Alibaba Cloud ApsaraDB for MySQL

安全白皮書

檔案版本：20190906

法律聲明

阿里雲提醒您在閱讀或使用本文檔之前仔細閱讀、充分理解本法律聲明各條款的內容。如果您閱讀或使用本文檔，您的閱讀或使用行為將被視為對本聲明全部內容的認可。

1. 您應當通過阿里雲網站或阿里雲提供的其他授權通道下載、擷取本文檔，且僅能用於自身的合法合規的商務活動。本文檔的內容視為阿里雲的保密資訊，您應當嚴格遵守保密義務；未經阿里雲事先書面同意，您不得向任何第三方披露本手冊內容或提供給任何第三方使用。
2. 未經阿里雲事先書面許可，任何單位、公司或個人不得擅自摘抄、翻譯、複製本文檔內容的部分或全部，不得以任何方式或途徑進行傳播和宣傳。
3. 由於產品版本升級、調整或其他原因，本文檔內容有可能變更。阿里雲保留在沒有任何通知或者提示下對本文檔的內容進行修改的權利，並在阿里雲授權通道中不時發布更新後的使用者文檔。您應當即時關注使用者文檔的版本變更並通過阿里雲授權渠道下載、擷取最新版的使用者文檔。
4. 本文檔僅作為使用者使用阿里雲產品及服務的參考性指引，阿里雲以產品及服務的”現狀“、“有缺陷”和“當前功能”的狀態提供本文檔。阿里雲在現有技術的基礎上盡最大努力提供相應的介紹及操作指引，但阿里雲在此明確聲明對本文檔內容的準確性、完整性、適用性、可靠性等不作任何明示或暗示的保證。任何單位、公司或個人因為下載、使用或信賴本文檔而發生任何差錯或經濟損失的，阿里雲不承擔任何法律責任。在任何情況下，阿里雲均不對任何間接性、後果性、懲戒性、偶然性、特殊性或刑罰性的損害，包括使用者使用或信賴本文檔而遭受的利潤損失，承擔責任（即使阿里雲已被告知該等損失的可能性）。
5. 阿里雲網站上所有內容，包括但不限於著作、產品、圖片、檔案、資訊、資料、網站架構、網站畫面的安排、網頁設計，均由阿里雲和/或其關係企業依法擁有其智慧財產權，包括但不限於商標權、專利權、著作權、商業秘密等。非經阿里雲和/或其關係企業書面同意，任何人不得擅自使用、修改、複製、公開傳播、改變、散布、發行或公開發表阿里雲網站、產品程式或內容。此外，未經阿里雲事先書面同意，任何人不得為了任何營銷、廣告、促銷或其他目的使用、公布或複製阿里雲的名稱（包括但不限於單獨為或以組合形式包含”阿里雲”、Aliyun”、“萬網”等阿里雲和/或其關係企業品牌，上述品牌的附屬標誌及圖案或任何類似公司名稱、商號、商標、產品或服務名稱、網域名稱、圖案標示、標誌、標識或通過特定描述使第三方能夠識別阿里雲和/或其關係企業）。
6. 如若發現本文檔存在任何錯誤，請與阿里雲取得直接聯絡。

通用約定

格式	說明	範例
	該類警示資訊將導致系統重大變更甚至故障，或者導致人身傷害等結果。	 **禁止:** 重設操作將丟失使用者配置資料。
	該類警示資訊可能導致系統重大變更甚至故障，或者導致人身傷害等結果。	 **警告:** 重啟操作將導致業務中斷，恢複業務所需時間約10分鐘。
	用於補充說明、最佳實務、竅門等，不是使用者必須瞭解的內容。	 **说明:** 您也可以通過按Ctrl + A選中全部檔案。
>	多級菜單遞進。	設定 > 網路 > 設定網路類型
粗體	表示按鍵、菜單、頁面名稱等UI元素。	單擊 確定。
`courier 字型`	命令。	執行 `cd / d C :/ windows` 命令，進入Windows系統檔案夾。
*## *	表示參數、變數。	`bae log list --instanceid` *Instance_ID*
[]或者[a|b]	表示可選項，至多選擇一個。	`ipconfig` *[-all|-t]*
{}或者{a|b}	表示必選項，至多選擇一個。	`swich` *{stand | slave}*

目錄

1 產品概述

雲資料庫RDS（Relational Database Service）是一種穩定可靠、可Auto Scaling的線上資料庫服務。基于飛天分布式系統和全SSD盤高效能儲存，支援MySQL、SQL Server、PostgreSQL、PPAS（高度相容Oracle）和MariaDB引擎，預設部署主備架構且提供了容災、備份、恢複、監控、遷移等方面的全套解決方案，徹底解決資料庫營運的煩惱。

雲資料庫RDS提供了多樣化的安全強化功能來保障使用者資料的安全，其中包括但不限於：

- 網路：IP 白名單、VPC 網路、SSL（安全套接層協議）
- 儲存：TDE（透明資料加密）、自動備份
- 容災：同城容災（多可用性區域執行個體）、異地容災（兩地多中心）

2 攻擊防護

防 DDoS 攻擊

當使用者使用外網串連和訪問 RDS 執行個體時，可能會遭受 DDoS 攻擊。RDS提供流量清洗和黑洞處理功能，完全由系統自動觸發和結束。當 RDS 安全體系認為使用者執行個體正在遭受 DDoS 攻擊時，會首先啟動流量清洗功能，如果流量清洗無法抵禦攻擊或者攻擊達到黑洞閾值，則會進行黑洞處理。

说明:

建議使用者通過內網訪問 RDS 執行個體，可以使 RDS 執行個體免受 DDoS 攻擊的風險。

流量清洗

只針對外網流入流量進行清洗，處於流量清洗狀態的 RDS 執行個體可正常訪問。

單個 RDS 執行個體滿足以下任一條件即觸發流量清洗：

- PPS（Package Per Second）達到 3 萬；
- BPS（Bits Per Second）達到 180 Mbps；
- 每秒建立並發串連達到 1 萬；
- 啟用並發串連數達到 1 萬；
- 非啟用並發串連數達到 10 萬。

黑洞處理

只針對外網流入流量進行黑洞處理，處於黑洞狀態的 RDS 執行個體不可被外網訪問，此時應用程式通常也處於不可用狀態。黑洞處理是保證 RDS 整體服務可用性的一種手段。

黑洞觸發條件如下：

- BPS（Bits Per Second）達到 2 Gbps；
- 流量清洗無效。

黑洞結束條件如下：

- 黑洞在 2.5 小時後自動解除。

檢測SQL注入威脅

Security Center基於第三代SQL注入威脅檢測資料智能演算法引擎，支援檢測RDS的SQL注入威脅，即時識別潛在的資料安全風險。詳情請參見SQL注入威脅檢測。

3 存取控制

當使用者建立執行個體後，RDS並不會為使用者建立任何初始的資料庫帳號。

有如下兩種方式來建立資料庫帳號：

- 使用者可以通過控制台或者API來建立普通資料庫帳號，並設定資料庫層級的唯讀、讀寫、DDL、DML許可權。
- 如果使用者需要更細粒度的許可權控制，比如表、視圖、欄位層級的許可權，也可以通過控制台或者API先建立高許可權資料庫帳號，然後登入資料庫建立普通資料庫帳號。高許可權資料庫帳號可以為普通資料庫帳號設定表層級的讀寫權限。

IP白名單

RDS提供了IP白名單來實現網路安全存取控制。

預設情況下，RDS執行個體被設定為不允許任何IP訪問，即127.0.0.1。使用者可以通過控制台的資料安全性模組或者API來添加IP白名單規則。IP白名單的更新無需重啟RDS執行個體，因此不會影響使用者的使用。

IP白名單可以設定多個分組，每個分組可配置1000個IP或IP段。

4 資料加密

SSL

RDS提供MySQL和SQL Server的安全套接層協議（Secure Sockets Layer，簡稱SSL）。您可以使用RDS提供的伺服器端的根憑證來驗證目標地址和連接埠的資料庫服務是不是RDS提供的，從而可有效避免中間人攻擊。除此之外，RDS還提供了伺服器端SSL認證的啟用和更新能力，以便使用者按需更替SSL認證以保障安全性和有效性。

需要注意的是，雖然RDS提供了應用到資料庫之間的串連加密功能，但是SSL需要應用開啟伺服器端驗證才能正常運轉。另外SSL也會帶來額外的CPU開銷，RDS執行個體的輸送量和回應時間都會受到一定程度的影響，具體影響與您的串連次數和資料轉送頻度有關。

具體操作請參見設定SSL。

TDE

RDS提供MySQL和SQL Server的透明資料加密（Transparent Data Encryption，簡稱TDE）功能。MySQL版的TDE由阿里雲自研，SQL Server版的TDE是基於SQL Server企業版的功能改造而來。

當RDS執行個體開啟TDE功能後，您可以指定參與加密的資料庫或者表。這些資料庫或者表中的資料在寫入到任何裝置（磁碟、SSD、PCIe卡）或者服務（Table StoreOSS、Archive StorageOAS）前都會進行加密，因此執行個體對應的資料檔案和備份都是以密文形式存在的。

TDE加密採用國際流行的AES演算法，密鑰長度為128位元。密鑰由KMS服務加密儲存，RDS只在啟動執行個體和遷移執行個體時動態讀取一次密鑰。您可以自行通過KMS控制台對密鑰進行更換。

具體操作請參見設定透明資料加密。

5 備份恢複

備份功能

為保證資料的完整性和可靠性，資料庫需要常規的自動備份來保障資料的可恢複性。

RDS提供如下兩種備份功能：

- 資料備份：強制項，您每周必須選擇兩天及兩天以上的備份周期和備份時間段來進行全量的常規物理備份。另外，您也可以根據營運需要，通過控制台或者API隨時發起全量的臨時物理備份。
- 記錄備份：可選項，您可以選擇開啟或者關閉。如果關閉記錄備份，那麼恢複資料時只能恢複到資料備份集所在的時間點。資料備份和記錄備份使用相同的到期刪除策略。您可以將備份到期的天數設定為7到730中的任何一個數字，也可以通過調整到期策略即時刪除較老的備份。

恢複功能

資料可恢複性是判斷資料庫營運可靠性的關鍵計量。

RDS提供如下三種恢複功能：

- 按備份組恢複：您可以將指定備份組的資料恢複到一個臨時執行個體或複製執行個體上。您可以在臨時執行個體或複製執行個體上檢查自己的資料是否完好。
- 按時間點恢複：您可以選擇臨近時間點，系統根據全量備份以及之後的記錄備份，將資料重新放到一個臨時執行個體或複製執行個體上。
- 覆蓋性恢複：您可以將指定備份組的資料恢複到當前RDS執行個體上，而非臨時執行個體或複製執行個體。但若您使用這種恢複方式，恢複後的執行個體將不具備資料恢複功能，謹慎使用。資料恢複功能和備份策略緊密相關，其中：
  - 資料恢複的早時間取決於早一個資料備份（與資料備份的頻率和到期策略相關）。
  - 資料恢複的晚時間取決於後一個記錄備份（與日誌產生量有很大關係）。
  - 資料恢複是否支援按時間點恢複取決於記錄備份是否開啟。
  - 資料恢複的速度取決於資料備份的頻率（也與日誌產生量有很大關係）。

相關文檔

- #unique_10
- #unique_11
- #unique_12
- #unique_13
- #unique_14

6 軟體升級

RDS會為您提供資料庫軟體的新版本。

在絕大多數情況下，版本升級都是非強制性的。但在您主動重啟RDS執行個體時，該執行個體的資料庫版本會在重啟時升級到最新的相容版本。

在極少數情況下（如致命的重大Bug、安全性漏洞），RDS執行個體（除基礎版外）會在可營運時間內發起資料庫版本的強制升級。需要注意的是，強制升級僅會引起幾次資料庫連接閃斷，在應用程式正確配置了資料庫連接池的情況下，不會對應用程式造成明顯的影響。

您可以通過控制台或者API來修改可營運時間，以避免RDS在業務高峰期發生了強制升級。

7 產品安全方案