Alibaba Cloud ApsaraDB for RDS

Security White Paper

Issue: 20200624

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 **Notice:** If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings** > **Network** > **Set network type**.
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click **OK**.
Courier font	Courier font is used for commands.	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

Contents

1 Performance overview

ApsaraDB for RDS is a stable, reliable, and automatically scalable online database service.

Based on the Apsara distributed file system of Alibaba Cloud and the full SSD high-performance storage, RDS provides a complete set of solutions for disaster tolerance, backup, recovery, monitoring, and migration to free you from the burden of database O&M . RDS supports a variety of engines such as MySQL, SQL Server, PostgreSQL, and PPAS which is highly compatible with Oracle.

ApsaraDB for RDS provides a variety of security hardening features to secure user data, including but not limited to:

- Network: whitelist, VPC, SSL encryption etc.
- Storage: #unique_7, automatically back up data etc.
- Disaster recovery: zone-disaster recovery (multi-zone instances), geo-disaster recovery (across two data centers and multiple data centers).

2 Attack protection

This topic provides an overview of attach protection for ApsaraDB for RDS.

DDoS attack prevention

When you access an ApsaraDB for RDS instance from the Internet, the instance is vulnerable to DDoS attacks. ApsaraDB for RDS provides the traffic scrubbing and black hole filtering features that are automatically triggered and terminated by the RDS security system. When a DDoS attack is detected, the RDS security system first scrubs the inbound traffic. If traffic scrubbing is not sufficient or if the traffic exceeds a specified threshold, black hole filtering is triggered.

> **Note:**
> We recommend that you access RDS instances over an internal network to protect them against DDoS attacks.

Traffic scrubbing

Traffic scrubbing is only for traffic flows from the Internet and does not affect normal operations of your instance.

Traffic scrubbing is triggered for a single ApsaraDB for RDS instance if any of the following conditions are met:

- Packets per second (PPS) reaches 30,000.
- Bits per second (BPS) reaches 180 Mbit/s.
- The number of new concurrent connections per second reaches 10,000.
- The number of active concurrent connections reaches 10,000.
- The number of idle concurrent connections reaches 100,000.

Black hole filtering

Black hole filtering is only for traffic flows from the Internet. If an RDS instance is undergoing black hole filtering, the instance cannot be accessed from the Internet and the connected applications are unavailable. Black hole filtering guarantees availability of RDS.

Black hole filtering is triggered if any of the following conditions are met:

- BPS reaches 2 Gbit/s.
- Traffic scrubbing is insufficient to protect against DDoS attacks.

Black hole is automatically deactivated in 2.5 hours.

3 Access control

ApsaraDB for RDS implements multi-dimensional access control to ensure data security.

You can create database accounts by using one of the following methods:

- Create a standard database account in the ApsaraDB for RDS console or by calling an API operation. Then, grant read-only, read/write, DDL, or DML permissions on different databases to the account. For more information, see Create an account for an ApsaraDB RDS for MySQL instance.
- If you want to implement access control at a fine-grained level, such as for tables, views, and fields, create a privileged account in the ApsaraDB for RDS console or by calling an API operation. Then, log on to a database to create standard accounts. The privileged account can grant fine-grained permissions to the standard accounts. For more information, see Authorize accounts to manage tables, views, and fields.

Whitelists

ApsaraDB for RDS supports whitelists for access control to ensure network security.

By default, RDS instances block access from all IP addresses. The default IP address whitelist contains only 127.0.0.1. You can configure a whitelist on the Data Security page in the ApsaraDB for RDS console or by calling an API operation. If you update a whitelist of an RDS instance, no restart of the RDS instance is required. Your businesses are not affected.

4 Network isolation

ApsaraDB for RDS provides multiple network isolation mechanisms to ensure network security.

VPC

In addition to the IP address whitelist, ApsaraDB for RDS allows you to use virtual private cloud to obtain advanced network access control.

VPC is a private network environment, it strictly isolates packets through network protocols and implements control access at layer 2. You can connect the servers you build in IDCs to Alibaba Cloud through VPN or physical connections. You can also use the RDS IP address segment defined in VPC to handle IP address conflicts, allows both your own server and Alibaba Cloud ECS to access RDS.

The combination of VPCs and IP address whitelists is an ideal option for you to secure apsaradb for RDS instances.

For more information about VPC, see #unique_16.

Internet

By default, RDS instances deployed in a VPC network are only accessible from the ECS instances in the same VPC network. You can also apply for a public IP address to receive access requests from the public network (not recommended). The requests include but are not limited to:

- Access requests from ECS EIPs.
- Access requests from the user-created IDC to the egress.

IP address whitelists apply to all connections to ApsaraDB for RDS instances. We recommend that you configure the whitelist before applying for a public IP address.

For more information, see #unique_17.

5 Data encryption

SSL

ApsaraDB for RDS supports Secure Sockets Layer (SSL) for MySQL and SQL Server. You can use the server root certificate provided by ApsaraDB for RDS to determine whether the database service that you access by using the target IP address and port is provided by ApsaraDB for RDS. This can effectively prevent against man-in-the-middle attacks. ApsaraDB for RDS also allows you to enable and update SSL certificates for servers to ensure data security and validity.

Although ApsaraDB for RDS can encrypt the connection between your application and database, SSL cannot run properly until the server authentication is enabled for your application. SSL consumes extra CPU resources. This affects the throughput and response time of instances. The severity of the impact depends on the number of user connections and the frequency of data transmission.

For more information, see Configure SSL encryption for an RDS instance.

TDE

ApsaraDB for RDS provides Transparent Data Encryption (TDE) for MySQL and SQL Server . TDE for MySQL is independently developed by Alibaba Cloud, and TDE for SQL Server is based on the SQL Server Enterprise Edition.

After TDE is enabled for an ApsaraDB for RDS instance, you can specify the database or table to be encrypted. The data of the specified database or table is first encrypted and then written to a device such as an HDD, SSD, or PCIe card, or to a service such as Object Storage Service (OSS). This way, all data files and instance backups are stored in ciphertext.

TDE adopts the Advanced Encryption Standard (AES) algorithm. The key length is 128 bits. The key for TDE is encrypted and stored by Key Management Service (KMS). ApsaraDB for RDS only reads the key once when the instance is started or migrated. You can replace the key in the KMS console.

For more information, see Configure TDE encryption for an RDS instance.

Disk encryption

ApsaraDB for RDS provides the disk encryption feature for free for RDS instances that are equipped with standard or enhanced SSDs. This feature encrypts the data on each disk of

your RDS instance based on block storage. This way, your data cannot be deciphered even if it is leaked. The encryption does not affect your businesses and your applications do not need changes.

For more information, see #unique_21.

6 Backup and restoration

Backup

Databases require regular automatic backup to ensure data integrity, reliability, and restorability.

ApsaraDB for RDS provides the following backup functions:

- Data backup: required. You must configure at least two physical backup tasks every week. You can also initiate a temporary backup task in the ApsaraDB for RDS console or by calling an API operation based on O&M requirements.Backup files can be retained for 7 to 730 days.
- Log backup: optional. If you disable log backup, data can only be restored to the point in time when the backup set is created. Data backup and log backup support the same retention policy.

ApsaraDB RDS for MySQL also supports backup archiving and cross-region backup. For more information, see #unique_23.

Restoration

Data restorability is essential to ensure the reliability of database O&M.

ApsaraDB for RDS provides the following restoration functions:

- Restoration by backup set: You can restore data from a specified backup set to a temporary or cloned instance. Then, you can check whether your data is intact on the temporary or cloned instance.
- Restoration by point in time: You can select a near point in time to restore data to a temporary or cloned instance by using the last full backup and subsequent log backups.

ApsaraDB RDS for MySQL also supports cross-region restoration and the restoration of individual databases or tables. For more information, see Restore individual databases or tables for an RDS MySQL instance and #unique_26.

7 Instance disaster tolerance

ApsaraDB for RDS provides a variety of disaster tolerance solutions.

Multi-zone instances

Alibaba Cloud provides cloud computing services among multiple regions around the world. Each Region covers multiple zones. Zones in the same region have an extremely low network latency and are isolated upon failures.

Single-zone RDS instances run on two physical servers in the same zone, with redundant racks, air conditioners, circuits, and networks. Through asynchronous or semi-synchronous data replication and efficient master-slave switching, RDS provides users with database availability that is higher than the limits of physical servers.

ApsaraDB for RDS supports multi-zone to provide higher availability than single-zone. Physical servers are deployed across different zones. When a zone fails, traffic can be quickly switched to another zone. The entire switchover process is transparent, and does not require changes to the application code.

Note:

During a failover, the connection to all ApsaraDB for RDS instances is broken, and you need to reconnect the application to the ApsaraDB for RDS instance.

For information about migration zone, see #unique_9.

Disaster recovery instance

The disaster recovery capability of a multi-zone RDS instance is limited to different zones in the same region. ApsaraDB for RDS also supports cross-region data disaster recovery. For example, you can asynchronously replicate instance A in the China (Hangzhou) region to instance B in the China (Shanghai) region by using Data Transmission service. Instance B is a complete and independent RDS instance, has independent connection addresses, accounts, and permissions.

After a disaster recovery instance is created, if the region where instance A is located encounters major fault that cannot be restored for short-term, you can switchover instance B in another region at any time. After the switchover is completed, you can change the database connection configurations in your application to redirect requests to instance B. This way, database availability above the region limit is guaranteed.

Note:

Before switchover, you must stop data replication from instance A to instance B to avoid data errors.

For more information about how to create a secondary instance, see #unique_10.

8 Software upgrade

Apsaradb for RDS provides you with new versions of your database software.

In the vast majority of cases, minor version upgrade are all non-mandatory. Only when you manually restart an ApsaraDB for RDS instance does the system update the database software to the latest compatible version.

In rare cases (such as fatal major bugs and security vulnerabilities),RDS instances (except basic edition it will initiate a mandatory update of the database version during the maintenance period. Such mandatory updates only result in temporary database disconnections, and will not have any adverse impact on the application if the database connection pool is configured properly.

You can use the console or API set the maintenance window of an ApsaraDB RDS MySQL instance to prevent RDS from being forcibly upgraded during peak hours.

9 Service Authorization

If you are seeking for technical support from Alibaba Cloud and if it is necessary to operate your database instance during technical support, you must authorize the technical support staff to provide technical support services through the service account. After the specified expiration time, the system deletes the service account.

Without your authorization service account the Ali Cloud's after-sales team and DBA team can only view the information related to the RDS instance resources, fees, and performance. Such as the purchase time, Expiration Time, CPU, memory, storage capacity and consumption, backup space, Internet traffic, and SQL audit.

If you need Alibaba Cloud after-sales and DBA teams to view other issues about your instance, you can authorize them as follows:

- Configure permissions

  After you grant the permission, Alibaba Cloud after-sales team and DBA team can view and modify the configuration information of the RDS instance in a user-defined time period. Such as RDS whitelists, data replication modes, backup policies, and database parameters. In all cases, Alibaba Cloud after-sales team and DBA team will not change the connection information (including the IP address and database account) of the RDS instance without authorization.
- Data permissions

  After you grant the permission, Alibaba Cloud after-sales team and DBA team can view the user data of the RDS instance in a custom time period. For example, you can view the database and table structure, index fields, data samples, and SQL History data of an ApsaraDB for RDS instance. In all cases, the Alibaba Cloud after-sales team and DBA team will not modify the database structure, index fields, and data of the RDS instance without authorization.

Expires On

You can set a validity period to automatically revoke permissions. You can also revoke the permissions at any time.