Alibaba Cloud

数据安全中心

Quick Start

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.
⑦ Note	A note indicates supplemental instructions, best practices, tips, and other content.	⑦ **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.Quick start

After you activate Sensitive Data Discovery and Protection (SDDP), it automatically scans your data stored in Alibaba Cloud services, such as MaxCompute, ApsaraDB RDS, and Object Storage Service (OSS), for sensitive data. Then, SDDP marks the sensitive data with risk levels. You can check the overall risks and details of the sensitive data in the SDDP console.

Prerequisites

- At least one of the following services is activated or deployed: MaxCompute, ApsaraDB RDS, OSS, DRDS, PolarDB, Tablestore, and a self-managed database hosted on Elastic Compute Service (ECS). This ensures that DSC has data to scan.
- A data asset is created in MaxCompute, ApsaraDB RDS, OSS, DRDS, PolarDB, Tablestore, or a self-managed database hosted on ECS. You can create a data asset based on the following instructions:
  - **Create a project in MaxCompute and import data to the project for SDDP to scan**

    For more information, see Create a project.
  - **Create a database in an ApsaraDB RDS instance**

    For more information, see Create a database.
  - **Create a bucket in OSS and upload objects to the bucket**

    For more information, see Create buckets and Upload objects.
  - **Create a database in a DRDS instance**
  - **Create a PolarDB cluster**

    For more information, see Purchase a pay-as-you-go cluster.
  - **Create a Tablestore instance and a table**

    For more information, see Create instances and Create tables.
  - **Manage a database hosted on an ECS instance**

    For more information, see Manage user-created databases on ECS instances.

Procedure

1. Activate DSC and authorize DSC to access your Alibaba Cloud resources.After you activate DSC, you must authorize DSC to access your Alibaba Cloud resources. For more information, see Authorize DSC to access Alibaba Cloud resources.

2. Authorize SDDP to access your data assets in Alibaba Cloud services such as MaxCompute, ApsaraDB RDS, and OSS.DSC must be authorized to access your data assets before it can scan the data assets for sensitive data. For more information, see Grant access to data assets.

3. (Optional)Configure sensitive data detection rules.DSC detects sensitive data in objects or tables and generates alerts based on sensitive data detection rules. You can use built-in sensitive data detection rules provided by DSC. If the built-in sensitive data detection rules cannot meet your requirements, you can customize sensitive data detection rules based on your business needs. For more information, see Create a custom rule.

4. View the sensitive objects or tables detected by DSC and their statistics.For more information, see View summary information and View sensitive data.

5. De-identify the sensitive data that is detected.For more information, see Perform static de-

identif icat ion.