ALIBABA CLOUD

Alibaba Cloud

AnalyticDB for MySQL

Data Security

Document Version: 20220701

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

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

Table of Contents

1.Configure a whitelist

After you create an cluster, you must configure a whitelist for the cluster to allow access from external devices to the cluster.

Context

- The default whitelist of an AnalyticDB for MySQL cluster contains only the default IP address 127.0.0.1, which indicates that no devices are allowed to access the cluster.
- Whitelists can enhance access security for AnalyticDB for MySQL clusters. We recommend that you maintain the whitelists on a regular basis.
- Whitelists do not affect the normal operation of AnalyticDB for MySQL clusters.

Procedure

1.
2.
3.
4.
5. In the left-side navigation pane, click **Data Security**.
6. On the **Whitelist Settings** tab, click **Edit** to the right of the **default** whitelist.

   > **Note** You can also click **Create Whitelist** to create a whitelist.

7. In the **Edit Whitelist** panel, remove the default IP address 127.0.0.1 and enter the IP addresses or CIDR blocks that you want to allow. Then, click **OK**.
   - If you enter a CIDR block, access from all IP addresses in the CIDR block is allowed.
   - Do not add 0.0.0.0 to the whitelist.
   - If your public IP addresses change frequently and you want to allow all your public IP addresses, you can add 10.0.0.0/0 to the whitelist.

     > **Warning** Risks may arise if you add 10.0.0.0/0 to the whitelist. Proceed with caution.

   - If you want to add multiple IP addresses or CIDR blocks, separate multiple entries with commas (,). Do not add spaces before or after the commas. Example: 192.168.0.1,172.16.213.9.
   - The whitelist modification takes effect in 1 minute.

2.SQL audit

AnalyticDB for MySQL provides the SQL audit feature to log data manipulation language (DML) and data definition language (DDL) operations that are executed in databases in real time. You can retrieve database operation information from audit logs. This improves the security of databases.

Features

- SQL audit logging

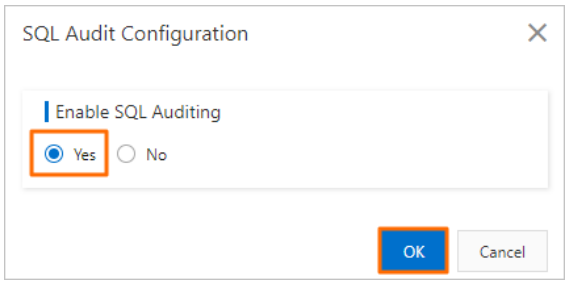
  AnalyticDB for MySQL logs all operations that are performed on databases. You can use audit logs to identify faults, analyze database activities, and audit databases for security purposes. If you require more detailed diagnostics and analysis, go to the **Diagnostics and Optimization** page in the AnalyticDB for MySQL console.

- Data search

  You can search data by combining multiple conditions, such as database, client IP address, execution duration, and execution status. You can also export search results.

Enable SQL audit

1.
2.
3.
4.
5.
6. On the **Data Security** page, click the **SQL Audit** tab.
7. On the **SQL Audit** tab, click **Enable SQL Audit** in the upper-right corner.
8. In the dialog box that appears, select **Yes** and click **OK**.



Query and export SQL audit logs

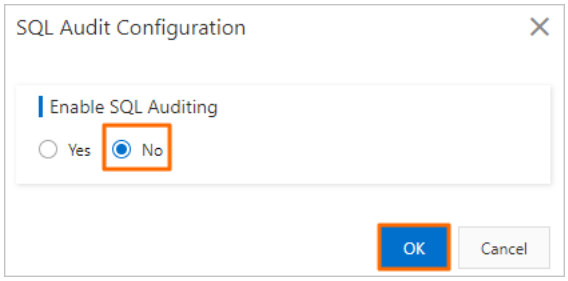
1.
2.
3.
4.
5.
6. On the **Data Security** page, click the **SQL Audit** tab.
7. On the **SQL Audit** tab, query SQL audit logs within a specific period of time based on **Operation Type** or **Execution Status**.

> **Note**
> - You can query SQL audit logs that are generated only within the last 30 days.
> - The time range to query must be within 24 hours. If you want to save SQL audit logs to your computer, click **Export Current Page**.

Disable SQL audit

> **Note** After SQL audit is disabled, SQL audit logs are cleared. You must query and export SQL audit logs before you disable SQL audit. For more information, see Query and export SQL audit logs. When you enable SQL audit again, audit logs generated from the last time when SQL audit was enabled are available for queries.

1.
2.
3.
4.
5.
6. On the **Data Security** page, click the **SQL Audit** tab.
7. On the **SQL Audit** tab, click **Audit Configuration** in the upper-right corner.
8. In the dialog box that appears, select **No** and click **OK**.



Related operations

- DescribeAuditLogConfig
- ModifyAuditLogConfig
- DescribeAuditLogRecords

3.Disk encryption

provides the disk encryption feature. This feature encrypts the data on each disk in your cluster based on block storage. This way, your data cannot be decrypted even if it is leaked.

Features

After disk encryption is enabled, creates an encrypted disk, attaches the disk to an Elastic Compute Service (ECS) instance, and encrypts the following data in the disk:

- All data in reserved clusters
- Hot data in elastic clusters

> **Note** Cold data in elastic clusters is not stored on disks and cannot be encrypted within elastic clusters.

- Data that is transmitted between disks and clusters
- All snapshots of the encrypted disk, which are classified as encrypted snapshots

Precautions

- Disk encryption can be enabled for an cluster when you first create the cluster. You cannot enable this feature after the cluster is created.
- Disk encryption cannot be disabled after it is enabled.
- After disk encryption is enabled, both the snapshots generated from reserved clusters and the reserved clusters created from those snapshots are automatically encrypted.
- If you enable disk encryption, the read and write performance of the cluster is affected. Typically, the read and write performance is reduced by about 10%.
- You do not need to modify the code to allow access to the services.

Pricing

Disk encryption requires the use of Key Management Service (KMS). You are charged for key management and API calls in KMS. For more information, see Billing of KMS.

Method to enable disk encryption

Disk encryption can be enabled only when you create an AnalyticDB for MySQL cluster. For more information, see Create a cluster. To enable disk encryption, you must specify the related parameters on the cluster buy page.

1. On the cluster buy page, select **Disk Encryption**.
2. If you enable disk encryption for the first time, click **Create Service Linked Role**.

> **Note**
>
> - **Create Service Linked Role** is required only when disk encryption is enabled for the first time. If **Created** is displayed in the Service-linked Role section, a service-linked role has already been created. You can skip this step.
> - If you want to use disk encryption, you must authorize the service-linked role and use related KMS features. For more information, see Manage the service-linked role for disk encryption.

3. Select the key that you want to use from the **Key** drop-down list.

> **Note**
>
> - If no keys are available in the drop-down list, you must create a key. For more information, see Create a CMK.
> - Disk encryption of supports only the keys that are manually created. When you create a key in the KMS console, you must set **Rotation Period** to Disable.
> - After KMS is activated, ActionTrail records the operations that you perform on KMS resources. For more information, see Use ActionTrail to query KMS event logs.

After you specify the disk encryption parameters, perform the subsequent steps in Create a cluster to create the cluster.