 있거나 0이 전달되면 최대 연결 수 매개변수가 적용됩니다.

Create

Account Name *

Account Name

The account name contain 1-32 letters, digits, or symbols (-), and must start with a letter.

Create as Read-Only Account

 Yes No

If yes, you can set the parameters of the read-only account after clicking OK.

Host *

Host

It is in the format of an IP ending with %. You can also enter % or 127.0.0.1.

Set Password *

Enter the password



The password must contain 8-32 characters in all of the following four types: lowercase letters, uppercase letters, digits, and symbols (0~!@#\$%^&*-+=_[];<>,.?/). It cannot start with a slash (/).

Confirm Password *

Please enter confirm pass



The password must contain 8-32 characters in all of the following four types: lowercase letters, uppercase letters, digits, and symbols (0~!@#\$%^&*-+=_[];<>,.?/). It cannot start with a slash (/).

Maximum Connections

- 0 +

If left empty or '0' is passed in, the "max_connections" parameter will take effect.

Remarks

Enter remarks

Up to 256 characters for remarks

Confirm and Go Next**Cancel**

4. RO 계정을 생성하기 위해서는 [읽기/쓰기 분리 설정](#)이 필요합니다. 입력한 정보를 확인하고 **확인**을 클릭합니다.

다.

- 원본 서버를 선택한 경우 복제 서버의 지연 시간 초과 시 원본 서버에서 읽어옵니다.
- 오류 보고를 선택하면 모든 복제 서버가 지연될 때 오류가 보고됩니다.
- 복제 서버에서 읽기 전용이 선택된 경우 복제 지연을 무시하고 항상 복제 서버에서 읽습니다(일반적으로 동기화를 위해 binlog를 가져오는 데 사용됨).
- 인스턴스 아키텍처가 1 원본 1 복제본인 경우 복제 서버에서만 읽기를 신중하게 선택하여, 대규모 트랜잭션과 같은 고부하 작업이 백업 작업 및 복제 서버의 가용성에 미치는 영향을 방지하십시오.

Read-Only Account Settings

Account Name

cycloneli

Host

%

Read-Only Request Allocation Policy *

 Primary Server Report Errors
 Read Only from Replica Server

If "Primary Server" is selected, read from the primary server when the delay of replica server times out.

If "Report Errors" is selected, report errors for the replica delay.

If "Read Only from Replica Server" is selected, ignore the delay parameter and always read from replica server (generally used to fetch binlog for sync).

If your instance architecture is 1-source-1-replica, please select "Read Only from Replica Server" carefully to avoid the impact on the backup tasks and availability of the replica server by high-load tasks such as large transactions.

Specified Read-Only Replica Server *



When the specified read-only replica server is enabled, the read-only requests will be automatically disconnected and will not be switched to another replica server if the source-replica delay exceeds the delay parameter.

When the specified read-only replica server is disabled, another available replica server will be automatically selected if the source-replica delay exceeds the delay parameter.

Read-Only Replica Server Delay Parameter *

 sec

If the replica server delay exceeds this parameter value, the replica server is considered faulty. We recommend that you set this parameter to a value larger than 10.

5. 권한 설정 팝업 창에서 필요에 따라 권한을 부여하고 **수정**을 클릭합니다. 변경 사항을 취소하려면 **수정 취소**를

Account name: cyclone1@%

Modify the database permissions for one or more objects

Global Privileges

Object Level Privilege

ALTER
 ALTER ROUTINE
 CREATE
 CREATE ROUTINE
 CREATE TEMPORARY TABLES
 CREATE VIEW
 DELETE
 DROP
 EVENT
 EXECUTE
 INDEX
 Select All

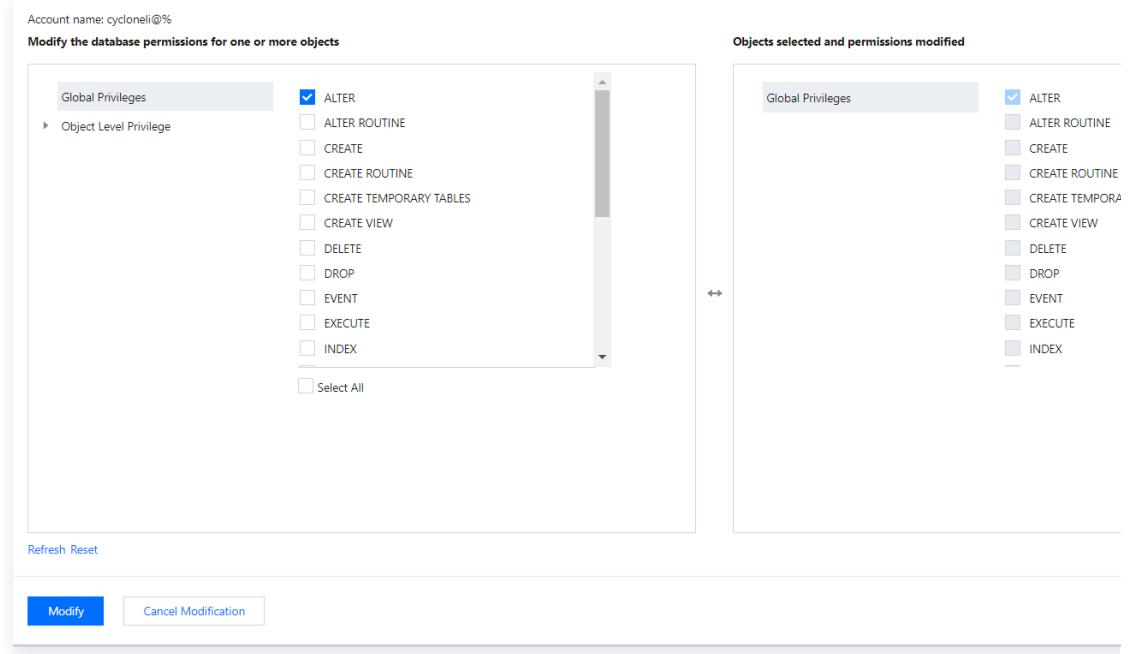
Objects selected and permissions modified

Global Privileges

ALTER
 ALTER ROUTINE
 CREATE
 CREATE ROUTINE
 CREATE TEMPORARY TABLES
 CREATE VIEW
 DELETE
 DROP
 EVENT
 EXECUTE
 INDEX

Refresh Reset

Modify Cancel Modification



관련 API

API 이름	설명
CreateAccount	계정 생성

계정 권한 설정

최종 업데이트 날짜: 2024-01-06 15:18:59

개요

콘솔에서 TDSQL for MySQL 계정에 대한 전역/객체 레벨 권한을 부여할 수 있습니다.

작업 단계

1. [TDSQL 콘솔](#)에 로그인합니다. [인스턴스 목록](#)에서 인스턴스 ID를 클릭하거나 [작업 열의 관리](#)를 클릭하여 인스턴스 관리 페이지로 이동합니다.
2. 인스턴스 관리 페이지에서 [계정 관리](#) 탭을 선택하고 권한을 수정할 계정을 찾아 [권한 설정](#)을 클릭합니다.

Account Name	Host	Account Type	Read-Only Request Alloc...	Creation Time	Update Time	Remarks
cycloneli	%	General Account	None	2022-12-19 16:40:14	2022-12-19 16:40:14	

3. 팝업 창에서 권한을 선택 또는 선택 취소하고 [확인](#)을 클릭하면 수정이 완료됩니다.

- 전역 권한: 인스턴스의 모든 데이터베이스에 권한을 부여합니다.
- 객체 레벨 권한: 인스턴스의 특정 데이터베이스에 권한을 부여합니다.

Account name: cycloneli@%

Modify the database permissions for one or more objects

Global Privileges

Object Level Privilege

ALTER
ALTER ROUTINE
CREATE
CREATE ROUTINE
CREATE TEMPORARY TABLES
CREATE VIEW
DELETE
DROP
EVENT
EXECUTE
INDEX

Select All

Objects selected and permissions modified

Global Privileges

ALTER
ALTER ROUTINE
CREATE
CREATE ROUTINE
CREATE TEMPORARY TABLES
CREATE VIEW
DELETE
DROP
EVENT
EXECUTE
INDEX

Refresh Reset

Modify Cancel Modification

관련 API

API 이름	설명
DescribeAccountPrivileges	계정 권한 쿼리
GrantAccountPrivileges	계정 권한 설정

계정 클론

최종 업데이트 날짜: 2024-01-06 15:18:59

개요

TDSQL for MySQL 콘솔에서 데이터베이스 계정을 복제하고 원본 계정 암호를 유지하여 각기 다른 권한을 제공할 수 있습니다.

작업 단계

1. [TDSQL 콘솔](#)에 로그인합니다. **인스턴스 목록**에서 인스턴스 ID를 클릭하거나 **작업** 열의 **관리**를 클릭하여 인스턴스 관리 페이지로 이동합니다.
2. 데이터베이스 관리 페이지에서 **계정 관리** 탭을 선택하고 비밀번호를 재설정할 계정을 찾은 후 **계정 클론**을 클릭합니다.

Account Name	Host	Account Type	Read-Only Request Allocat...	Creation Time	Update Time	Remarks
cycloneli	%	General Account	None	2022-12-19 16:40:14	2022-12-19 16:40:14	

3. 팝업 창에 원본 서버 IP, 계정 이름, 비밀번호(원래 계정과 동일할 수 있음)를 입력하고 **확인**, **다음 단계**를 클릭합니다.

Clone Account



Account Name *

cycloneli

The account name contain 1-32 letters, digits, or symbols (-), and must start with a letter.

 Clone Original Account Password

Create as Read-Only Account

 Yes No

If yes, you can set the parameters of the read-only account after clicking OK.

Host *

%

It is in the format of an IP ending with %. You can also enter % or 127.0.0.1.

Set Password *

Enter the password



The password must contain 8-32 characters in all of the following four types: lowercase letters, uppercase letters, digits, and symbols (0~!@#\$%^&*-+=_{}:;<>,.?/). It cannot start with a slash (/).

Confirm Password *

Please enter confirm pas:



The password must contain 8-32 characters in all of the following four types: lowercase letters, uppercase letters, digits, and symbols (0~!@#\$%^&*-+=_{}:;<>,.?/). It cannot start with a slash (/).

Maximum Connections

- 0 +

If left empty or '0' is passed in, the "max_connections" parameter will take effect.

Remarks

Enter remarks

Up to 256 characters for remarks

Confirm and Go NextCancel

4. 복제된 계정을 보려면 계정 관리 페이지로 돌아갑니다.

관련 API

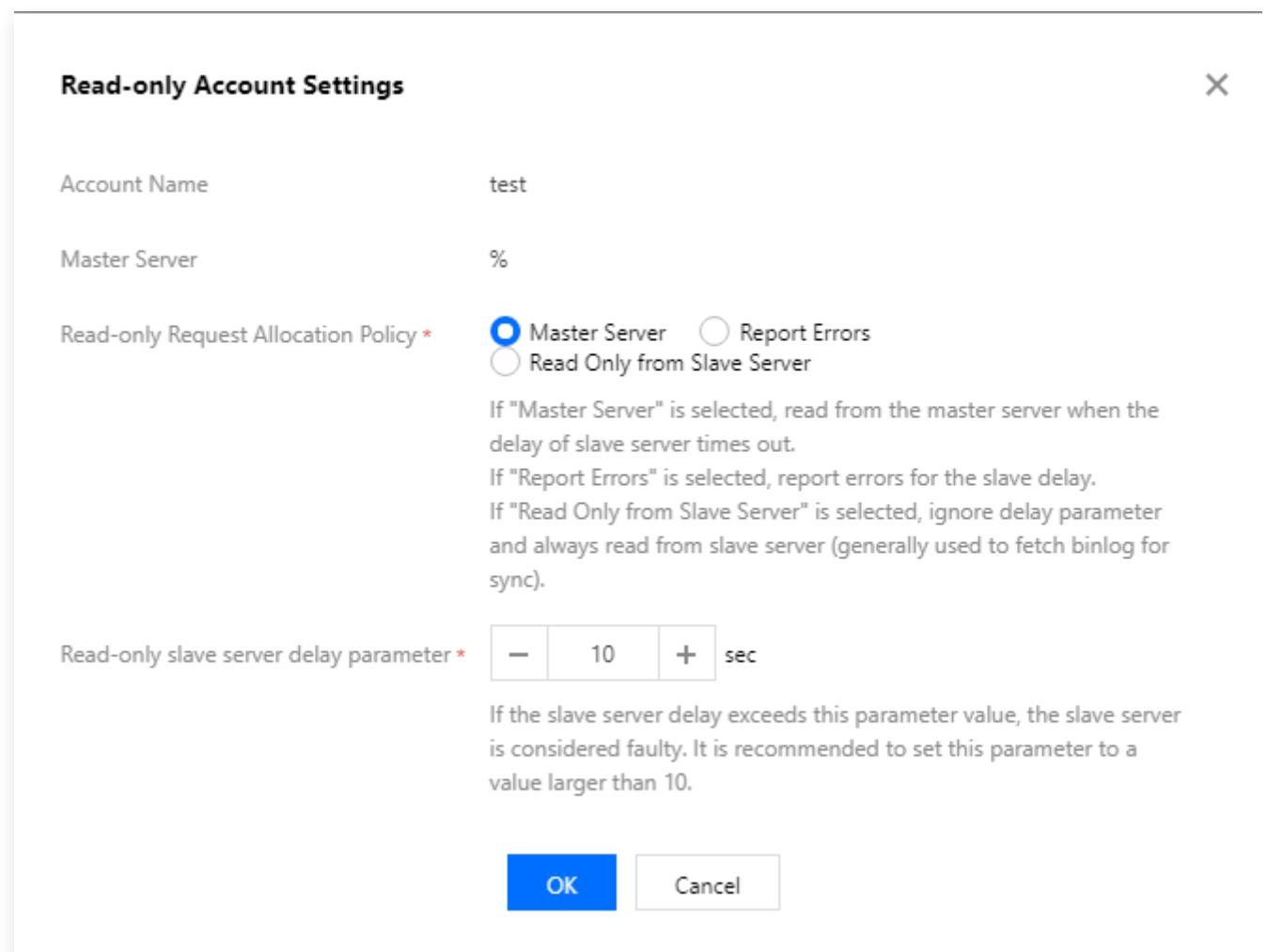
API 이름	설명
CloneAccount	계정 클론

읽기/쓰기 분리 설정

최종 업데이트 날짜: 2024-01-06 15:18:59

읽기 전용 계정에 따른 읽기/쓰기 분리

1. [TDSQL for MySQL 콘솔](#) 로그인 후, 인스턴스 리스트에서 인스턴스 ID 또는 **작업열의 관리**를 클릭하여 인스턴스 관리 페이지로 이동합니다.
2. **계정 관리** 탭을 선택하고 **계정 생성**을 클릭합니다.
3. 팝업 창에서 계정 정보를 설정하고 **읽기 전용 계정으로 생성**을 **Yes**로 설정한 후 **확인** 후 **다음으로 이동**을 클릭합니다.
4. 팝업 창에서 **읽기 전용 요청 할당 정책**을 설정하여 보조 서버 장애(또는 긴 지연) 발생 시 읽기 정책을 정의하고 **읽기 전용 보조 서버 지연 매개변수**를 구성한 다음 **확인**을 클릭합니다.
 - **프라이머리**를 선택하면 세컨더리의 지연이 제한을 초과할 경우 프라이머리 서버에서 읽습니다.
 - 세컨더리의 지연이 제한을 초과할 때 오류를 보고하려면 **오류 보고**를 선택합니다.
 - 지연 매개변수를 무시하고 항상 세컨더리에서 읽으려면 세컨더리에서 읽기 전용을 선택합니다(일반적으로 동기화를 위해 binlog를 가져오는 데 사용됨).
 - 읽기 전용 세컨더리 지연 매개변수를 설정하여 읽기 전용 요청 할당 정책에서 기본 서버 및 오류 보고와 함께 사용되는 데이터 동기화 지연 임계값을 정의합니다.



주석에 따른 읽기/쓰기 분리

세컨더리에서 읽을 각 SQL 문 앞에 `/*slave*/` 필드를 추가하고 mysql 뒤에 -c 매개변수를 추가하여 mysql -c -e "/*slave*/sql" 와 같은 주석을 구문 분석하여 세컨더리에 읽기 요청을 자동으로 할당합니다. 예시는 다음과 같습니다.

```
//프라이머리에서 읽기//
select * from emp order by sal, deptno desc;
//세컨더리에서 읽기//
/*slave*/ select * from emp order by sal, deptno desc;
```

⚠ 주의 사항:

- 이 기능은 다른 작업이 아닌 세컨더리(select)에서 읽기만 지원합니다. 비 select 문은 실패합니다.
- 주석을 구문 분석하려면 mysql 다음에 -c 매개변수를 추가해야 합니다.
- `/*slave*/` 는 소문자여야 하며, 문장 앞뒤에 공백이 필요하지 않습니다.

- MAR(strong sync) 메커니즘이 세컨더리 예외의 영향을 받는 경우 세컨더리에서 읽기가 자동으로 프라이머리에서 읽기로 전환됩니다.

계정 비밀번호 재설정

최종 업데이트 날짜: 2024-01-06 15:18:59

개요

TDSQL for MySQL을 사용하는 동안 데이터베이스 계정 비밀번호를 잊어버렸거나 변경해야 하는 경우 콘솔에서 재설정할 수 있습니다.

설명:

데이터 보안을 위해 최소 3개월에 한 번은 정기적으로 비밀번호를 재설정할 것을 권장합니다.

작업 단계

- TDSQL 콘솔에 로그인합니다. 인스턴스 목록에서 인스턴스 ID를 클릭하거나 작업 열의 관리를 클릭하여 인스턴스 관리 페이지로 이동합니다.
- 인스턴스 관리 페이지에서 계정 관리 탭을 선택하고 비밀번호를 재설정할 계정을 찾은 후 더보기 > 비밀번호 재설정을 선택합니다.

Account Name	Host	Account Type	Read-Only Request Allocatio...	Creation Time	Update Time	Remarks	Operation
cycloneli	%	General Account	None	2022-12-19 16:40:14	2022-12-19 16:40:14		Modify Permissions Clone Account More

- 팝업 창에서 새 비밀번호를 입력하고 비밀번호를 확인한 다음 확인을 클릭합니다.

설명:

계정 정보의 생성, 수정, 삭제로 인한 위험을 방지하기 위해 액세스 관리를 설정하고, 비밀번호 재설정에 주의를 기울이는 것이 좋습니다.

Reset Password

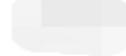


! To avoid your business risks caused by creating, modifying, or deleting account info, it is recommended to carefully control the function menu permissions (API keyword: *Account*) when you configure access management.

Instance Name



Account Name



Host

%

Set Password *

 Enter the password

The password must contain 8-32 characters in all of the following four types: lowercase letters, uppercase letters, digits, and symbols (0~!@#\$%^&*-+=_|{}[]: <>,.?/). It cannot start with a slash (/).

Confirm Password *

 Please enter confirm pass

The password must contain 8-32 characters in all of the following four types: lowercase letters, uppercase letters, digits, and symbols (0~!@#\$%^&*-+=_|{}[]: <>,.?/). It cannot start with a slash (/).

관련 API

API 이름	설명
ResetAccountPassword	계정 비밀번호 재설정

계정 삭제

최종 업데이트 날짜: 2024-01-06 15:18:59

개요

본문은 콘솔에서 TDSQL for MySQL 계정을 삭제하는 방법을 설명합니다.

설명:

삭제된 데이터베이스 계정은 복구할 수 없습니다. 계정이 더 이상 사용되지 않는지 확인하고 주의해서 진행하십시오.

작업 단계

- TDSQL 콘솔에 로그인합니다. 인스턴스 목록에서 인스턴스 ID를 클릭하거나 작업 열의 관리를 클릭하여 인스턴스 관리 페이지로 이동합니다.
- 인스턴스 관리 페이지에서 계정 관리 탭을 선택하고 비밀번호를 재설정할 계정을 찾은 후 더보기 > 계정 삭제를

Account Name	Host	Account Type	Read-Only Request Allocat...	Creation Time	Update Time	Remarks
cycloneli	%	General Account	None	2022-12-19 16:40:14	2022-12-19 16:40:14	

- 팝업 창에서 모든 것이 올바른지 확인하고 확인을 클릭합니다.

관련 API

API 이름	설명
DeleteAccount	계정 삭제

보안 관리

액세스 관리

개요

최종 업데이트 날짜: 2024-01-06 15:18:59

귀하가 Tencent Cloud의 CDB, CVM, 사설 네트워크 등의 서비스를 사용 중이며, 해당 서비스가 여러 사람에 의해 관리되지만 모든 인원이 귀하의 클라우드 계정 키를 공유할 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.

이것이 바로 CAM이 개발된 이유입니다.

CAM에 대한 상세 정보는 [CAM 개요](#)를 참고하십시오.

CAM에 액세스하면 서브 계정을 통해 여러 사람이 각각 다른 서비스를 관리함으로써 위와 같은 문제 발생을 피할 수 있습니다. 기본적으로 서브 계정은 CDB 인스턴스 또는 CDB 관련 리소스를 사용할 권한이 없습니다. 그러므로 서브 계정이 필요한 리소스나 권한 사용을 허용하는 정책을 생성해야 합니다.

정책은 하나 또는 다수 권한의 구문 범위를 정의 및 설명합니다. 정책은 사용자 또는 사용자 그룹으로부터 권한을 부여받아 지정된 리소스에 대한 사용을 허가하거나 금지시킵니다. CAM 정책의 자세한 기본 정보는 [정책 구문](#), 사용 정보에 대한 내용은 [정책](#)을 참고하십시오.

서브 계정을 통한 CDB 관련 리소스 CAM 진행이 필요하지 않을 경우 이 섹션을 건너뛸 수 있습니다. 이 섹션을 건너뛰더라도 문서의 나머지 섹션을 이해하고 사용하는 데 영향을 미치지 않습니다.

가이드

CAM 정책은 반드시 하나 또는 그 이상의 CDB 작업 사용에 권한을 부여하거나 거부해야 합니다. 동시에 작업에 사용할 수 있는 리소스(모든 리소스일 수도 있고, 일부 리소스일 수도 있음)를 지정해야 하며, 정책에 작업 리소스에서 설정한 조건을 포함할 수 있습니다.

⚠ 주의 사항:

- CAM 정책을 사용하여 CDB 리소스 관리와 CDB 작업 권한 부여를 진행할 것을 권장합니다. 인벤토리 프로젝트별 권한의 사용자 체험은 동일하나, 프로젝트별 권한을 사용하여 리소스 관리와 권한 부여 작업을 진행하는 것은 권장하지 않습니다.
- CDB는 현재 효력 발생 조건 설정을 지원하지 않습니다.

정책 구조

최종 업데이트 날짜: 2024-01-06 15:18:59

정책 구문

CAM 정책 설정 예시:

```
{  
  "version": "2.0",  
  "statement": [  
    {  
      "effect": "effect",  
      "action": ["action"],  
      "resource": ["resource"],  
      "condition": { "key": {"value"} }  
    }  
  ]  
}
```

- 버전 version:** 버전이 필요합니다. 현재 '2.0'만 허용됩니다(이 값은 실제로 CAM에서 허용되는 TencentCloud API의 버전을 나타냅니다.).
- 명령 statement:** 하나 또는 다수의 권한과 관련한 자세한 정보를 설명하는 데 사용합니다. 이 요소에는 effect, action, resource, condition 등 기타 여러 요소의 권한 또는 권한 집합이 포함됩니다. 하나의 정책은 하나의 statement 요소만 가지고 있습니다.
- 작업 action:** 허용되거나 거부된 작업을 설명합니다. 여기에 입력된 action은 'dcdb:' 접두사가 붙고 [TDSQL for MySQL API](#)는 접미사가 붙은 문자열입니다. 필수 입력 항목입니다.
 - 리소스 resource:** 권한 부여의 구체적인 데이터를 기술합니다. 리소스는 6단식 기술을 사용하며, 모든 제품마다 리소스의 정의의 차이가 있습니다. 리소스 정보를 어떻게 지정할지에 대한 것은 작성한 리소스 선언에 대한 제품 문서를 참고하십시오. 필수 입력 항목입니다.
 - 조건 condition:** 정책의 효력이 발생하는 규제 조건을 기술합니다. condition에는 오퍼레이터, 작업 키와 작업 값 구성이 포함됩니다. 작업 값은 시간, IP 주소 등의 정보를 포함합니다. 어떤 서비스는 조건에 기타 값을 지정하는 것을 허용합니다. 필수 입력 항목입니다.
 - 영향 effect:** 명령문에 의해 생성된 결과가 'allow'(허용) 또는 'deny'(거부)인지 여부를 설명합니다. 필수 입력 항목입니다.

⚠ 주의 사항:

기존 이유로 액세스 관리에서 TDSQL for MySQL의 인터페이스 키워드는 dcdb입니다.

CDB의 작업

TencentDB 정책 설명에서 TencentDB를 지원하는 모든 서비스의 API 작업을 지정할 수 있습니다.

dcdb:CreateDBInstance(인스턴스 생성 – 월간 구독) 또는 dcdb:CloseDBExtranetAccess(공용 네트워크 액세스 비활성화)와 같이 dcdb: 접두사가 붙은 API를 TencentDB에 사용해야 합니다.

- 단일 명령문에 여러 작업을 지정하려면 아래와 같이 영어 쉼표로 구분합니다.

```
"action": ["dcdb:action1", "dcdb:action2"]
```

1. 와일드카드를 사용해서 여러 항목의 작업을 지정할 수도 있습니다. 예를 들어, 다음과 같이 이름이 'Describe'로 시작하는 모든 작업을 지정할 수 있습니다.

```
"action": ["dcdb:Describe*"]
```

2. 만약 CDB의 모든 작업을 지정할 경우, 다음과 같이 * 와일드카드를 사용하십시오.

```
"action": ["dcdb:*"]
```

CDB의 리소스

각각의 CAM 정책 명령어는 모두 자신에게 적용되는 리소스가 있습니다.

리소스의 일반 형식은 아래와 같습니다.

```
qcs:project_id:service_type:region:account:resource
```

- **project_id**: 프로젝트 정보 설명은 CAM 초기 로직을 호환하기 위한 것이므로 입력하지 않아도 됩니다.
- **service_type**: dcdb와 같은 제품 약칭입니다.
- **region**: ap-guangzhou와 같은 리전 정보를 설명합니다. 자세한 내용은 [리전 관련 정보](#)를 참고하십시오.
- **account**: uin/65xxx763과 같은 리소스 소유자의 루트 계정 정보입니다.
- **resource**: instance/instance_id1 또는 instance/*와 같은 각 제품의 구체적인 리소스 정보.

예시:

- 명령 중인 특정 인스턴스(dcdb-k05xdcta)를 사용하여 아래와 같이 리소스를 지정할 수 있습니다.

```
"resource": [ "qcs::dcdb:ap-guangzhou:uin/65xxx763:instance/dcdb-k05xdcta" ]
```

1. • 와일드카드를 사용할 경우에도 아래와 같이 특정 계정의 모든 인스턴스를 지정할 수 있습니다.

```
"resource": [ "qcs::dcdb:ap-guangzhou:uin/65xxx763:instance/*"]
```

2. 모든 리소스를 지정해야 하거나 특정 API 작업이 리소스 권한을 지원하지 않을 경우, 아래와 같이 Resource 요소에서 * 와일드카드를 사용하십시오.

```
"resource": [ "*" ]
```

3. 단일 명령어에 동시에 여러 리소스를 지정하고 싶을 경우, 영어 쉼표를 이용해 분리하십시오. 다음은 두 개의 리소스를 지정한 예시를 보여 줍니다.

```
"resource": ["resource1", "resource2"]
```

아래의 표는 CDB가 사용할 수 있는 리소스와 이에 상응하는 리소스의 기술 방법에 대한 설명입니다.

아래의 표에서 \$가 접두사인 단어는 모두 별칭입니다.

- 이 중, region은 리전을 나타냅니다.
- 이 중, account는 계정 ID를 나타냅니다.

리소스	권한 부여 정책 중 리소스 기술 방법
인스턴스	qcs::dcdb:\$region:\$account:instance /\$instanceId

리소스 수준 권한 지원

최종 업데이트 날짜: 2024-01-06 15:18:59

⚠ 주의 사항:

기존 이유로 액세스 관리에서 TDSQL for MySQL의 인터페이스 키워드는 dcdb입니다.

리소스 수준 권한을 사용하여 사용자가 조작할 수 있는 리소스를 지정할 수 있습니다. TencentDB는 특정 리소스 수준 권한을 지원합니다. 즉, 일부 TencentDB 작업의 경우 사용자가 작업(필수 조건에 따라)을 수행하거나 지정된 리소스를 사용하도록 허용되는 시간을 제어할 수 있습니다. 다음 표는 TencentDB에서 권한을 부여할 수 있는 리소스 유형을 설명합니다.

CAM에서 승인할 수 있는 리소스 유형:

리소스 유형	권한 부여 정책 중 리소스 메소드 설명
CDB 인스턴스 관련	qcs::dcdb:\$region:\$account:instance/* qcs::dcdb:\$region:\$account:instance/\$instanceId

아래 표에서는 현재 리소스 권한 부여를 지원하는 CDB API 작업과 더불어, 각 작업에서 지원되는 리소스 및 조건 키에 대해 소개하고 있습니다. 리소스 경로를 지정할 때에는 * 와일드카드 문자를 사용할 수 있습니다.

ⓘ 설명:

상기에 나열되지 않은 TencentDB API 작업은 리소스 수준 권한을 지원하지 않습니다. TencentDB API 작업이 리소스 수준 권한을 지원하지 않는 경우에도 사용자에게 이 작업을 수행하도록 권한을 부여할 수 있지만 정책 설명의 리소스 요소에 *를 지정해야 합니다.

다음 작업은 리소스 수준 권한 제어 지원

작업 이름	API 이름	설정 후 콘솔 적용 여부
전용 인스턴스 복구	ActiveDedicatedDBInstance	YES
보안 그룹 바인딩	AssociateSecurityGroups	YES
IP 상태 확인	CheckIpStatus	YES
계정 복제	CloneAccount	YES
인스턴스에 대한 공용 네트워크 액세스 비활성화	CloseDBExtranetAccess	YES
계정 권한 복사	CopyAccountPrivileges	YES

계정 생성	CreateAccount	YES
인스턴스 생성	CreateDCDBInstance	YES
계정 삭제	DeleteAccount	YES
계정 권한 쿼리	DescribeAccountPrivileges	YES
계정 목록 쿼리	DescribeAccounts	YES
감사 로그 쿼리	DescribeAuditLogs	YES
감사 규칙 세부 정보 쿼리	DescribeAuditRuleDetail	YES
감사 규칙 목록 쿼리	DescribeAuditRules	YES
감사 정책 쿼리	DescribeAuditStrategies	YES
일괄 인스턴스 갱신 가격 쿼리	DescribeBatchDCDBRenewalPrice	YES
인스턴스 객체 쿼리	DescribeDatabaseObjects	YES
인스턴스 BD 이름 쿼리	DescribeDatabases	YES
인스턴스 테이블의 컬럼 정보 쿼리	DescribeDatabaseTable	YES
로그 목록 가져오기	DescribeDBLogFile	YES
모니터링 정보 쿼리	DescribeDBMetrics	YES
데이터베이스 매개변수 조회	DescribeDBParameters	YES
인스턴스 보안 그룹 정보 쿼리	DescribeDBSecurityGroups	YES
슬로우 로그 기록 세부 정보 가져오기	DescribeDBSlowLogAnalysis	YES
슬로우 로그 목록 가져오기	DescribeDBSlowLogs	YES
인스턴스 동기화 모드 쿼리	DescribeDBSyncMode	YES
인스턴스 세부정보 가져오기	DescribeDCDBInstanceDetail	YES
인스턴스 목록 보기	DescribeDCDBInstances	YES
가격 쿼리	DescribeDCDBPrice	YES

인스턴스 갱신 가격 쿼리	DescribeDCDBRenewalPrice	YES
구매 가능한 AZ 쿼리	DescribeDCDBSaleInfo	YES
인스턴스 색상 쿼리	DescribeDCDBShards	YES
인스턴스의 업그레이드 가격 쿼리	DescribeDCDBUpgradePrice	YES
전용 클러스터 사양 쿼리	DescribeFenceShardSpec	YES
흐름 상태 쿼리	DescribeFlow	YES
최신 DBA 점검 결과 쿼리	DescribeLatestCloudDBAReport	YES
백업 로그 설정 보기	DescribeLogFileRetentionPeriod	YES
주문 정보 쿼리	DescribeOrders	YES
프로젝트 쿼리	DescribeProjects	YES
프로젝트의 보안 그룹 정보 쿼리	DescribeProjectSecurityGroups	YES
인스턴스 사양 쿼리	DescribeShardSpec	YES
SQL 로그 가져오기	DescribeSqlLogs	YES
Tencent Cloud 리소스에서 보안 그룹을 일괄적으로 바인딩 해제	DisassociateSecurityGroups	YES
계정 권한 설정	GrantAccountPrivileges	YES
인스턴스 초기화	InitDCDBInstances	YES
전용 인스턴스 격리	IsolateDedicatedDBInstance	YES
데이터베이스 계정 비고 수정	ModifyAccountDescription	YES
일괄 자동 연장 설정	ModifyAutoRenewFlag	YES
인스턴스 이름 수정	ModifyDBInstanceName	YES
TencentDB 인스턴스에 바인딩된 보안 그룹 수정	ModifyDBInstanceSecurityGroups	YES

인스턴스 프로젝트 수정	ModifyDBInstancesProject	YES
데이터베이스 매개변수 수정	ModifyDBParameters	YES
인스턴스 동기화 모드 수정	ModifyDBSyncMode	YES
인스턴스 네트워크 수정	ModifyInstanceNetwork	YES
인스턴스 VIP 수정	ModifyInstanceVip	YES
백업 로그 설정 수정	ModifyLogFileRetentionPeriod	YES
공용 네트워크 액세스 활성화	OpenDBExtranetAccess	YES
인스턴스 갱신	RenewDCDBInstance	YES
계정 비밀번호 재설정	ResetAccountPassword	YES
스마트 DBA 활성화	StartSmartDBA	YES
인스턴스 확장	UpgradeDCDBInstance	YES
전용 인스턴스 업그레이드	UpgradeDedicatedDCDBInstance	YES

콘솔 예시

최종 업데이트 날짜: 2024-01-06 15:18:59

TencentDB CAM 정책 예시

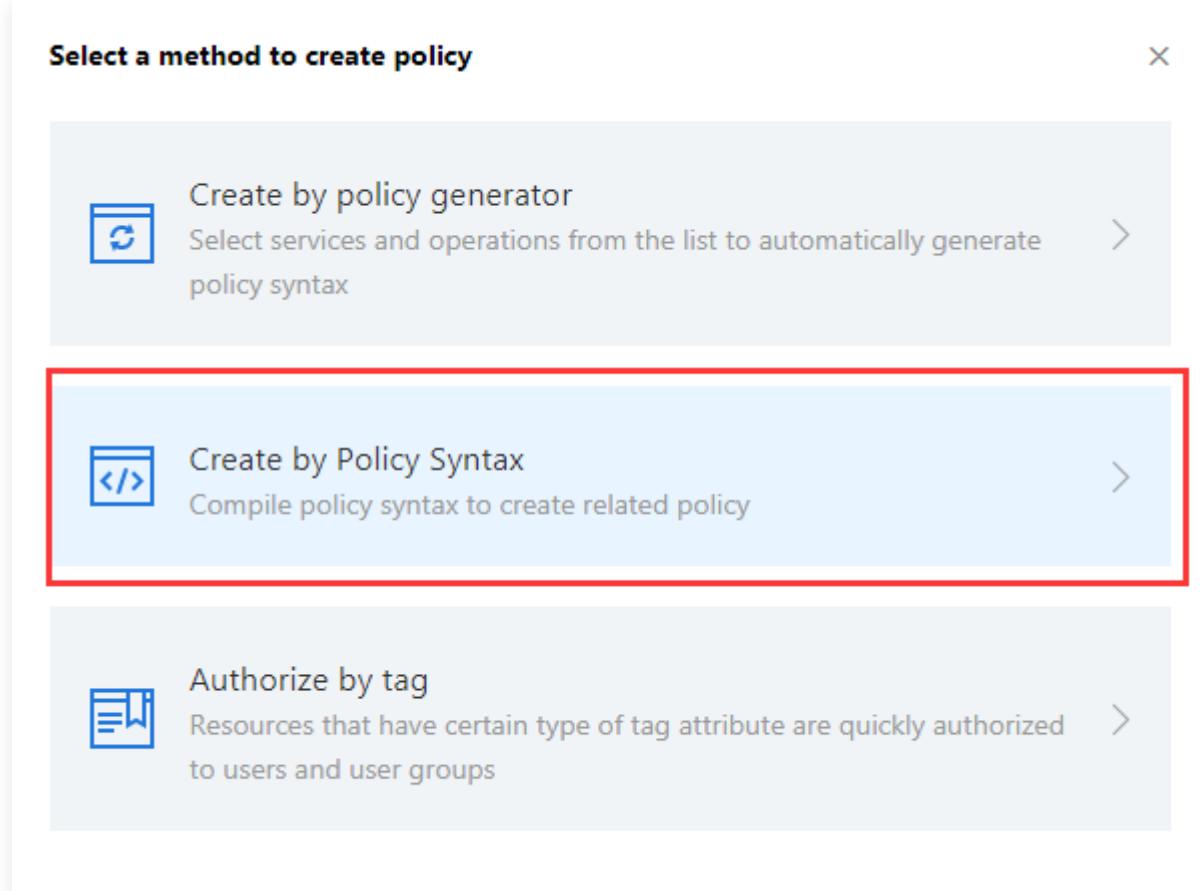
CAM 정책을 통해 사용자에게 CDB 콘솔에서 특정 리소스에 대한 조회 및 사용 권한을 부여할 수 있습니다. 이 예시는 사용자가 콘솔에서 특정 정책을 사용할 수 있도록 설정하는 방법에 관해 설명합니다.

! 설명:

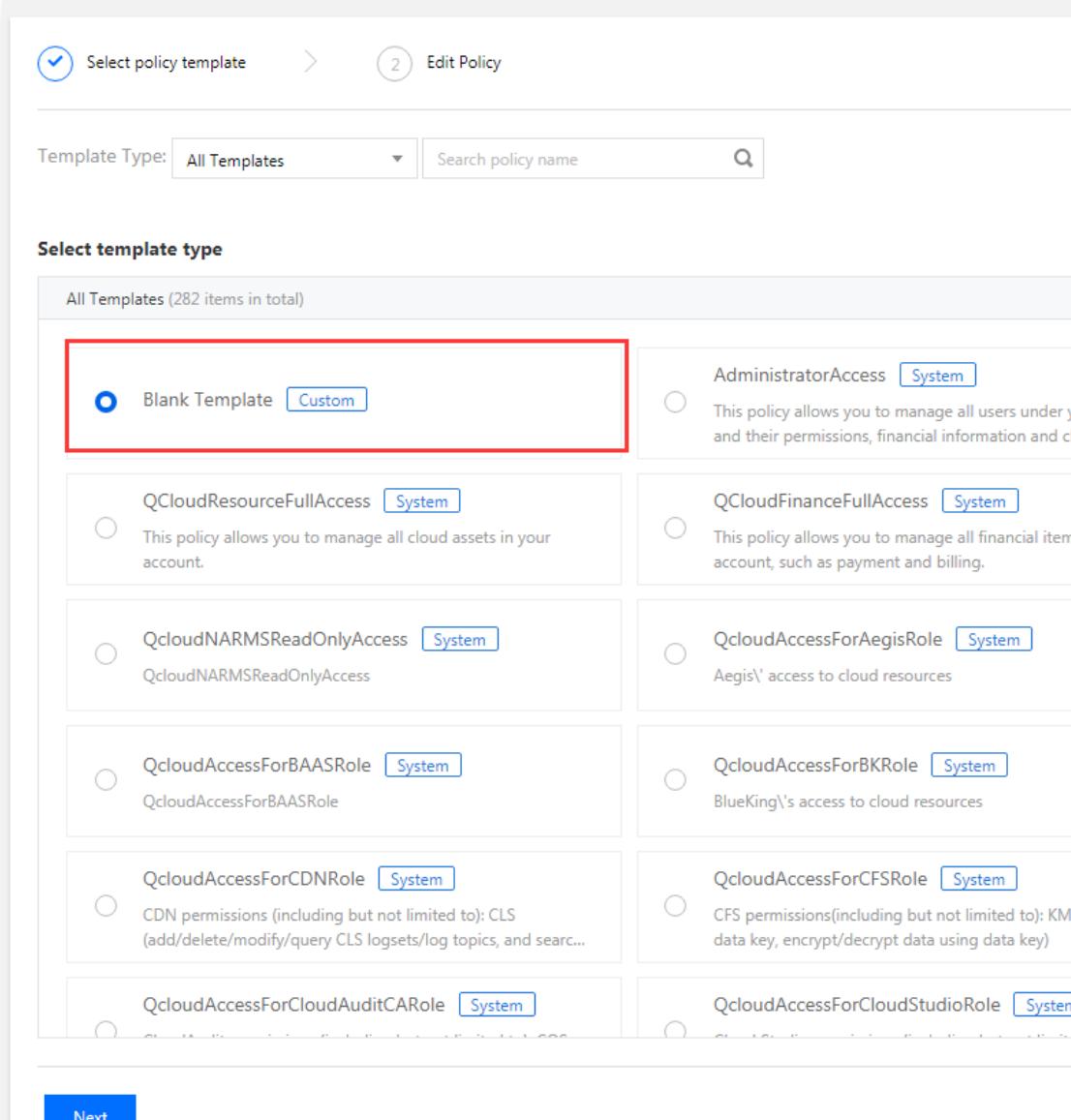
TDSQL for MySQL은 이전에 dcdb로 알려졌으므로 CAM의 API 키워드는 dcdb입니다.

사용자 정의 정책 생성 구문

- 정책 구문 설정 페이지로 이동하여 사용자 정의 정책 생성을 클릭합니다.
- 팝업 창에서 정책 구문으로 생성을 클릭합니다.



- 빈 템플릿을 선택하고 다음을 클릭합니다.



1 Select policy template > 2 Edit Policy

Template Type: All Templates Search policy name

Select template type

All Templates (282 items in total)	
<input checked="" type="radio"/> Blank Template Custom	AdministratorAccess System This policy allows you to manage all users under y and their permissions, financial information and cl
<input type="radio"/> QCloudResourceFullAccess System This policy allows you to manage all cloud assets in your account.	<input type="radio"/> QCloudFinanceFullAccess System This policy allows you to manage all financial item account, such as payment and billing.
<input type="radio"/> QcloudNARMSReadOnlyAccess System QcloudNARMSReadOnlyAccess	<input type="radio"/> QcloudAccessForAegisRole System Aegis\ access to cloud resources
<input type="radio"/> QcloudAccessForBAASRole System QcloudAccessForBAASRole	<input type="radio"/> QcloudAccessForBKRole System BlueKing\ access to cloud resources
<input type="radio"/> QcloudAccessForCDNRole System CDN permissions (including but not limited to): CLS (add/delete/modify/query CLS logsets/log topics, and searc...	<input type="radio"/> QcloudAccessForCFSRole System CFS permissions(including but not limited to): KM: data key, encrypt/decrypt data using data key)
<input type="radio"/> QcloudAccessForCloudAuditCARole System	<input type="radio"/> QcloudAccessForCloudStudioRole System

Next

4. 해당 정책 구문을 입력합니다.

Policy Name * policygen-20191016221243

Notes

Edit Policy Content

```
1 {  
2   "version": "2.0",  
3   "statement": []  
4 }
```

Policy Syntax Description [\[\]](#) Support service list [\[\]](#)

Previous [Create Policy](#)

서브 계정/협업 파트너 연결 및 확인

정책을 만든 후 사용자/그룹과 연결합니다. 연결이 완료되면 다른 브라우저(또는 서버)를 이용하여 서브 계정/협력자가 정상적으로 작동하는지 확인합니다. 정책 구문이 올바르게 작성되면 다음을 관찰할 수 있습니다.

- 의도한 타깃 제품 및 리소스에 대한 일반적인 액세스 권한이 있으며 예상되는 모든 기능을 사용할 수 있습니다.
- 다른 승인되지 않은 제품이나 리소스에 액세스할 때 **이 작업을 수행할 권한이 없습니다**라는 메시지가 표시됩니다.

! 설명:

여러 정책의 상호 영향을 방지하려면 한 번에 하나의 정책만 서브 계정에 연결하는 것이 좋습니다.
계정 접근 권한에 대한 변경 사항은 1분 이내에 적용됩니다.

부록: 일반적으로 사용되는 정책 구문

모든 TencentDB 인스턴스의 모든 기능 사용을 승인하기 위한 정책

사용자에게 TencentDB 인스턴스를 만들고 관리할 수 있는 권한을 부여하려면 사용자에 대해

QcloudDCDBFullAccess라는 정책을 구현합니다.

정책 구문은 아래와 같습니다.

```
{  
  "version": "2.0",  
  "statement": [  
    {  
      "action": [  
        "dcdb:*"  
      ],  
      "resource": "*",  
      "effect": "allow"  
    }  
  ]  
}
```

모든 TencentDB 인스턴스의 쿼리 권한 부여 정책

사용자에게 TencentDB 인스턴스를 볼 수 있는 권한을 부여하되 생성, 삭제 또는 수정하지 않으려면 사용자에 대해

QcloudDCDBInnerReadOnlyAccess라는 정책을 구현합니다.

정책 구문은 아래와 같습니다.

```
{  
  "version": "2.0",  
  "statement": [  
    {  
      "action": [  
        "dcdb:Describe*"  
      ],  
      "resource": "*",  
      "effect": "allow"  
    }  
  ]  
}
```

]
}

상기 정책은 사용자가 CAM 정책으로 TencentDB에서 ‘Describe’로 시작하는 모든 작업의 사용을 별도로 권한을 부여함으로써 목적을 달성합니다.

① 설명:

현재 모든 기능적 API를 다루는 것은 아니므로 일부 작업이 CAM에 포함되지 않은 것을 볼 수 있습니다. 이는 정상적인 현상입니다.

사용자에게 특정 리전 CDB 작업 권한을 부여하는 정책

사용자에게 특정 리전의 CDB에 대한 작업 권한을 부여할 경우, 아래 정책을 해당 사용자에게 연결할 수 있습니다. 아래 정책은 사용자에게 광저우 리전의 CDB 디바이스에 대한 작업 권한을 허용합니다.

{
 "version": "2.0",
 "statement": [
 {
 "action": "dcdb:*",
 "resource": "qcs::dcdb:ap-guangzhou::*",
 "effect": "allow"
 }
]
}

여러 특정 리전에서 TencentDB 인스턴스를 조작할 수 있는 사용자 권한 부여 정책

특정 리전에서 TencentDB 인스턴스를 조작할 수 있는 권한을 사용자에게 부여하려면 다음 정책을 사용자와 연결합니다. 예를 들어, 아래 정책은 사용자가 광저우 및 청두에서 TencentDB 인스턴스를 조작하도록 허용합니다.

{
 "version": "2.0",
 "statement": [
 {
 "action": "dcdb:*",
 "resource": "qcs::dcdb:ap-guangzhou::*", "qcs::dcdb:ap-chengdu::*",
 "effect": "allow"
 }
]
}

]
}

하나의 특정 TencentDB 인스턴스를 조작할 수 있는 사용자 권한 부여 정책

사용자에게 특정 데이터베이스를 조작할 수 있는 권한을 부여하려면 다음 정책을 사용자와 연결합니다. 예를 들어, 아래 정책은 사용자가 광저우에서 TencentDB 인스턴스 dcdb-xxx를 조작하도록 허용합니다.

```
{  
  "version": "2.0",  
  "statement": [  
    {  
      "action": [  
        "dcdb:*"  
      ],  
      "resource": "qcs::dcdb:ap-guangzhou::instance/dcdb-xxx",  
      "effect": "allow"  
    }  
  ]  
}
```

여러 TencentDB 인스턴스를 조작할 수 있는 사용자 권한 부여 정책

사용자에게 TencentDB 인스턴스를 일괄적으로 조작할 수 있는 권한을 부여하려면 다음 정책을 사용자와 연결하십시오. 예를 들어, 아래 정책은 사용자가 광저우의 TencentDB 인스턴스 dcdb-xxx 및 dcdb-yyy 및 베이징의 dcdb-zzz를 조작하도록 허용합니다.

```
{  
  "version": "2.0",  
  "statement": [  
    {  
      "action": "dcdb:*",  
      "resource": ["qcs::dcdb:ap-guangzhou::instance/dcdb-xxx",  
      "qcs::dcdb:ap-guangzhou::instance/dcdb-yyy", "qcs::dcdb:ap-  
      beijing::instance/dcdb-zzz"],  
      "effect": "allow"  
    }  
  ]  
}
```

사용자에게 여러 TencentDB 인스턴스를 조작할 수 있는 다른 권한을 부여하는 정책

사용자에게 TencentDB 인스턴스를 일괄적으로 조작할 수 있는 권한을 부여하려면 다음 정책을 사용자와 연결하십시오. 예를 들어, 아래 정책은 사용자가 광저우의 TencentDB 인스턴스 dcdb-xxx 및 dcdb-yyy 및 베이징의 dcdb-zzz를 조작하도록 허용합니다.

```
{  
  "version": "2.0",  
  "statement": [  
    {  
      "action": "dcdb:Describe*", "dcdb:Create*",  
      "resource": ["qcs::dcdb:ap-guangzhou::instance/dcdb-xxx",  
      "qcs::dcdb:ap-guangzhou::instance/dcdb-yyy", "qcs::dcdb:ap-  
      beijing::instance/dcdb-zzz"],  
      "effect": "allow"  
    }  
  ]  
}
```

TencentDB 계정 생성에 대한 사용자 권한 거부

TencentDB 계정 생성에 대한 사용자 권한을 거부하려면 `'effect': 'deny'` 를 구성하십시오.

```
{  
  "version": "2.0",  
  "statement": [  
    {  
      "action": "dcdb:CreateAccount",  
      "resource": "*",  
      "effect": "deny"  
    }  
  ]  
}
```

기타 사용자 정의 정책

사전 설정된 정책이 요구 사항을 충족할 수 없는 경우 아래와 같이 사용자 정의 정책을 만들 수 있습니다.

```
{  
  "version": "2.0",
```

```
"statement": [
  {
    "action": [
      "Action"
    ],
    "resource": "Resource",
    "effect": "Effect"
  }
]
```

- Action에서 허용 또는 거부할 작업으로 변경합니다.
- Resource에서 권한을 부여할 구체적인 리소스로 변경합니다.
- Effect에서 허용 또는 거부로 변경합니다.

CAM 지원 작업

최종 업데이트 날짜: 2024-01-06 15:18:59

리소스 수준 권한 제어가 지원되는 작업

작업 이름	API 이름	설정 후 콘솔 적용 여부
전용 인스턴스 복구	ActiveDedicatedDBInstance	YES
보안 그룹 바인딩	AssociateSecurityGroups	YES
IP 상태 확인	CheckIpStatus	YES
클로닝 계정	CloneAccount	YES
인스턴스 공용 네트워크 액세스 비활성화	CloseDBExtranetAccess	YES
계정 권한 복사	CopyAccountPrivileges	YES
계정 생성	CreateAccount	YES
인스턴스 생성	CreateDCDBInstance	YES
계정 삭제	DeleteAccount	YES
계정 권한 쿼리	DescribeAccountPrivileges	YES
계정 목록 쿼리	DescribeAccounts	YES
감사 로그 쿼리	DescribeAuditLogs	YES
감사 규칙 세부 정보 쿼리	DescribeAuditRuleDetail	YES
감사 규칙 목록 쿼리	DescribeAuditRules	YES
감사 정책 쿼리	DescribeAuditStrategies	YES
일괄 인스턴스 갱신 가격 쿼리	DescribeBatchDCDBRenewalPrice	YES
인스턴스 객체 쿼리	DescribeDatabaseObjects	YES
인스턴스 BD 이름 쿼리	DescribeDatabases	YES
인스턴스 테이블의 컬럼 정보 쿼리	DescribeDatabaseTable	YES

로그 목록 가져오기	DescribeDBLogFiles	YES
모니터링 정보 쿼리	DescribeDBMetrics	YES
데이터베이스 매개변수 조회	DescribeDBParameters	YES
인스턴스의 보안 그룹 정보 쿼리	DescribeDBSecurityGroups	YES
슬로우 로그 기록 세부 정보 가져오기	DescribeDBSlowLogAnalysis	YES
슬로우 로그 목록 가져오기	DescribeDBSlowLogs	YES
인스턴스 동기화 모드 쿼리	DescribeDBSyncMode	YES
인스턴스 세부정보 가져오기	DescribeDCDBInstanceDetail	YES
인스턴스 목록 보기	DescribeDCDBInstances	YES
가격 쿼리	DescribeDCDBPrice	YES
인스턴스 갱신 가격 쿼리	DescribeDCDBRenewalPrice	YES
구매 가능한 AZ 쿼리	DescribeDCDBSaleInfo	YES
인스턴스 샤드 쿼리	DescribeDCDBShards	YES
인스턴스의 업그레이드 가격 쿼리	DescribeDCDBUpgradePrice	YES
전용 클러스터 사양 쿼리	DescribeFenceShardSpec	YES
플로우 상태 쿼리	DescribeFlow	YES
최신 DBA 점검 결과 쿼리	DescribeLatestCloudDBAReport	YES
백업 로그 설정 보기	DescribeLogFileRetentionPeriod	YES
주문 정보 쿼리	DescribeOrders	YES
프로젝트 쿼리	DescribeProjects	YES
프로젝트의 보안 그룹 정보 쿼리	DescribeProjectSecurityGroups	YES

인스턴스 사양 쿼리	DescribeShardSpec	YES
SQL 로그 가져오기	DescribeSqlLogs	YES
Tencent Cloud 리소스에서 보안 그룹을 일괄적으로 바인딩 해제	DisassociateSecurityGroups	YES
계정 권한 설정	GrantAccountPrivileges	YES
인스턴스 초기화	InitDCDBInstances	YES
전용 인스턴스 격리	IsolateDedicatedDBInstance	YES
데이터베이스 계정 비고 수정	ModifyAccountDescription	YES
일괄 자동 갱신 설정	ModifyAutoRenewFlag	YES
인스턴스 이름 수정	ModifyDBInstanceName	YES
TencentDB 인스턴스에 바인딩된 보안 그룹 수정	ModifyDBInstanceSecurityGroups	YES
인스턴스 프로젝트 수정	ModifyDBInstancesProject	YES
데이터베이스 매개변수 수정	ModifyDBParameters	YES
인스턴스 동기화 모드 수정	ModifyDBSyncMode	YES
인스턴스 네트워크 수정	ModifyInstanceNetwork	YES
인스턴스 VIP 수정	ModifyInstanceVip	YES
백업 로그 설정 수정	ModifyLogFileRetentionPeriod	YES
공용 네트워크 액세스 활성화	OpenDBExtranetAccess	YES
인스턴스 갱신	RenewDCDBInstance	YES
계정 비밀번호 재설정	ResetAccountPassword	YES
스마트 DBA 활성화	StartSmartDBA	YES
인스턴스 확장	UpgradeDCDBInstance	YES
전용 인스턴스 업그레이드	UpgradeDedicatedDCDBInstance	YES

보안 그룹 설정

최종 업데이트 날짜: 2024-01-06 15:18:59

보안 그룹은 필터링이 가능한 상태 저장 가상 방화벽입니다. Tencent Cloud에서 제공하는 네트워크 보안 격리를 위한 중요한 수단으로 하나 이상의 TencentDB 인스턴스에 대한 네트워크 액세스 제어를 설정하는 데 사용할 수 있습니다. 한 리전에서 동일한 네트워크 보안 격리 요구가 있는 VPC의 인스턴스는 논리적 그룹인 동일한 보안 그룹에 넣을 수 있습니다(현재 클래식 네트워크의 인스턴스에서는 지원되지 않음). TencentDB와 CVM은 보안 그룹 목록을 공유하며 보안 그룹 내에서 규칙에 따라 서로 매칭됩니다. TencentDB에서 지원하지 않는 규칙은 적용되지 않습니다.

설명:

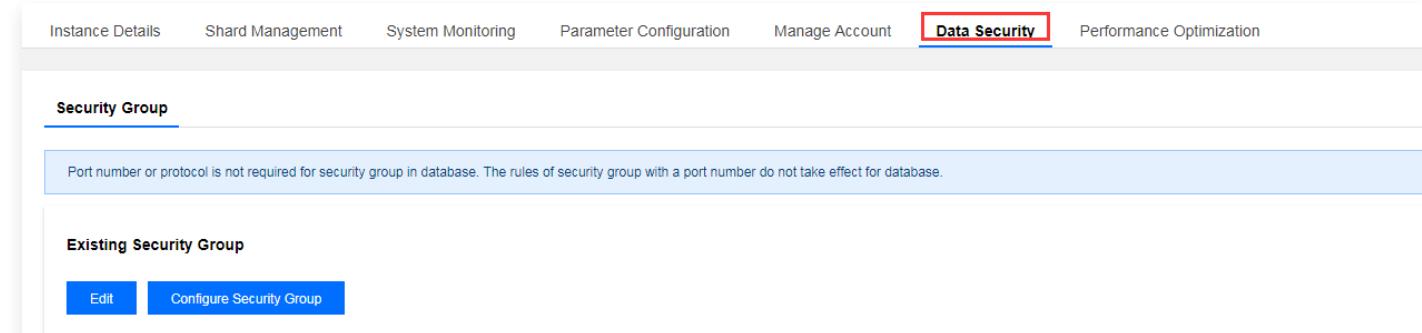
TencentDB 보안 그룹은 현재 VPC의 사설망 액세스를 위한 네트워크 제어를 지원합니다. 광저우, 청두, 상하이, 베이징, 난징 리전에 대해 공중망 액세스의 인스턴스를 활성화하였으며 보안 그룹은 공중망 환경을 지원합니다.

TencentDB 보안 그룹 관리

TDSQL for MySQL 콘솔에 로그인하고 인스턴스 목록에서 인스턴스 ID를 클릭하여 관리 페이지로 들어간 다음 데이터 보안 > 보안 그룹을 선택하여 보안 그룹을 관리합니다.

주의 사항:

- TencentDB는 CVM의 보안 그룹 규칙을 공유합니다. TencentDB 보안 그룹 관리 페이지에서 필요에 따라 규칙 우선 순위를 일치시키거나 조정할 수 있습니다.
- TencentDB 보안 그룹 관리 페이지에서는 보안 그룹 규칙을 생성하거나 삭제할 수 없습니다. 그렇게 하려면 [Viewing a Security Group](#)을 참고하십시오.



Instance Details Shard Management System Monitoring Parameter Configuration Manage Account **Data Security** Performance Optimization

Security Group

Port number or protocol is not required for security group in database. The rules of security group with a port number do not take effect for database.

Existing Security Group

[Edit](#) [Configure Security Group](#)

보안 그룹 정책

보안 그룹 정책은 트래픽 허용과 거부로 나뉩니다. VPC에 배포된 인스턴스의 인바운드 트래픽을 허용하거나 거부하도록 보안 그룹 규칙을 구성할 수 있습니다.

TencentDB 보안 그룹 기본 정책

현재 TencentDB 인스턴스를 구매할 때 네트워크 유형으로 VPC를 선택하면 보안 그룹을 연결할 필요가 없습니다. 이 경우 기본 정책은 ‘모든 IP 및 포트 개방’입니다.

보안 그룹 템플릿

사용자 지정 보안 그룹을 생성하거나 템플릿에서 보안 그룹을 생성할 수 있습니다. 보안 그룹 규칙을 구성하여 CVM 인스턴스의 인바운드 및 아웃바운드 패킷을 제어할 수 있습니다.

보안 그룹 규칙

보안 그룹 규칙은 보안 그룹과 연결된 인스턴스의 인바운드 및 아웃바운드 트래픽을 제어하는 데 사용됩니다(규칙에 따라 위에서 아래로 필터링됨). 기본적으로 신규 보안 그룹은 모든 트래픽을 거절합니다(All Drop). 보안 그룹 규칙은 언제든지 수정할 수 있으며 신규 규칙은 즉시 적용됩니다.

각 보안 그룹 규칙에는 다음 항목이 포함됩니다.

- **프로토콜 및 포트:** TencentDB는 고정 포트를 통한 액세스만 제공하므로 다른 포트로 구성된 보안 그룹 규칙은 TencentDB에 적용되지 않습니다. 예를 들어 TencentDB 인스턴스가 액세스에 포트 3306을 사용하는 경우 보안 그룹 규칙에서 TCP:3306 또는 ALL을 구성할 수 있습니다.
- **권한 부여 유형:** 주소 범위(CIDR/IP) 기반 액세스.
- **원본(인바운드 규칙) 또는 대상(아웃바운드 규칙),** 다음 옵션 중 하나를 선택합니다.
 - CIDR 표기법으로 단일 IP를 지정합니다.
 - CIDR 표기법으로 IP 범위를 지정합니다.
- **정책:** 허용 또는 거부.

보안 그룹 우선 순위

TencentDB 콘솔에서 보안 그룹 우선 순위를 설정할 수 있으며 숫자가 작을수록 우선 순위가 높아집니다. 인스턴스가 여러 보안 그룹과 연결된 경우 우선 순위가 이 인스턴스에 대한 보안 규칙을 평가하는 기준으로 사용됩니다. 또한 인스턴스와 연결된 여러 보안 그룹의 마지막 정책이 **ALL Traffic 거절됨**인 경우 우선 순위가 가장 낮은 보안 그룹을 제외한 모든 보안 그룹의 마지막 정책 **ALL Traffic 거절됨**은 적용되지 않습니다.

보안 그룹의 제한

- 보안 그룹은 VPC **네트워크 환경**의 TencentDB 인스턴스에 적용할 수 있습니다.
- 보안 그룹 정책은 현재 사설망 IP에만 적용되고 있으며, 데이터베이스 공중망 액세스를 활성화할 경우 CVM 포워딩과 함께 사용하여 기업의 최상의 보안을 보장합니다.

- 각 사용자는 동일한 리전의 동일한 프로젝트에 최대 50개의 보안 그룹을 생성할 수 있습니다.
- 보안 그룹에 대해 최대 100개의 인바운드 또는 아웃바운드 규칙을 구성할 수 있습니다. TencentDB에는 활성 아웃바운드 트래픽이 없으므로 TencentDB에는 아웃바운드 규칙이 적용되지 않습니다.
- TencentDB 인스턴스는 여러 보안 그룹과 연결될 수 있고 보안 그룹은 여러 TencentDB 인스턴스와 연결될 수 있습니다. 수에는 제한이 없습니다.

⚠ 주의 사항:

인스턴스 수에는 제한이 없지만 너무 많은 인스턴스를 보안 그룹에 연결하지 않는 것이 좋습니다.

기능 설명	수량
보안 그룹	50개/리전
액세스 정책	100개/인바운드, 100개/아웃바운드
인스턴스와 연결된 보안 그룹의 수	무제한
보안 그룹과 연결된 인스턴스 수	무제한

보안 그룹 규칙 생성, 관리 및 삭제

TencentDB는 CVM의 보안 그룹 규칙을 공유합니다. TencentDB 콘솔의 보안 그룹 관리 페이지에서 필요에 따라 규칙 우선 순위를 일치시키거나 조정할 수 있습니다. 보안 그룹 규칙을 생성, 관리 또는 삭제하려면 VPC 콘솔의 [보안 그룹 페이지](#)에서 수행하십시오. 자세한 지침은 [Viewing a Security Group](#)을 참고하십시오.

TDE 데이터 암호화

최종 업데이트 날짜: 2024-01-06 15:18:59

작업 시나리오

TDSQL for MySQL은 TDE(Transparent Data Encryption) 기능과 함께 제공됩니다. TDE란 데이터의 암호화, 복호화 작업을 사용자에게 투명하게 보여주는 것으로, 데이터 파일에 대한 I/O 암호화 및 복호화를 실시간으로 진행합니다. 데이터를 디스크에 입력하기 전에 암호화하고 디스크에서 메모리를 읽을 때 복호화함으로써 정적 데이터 암호화의 컴플라이언스 요구를 충족할 수 있습니다.

본문은 콘솔에서 데이터 암호화를 활성화하고 데이터를 암호화/복호화하는 방법을 설명합니다.

제한 조건

- TDE 기능은 현재 홍콩의 Percona 5.7 및 MySQL 8.0.24에서만 지원됩니다.

설명:

TDE 암호화 기능을 사용하려면 [Submit Ticket](#)을 통해 신청할 수 있습니다.

- [Key Management Service](#)는 사전에 활성화하거나 TDE 활성화 시 안내에 따라 활성화해야 합니다.
- KMS 키 권한은 사전에 부여하거나 TDE가 활성화된 경우 안내에 따라 부여해야 합니다.

주의 사항

- KMS 활성화 후 [Purchase Method](#)에 설명된 대로 KMS 요금이 발생할 수 있습니다.
- 활성화한 TDE 암호화 기능은 비활성화할 수 없습니다.
- 재해 복구 읽기 전용 인스턴스가 생성되면 TDE를 활성화할 수 없습니다.
- TDE가 활성화된 후에는 재해 복구 읽기 전용 인스턴스를 생성할 수 없습니다.
- TDE 암호화가 활성화된 후에는 백업 파일에서 데이터베이스 인스턴스를 복구할 수 없습니다. [데이터베이스 를 백](#)에 설명된 대로 복구하는 것이 좋습니다.
- TDE 암호화 기능을 활성화하면 정적 데이터의 보안성은 향상되지만 암호화된 데이터베이스에 액세스 시 읽기 및 쓰기 성능에 영향을 미치므로, 실제 상황에 따라 TDE 암호화 기능의 활성화 여부를 선택하시기 바랍니다.
- TDE가 활성화되면 더 많은 CPU 리소스가 소비되고 성능의 약 5%가 손상됩니다.

작업 단계

- [TDSQL 콘솔](#)에 로그인합니다. 인스턴스 ID 또는 작업 열의 관리를 클릭하여 인스턴스 관리 페이지로 이동합니다.
- 인스턴스 관리 페이지에서 [데이터 보안 > 데이터 암호화](#)를 선택하고 ‘암호화 상태’를 켭니다.

Security Group Connection Encryption **Data Encryption**

1. Currently, only MySQL/Percona 5.7 or later supports data encryption. Since encryption will consume more CPU performance, please fully test before enabling it.
2. After data encryption is enabled, users also need to perform DDL operations on database tables, so that the data can be encrypted or decrypted. The details are as below:
 - Encrypt table upon creation: `CREATE TABLE t1 (c1 INT) ENCRYPTION='Y'`
 - Encrypt table after creation: `ALTER TABLE t1 ENCRYPTION = 'Y'`
 - Decrypt: `ALTER TABLE t1 ENCRYPTION='N'`
3. Currently, cross-region disaster recovery read-only instances can't be created after KMS is enabled for the instance.

Data Encryption Settings

Encryption Status **Disabled** (can't be disabled once enabled)
 Encrypt Backup File After data encryption is enabled and DDL encryption is executed, the corresponding table data in the backup file is automatically encrypted.
 Please read [Backup Encryption](#).

3. 팝업 창에서 KMS 서비스 활성화 및 KMS 키 권한을 부여 받고, 키를 선택한 후에 **확인**을 클릭합니다.

Settings**Notes**

1. The data encryption feature may incur the Key Management Service (KMS) service fee. For details, see [KMS Purchase Guide](#)
2. After the feature is enabled, DDL operation is required to encrypt or decrypt the tablespace data.
3. If you want to disable this feature, you need to decrypt all the tablespaces, and submit a ticket after disabling the KMS service.
4. You can't create disaster recovery read-only instance for the instance after data encryption is enabled.

KMS Service

Disabled [Enable KMS](#)

KMS Key Authorization

Authorized

Select Key

 Use auto-generated key

I have read and agreed to the supplementary statement about data encryption in [TencentDB Service Level Agreement](#)

I have read and agreed to [Disclaimer of Tencent Cloud for Information Security During Data Encryption](#)

OK**Cancel**

4. 데이터 암호화가 활성화된 후 데이터를 암호화하거나 해독할 수 있도록 데이터베이스 테이블에 대한 DDL 작업

도 수행해야 합니다. 자세한 내용은 다음과 같습니다:

- 새 테이블 암호화:

```
CREATE TABLE t1 (c1 INT) ENCRYPTION='Y'
```

- 기존 테이블 암호화:

```
ALTER TABLE t1 ENCRYPTION='Y'
```

- 테이블 복호화:

```
ALTER TABLE t1 ENCRYPTION='N'
```

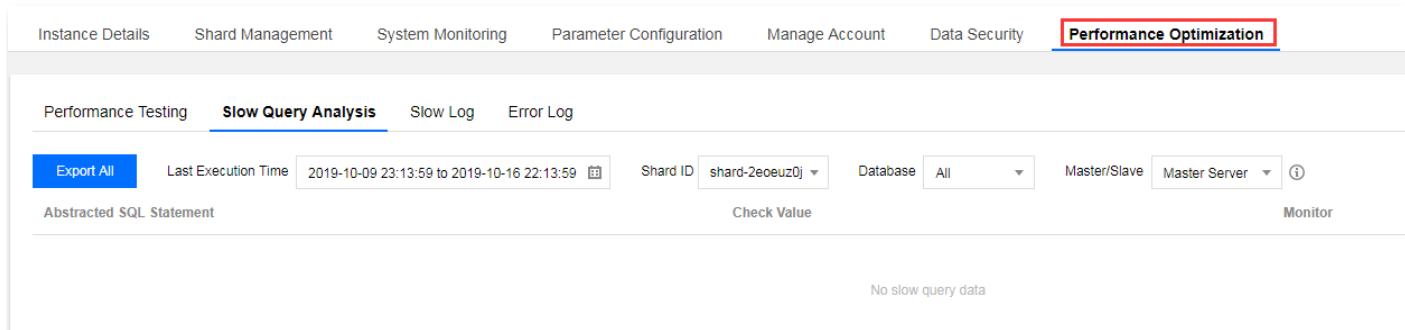
슬로우 쿼리 분석

최종 업데이트 날짜: 2024-01-06 15:18:59

기능 설명

지정된 값보다 더 많은 시간이 소요되는 SQL 문 쿼리를 ‘슬로우 쿼리’라고 하고 해당 문을 ‘슬로우 쿼리 문’이라고 합니다. 데이터베이스 관리자(DBA)가 슬로우 쿼리 문을 분석하고 슬로우 쿼리가 발생하는 이유를 찾는 프로세스를 슬로우 쿼리 분석이라고 합니다.

[TDSQL for MySQL 콘솔](#)에 로그인하고 인스턴스 목록에서 인스턴스 ID를 클릭하여 관리 페이지로 들어간 후 **성능 최적화 > 슬로우 쿼리 분석** 탭을 선택하면 슬로우 쿼리 분석을 수행할 수 있습니다.



설명:

- 오른쪽 상단의    을(를) 클릭하여 표시된 필드를 사용자 정의합니다.
- 현재 슬로우 쿼리 분석은 각 샤드에서 개별적으로만 수행하고 볼 수 있습니다.
- 슬로우 로그를 다운로드하려면 다운로드 주소를 복사하고 [TencentDB 인스턴스와 동일한 VPC의 CVM 인스턴스\(Linux\)에 로그인](#) 한 다음 사설 네트워크를 통한 다운로드를 위해 wget 명령을 실행해야 합니다.

주요 매개변수

주요 기본 설정

- 슬로우 쿼리 기능: 기본적으로 활성화되어 있습니다.
- 슬로우 쿼리 임계값(long_query_time): 기본적으로 1초, 즉 1초 이상 실행된 쿼리 명령만 기록됩니다.
- 분석 데이터 출력 지연: 1분 – 5분.
- 로깅 기간: 백업 및 로그 설정에 따라 30일.

분석 목록 필드

- 체크섬(checksum): 슬로우 쿼리 문(기본값은 64bit)을 식별하는 데 사용되는 일련의 숫자.

- 추상화된 SQL 문(fingerprint): 사용자 데이터가 숨겨진 슬로우 쿼리 문.
- 데이터베이스: 슬로우 쿼리 문이 실행된 데이터베이스.
- 계정: 슬로우 쿼리 문이 발생하는 계정.
- 마지막 실행 시간(last_seen): 지정된 시간 범위 내에서 슬로우 쿼리 문이 마지막으로 실행된 시간.
- 첫 번째 실행 시간(first_seen): 지정된 시간 범위 내에서 슬로우 쿼리 문이 처음 실행된 시간.
- Total(ts_cnt): 지정된 시간 범위 내에서 슬로우 쿼리 문의 실행 횟수.
- 실행 비율(%): 지정된 시간 범위 내 모든 슬로우 쿼리 문의 총 실행에 대한 슬로우 쿼리 문의 총 실행 비율.
- 총 시간(query_time_sum): 지정된 시간 범위 내에서 슬로우 쿼리 문이 소비한 총 시간.
- 총 시간(%): 지정된 시간 범위 내에서 모든 슬로우 쿼리 명령문이 소비한 총 시간에 대한 슬로우 쿼리 명령문이 소비한 총 시간의 비율.
- 평균 시간(query_time_avg): 평균 시간은 슬로우 쿼리 문에서 소비한 총 시간을 슬로우 쿼리 문의 총 실행 횟수로 나누어 계산.
- 최소 시간(query_time_min): 슬로우 쿼리 문의 전체 실행 시간 중 최소값.
- 최대 시간(query_time_max): 슬로우 쿼리 문의 전체 실행 시간 중 최대값.
- 총 잠금 시간(lock_time_sum): 슬로우 쿼리 문의 총 잠금 시간.
- 전체 잠금 시간 비율: 모든 슬로우 쿼리 문의 총 잠금 시간에 대한 슬로우 쿼리 문의 총 잠금 시간의 비율(퍼센트).
- 평균 잠금 시간(lock_time_avg): 슬로우 쿼리 문의 총 잠금 시간을 슬로우 쿼리 문의 총 잠금 횟수로 나누어 계산한 평균 시간.
- 최소 잠금 시간(lock_time_min): 슬로우 쿼리 문의 전체 잠금 시간 중 최소값.
- 최대 잠금 시간(lock_time_max): 슬로우 쿼리 문의 전체 잠금 시간 중 최대값.
- 보낸 행(Rows_sent_sum): 슬로우 쿼리 문에서 보낸 데이터 행의 총 수.
- 스캔된 행(Rows_examined_sum): 슬로우 쿼리 문으로 스캔한 데이터 행의 총 수.
- 호스트 주소(Host): 이 슬로우 쿼리가 발생하는 호스트입니다.
- 모니터링: 클릭하면 SQL 문의 분석 내용을 볼 수 있습니다.
- SQL 예시: SQL 문의 일반적인 예시입니다.

백업과 롤백

백업 방식

최종 업데이트 날짜: 2024-01-06 15:18:59

TDSQL for MySQL은 전체 백업 및 증분 백업을 지원합니다.

백업 유형

전체 백업

전체 백업의 시작 시간과 저장 기간을 설정할 수 있습니다. 저장 기간은 기본적으로 7일입니다.

증분 백업

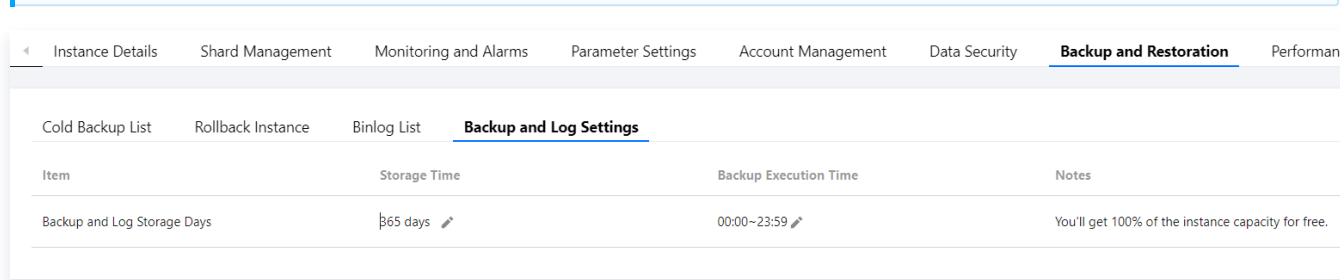
증분 백업은 실시간으로 생성되는 binlog를 기반으로 구현됩니다. binlog는 일정량의 디스크 용량을 사용하며 주기적으로 TencentDB 백업 시스템에 업로드됩니다.

사용자 지정 백업 시간

1. [TDSQL for MySQL 콘솔](#)에 로그인하고 **작업** 열에서 인스턴스 ID 또는 **관리**를 클릭하여 인스턴스 관리 페이지로 이동합니다.
2. 인스턴스 관리 페이지에서 **백업과 복원**을 클릭합니다.
3. **백업과 복원 > 백업 및 로그 설정** 페이지에서 저장 기간과 백업 실행 시간을 설정합니다.
 - 보관 시간: 데이터 및 로그 백업은 1일 – 365일 동안 보관할 수 있습니다. 기본값: 7일.
 - 백업 실행 시간: 시간 단위로 임의의 기간으로 설정할 수 있습니다. 기본 값: 전일.

설명:

로그 백업은 기본적으로 활성화되어 있으며 비활성화할 수 없습니다. 로그에는 오류 로그, 슬로우 로그, 트랜잭션 로그(binlog) 등이 포함됩니다.



Item	Storage Time	Backup Execution Time	Notes
Backup and Log Storage Days	365 days	00:00~23:59	You'll get 100% of the instance capacity for free.

백업 파일 다운로드

최종 업데이트 날짜: 2024-01-06 15:18:59

작업 시나리오

TDSQL for MySQL 콘솔에서 TencentDB 콜드 백업 데이터 및 binlog를 다운로드할 수 있습니다.

작업 단계

1. [TDSQL for MySQL 콘솔](#)에 로그인하고 **작업** 열에서 인스턴스 ID 또는 **관리**를 클릭하여 인스턴스 관리 페이지로 이동합니다.
2. **백업 및 복원 > 콜드 백업 목록** 또는 **Binlog 목록**을 선택합니다.
3. 대상 색상 ID와 시간을 선택합니다. 그 다음 **작업** 열에서 **다운로드**를 클릭합니다.
4. 팝업 창에서 **다운로드 주소 가져오기**를 클릭하여 VPC의 다운로드 주소를 가져옵니다.
5. [Linux CVM 커스텀 설정](#)의 지침에 따라 데이터베이스가 있는 VPC에서 CVM(Linux 시스템)에 로그인하고 `wget` 명령을 실행하여 파일을 다운로드합니다.

설명:

- 공중망에서 다운로드: 데이터베이스 백업 페이지의 **다운로드 설정**에서 이 옵션을 활성화합니다. 그 다음 다운로드 링크를 브라우저에 직접 복사하여 다운로드할 수 있습니다.
- 사설망에서 다운로드: VPC의 인스턴스에 액세스하고 `wget` 명령을 사용하여 다운로드하십시오:
`wget -O <사용자 정의 이름.log> '<파일 다운로드 주소>' .`
- 주소는 15분 동안 유효합니다. 만료 후에는 페이지를 새로고침하여 다시 가져와야 합니다.

Download

X

Notes

1. To ensure data security, **Each address is valid for 15 minutes**. Upon expiration, click "Get Download Address" again to get a new one.
2. Download over public network: Enable it on "Database Backup" > "Download Settings", and copy the download address to the browser for download.
3. Download over private network: Run the `wget` command (format: wget -O <custom filename.log> '<backup download address>') for download in a VPC.
4. View and download [Help Documentation](#)

Get Download Address**Close**

백업 암호화

최종 업데이트 날짜: 2024-01-06 15:18:59

기능 개요

분산형 TDSQL for MySQL은 TDE(Transparent Data Encryption) 기능을 지원합니다. TDE란 데이터의 암호화, 복호화 작업을 사용자에게 투명하게 보여주는 것으로, 데이터 파일에 대한 I/O 암호화 및 복호화를 실시간으로 진행합니다. 데이터를 디스크에 입력하기 전에 암호화하고 디스크에서 메모리를 읽을 때 복호화함으로써 정적 데이터 암호화의 컴플라이언스 요구를 충족할 수 있습니다.

TDE는 홍콩 리전의 Percona 5.7 버전에서만 지원되지만 향후 더 많은 커널 버전에서 사용할 수 있습니다. [TDSQL 콘솔](#)의 인스턴스 관리 페이지에서 [데이터 보안 > 데이터 암호화](#)에 액세스할 수 있습니다.

데이터 암호화가 활성화된 후에는 백업 파일에서 데이터베이스 인스턴스를 복구할 수 없습니다. [데이터베이스 롤백](#)에 설명된 대로 복구하는 것이 좋습니다.

설명:

데이터 암호화 기능을 사용하려면 [Submit Ticket](#)을 통해 신청할 수 있습니다.

주의 사항

- 현재 KMS가 활성화된 인스턴스에 대해 재해 복구 읽기 전용 인스턴스를 생성할 수 없습니다. KMS에 대한 자세한 내용은 [Getting Started](#)를 참고하십시오.
- 활성화한 TDE 암호화 기능은 비활성화할 수 없습니다.
- TDE 암호화 기능을 활성화하면 정적 데이터의 보안성은 향상되지만 암호화된 데이터베이스에 액세스 시 읽기 및 쓰기 성능에 영향을 미치므로, 실제 상황에 따라 TDE 암호화 기능의 활성화 여부를 선택하시기 바랍니다.
- TDE가 활성화되면 더 많은 CPU 리소스가 소비되고 성능의 약 5%가 손상됩니다.

데이터베이스 롤백

최종 업데이트 날짜: 2024-01-06 15:18:59

롤백 설명

TDSQL for MySQL은 백업 및 로그 보존을 기반으로 지난 30일의 어느 시점으로든 데이터를 롤백할 수 있습니다. 데이터베이스 롤백 기능으로 시스템 손실을 최소화할 수 있습니다.

TDSQL for MySQL의 롤백 기능은 프로덕션 인스턴스에 영향을 미치지 않으며 Tencent Cloud에서 생성한 새로운 종량제 인스턴스로 데이터를 직접 롤백할 수 있습니다. 이 새로운 롤백 인스턴스는 표준 인스턴스이며 필요에 따라 구성할 수 있습니다.

제한 조건

- 임시 인스턴스를 롤백하고 생성하는 동안 Tencent Cloud 콘솔에서 프로덕션 인스턴스의 일부 관리 기능을 사용할 수 없으며 이러한 기능은 작업이 완료된 후에 사용할 수 있습니다.
- binlog는 롤백 작업 중 강제로 샤딩될 수 있으며, 100MB 미만의 파일은 별도로 백업됩니다.
- 롤백 후 새로 구매한 인스턴스는 Tencent Cloud 콘솔에서 프로덕션 인스턴스의 매개변수 정보(계정, 데이터베이스 매개변수 등)를 갖게 됩니다. 따라서 계정 관리에 주의를 기울여야 합니다.

인스턴스 롤백

- TDSQL for MySQL 콘솔에 로그인하고 인스턴스 ID를 클릭하고 인스턴스 관리 페이지로 들어갑니다.
- 인스턴스 관리 페이지에서 **백업 및 복원 > 인스턴스 롤백** 탭을 선택하고 **롤백 인스턴스 생성**을 클릭합니다.

- 팝업 창에서 롤백 시간을 설정하고 **확인**을 클릭합니다.

Rollback Settings



Create a pay-as-you-go instance (the rollback instance) based on the data of the selected instance (the data source instance) backed up at the specified point in time

Set Rollback Time *

Select time



1. The rollback time must be within the backup retention period (2022-05-19 16:09:21 - 2022-05-26 14:44:29).
2. The pay-as-you-go instance will be created based on backup data without affecting the data source instance.

OK

Cancel

4. 인스턴스 구매 페이지에서 필요에 따라 구성을 조정하고 **구매하기**를 클릭한 다음 인스턴스 롤백이 완료될 때까지 기다립니다.
5. 롤백이 완료된 후 **백업 및 복원 > 인스턴스 롤백** 페이지 또는 인스턴스 목록에서 생성된 롤백 인스턴스를 볼 수 있습니다.

데이터 마이그레이션

최종 업데이트 날짜: 2024-01-06 15:18:59

MySQL에서 MySQL로 마이그레이션의 지침에 따라 Data Transmission Service를 통해 TDSQL for MySQL로 데이터를 마이그레이션할 수 있습니다.

데이터베이스 감사

데이터베이스 감사 활성화

최종 업데이트 날짜: 2024-01-06 15:18:59

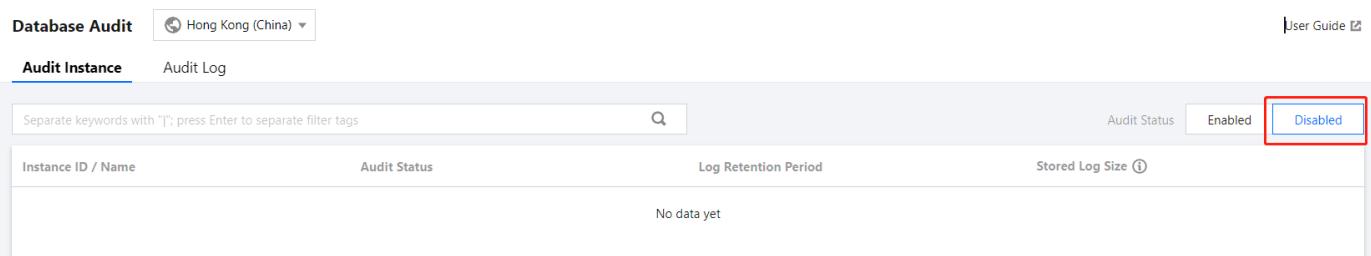
TDSQL for MySQL은 데이터베이스 감사 기능을 제공하여, 데이터베이스 액세스 및 SQL 명령 실행 상황을 기록하고 기업의 리스크 관리와 데이터 보안 등급 향상을 지원합니다.

설명:

데이터베이스 감사 기능은 현재 베타 테스트 중입니다. 이 기능을 사용하려면 [티켓 제출](#)을 통해 신청할 수 있습니다.

SQL 감사 서비스 활성화

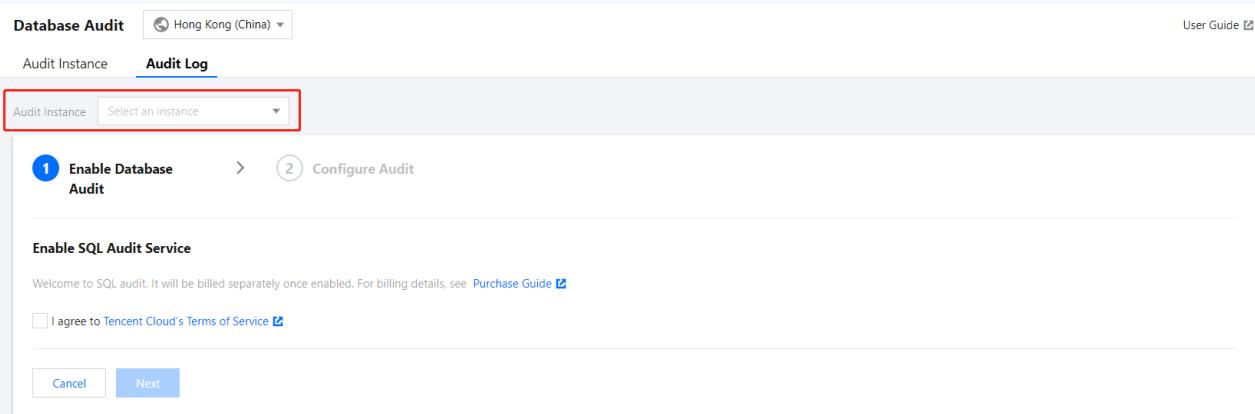
1. [TDSQL for MySQL 콘솔](#)에 로그인하여 왼쪽 사이드바에서 **데이터베이스 감사**를 선택하고 상단에서 리전을 선택합니다. 감사 인스턴스 탭을 클릭하고 **비활성화**를 클릭하여 감사가 비활성화된 인스턴스를 필터링합니다.



Instance ID / Name	Audit Status	Log Retention Period	Stored Log Size
No data yet			

설명:

또는 감사 로그 탭의 감사 인스턴스에서 감사가 미활성화된 인스턴스를 직접 검색한 다음 감사를 활성화합니다.



1 Enable Database Audit > 2 Configure Audit

Enable SQL Audit Service

Welcome to SQL audit. It will be billed separately once enabled. For billing details, see [Purchase Guide](#)

I agree to Tencent Cloud's Terms of Service

[Cancel](#) [Next](#)

2. 감사 인스턴스 탭에서 대상 인스턴스의 ID를 클릭하여 활성화 페이지로 이동하고 계약에 대한 동의를 표시한

후 다음 단계를 클릭합니다.

3. SQL 감사 서비스 설정 페이지에서 감사 로그 저장 기간을 선택하고 활성화를 클릭합니다.

 설명:

- 감사 로그의 보관 기간은 7일, 30일, 3개월, 6개월, 1년, 3년, 5년 중에서 선택할 수 있습니다. 감사 를 활성화한 후 콘솔에서 수정할 수도 있습니다. 자세한 내용은 [Modifying Log Retention Period](#) 를 참고하십시오.
- SQL 로그 저장 기간에 대한 보안 컴플라이언스 요구 사항을 충족하기 위해, 180일 이상으로 선택 하는 것이 좋습니다.

감사 로그 조회

감사를 활성화한 후 감사 로그 탭에서 SQL 감사 로그를 볼 수 있습니다. 자세한 내용은 [Viewing Audit Logs](#)를 참 고하십시오.

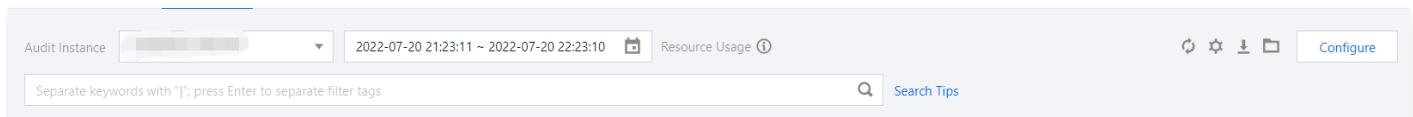
감사 로그 조회

최종 업데이트 날짜: 2024-01-06 15:18:59

로그 조회

1. TDSQL for MySQL 콘솔 로그인 후, 왼쪽 사이드바에서 **데이터베이스** 감사를 선택하고, 상단의 리전 선택 후, **감사 로그** 탭을 클릭합니다.
2. 감사 로그 탭의 감사 인스턴스 섹션에서 감사가 활성화된 데이터베이스 인스턴스를 선택하여 SQL 감사 로그를 봅니다. 또는 감사 인스턴스 탭에서 인스턴스 ID를 클릭하여 **감사 로그** 탭으로 이동하여 감사 로그를 봅니다.

툴 리스트



- **시간 창**에서 기간을 선택하면 선택한 기간의 감사 결과를 볼 수 있습니다.

① 설명:

검색할 데이터가 있는 기간을 선택할 수 있습니다. 처음 60000개의 적합한 레코드를 표시할 수 있습니다.

- **검색 창**에서 키 태그로 검색하여 관련 감사 결과를 볼 수 있습니다. 공통 키 태그에는 SQL 명령, 클라이언트 IP, 데이터베이스 이름, 데이터베이스 계정, 실행 시간, 영향을 받는 행 수 및 반환 행 수가 포함됩니다.
- 검색을 위해 여러 키 태그를 입력할 때 엔터 키를 눌러 분리할 수 있습니다.
- 와일드카드 ‘*’를 사용하여 IP 주소를 필터링할 수 있습니다. 예를 들어 ‘클라이언트 IP: 10.0.0.0’를 입력하면 10.0.0.0로 시작하는 IP 주소가 검색됩니다.

로그 리스트

반환된 행 수 필드는 주로 SELECT 명령의 영향을 판단하는 데 사용되는 SQL 명령을 실행하여 반환된 행 수를 나타냅니다.

SQL 감사 필드

TDSQL for MySQL 콘솔의 **감사 로그** 탭에서 다음 아이콘을 클릭하여 전체 SQL 감사 로그를 가져와 확인할 수 있습니다.

Audit Instance	2022-07-20 21:23:11 ~ 2022-07-20 22:23:10	Resource Usage	Configure				
Separate keywords with " "; press Enter to separate filter tags							
Time	Client IP	Database Name	User Account	SQL Details	Returned Rows	Affecte...	Executi...
No data yet							

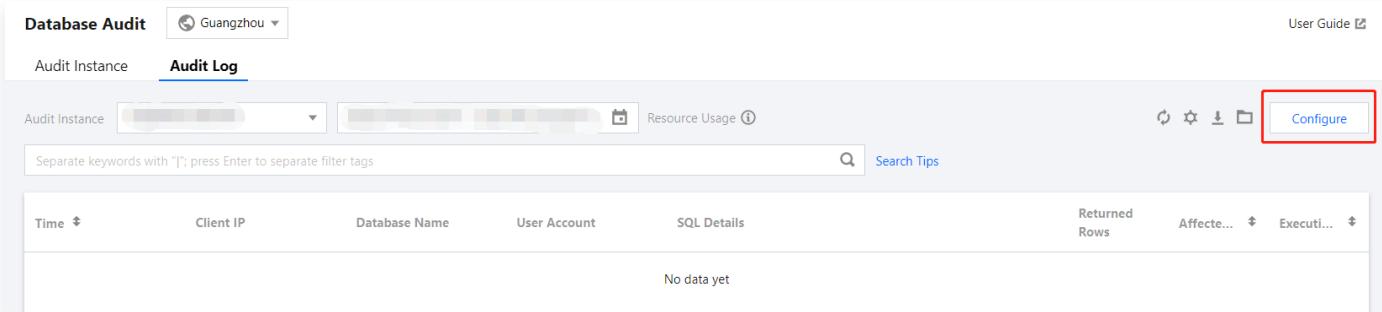
로그 저장 기간 설정

최종 업데이트 날짜: 2024-01-06 15:18:59

본문에서는 데이터베이스 감사 서비스가 활성화된 후 로그 저장 기간을 수정하는 방법에 대해 설명합니다.

작업 단계

1. [TDSQL for MySQL 콘솔](#) 로그인 후, 왼쪽 사이드바에서 **데이터베이스 감사**를 선택하고, 상단의 리전 선택 후, **감사 로그** 탭을 클릭합니다.
2. 감사 로그 탭의 오른쪽 상단에서 **서비스 구성**을 클릭합니다.



The screenshot shows the 'Audit Log' configuration page. At the top, there are tabs for 'Database Audit' and 'Audit Log', with 'Audit Log' being the active tab. Below the tabs, there are dropdowns for 'Audit Instance' and 'Region' (set to Guangzhou). A search bar with placeholder text 'Separate keywords with ":"; press Enter to separate filter tags' and a 'Search Tips' link are also present. The main area contains a table with the following columns: Time, Client IP, Database Name, User Account, SQL Details, Returned Rows, Affected Rows, and Executed Rows. The table body displays the message 'No data yet'. On the far right of the table, there are several icons for filtering and sorting. A red box highlights the 'Configure' button in the top right corner of the main content area.

3. 팝업 창에서 로그 저장 기간을 수정하고 **제출**을 클릭합니다.