TDSQL-C for MySQL

Data security audit

Product Documentation

Contents

Data security audit
- Introduction to Data Security Audit
- Purchasing Data Security Audit
- Enabling or Disabling Data Security Audit
- Access Topology
- Data Identification
- Audit Logs
- Alarm
- Risk

Data security audit
Introduction to Data Security Audit

Last updated：2026-08-25 15:41:06

Data Security Posture Management (DSPM) and database build a unified operational view for cloud data security, allowing you to gain full visibility into the distribution and access of cloud data assets and sensitive data. Leveraging cloud-native behavior logs and a dynamic risk detection engine, the system performs end-to-end monitoring across public and private network entry points, covering asset discovery, access permission control, and risk identification. This enables visualized, controllable, and precise protection of data assets, ensures data security and compliance in the cloud, and truly delivers "visibility, control, and precision in protection."

Key Challenges in Data Security

- **Data assets have blind spots, and the distribution of sensitive data is unclear:** Database instances are scattered across different regions, VPCs, and business departments, lacking a unified asset inventory. With a massive number of database tables and fields, the locations of sensitive data are unclear, making it difficult for security teams to accurately identify protection targets.
- **Data access behaviors are invisible, making traceability difficult:** Every query, export, and modification operation on the database lacks a unified audit view, and high-risk behaviors such as public IP address access, operations during abnormal hours, and batch downloads cannot be detected in a timely manner. Once a data breach occurs, administrators must manually piece together logs across platforms, resulting in a lengthy traceability cycle and an incomplete evidence chain, which can easily cause them to miss the golden window for response.
- **Abnormal operations are difficult to identify, and risk response is delayed:** Traditional rule engines generate alarms only through single-point feature matching, such as the number of failed logins, and cannot identify combined behavior risks, such as "public network access + sensitive data + batch export." As a result, a large number of alarms are generated with little useful information, causing security teams to suffer from "alarm fatigue" and struggle to prioritize responses and quickly contain the impact.
- **Compliance audit pressure is high, and sensitive data processing lacks a clear basis:** To meet compliance requirements, enterprises need to classify and tier their data and possess full operation audit capabilities. However, manually inventorying assets, identifying sensitive data table by table and field by field, and auditing operation logs manually involve an enormous workload, resulting in high compliance costs that are difficult to sustain.

Use Cases

- **Core data asset protection:** Perform full access auditing on sensitive data in cloud databases, such as personal information and transaction records, to provide traceability evidence for events including data breaches and unauthorized access.
- **Cybersecurity Classified Protection Compliance Service and regulatory compliance:** Meet the requirements of laws and regulations for log retention and audit capabilities, as well as the compliance audit needs of industries such as finance and telecommunications for classified protection standards.
- **Database attack and risk monitoring:** Monitor and generate alarms for malicious activities targeting databases in real time, enabling in-process blocking and post-incident accountability.
- **Ops and development security audit:** Audit high-risk operations performed by Ops personnel through tools such as the console, including DROP/ALTER and batch export. Also identify risks in development and testing environments caused by sensitive data exposure or unauthorized export.

Advantages

- **Access relationships at a glance:** Access relationships are visualized and clearly displayed.
- **Full operation traceability:** Record every database operation to support post-incident restoration.
- **Real-time risk monitoring:** Monitor abnormal access and sensitive operations in real time to promptly identify potential risks.
- **Automatic sensitive data discovery:** Proactively identify the distribution of sensitive data to provide a basis for permission reduction.

Billing Overview

Data Security Audit uses a prepaid yearly/monthly subscription model and is sold in packages. You can choose an appropriate number of packages based on your actual needs. The billable items and billing standards are listed in the following table.

> **Note:**
> Each of the following packages includes: one database instance, a throughput of 1,000 SQL/second, storage for 20 million online SQL statements, and 100 GB of storage space.

Billable Item	Specifications	Unit Price
Enterprise Edition	1 – 3 sets	USD 280/set/month
	4 – 20 sets	USD 270/set/month
	21 – 50 sets	USD 255/set/month
	51 – 100 sets	USD 240/set/month
	101 – 200 sets	USD 225/set/month

	201 – 300 sets	USD 210/set/month
	301 – 400 sets	USD 195/set/month
	401 – 500 sets	USD 180/set/month
	More than 500 sets (excluding 500)	USD 150/set/month
Log Storage Expansion Pack	1TB	USD 150/month

Supported Versions

Database Type	Version		Security audit	Data Identification
TDSQL-C for MySQL	Provisioned resource	Transaction cluster – MySQL 5.7	✓	✓
		Transaction cluster – MySQL 8.0	✓	✓
		Read-only instances	✓	✓
	Serverless	Serverless – MySQL 5.7	✓	✓
		Serverless – MySQL 8.0	✓	✓

Supported Region

TDSQL-C for MySQL supports Data Security Audit in the following regions: Guangzhou, Shanghai, Beijing, Nanjing, Chengdu, Chongqing, Shanghai Finance, Beijing Finance, and Shenzhen Finance.

References

Related Feature	Description	Documentation Link
Purchase Data Security Audit	Describes how to purchase Data Security Audit in the console.	Purchase Data Security Audit
Enable or Disable Data Security Audit	Describes how to enable or disable Data Security Audit in the console.	Enable or Disable Data Security Audit
Data identification	Describes operations related to the data identification capability of Data Security Audit.	Data Identification

Access topology	Describes the CAM capability of Data Security Audit.	Access topology
Log audit	Describes the audit log capability of Data Security Audit.	Audit logs
Alarm	Describes the alarm capability of Data Security Audit.	Alarm
Risk	Describes the risk monitoring capability of Data Security Audit.	Risk

Purchasing Data Security Audit

Last updated：2026-08-25 15:41:06

This document describes how to purchase Data Security Audit in the console.

Prerequisites

You have created a cluster. For more information, see Creating Cluster.

Operation Steps

1. Log in to the TDSQL-C for MySQL console, and click **Data Security Audit** in the left sidebar.
2. On the DSAudit page, click **Enable Security Audit**.
3. In the pop-up, read the service authorization information and click **Agree and Authorize**.
4. In the pop-up, select the configuration you want to purchase, click **Confirm**, and complete the payment to purchase Data Security Audit.

Parameter	Description
Audit Instance	Select the quota for audit instances. The default is 1, with a configurable range of 1 – 9999. A value of 5 or greater is recommended. The quota can be modified after configuration.
Log storage	Set the log storage capacity. All database instances share this space. Range: 0 – 9999TB. Scale-up or scale-down is supported after configuration.
Duration	Select a duration. Supported options: 1 month, 3 months, 6 months, 1 year, 2 years, 3 years.
Auto-Renewal	Select whether to enable auto-renewal. If auto-renewal is not enabled, you can still enable it manually after the configuration is complete. **Note:** If auto-renewal is not enabled, you can click **Enable Auto-Renewal** after **Renewal Method** on the **DS Audit** page > **Manage Usage** after the settings are complete.

Enabling or Disabling Data Security Audit

Last updated：2026-08-25 15:41:06

This document describes how to enable/disable Data Security Audit in the console.

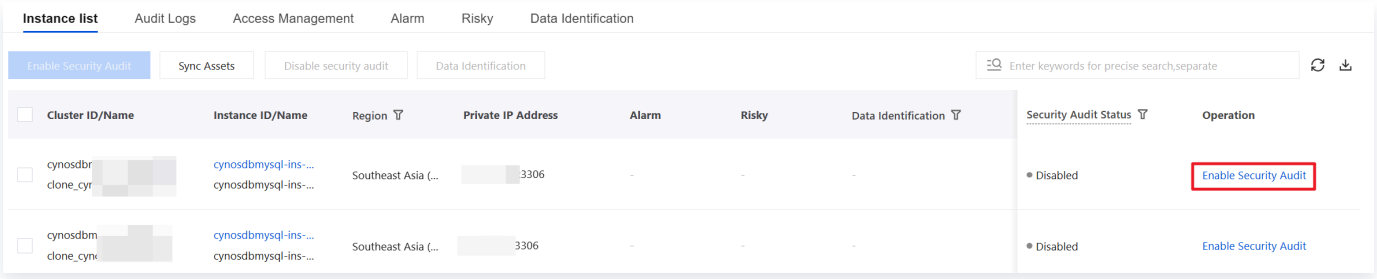
Prerequisites

You have created a cluster. For more information, see Creating Cluster.
You have purchased Data Security Audit.

Enabling Data Security Audit

Enable security auditing for the target database assets. After it is enabled, the system monitors the security status of the assets in real time, including access behaviors and violations, and generates alarms and risk information.

1. Log in to the TDSQL-C for MySQL console, and click **Data Security Audit** in the left sidebar.
2. Locate the target instance in the instance list, and click **Enable Security Audit** in its operation column.



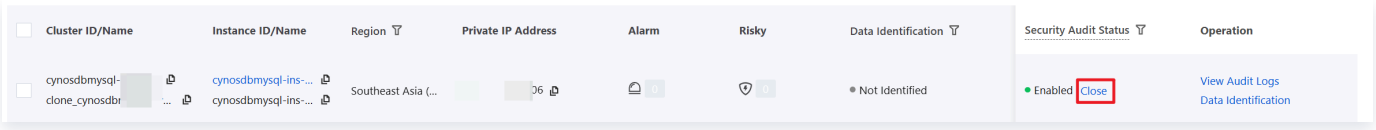
3. In the pop-up window, confirm the instance ID/name, region, private network address, consumed quota, and available quota, and then click **Confirm**.

> **Note:**
> - Enabling security audit consumes License authorization assets. Make sure you have sufficient remaining authorization quota.
> - After you enable security audit, the system needs a short period to initialize the monitoring policy, during which there may be a slight delay.
> - Enabling security audit is a prerequisite for viewing alarms and risk information. Without it, no monitoring data can be generated.

Disabling Data Security Audit

1. Log in to the TDSQL-C for MySQL console, and click **Data Security Audit** in the left sidebar.

2. Locate the target instance in the instance list, hover over its row, and click **Close** under the Security Audit Status field.



3. In the pop-up window, confirm the Instance ID/Name, Region, and Private IP Address to be disabled, and then click **OK**.

> **Note:**
> After you click OK, security protection will be disabled for the selected instance, security audit will stop, and historical audit logs will be cleared.

Access Topology

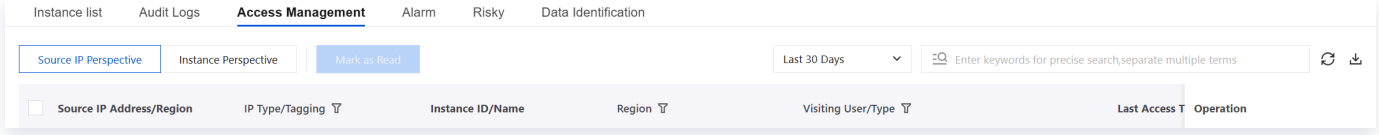
Last updated：2026-08-25 15:41:06

The data security audit access management module achieves refined control over database access behaviors through complementary dual-dimension governance from the "source IP address perspective" and the "instance perspective". It supports visual presentation of access behaviors (such as access topology diagrams) and IP address/account labeling operations, enabling fine-grained access control. It manages access behaviors from both the "source IP address" and "instance" dimensions to address the core questions of "who can access, from where, and what they access", preventing security vulnerabilities caused by coarse-grained access control.

Management Perspective	Description	Applicable Scenarios
Source IP Perspective	With the source IP address of the access initiator as the core control dimension, integrate the access data of this IP address to database instances, provide capabilities for access topology visualization, precise IP address/account tagging, and rapid security group policy adjustment, and implement centralized and refined control over the access initiator.	Identify cross-instance access risks of a single IP address and batch mark certain types of access sources.
Instance Perspective	With the database instance on the access target side as the core resource dimension, integrate the access data of source IP addresses to this instance, provide capabilities for asset access topology visualization, precise IP address/account tagging, and rapid security group policy adjustment, and implement centralized and refined control over the access target.	Identify all access sources of a single instance and implement targeted control for core instances.

Source IP Perspective

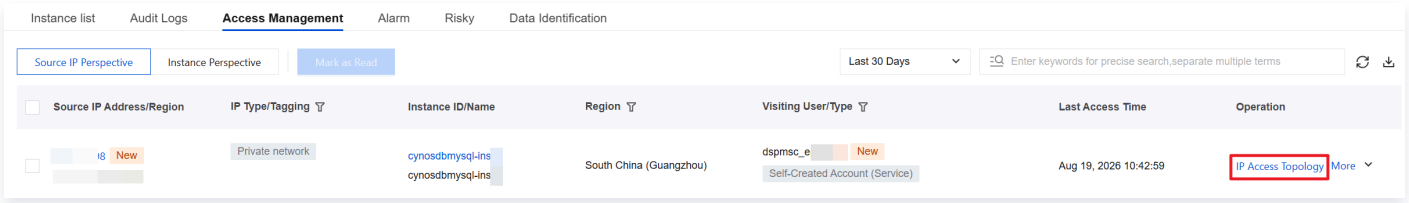
1. Log in to the TDSQL-C for MySQL console and click **Data Security Audit** in the left sidebar.
2. On the DSAudit page, choose **Access Management** > **Source IP Perspective**.



3. On the Source IP Perspective tab, you can view information such as **Source IP Address/Region**, **IP Type/Tagging**, **Instance ID/Name**, **Region**, **Visiting User/Type**, and **Last Access Time**.

IP Access Topology

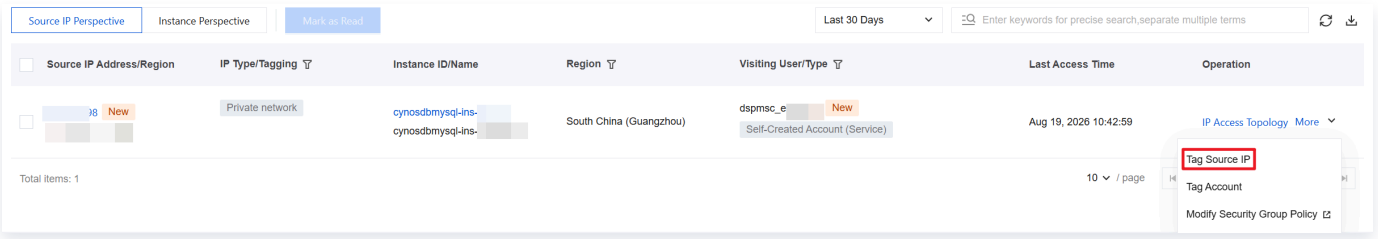
Visually present the access relationships, access frequency, and security status between a single source IP address and all associated accounts and database instances in the form of a visual topology map.
In the source IP perspective list, click **IP Access Topology** in the operation column of the target IP address to view the access relationship map between the IP address and its associated database instances.



IP Tagging

Add preset or custom tags to target source IPs to classify and manage the IPs, facilitating differentiated assessment during subsequent risk monitoring.

1. In the source IP perspective list, click **More** > **Tag Source IP** in the operation column of the target IP address.



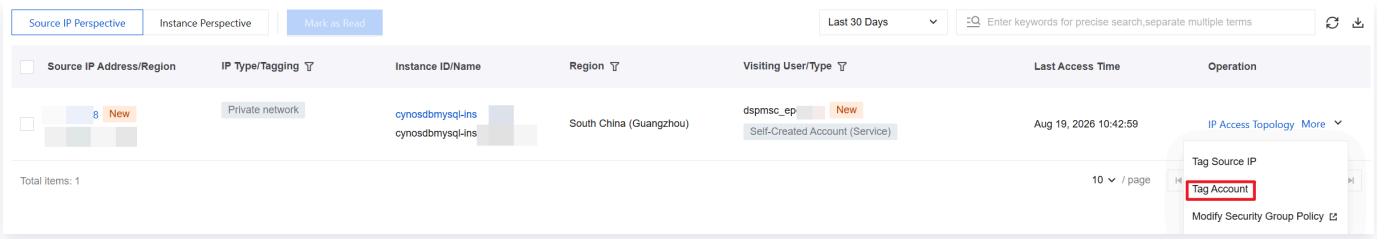
2. In the Tag Source IP window, edit the source IP remarks and click **Confirm** to complete the tagging.

> **Note:**
> The tagging operations in the source IP perspective and the instance perspective are mutually linked. After you tag an IP address in the source IP perspective, the tag status is synchronously updated when you view the IP address in the instance perspective, and vice versa.

Account Tagging

Add preset or custom tags to the accounts used by target source IPs to access databases, enabling classified management of access accounts for subsequent auditing and risk investigation.

1. In the source IP perspective list, click **More** > **Tag Account** in the operation column of the target IP address.

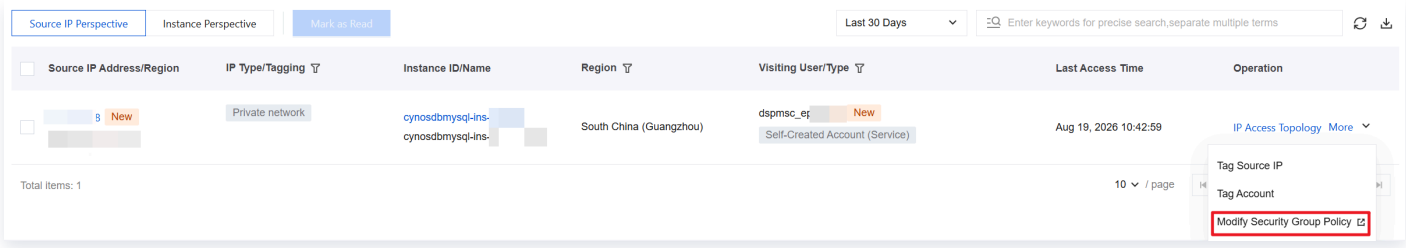


2. In the Tag Account window, select the account type, edit the account remarks, and click **Confirm** to complete the tagging.

> **Note:**
> You can edit the access account type if it is a self-built account. If the current access account is a cloud root account/sub-account, the system automatically identifies it, and no manual editing is required.

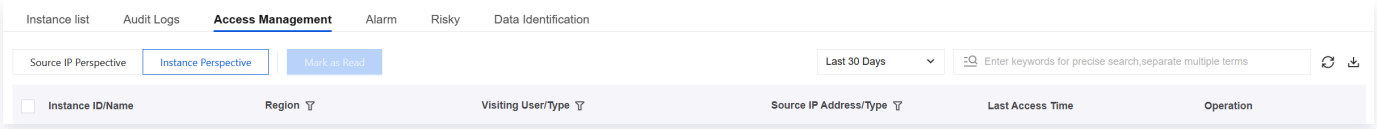
Modifying a Security Group Policy

Quickly go to the asset page of the database instance associated with the target IP address and directly modify the security group policy to quickly control access permissions for the IP address (allow/deny access).
In the source IP perspective list, click **More** > **Modify Security Group Policy** in the operation column of the target IP address to go to the database instance asset page and modify the security group policy.



Instance Perspective

1. Log in to the TDSQL-C for MySQL console and click **Data Security Audit** in the left sidebar.
2. On the DSAduit page, choose **Access Management** > **Instance Perspective**.

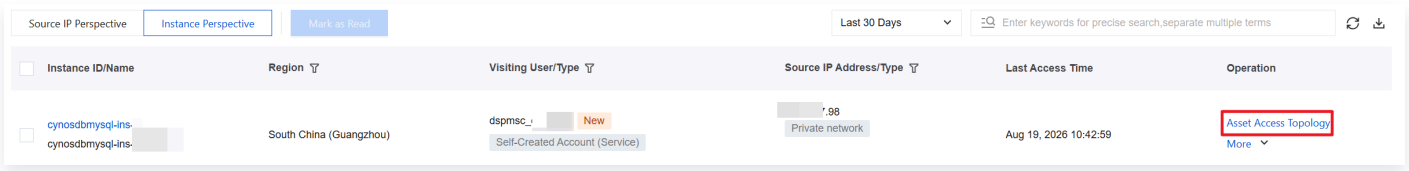


3. On the Instance Perspective page, you can view information such as **Instance ID/Name**, **Region**, **Visiting User/Type**, **Source IP Address/Type**, and **Last Access Time**.

Asset Access Topology

Visually present the access relationships, access frequency, and risk status between all source IPs and associated access accounts of a single database instance in the form of a visual topology map.

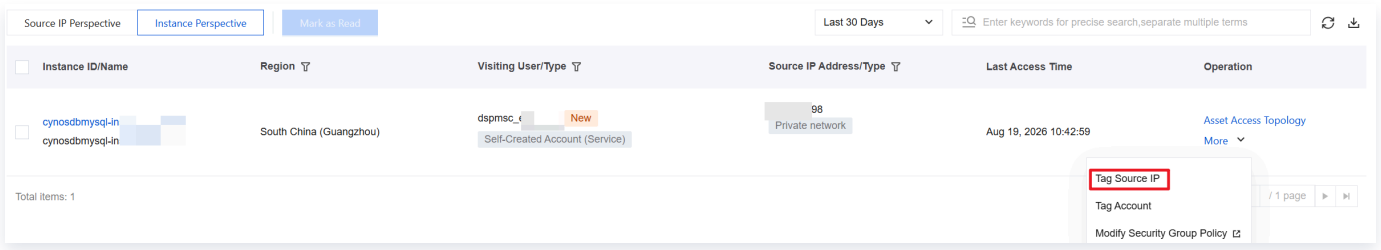
In the instance perspective list, click **Asset Access Topology** in the operation column of the target instance to view the topological relationships between all source IPs and associated accounts of the instance.



IP Address Tagging

Add preset or custom tags to the specified source IPs that access the target instance to achieve precise classification and control of IPs accessing the instance, facilitating subsequent risk monitoring and auditing.

1. In the instance perspective list, click **More** > **Tag Source IP** in the operation column of the target instance.



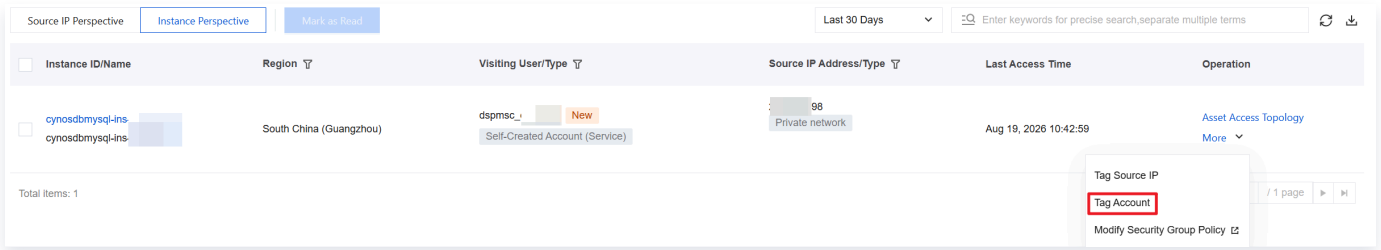
2. In the Tag Source IP window, edit the source IP remarks and click **Confirm** to complete the tagging.

> **Note:**
> The tagging operations in the source IP perspective and the instance perspective are mutually linked. After you tag an IP address in the source IP perspective, the tag status is synchronously updated when you view the IP address in the instance perspective, and vice versa.

Account Tagging

Add preset or custom tags to the specified accounts that access the target instance to achieve precise classification and control of accounts accessing the instance, facilitating subsequent risk investigation and permission auditing.

1. In the instance perspective list, click **More** > **Tag Account** in the operation column of the target instance.

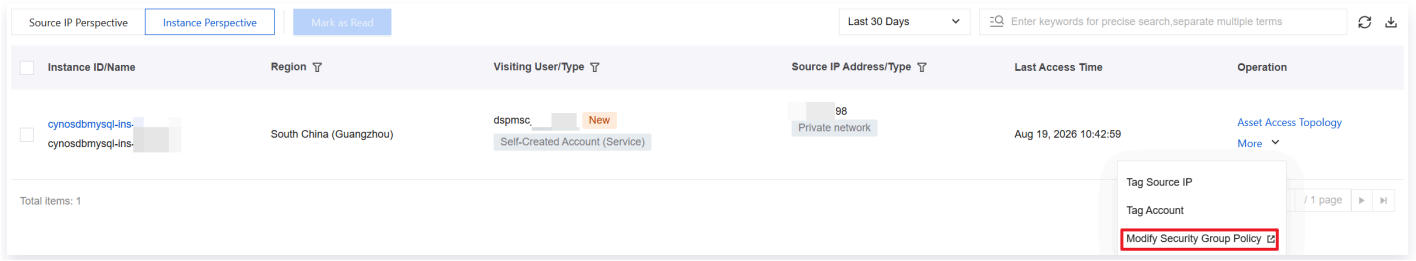


2. In the Tag Account window, select the account type, edit the account remarks, and click **Confirm** to complete the tagging.

> **Note:**
> You can edit the access account type if it is a self-built account. If the current access account is a cloud root account / sub-account, the system automatically identifies it, and no manual editing is required.

Modifying a Security Group Policy

Quickly go to the asset page of the target database instance and directly modify the security group policy to control all source IPs that access the instance.
In the instance perspective list, click **More** > **Modify Security Group Policy** in the operation column of the target instance to go to the database instance asset page and modify the security group policy.



Data Identification

Last updated：2026-08-25 15:41:06

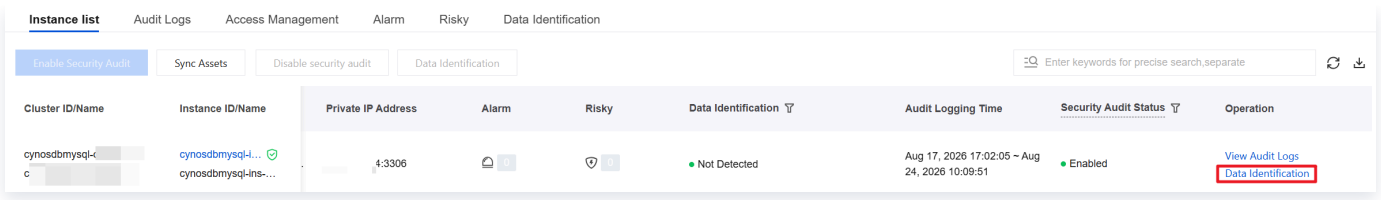
Data classification and grading is a core governance module of data security posture management, providing capability support for business scenarios such as compliant inventory of data assets, sensitive data control, and dedicated protection of critical data.

Related Documentation

Operation Item		Applicable Scenarios
Enable Data Identification.		Enable data identification for the target database asset. The system will automatically scan sensitive data based on the classification and grading template.
View Data Identification Results.		View the classification and grading distribution, sensitive data details, and statistics information after data identification scanning.
Classification and Grading Management	Create Classification and Grading Template.	When built-in templates cannot meet business requirements, you can customize data classification and grading systems.
	Switch Classification and Grading Template.	Replace the currently used classification and grading template in different business scenarios.
	Copy Classification and Grading Template.	Quickly create a template based on an existing one and reuse its classification and grading configurations.
	Create Data Item.	Define specific sensitive data types in classification and grading identification, such as ID card numbers and mobile phone numbers.

Enabling Data Identification

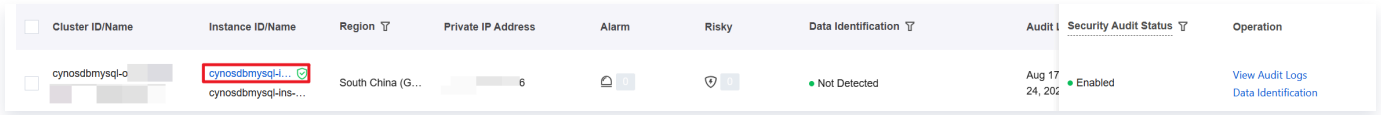
1. Log in to the TDSQL-C for MySQL console and click **Data Security Aduit** in the left sidebar.
2. On the Instance List tab, select the target database asset, and click **Data Identification** in the operation column.



3. In the data identification configuration window, select **Immediate Identification** or **Cycle Recongnition**. If you select **Cycle Recongnition**, configure the identification frequency, such as daily, weekly, or monthly, and specify the identification cycle. After the configuration is complete, click Confirm.
4. After successful identification, the database asset table details will be automatically refreshed, and data asset content tags will be added.

Viewing Classification and Grading Results

1. On the Instance List tab page, locate the target database asset, and click its **Instance ID**.

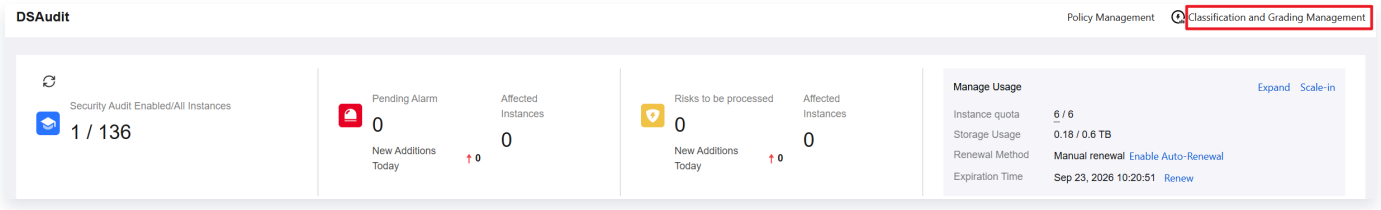


2. On the instance details page, click the **Data Identification** tab.
3. On the Data Identification tab page, the classification and grading details under the current classification and grading template will be displayed. Click **Data Name or Table Name** to view the classification and grading identification results for specific databases, tables, and fields.

Creating a Classification and Grading Template

A classification and grading template is a standardized data classification and grading standard generated by configuring the relationships among classifications, grades, and data items. It serves as the unified standard for data classification and grading identification.

1. Log in to the TDSQL-C for MySQL console and click **Data Security Aduit** in the left sidebar.
2. On the DSAduit page, click **Classification and Grading Management** to open the Classification and Grading Management panel.



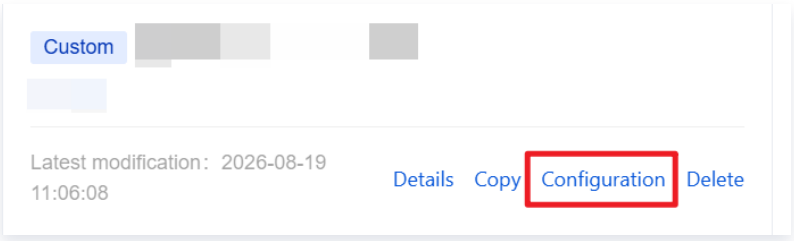
3. On the Classification and Grading tab, click **Create Template**.
4. In the Create Template window that appears, configure the basic template information:

Configuration Item	Description

Template Name	Customize the template name. It cannot exceed 64 characters.
Description	Description of the classification and grading template. It cannot exceed 200 characters.
Grading Scheme	Used to associate corresponding classification grades with data items during template configuration. You can only select from existing classification schemes. If no classification scheme meets your requirements, click **Create a grading scheme** to quickly create one.

5. Click **Confirm** to successfully create the classification and grading template.
6. After creation, on the Classification and Grading tab, select the template you created and click **Configuration** to configure the classification and grading template.

> **Note:**
> System built-in templates are configured by the system by default, while custom templates can be configured manually.

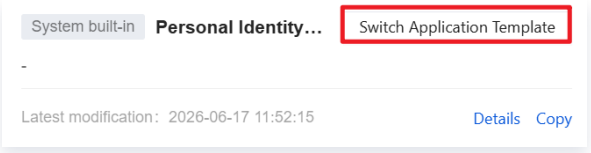


7. On the template configuration page, click the "+" button to add the required classifications.
8. After the classification is added successfully, select the target classification and click **Add Data Item**.
9. In the Add Data Item window that appears, select the data items to associate with the classification and configure a grade for each data item.
10. Repeat the above steps as needed to add multiple classifications and data items to the template. You can then complete the creation of a classification and grading template.

Switching Classification and Grading Templates

Templates in the application are globally applicable. You can switch templates to select a classification and grading template that meets your requirements.

1. On the Classification and Grading tab, select the template you want to apply and click **Switch Application Template** in the upper-right corner.



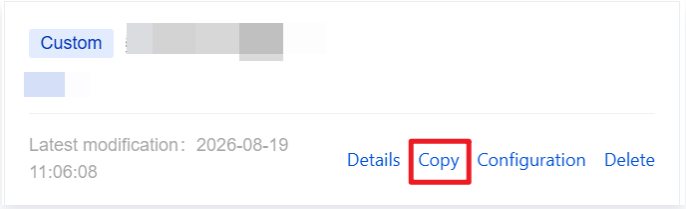
2. In the confirmation window, click **Confirm** to switch successfully.

> **Note:**
> The change takes effect immediately after a switch is performed and only affects new data identification results, while historical scan data records are retained.

Copying a Classification and Grading Template

You can quickly create a template by copying an existing one and then make modifications based on the copied template.

1. On the Classification and Grading tab, select the template you want to apply and click **Copy**.



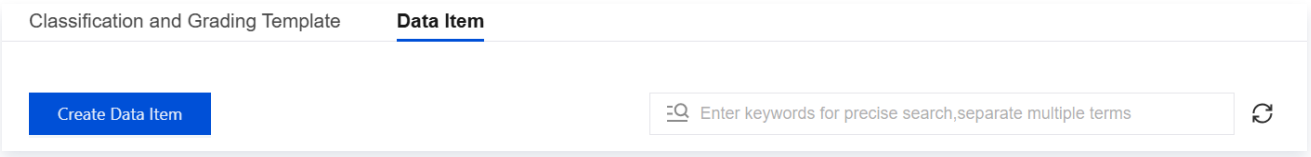
2. In the Copy Template window, enter the template name and description, and click **Confirm** to copy the template successfully.

> **Note:**
> System built-in templates cannot be edited or deleted. To make adjustments based on a built-in template, use the copy feature to create a duplicate and then modify it.

Creating a Data Item

A data item is the smallest rule unit used to identify sensitive data. It determines the sensitive attributes of fields through matching logic such as keywords and regular expressions, and serves as the core rule basis for automated scanning and identification of sensitive data. The system has **797** built-in data items and also allows you to create custom ones.

1. Log in to the TDSQL-C for MySQL console and click **Data Security Aduit** in the left sidebar.
2. On the DSAduit page, click **Classification and Grading Management** to open the Classification and Grading Management panel.
3. In the Classification and Grading Management window, click the **Data Items** tab.
4. On the Data Items tab, click **Create Data Item**.



5. On the Create Data Item page, configure the required data item settings and click **Confirm** to create it successfully.

Parameter		Description
Basic Information	Data Item Name	The data item name is the identifier of a category–data item and is used to uniquely identify each data item in the system.
	Description	The data item description provides details about the identified data item and helps users better understand its purpose, function, and expected effect.
	Enabled State	Indicates whether this data item takes effect when a classification and grading task is executed.
Rule Configuration	Match Logic	AND: All conditions must be met for successful identification. OR: Identification succeeds as long as one of the conditions is met.
	Recognition Object	Recognition object refers to the object on which data recognition is performed. You can configure multiple features of the recognition object at the same time, such as field names and content.
	Recognition Method	You can freely select the desired recognition method (match / mismatch).
	Recognition Logic	**Keyword:** Keyword matching is a matching mode that identifies data by searching for specific keywords in the data. Once these keywords are found in the data, the data will be marked and classified and graded. **Regex:** Regex matching uses regular expressions to define complex matching patterns. Matching with regular expressions improves matching accuracy and flexibility.
	Ignore Case	If Ignore Case is enabled, letter case is not distinguished during matching.
	Full–text Match	Full–text matching compares the data to be identified with the recognition content to check for exact consistency. If the data is exactly the same as the recognition content, it will be marked and then classified and graded.

6. After the configuration is complete, click **Test** to verify the configured identification rules.

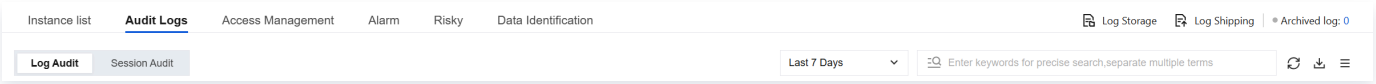
Audit Logs

Last updated：2026-08-25 15:41:06

The Data Security Audit audit logs module comprehensively records all database operations, including key traceability information such as SQL statements, operators, source IPs, and timestamps. It supports multi-dimensional precise search and detail viewing, providing full traceability for database operation behaviors.

Log Audit

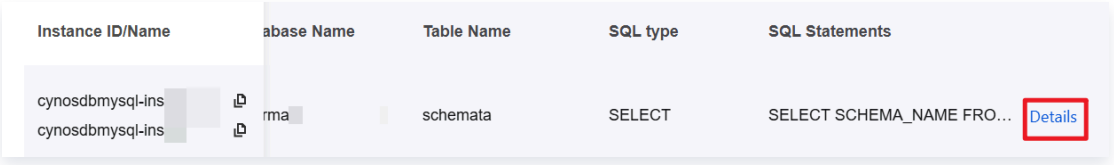
1. Log in to the TDSQL-C for MySQL console and click **Data Security Audit** in the left sidebar.
2. On the DSAudit page, click **Audit Logs** > **Log Audit**.



3. On the audit logs page, operation records of synchronized database assets are displayed.
4. On the audit logs page, you can search logs by instance, database account, client IP address, client port, database name, table name, SQL statement, and SessionID.

SQL Statement Details

1. On the audit logs tag page, hover over the target log row and click **Details** in the SQL statement column of the target log.

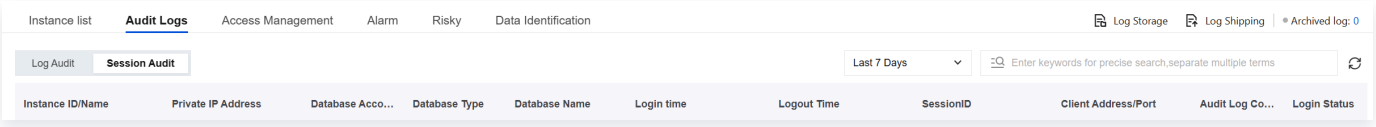


2. On the SQL statement details page, you can view the complete SQL statement information.

Session audit

Session auditing helps you perform security analysis from the perspective of database connection sessions.

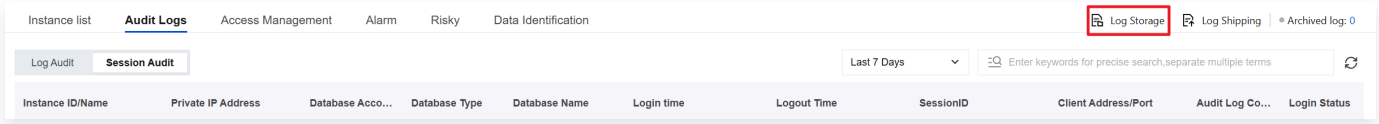
1. Log in to the TDSQL-C for MySQL console and click **Data Security Audit** in the left sidebar.
2. On the DSAudit page, click **Audit Logs** > **Session Audit**.
3. On the audit logs page, synchronized database session connection records are displayed.



Storage Settings

> **Note:**
> - When the log volume or log retention period reaches the corresponding threshold, earlier logs are automatically archived as files.
> - During archiving, the earliest log units are archived first. A single log unit can contain up to 45 GB or 80 million logs.
> - After logs are successfully archived, the corresponding online logs are deleted, and archived logs must be restored before they can be viewed.

1. On the audit logs tag page, click **Log Storage**.

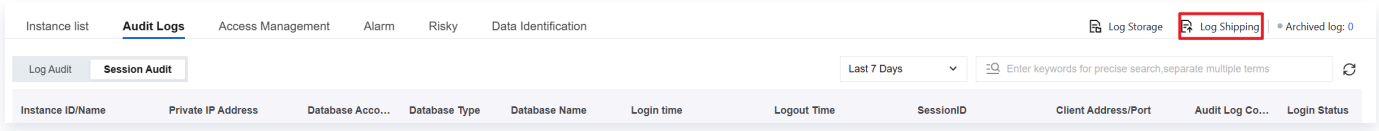


2. In the log storage settings window, you can enable/disable archived log storage and adjust the online log retention period, restored log retention period, and log lifecycle.

Log Shipping

> **Note:**
> - Purchase a Ckafka instance: Go to the message queue console to purchase a Ckafka instance. The Pro Edition is recommended.
> - Enable network access: Follow the message queue CKafka documentation to enable VPC-based network access or public domain access.

1. Log in to the TDSQL-C for MySQL console and click **Data Security Audit** in the left sidebar.
2. On the DSAudit page, click **Audit Logs**.
3. On the audit logs page, click **Log Shipping**.



4. In the Log Shipping window, configure the log shipping information.

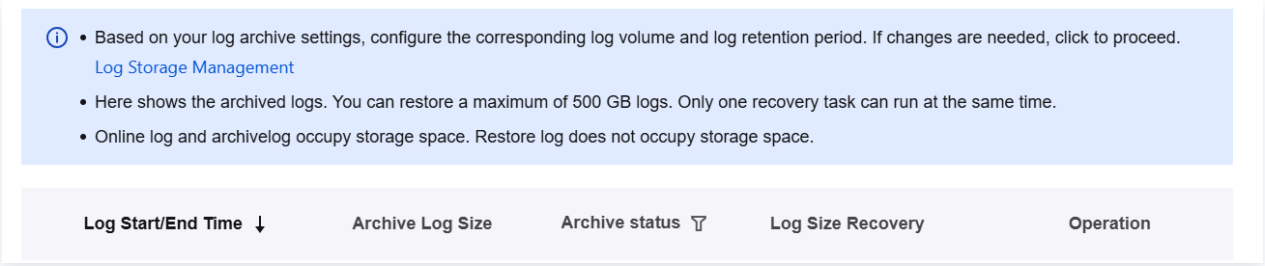
Parameter Name	Description
Network Access Method	Select the access method for the message queue. • Support environment access. • Public domain access.

Message Queue Instance	Select the message queue instance for log shipping.
Network	Select the network to use. The **PLAINTEXT** type is supported.
Username	Set the username. This field is required only for public network domain access.
Password	Set the password. This field is required only for public network domain access.
Topic ID/Name	Select the Topic for delivery.

Archive Log Management

> **Note:**
> - A maximum of 500 GB of logs can be restored.
> - Only one restore task can be performed at a time.
> - Online logs and archived logs occupy storage space, while restored logs do not.

1. Log in to the TDSQL-C for MySQL console and click **Data Security Audit** in the left sidebar.
2. On the CDS page, click **Audit Logs**.
3. On the audit logs page, click **Archived Log**.
4. In the Archived Logs window, all archived audit logs are displayed. You can delete or restore archived logs (restore them to online logs).



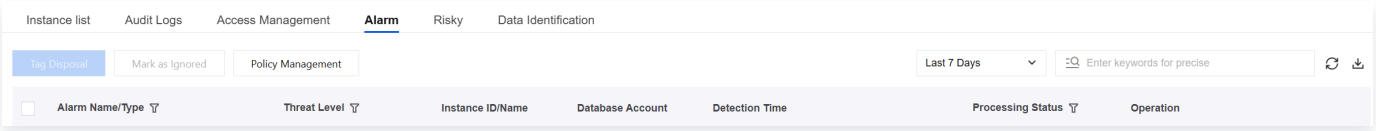
Alarm

Last updated：2026-08-25 15:41:06

The database risk monitoring and alarm module enables precise identification and closed-loop handling of violations through a real-time security event monitoring and response system for database assets.

Alarm List

1. Log in to the TDSQL-C for MySQL console, and click **Data Security Audit** in the left sidebar.
2. On the DSAudit page, click **Alarm**.



3. On the Alarm Tag page, you can view alarm information related to the current database assets. The alarm list displays the Alarm Name/Type, Threat Level, Instance ID/Name, Database Account, Detection Time, and Processing Status.

> **Note:**
> During alarm export, the detection time in the alarm list is automatically converted to UTC+08:00 (East Eight Time Zone/Beijing Time). The two sets of times correspond to the same event occurrence moment, with only the display time zone differing. The original data remains consistent.

Viewing Alarm Details

On the Alarm Tag page, click the target **Alarm Name** to view details such as the alarm trigger reason, violation operation details (SQL statement, source IP address), and associated assets.

Alarm Handling Operations

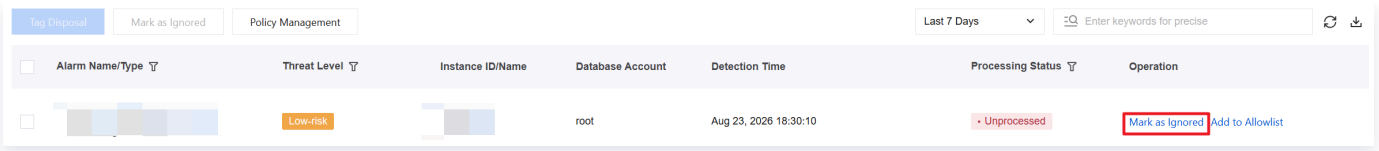
Marking as Ignored

Mark the status of false positive alarms or alarms that do not require handling to eliminate interference in risk statistics.

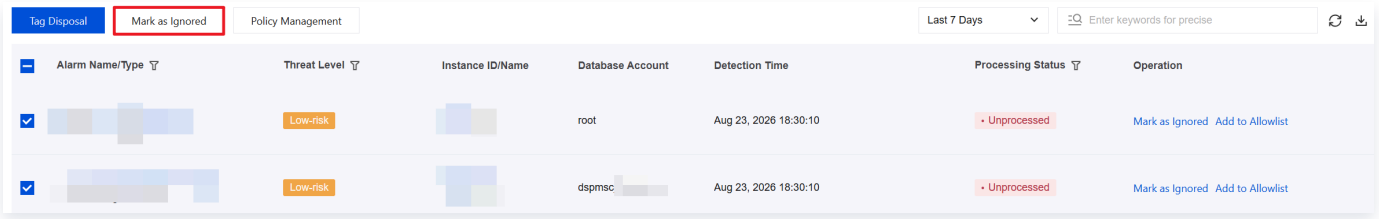
> **Note:**
> If the alarm handling status is marked as ignored, the risk will not be included in risk statistics.

1. On the Alarm Tag page, you can handle target alarms individually or in batches:

- **Individual handling**: Click **Mark as Ignored** in the operation column of the target alarm.



- **Batch handling**: Select multiple target alarms, and click **Mark as Ignored** above the list.

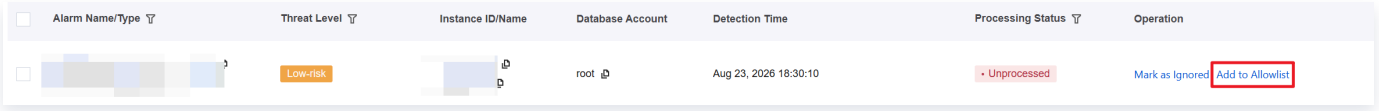


2. In the confirmation dialog, click **OK** to mark the alarm as ignored.

Adding Allowlists

For behaviors that require long-term permission, you can add the policy triggered by the alarm to the rule allowlist.

1. On the Alarm Tag page, click **Add to Allowlist** in the operation column of the target alarm.



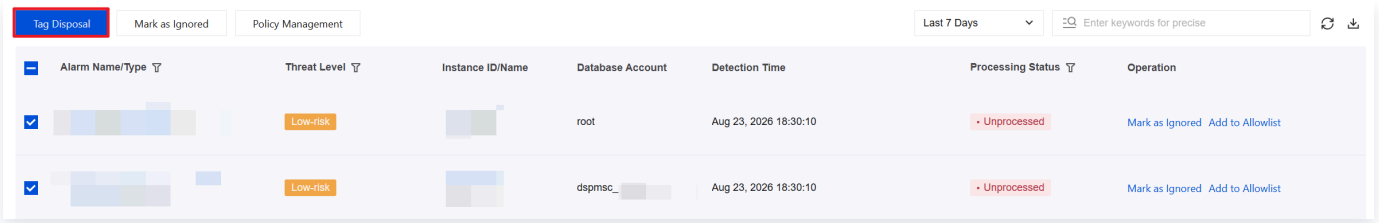
2. In the Add to Allowlist window, review the allowlist policy content. After confirming that it is correct, click **Confirm** to add the policy information triggered by the alarm to the allowlist.

> **Note:**
> After the alarm allowlist policy rule takes effect, the behavior no longer triggers alarms.

Marking as Handled

Update the status of alarms for which emergency response has been completed to close the handling loop.

1. On the Alarm Tag page, select one or more target alarms and click **Tag Disposal**.



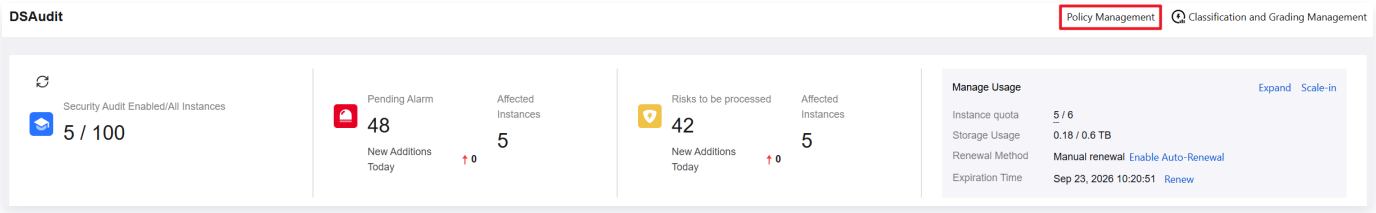
2. In the confirmation window, review the alarm information. After confirming that it is correct, click **OK** to mark the alarm as handled.

> **Note:**

> After the alarm handling status is marked as handled, the alarm will not be included in risk statistics.

Alarm Policy Configuration

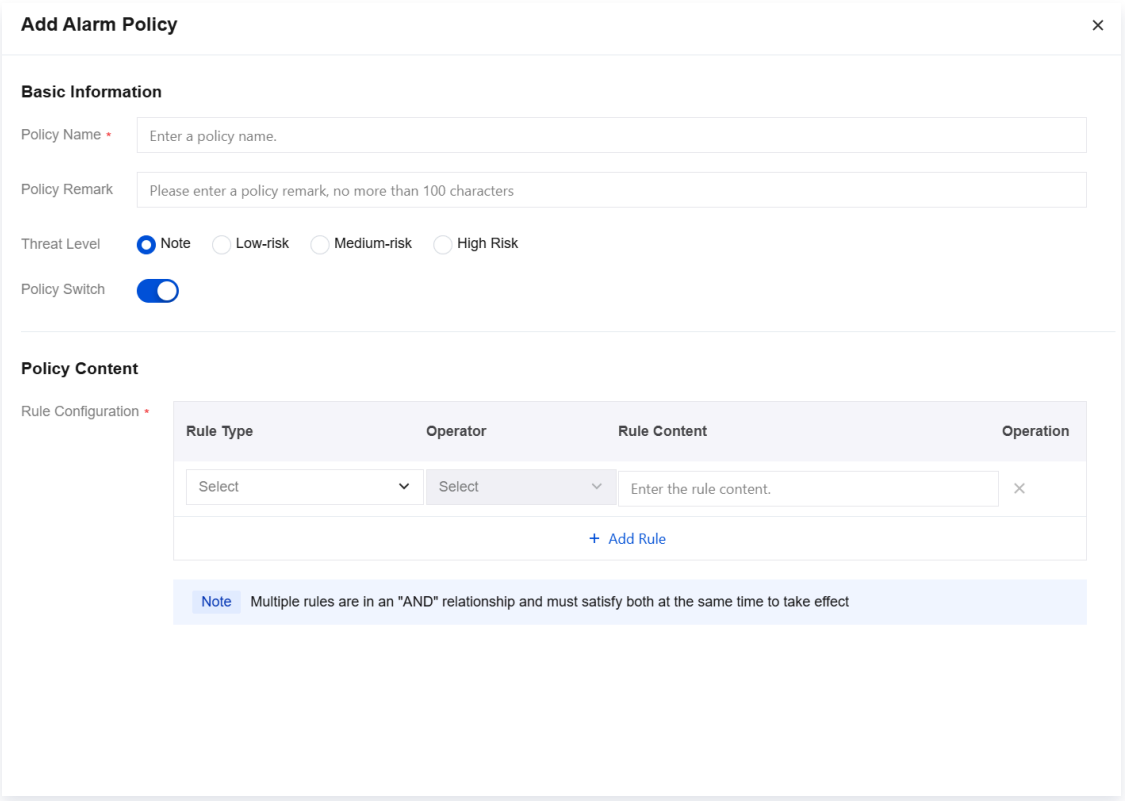
1. Log in to the TDSQL-C for MySQL console, and click **Data Security Audit** in the left sidebar.
2. On the CDS page, click **Policy Management** in the upper-right corner.



3. In the Policy Management window, click **Alarm Policy**.
4. On the Alarm Policy tab, all built-in preset alarm policies are displayed. You can enable/disable alarm policies, adjust threat levels, and modify policy content on this tab.

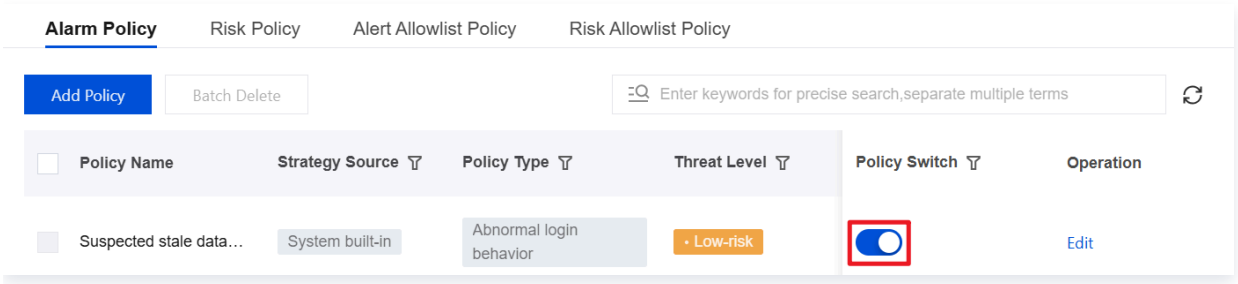
Adding Alarm Policies

1. On the Alarm Policy tab, click **Add Policy**.
2. In the pop-up window, set the policy name, policy remarks, threat level, policy switch, and policy content, and then click **Confirm**.



Enabling/Disabling Alarm Policies

On the Alarm Policy tab, select the target alarm policy and click the **toggle** in the policy switch column to enable or disable the alarm policy.

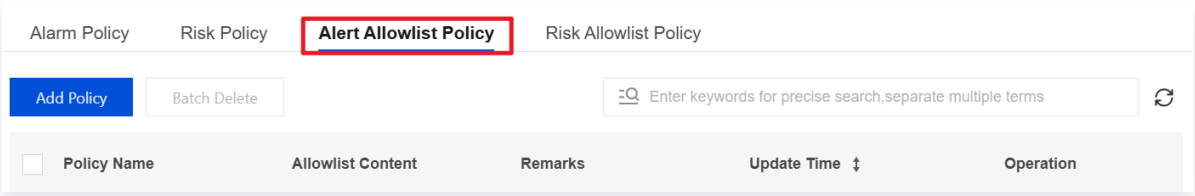


Editing Alarm Policies

1. On the Alarm Policy tab, select the target alarm policy and click **Edit** in the operation column.
2. In the Edit Policy window, you can modify the threat level and policy content, excluding service accounts.

Alarm Allowlist Management

1. In the Policy Management window, click **Alert Allowlist Policy**.



2. On the Alarm Allowlist Policy tab, all added alarm allowlist policies are displayed.
3. On the Alarm Allowlist Policy tab, you can periodically view the allowlist. Click Edit to modify rules, or click Delete to expire/invalidate rules.

Risk

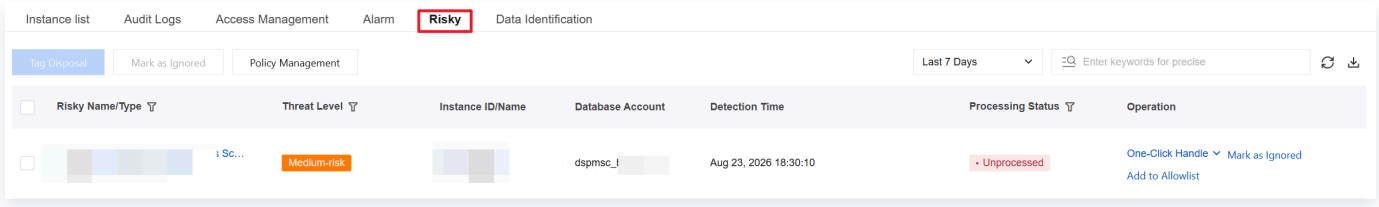
Last updated：2026-08-25 15:41:06

The database risk monitoring module focuses on behaviors that have not triggered risks but pose long-term security hazards. It covers core scenarios such as permission compliance remediation, attack surface hardening, and account security optimization, reducing the probability of security incidents.

Policy Name	Policy Content	Remediation Suggestion
Excessive operation permission scope	Calculate the permission utilization based on the permissions used by the account over the past 7 days (used permissions / granted permissions), and trigger a risk when it is less than the configured ratio.	• Risk Ignored • Add Risk to Allowlist • One-Click Handling
Exposing public network access entry	A risk is triggered when a database instance enables a public network address.	One-click Handling

Risk List

1. Log in to the TDSQL-C for MySQL console and click **Data Security Audit** in the left sidebar.
2. On the DSAudit page, click the **Risky** tag.



3. On the Risk page, data security risks that have triggered risk policies are displayed, including Risky Name/Type, Threat Level, Instance ID/Name, Database Account, Detection Time, and Processing Status.

Risk Details

On the Risk tag page, locate the target risk and click its name to view the risk details.

Risk Handling

Marking as Ignored

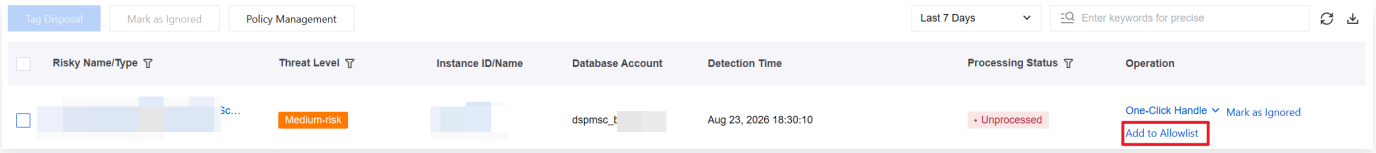
Mark the status of **risk items with overly broad operation permissions** to eliminate interference in risk statistics.

> **Note:**
> If the risk handling status is marked as ignored, the risk will not be included in risk statistics.

1. On the Risk tag page, you can handle target risks individually or in batches:
- **Individual handling**: Click **Mark as Ignored** in the operation column of the risk named **Excessive Operational Permissions Scope**.
- **Batch handling**: On the Risk page, select the risk named **Excessive Operational Permissions Scope** and click **Mark as Ignored** above the list.
2. In the confirmation dialog, click **Confirm** to mark the risk as ignored.

Adding Allowlists

1. On the Risk tag page, click **Add to Allowlist** in the operation column of the risk named **Excessive Operational Permissions Scope**.



2. In the Add to Allowlist window, review the allowlist policy content. After confirming that it is correct, click **Confirm** to add the policy information triggered by the risk to the allowlist.

> **Note:**
> After the risk allowlist policy rule takes effect, the behavior no longer triggers risks.

Marking as Resolved

Update the status of risks for which emergency response has been completed to close the handling loop.

1. On the Risk tag page, select one or more target risks and click **Tag Disposal**.
2. In the confirmation window, review the risk information. After confirming that it is correct, click **OK** to mark the risk as handled.

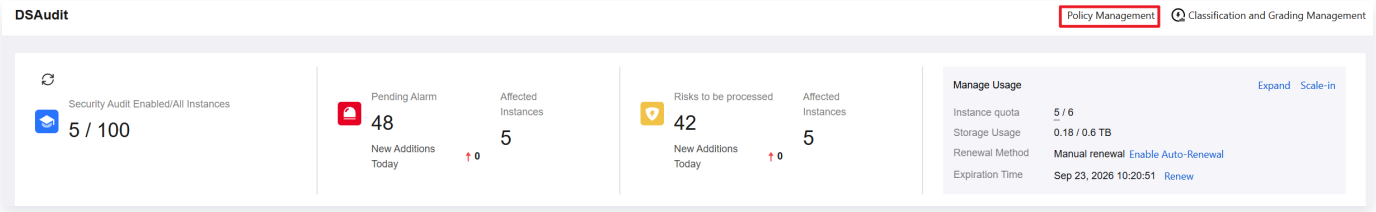
> **Note:**
> After the risk handling status is marked as handled, the risk will not be included in risk statistics.

One-Click Handling

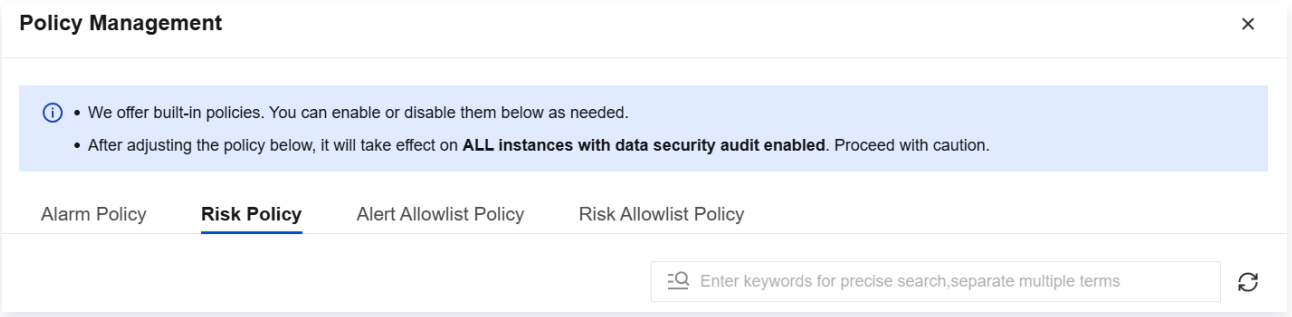
For different risk items, you can perform risk handling operations through one-click handling.
On the Risk tag page, select the target risk and click **One-click Handle** in the operation column. You can handle risks using the preset handling operations provided by the system.

Risk Policy Configuration

1. Log in to the TDSQL-C for MySQL console and click **Data Security Audit** in the left sidebar.
2. On the database risk monitoring page, click **Policy Management** in the upper-right corner.



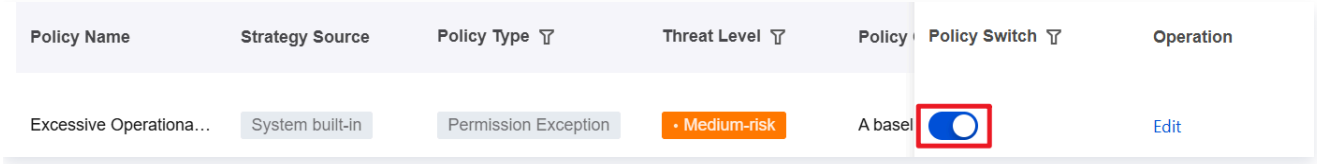
3. In the policy management window, click the **Risk Policy** tag.



4. On the Risk Policy tag page, all built-in preset risk policies are displayed. You can enable/disable risk policies, adjust threat levels, and modify policy content on this tag page.

Enabling/Disabling Risk Policies

On the Risk Policy tag page, select the target risk policy and click the **toggle** in the policy switch column to enable or disable the risk policy.



Editing Risk Policies

1. On the Risk Policy tag page, select the target risk policy and click **Edit** in the operation column.
2. In the Edit Policy window, you can modify the threat level and policy content, excluding service accounts.