ALIBABA CLOUD

Alibaba Cloud

数据安全中心

Best practices

Document Version: 20210508

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.Best practices for protecting data stored in OSS

This topic shows you how to use Data Security Center (DSC) to detect, classify, and protect sensitive data that is stored in Object Storage Service (OSS).

Context

Sensitive data includes personal privacy information, passwords, keys, and images that contain sensitive content. Such data is of high value and is stored in your OSS buckets in different formats. The leaks of sensitive data can cause serious economic and brand losses to your enterprise.

After you authorize DSC to access an OSS bucket, DSC detects sensitive data in the OSS bucket, classifies and displays the sensitive data, and tracks the use of the sensitive data. In addition, DSC protects and audits the sensitive data based on predefined security rules, so that you can obtain the security status of your data assets in OSS at any time.

Scenarios

- **Sensitive data detection**

  You store a large amount of data in OSS. You cannot determine whether data stored in OSS contains sensitive data and where the sensitive data is stored.

  DSC scans data that is stored in OSS for sensitive data and classifies the sensitive data based on built-in or custom rules. Then, you can use OSS features such as access control and encryption to protect the sensitive data.

- **Data de-identification**

  If you share data for analysis or use without de-identifying sensitive data, the sensitive data may be leaked.

  DSC supports built-in and custom de-identification algorithms. You can use these algorithms to de-identify sensitive data that is obtained from the production environment before you transfer the sensitive data to other environments such as the development or test environment. DSC ensures that the de-identified sensitive data is usable in other environments.

Benefits

- **Visualized**: DSC visualizes the results of sensitive data detection. This allows you to obtain a clear view of the security status of your data assets.
  - Monitors data access and provides audit logs for you to trace anomalous activities, which reduces security risks to your data.
  - Increases the overall security transparency of your data assets and enhances data governance.
  - Reduces the cost of maintaining data security and provides fundamental data for you to formulate security rules that are suitable for your enterprise.
- **Intelligent**: DSC uses big data technologies, machine learning capabilities, and intelligent algorithms to detect and monitor sensitive data, high-risk activities such as anomalous data access, and potential data leaks. In addition, DSC provides suggestions on how to resolve detected issues.
  - Allows you to customize the rules to detect sensitive data so that you can ensure that the sensitive data is more accurately and efficiently detected and protected.

  - Integrates complex data formats and content to a unified data risk model and presents data in a standard manner for you to protect your key data assets.

- **Cloud-native**: DSC fully leverages its advantages as a cloud-native service and integrates with a variety of data assets on Alibaba Cloud.

  Compared with traditional sensitive data protection software, DSC provides a more robust service architecture and higher availability in a cost-efficient manner, and features higher system security.

Usage notes

You can activate DSC in pay-as-you-go mode for free. After you authorize DSC to access specific OSS buckets, DSC charges you at a price of USD 0.6 per GB for scanning objects that are stored in the OSS buckets.

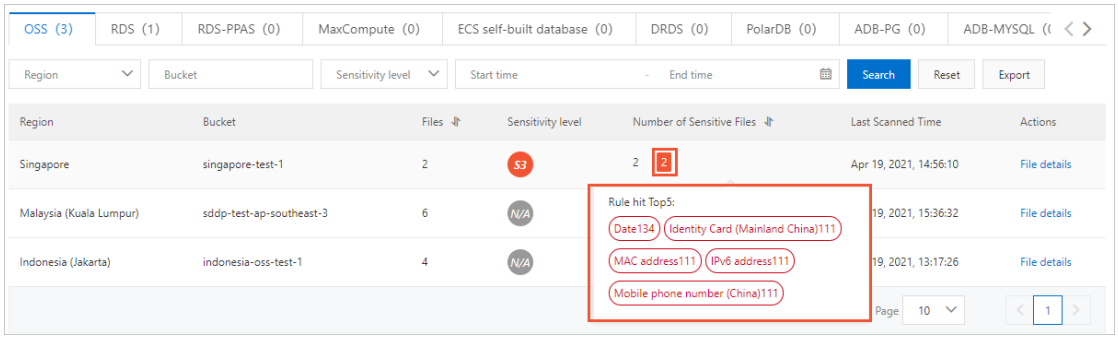
DSC scans all data that is stored in your OSS buckets at the first scan and charges you for a full scan. If you add new objects to or modify objects in your OSS buckets after the first scan, DSC charges you only for scanning the new or modified objects. This greatly reduces the expense.

Procedure

1. Activate Data Security Center (DSC).
2. Log on to the DSC console.
3. In the left-side navigation pane, choose **Data asset authorization > Data asset authorization**.
4. On the **OSS** tab, click **Unauthorized** and select multiple OSS buckets to authorize DSC to access these OSS buckets at a time.You can also find an OSS bucket and click **Authorization** in the Open protection column to authorize DSC to access the OSS bucket. For more information, see Authorize DSC to access OSS buckets.
   DSC starts to scan objects that are stored in your OSS buckets within 2 hours after the authorization. The time taken to scan objects in your OSS buckets depends on the total size of the objects. For more information, see the "How long does it take to scan data in my data asset after I authorize SDDP to access the data asset?" section of the Sensitive data scan and detection topic.

   When DSC scans data, the scan results are progressively updated on the **Overview** page in the DSC console. For more information, see View summary information.
5. In the left-side navigation pane, choose **Sensitive data discovery > Sensitive data assets**. On the **OSS** tab, view the results of scanning OSS for sensitive data. For more information, see View sensitive data detected in OSS. In addition, you must handle sensitive objects and risk activities based on the scan results at the earliest opportunity to prevent data security risks.We recommend that you perform the following operations:

i. Check the number of sensitive objects at each risk level in an OSS bucket that has a high risk level at the earliest opportunity. In addition, check the detection rules that are most frequently hit at each risk level and the number of objects that hit each rule.



ii. Click **File details** to view the information about the sensitive objects, such as the names, types, and sizes. Check whether the objects have data security risks.

iii. On the **Original log** page, find the sensitive objects based on their names and view the operations that were performed on the sensitive objects from clients. If necessary, record the IP addresses of the clients from which the operations were performed and check whether suspicious users exist.

iv. On the **Abnormal event alerts** page, view the anomalous activities based on the risk level and check whether high-risk activities exist.

v. De-identify sensitive data. For more information, see Perform static de-identification and Perform dynamic de-identification.

vi. In the OSS console, modify the read and write permissions on the risky OSS buckets or objects. For more information, see Modify bucket ACLs and Configure ACL for objects.

> **Note** You can configure server-side encryption to encrypt an object when you upload the object to OSS. This helps you prevent leaks of sensitive data. For more information, see Configure server-side encryption.

References

Subscription

Overview