Alibaba Cloud Common Solutions

Data Encryption

Issue: 20190329

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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Data Encryption at Storage

Alibaba Cloud products provide various methods to encrypt static data, as shown in the following table:

Product	Encryption Method	
OSS	*OSS client-side encryption*	*OSS Server-side encryption*
RDS	*SSL encryption*	*TDE encryption*
ECS Disk	To encrypt the data stored on a disk, you can use the *ECS disk encryption* function to encrypt cloud disks and shared block storage.	

OSS encryption

OSS supports client-side encryption and server-side encryption.

OSS client-side encryption

Client encryption means that the encryption is completed before the user data is sent to the remote server, whereas the plaintext of the key used for encryption is kept in the local computer only. Therefore, the security of user data can be ensured because others cannot decrypt the data to obtain the original data even if the data leaks.

- Main private key hosted by using KMS
- Private key managed by the user

OSS server-side Encryption

OSS supports server-side encryption for the data uploaded by users: When a user uploads data, OSS encrypts the user data and permanently stores the data with encryption; when the user downloads the data, OSS automatically decrypts the encrypted data, returns the original data to the user, and declares in the header of the returned HTTP request that the data has been encrypted on the server.

For the details, see *Server-side encryption*.

RDS encryption

RDS supports SSL and TDE encryption.

SSL encryption

RDS provides Secure Sockets Layer (SSL) for MySQL and SQL Server. You can use the server root certificate provided by RDS to verify whether the database service with the target IP address and port is provided by RDS, which can effectively prevent man-in-the-middle attacks. To guarantee security and validity, RDS allows you to enable and update the SSL certificates for servers.

Though RDS can encrypt the connection between an application and a database, the SSL service can run properly only after the application enables authentication on the server. In addition, SSL results in extra CPU resource consumption and affects the throughput and response time of RDS instances to a certain degree. The specific impact varies depending on the number of user connection times and the data transfer frequency.

For more information about enabling and configuring SSL encryption service, see *Set SSL Encryption*.

TDE encryption

RDS provides transparent data encryption (TDE) for MySQL and SQL Server. The TDE function of RDS for MySQL is developed by Alibaba Cloud and the TDE function of RDS for SQL Server is based on the SQL Server Enterprise Edition.

You can specify the database or table to be encrypted in a TDE-enabled RDS instance. The data of the specified database or table is encrypted before being written to any device such as an HDD, SSD, or PCIe card, or to any service such as OSS or Archive Storage. Therefore, data files and backups of the instance are all ciphertext.

TDE adopts the Advanced Encryption Standard (AES) algorithm. The key length is 128 bits. The key for TDE is encrypted and stored by KMS, and RDS dynamically reads the key only once when the instance is started or migrated. You can replace the key as needed on the KMS console.

For more information about the TDE encryption servcie, see *Set Trasparent Date Encryption*.

ECS disk encryption

When you want to encrypt the data stored on a disk due to business needs or certificat ion requirements, you can use ECS disk encryption function to encrypt cloud disks and shared block storage (referred to collectively as cloud disks, unless otherwise specified). This secure encryption feature allows you to encrypt new cloud disks. You

do not have to create, maintain, or protect your own key management infrastructure , nor change any of your existing applications or maintenance processes. In addition, no extra decryption operations are required, so the operation of the disk encryption function is practically invisible to your applications or your operations.

Encryption and decryption barely degrades cloud disk performance. For information on the performance testing method, see Disk parameters and performance test.

After an encrypted cloud disk is created and attached to an ECS instance, the data in the following list can be encrypted:

- Data on the cloud disk.
- Data transmitted between the cloud disk and the instance. However, data in the instance operating system is not encrypted.
- All snapshots created from the encrypted cloud disk. These snapshots are called encrypted snapshots.
- Encryption and decryption are performed on the host that runs the ECS instance, so the data transmitted from the ECS instance to the cloud disk is encrypted.

The ECS disk encryption function handles key management for you. Each new cloud disk is encrypted using a unique 256-bit key (derived from the CMK). This key is also associated with all snapshots created from this cloud disk and any cloud disks subsequently created from these snapshots. These keys are protected by Alibaba Cloud's key management infrastructure (provided by KMS). This approach implements strong logical and physical security controls to prevent unauthorized access. Your data and the associated keys are encrypted using an industry standard AES-256 algorithm.

Alibaba Cloud's overall key management infrastructure conforms with the recommendations in (NIST) 800-57 and uses cryptographic algorithms that comply with the (FIPS) 140-2 standard.

Each Alibaba Cloud ECS account has a unique CMK in each region. This key is separate from the data and stored in a system protected by strict physical and logical security controls. Each encrypted disk uses an encryption key unique to the specific disk and its snapshots. The encryption key is created from and encrypted by the CMK for the current user in the current region. The disk encryption key is only used in the memory of the host that runs your ECS instance. The key is never stored in plaintext in any permanent storage media (such as a disk).

For more information about cloud disk encryption, see *ECs disc encryption*.