Huawei Cloud Security Configuration Guide

Issue 2.0

Date 2024-04-30



Huawei Cloud Computing Technologies Co., Ltd.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

Information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road Qianzhong Avenue Gui'an New District Gui Zhou 550029 People's Republic of China

Website: https://www.huaweicloud.com/

Contents

1 Overview 1
1.1 Intended Audience 1
1.2 Definition of Terms 1
1.3 Rule Statisticss 2
2 Rules 3
2.1 C.CS.FOUNDATION.G_1 Identity and Access Management (IAM) 3
2.1.1 C.CS.FOUNDATION.G_1.R_1 Ensuring that AK/SK Are Disabled for Administrator Account 3
2.1.2 C.CS.FOUNDATION.G_1.R_2 Enabling MFA for Administrator Account 4
2.1.3 C.CS.FOUNDATION.G_1.R_3 Ensuring that No IAM Users Created in Admin User Group 5
2.1.4 C.CS.FOUNDATION.G_1.R_4 Ensuring that the Minimum Password Length Specified in IAM password Policy Is Not Less Than 8 5
2.1.5 C.CS.FOUNDATION.G_1.R_5 Ensuring that the IAM Password Policy Meets Password Strength Requirements 6
2.1.6 C.CS.FOUNDATION.G_1.R_6 Ensuring that IAM Password Policies Forbid Password Reuse 7
2.1.7 C.CS.FOUNDATION.G_1.R_7 Ensuring that the IAM Passwords Must Be Changed At Least Once Every 180 Days or Less 7
2.1.8 C.CS.FOUNDATION.G_1.R_8 Ensuring that the Minimum Password Age Is Set 8
2.1.9 C.CS.FOUNDATION.G_1.R_9 Enabling Login Protection 9
2.1.10 C.CS.FOUNDATION.G_1.R_10 Enabling User Operation Protection 9
2.1.11 C.CS.FOUNDATION.G_1.R_11 Enabling Access Key Management 10
2.1.12 C.CS.FOUNDATION.G_1.R_12 Avoiding Setting Access Keys for Users with Console Passwords When Setting Initial IAM Users 11
2.1.13 C.CS.FOUNDATION.G_1.R_13 Ensuring that Only One Active Access Key Is Available for an IAM User 11
2.1.14 C.CS.FOUNDATION.G_1.R_14 Ensuring that No IAM Policy Is Created to Allow the *:* Permissions 12
2.1.15 C.CS.FOUNDATION.G_1.R_15 Configuring a Login Authentication Policy 13
2.1.16 C.CS.FOUNDATION.G_1.R_16 Configuring an ACL 14
2.2 C.CS.FOUNDATION.G_2 Logging and Monitoring 15
2.2.1 C.CS.FOUNDATION.G_2.R_1 Enabling CTS 15
2.2.2 C.CS.FOUNDATION.G_2.R_2 Enabling the Key Event Notifications in CTS 16
2.2.3 C.CS.FOUNDATION.G_2.R_3 Ensuring that Log Retention Duration in LTS Meets Requirements 17
2.2.4 C.CS.FOUNDATION.G_2.R_4 Enabling LTS Log Transfer 18
2.2.5 C.CS.FOUNDATION.G_2.R_5 Enabling VPC Flow Logs 18

 Copyright © Huawei Technologies Co., Ltd.

2.2.6 C.CS.FOUNDATION.G_2.R_6 Enabling RDS Database Audit 19
2.2.7 C.CS.FOUNDATION.G_2.R_7 Enabling ECS Logs in LTS 20
2.2.8 C.CS.FOUNDATION.G_2.R_8 Enabling ELB Access Logs 21
2.2.9 C.CS.FOUNDATION.G_2.R_9 Enabling WAF Logs 21
2.2.10 C.CS.FOUNDATION.G_2.R_10 Enabling Logging for OBS Buckets 22
2.2.11 C.CS.FOUNDATION.G_2.R_11 Enabling FunctionGraph Logging 23
2.2.12 C.CS.FOUNDATION.G_2.R_12 Enabling the CFW Log Management Capability 23
2.2.13 C.CS.FOUNDATION.G_2.R_13 Enabling DBSS Database Audit 24
2.2.14 C.CS.FOUNDATION.G_2.R_14 Enabling DBSS Database Audit Alarm Notifications 25
2.2.15 C.CS.FOUNDATION.G_2.R_15 Enabling Log File Integrity Verification 26
2.2.16 C.CS.FOUNDATION.G_2.R_16 Enabling Encrypted Storage of Log Files 26
2.2.17 C.CS.FOUNDATION.G_2.R_17 Setting OBS Bucket for Storing Logs to Not Publicly Readable 27
2.3 C.CS.FOUNDATION.G_3 VMs and Containers 28
2.3.1 C.CS.FOUNDATION.G_3_1 Elastic Cloud Server (ECS) 28
2.3.1.1 C.CS.FOUNDATION.G_3_1.R_1 Using a Key Pair to Securely Log In to BMS 28
2.3.1.2 C.CS.FOUNDATION.G_3_1.R_2 Setting Firewall Policies in ECS to Restrict the Accesses to Metadata 29
2.3.1.3 C.CS.FOUNDATION.G_3_1.R_3 Updating the Password Reset Plug-in in ECS to the Latest Version 30
2.3.1.4 C.CS.FOUNDATION.G_3_1.R_4 Enabling Encryption for Private Images 31
2.3.2 C.CS.FOUNDATION.G_3_2 Bare Metal Server (BMS) 31
2.3.2.1 C.CS.FOUNDATION.G_3_2.R_1 Using a Key Pair to Securely Log In to BMS 31
2.3.2.2 C.CS.FOUNDATION.G_3_2.R_2 Setting Firewall Policies in BMS to Restrict the Accesses to Metadata 32
2.3.2.3 C.CS.FOUNDATION.G_3_2.R_3 Updating the Password Reset Plug-in in BMS to the Latest Version 33
2.3.3 C.CS.FOUNDATION.G_3_3 Cloud Container Engine (CCE) 34
2.3.3.1 C.CS.FOUNDATION.G_3_3.R_1 Disabling the Kubernetes Cluster Versions that has Reached EOS 34
2.3.3.2 C.CS.FOUNDATION.G_3_3.R_2 Enabling LTS and Collecting Container Logs 34
2.3.3.3 C.CS.FOUNDATION.G_3_3.R_3 Enabling the Container Security Edition of HSS 35
2.3.3.4 C.CS.FOUNDATION.G_3_3.R_4 Handling Vulnerabilities Released on the CCE Official Website in a Timely Manner 36
2.3.3.5 C.CS.FOUNDATION.G_3_3.R_5 Protecting the Cluster API Server 36
2.3.3.6 C.CS.FOUNDATION.G_3_3.R_6 Preventing Cluster Nodes from Being Exposed to Public Networks 37
2.3.3.7 C.CS.FOUNDATION.G_3_3.R_7 Hardening the Security Group Rules of the VPC Where the Kubernetes Cluster Resides 37
2.3.3.8 C.CS.FOUNDATION.G_3_3.R_8 Forbidding Containers to Obtain Host Machine Metadata 38
2.3.3.9 C.CS.FOUNDATION.G_3_3.R_9 Restricting the Access of Containers to the Management Plane 39
2.4 C.CS.FOUNDATION.G_4 Network 39
2.4.1 C.CS.FOUNDATION.G_4.R_1 Disabling Internet Access over SSH 39
2.4.2 C.CS.FOUNDATION.G_4.R_2 Disabling Internet Access over RDP 40

 Copyright © Huawei Technologies Co., Ltd.

2.4.3 C.CS.FOUNDATION.G_4.R_3 Disabling Access to Remote Management Ports and High-Risk Ports over the Source IP Address 0.0.0.0/0 for Subnet ACL 41
2.4.4 C.CS.FOUNDATION.G_4.R_4 Disabling Access to Remote Management Ports and High-Risk Ports over the Source IP Address 0.0.0.0/0 for Security Groups 42
2.4.5 C.CS.FOUNDATION.G_4.R_5 Ensuring the Principle of Least Privilege over VPC Peering Connections 43
2.4.6 C.CS.FOUNDATION.G_4.R_6 Enabling Access Control for ELB Listeners 44
2.5 C.CS.FOUNDATION.G_5 Storage 45
2.5.1 C.CS.FOUNDATION.G_5_1 Object Storage Service (OBS) 45
2.5.1.1 C.CS.FOUNDATION.G_5_1.R_1 Using OBS Server to Encrypt Stored Objects 45
2.5.1.2 C.CS.FOUNDATION.G_5_1.R_2 Disabling Anonymous Access 46
2.5.1.3 C.CS.FOUNDATION.G_5_1.R_3 Using OBS Temporary Data Sharing to Share Specified Data 46
2.5.1.4 C.CS.FOUNDATION.G_5_1.R_4 Controlling Permissions of OBS Resources Using Both VPC Endpoint and OBS Bucket Policies 47
2.5.1.5 C.CS.FOUNDATION.G_5_1.R_5 Using Bucket Policies to Restrict Access to OBS Buckets Using HTTPS 48
2.5.1.6 C.CS.FOUNDATION.G_5_1.R_6 Enabling Versioning 48
2.5.1.7 C.CS.FOUNDATION.G_5_1.R_7 Enabling WORM in Compliance Scenarios 49
2.5.1.8 C.CS.FOUNDATION.G_5_1.R_8 Avoiding Creating Public Objects in a Private Bucket 50
2.5.1.9 C.CS.FOUNDATION.G_5_1.R_9 Enabling URL Validation 50
2.5.1.10 C.CS.FOUNDATION.G_5_1.R_10 Using a User-Defined Domain Name in Scenarios Where OBS Objects Need to Be Previewed Online 51
2.5.1.11 C.CS.FOUNDATION.G_5_1.R_11 Enabling Cross-Region Replication 52
2.5.2 C.CS.FOUNDATION.G_5_2 Elastic Volume Service (EVS) 52
2.5.2.1 C.CS.FOUNDATION.G_5_2.R_1 Ensuring that EVS Encryption Is Enabled 52
2.5.3 C.CS.FOUNDATION.G_5_3 Scalable File Service (SFS) 53
2.5.3.1 C.CS.FOUNDATION.G_5_3.R_1 Ensuring that the SFS Turbo File System Encryption Is Enabled 53
2.5.4 C.CS.FOUNDATION.G_5_4 Cloud Backup and Recovery (CBR) 54
2.5.4.1 Select encrypted disks for C.CS.FOUNDATION.G_5_4.R_1 Selecting an Encryption Disk for EVS that Carries the Backup Data 54
2.5.4.2 C.CS.FOUNDATION.G_5_4.R_2 Enabling Re-confirmation for Deleting Backup Data 55
2.5.4.3 C.CS.FOUNDATION.G_5_4.R_3 Enabling Cross-Region Backup Replication 56
2.5.4.4 C.CS.FOUNDATION.G_5_4.R_4 Enabling Forcible Backup 56
2.6 C.CS.FOUNDATION.G_6 Databases 58
2.6.1 C.CS.FOUNDATION.G_6_1 RDS for MySQL 58
2.6.1.1 C.CS.FOUNDATION.G_6_1.R_1 Enabling Encrypted Communication 58
2.6.1.2 C.CS.FOUNDATION.G_6_1.R_2 Do Not Use the Default Port 59
2.6.1.3 C.CS.FOUNDATION.G_6_1.R_3 Enabling Transparent Data Encryption 60
2.6.1.4 C.CS.FOUNDATION.G_6_1.R_4 Update the Database Version to the Latest Version 60
2.6.1.5 C.CS.FOUNDATION.G_6_1.R_5 Do Not Bind an EIP to Access RDS for MySQL Through Internet. 61
2.6.1.6 C.CS.FOUNDATION.G_6_1.R_6 Configuring Proper Security Group Rules 62
2.6.1.7 C.CS.FOUNDATION.G_6_1.R_7 Enabling the Database Audit Logs 63
2.6.2 C.CS.FOUNDATION.G_6_2 Document Database Service (DDS) 63

2.6.2.1 C.CS.FOUNDATION.G_6_2.R_1 Enabling Encrypted Communication 63
2.6.2.2 C.CS.FOUNDATION.G_6_2.R_2 Limiting the Maximum Number of Connections..... 64
2.6.2.3 C.CS.FOUNDATION.G_6_2.R_3 Disabling the Script Running Function 65
2.6.2.4 C.CS.FOUNDATION.G_6_2.R_4 Enabling the Database Audit Logs 66
2.6.2.5 C.CS.FOUNDATION.G_6_4.R_7 Enabling the Backup Function and Configuring a Backup Policy.. 67
2.6.2.6 C.CS.FOUNDATION.G_6_2.R_6 Setting Second-Level Monitoring and Alarm Rules 68
2.6.2.7 C.CS.FOUNDATION.G_6_2.R_7 Do Not Use the Default Port 69
2.6.2.8 C.CS.FOUNDATION.G_6_2.R_8 Patch Upgrade..... 69
2.6.2.9 C.CS.FOUNDATION.G_6_2.R_9 Enabling Disk Encryption..... 70
2.6.3 C.CS.FOUNDATION.G_6_3 RDS for PostgreSQL 71
2.6.3.1 C.CS.FOUNDATION.G_6_3.R_1 Configuring Proper Security Group Rules 71
2.6.3.2 C.CS.FOUNDATION.G_6_3.R_2 Enabling the Backup Function and Configuring a Backup Policy.. 71
2.6.3.3 C.CS.FOUNDATION.G_6_2.R_4 Enabling the Database Audit Logs 72
2.6.3.4 C.CS.FOUNDATION.G_6_3.R_4 Do Not Use the Default Port 73
2.6.3.5 C.CS.FOUNDATION.G_6_3.R_5 Configuring the Timeout for Client Authentication 74
2.6.3.6 C.CS.FOUNDATION.G_6_3.R_6 Restricting IP Addresses for Connecting to the Database 75
2.6.3.7 C.CS.FOUNDATION.G_6_3.R_7 Enabling Log Recording for User Logins..... 76
2.6.3.8 C.CS.FOUNDATION.G_6_3.R_8 Update the Database Version to the Latest Version..... 76
2.6.4 C.CS.FOUNDATION.G_6_4 GaussDB 77
2.6.4.1 C.CS.FOUNDATION.G_6_4.R_1 Configuring Maximum Number of Concurrent Database Connections..... 77
2.6.4.2 C.CS.FOUNDATION.G_6_4.R_2 Security Authentication Configuration..... 78
2.6.4.3 C.CS.FOUNDATION.G_6_4.R_3 User Password Security 79
2.6.4.4 C.CS.FOUNDATION.G_6_4.R_4 Permission Management..... 80
2.6.4.5 C.CS.FOUNDATION.G_6_4.R_5 Enabling the Database Audit Logging Function 80
2.6.4.6 C.CS.FOUNDATION.G_6_4.R_6 WAL Archiving Configuration 81
2.6.4.7 C.CS.FOUNDATION.G_6_4.R_7 Enabling the Backup Function and Configuring a Backup Policy.. 82
2.7 C.CS.FOUNDATION.G_7 Enterprise Intelligence..... 84
2.7.1 C.CS.FOUNDATION.G_7_1 AI Development Platform ModelArts 84
2.7.1.1 C.CS.FOUNDATION.G_7_1.R_1 Using the IP Address Whitelist to Access the Notebook 84
2.7.1.2 C.CS.FOUNDATION.G_7_1.R_2 Using Dedicated Resource Pools..... 85
2.7.1.3 C.CS.FOUNDATION.G_7_1.R_3 Running a Custom Image as a Non-root User 86
2.7.1.4 C.CS.FOUNDATION.G_7_1.R_4 Using Independent Agencies for Different Sub-users 86
2.7.1.5 C.CS.FOUNDATION.G_7_1.R_5 Enabling "Strict Mode" 87
2.7.2 C.CS.FOUNDATION.G_7_2 MapReduce Service (MRS)..... 87
2.7.2.1 C.CS.FOUNDATION.G_7_2.R_1 Enabling Kerberos Authentication 87
2.7.2.2 C.CS.FOUNDATION.G_7_2.R_2 Separate Deployment of Management, Control, and Data Nodes 88
2.7.2.3 C.CS.FOUNDATION.G_7_2.R_3 EIP Security Group Management and Control 88
2.7.3 C.CS.FOUNDATION.G_7_3 GaussDB(DWS) 89
2.7.3.1 C.CS.FOUNDATION.G_7_3.R_1 Enabling Cluster Data Encryption..... 89
2.7.3.2 C.CS.FOUNDATION.G_7_3.R_2 Enabling Audit Logging on the GaussDB(DWS) Management Console..... 89

2.7.3.3 C.CS.FOUNDATION.G_7_3.R_3 Enabling GaussDB(DWS) Audit Logs 90
2.7.3.4 C.CS.FOUNDATION.G_7_3.R_4 Enabling Audit Log Dumping for a GaussDB(DWS) Database 91
2.7.3.5 C.CS.FOUNDATION.G_7_3.R_5 Enabling Rights Separation on GaussDB(DWS) 92
2.7.3.6 C.CS.FOUNDATION.G_7_3.R_6 Enabling SSL Encrypted Transmission 92
2.8 C.CS.FOUNDATION.G_8 Security 93
2.8.1 C.CS.FOUNDATION.G_8.R_1 Enabling WAF 93
2.8.2 C.CS.FOUNDATION.G_8.R_2 Configuring a Geolocation Access Rule in WAF 94
2.8.3 C.CS.FOUNDATION.G_8.R_3 Configuring the WAF Back-to-Source IP Addresses (Origin Server Deployed on ECSs) 94
2.8.4 C.CS.FOUNDATION.G_8.R_4 Configuring the WAF Back-to-Source IP Addresses (Origin Server Deployed on ELBs) 95
2.8.5 C.CS.FOUNDATION.G_8.R_5 Enabling WAF Basic Web Protection Block Mode 96
2.8.6 C.CS.FOUNDATION.G_8.R_6 Enabling Alarm Notifications for WAF Events 97
2.8.7 C.CS.FOUNDATION.G_8.R_7 Enabling HSS (Basic/Professional/Enterprise/Premium Edition) 98
2.8.8 C.CS.FOUNDATION.G_8.R_8 Enabling Ransomware Prevention (Premium/Container/WTP) 98
2.8.9 C.CS.FOUNDATION.G_8.R_9 Enabling the HSS Web Tamper Protection Edition 99
2.8.10 C.CS.FOUNDATION.G_8.R_10 Enabling CFW 100
2.8.11 C.CS.FOUNDATION.G_8.R_11 Enabling CFW Alarm Notification 101
2.8.12 C.CS.FOUNDATION.G_8.R_12 Enabling Automatic Notification of SecMaster High-Risk Alarms 102
2.8.13 C.CS.FOUNDATION.G_8.R_13 Enabling CBH and Multi-Factor Authentication 103
2.8.14 C.CS.FOUNDATION.G_8.R_14 Enabling DEW's Secret Hosting 103
3 Summary 105
4 Change History 106

1 Overview

Security configurations are the minimum security control measures required for IT systems and cloud environments. If cloud services fail to meet security configuration baseline requirements, services and assets on the cloud will suffer from high security risks. Huawei Cloud provides the security baseline check and configuration guide to help you improve the security protection for the cloud environment.

This document covers security configuration baseline for some important cloud services, including services in the identity and access management, log and monitoring, VMs and containers, networking, storage, databases, enterprise intelligence, and security domains. This document is designed for general purposes. It is subject to change based on your requirements.

1.1 Intended Audience

This document is intended for system administrators, application administrators, platform deployment personnel, security experts, auditors, and customer service who are responsible for developing, deploying, evaluating, or using Huawei Cloud services.

1.2 Definition of Terms

- **Rule Name**

  The name of a rule. Generally, the name of a negative rule starts with "Do not", that of a positive rule starts with "Ensure", and that of a recommendation starts with "Avoid" or uses the "should be" structure.

- **Level**

  A level indicates the level of the current rule.

  Level 1: Basic requirements for ensuring security and minimizing attack surface.

  Level 2: Additional configuration requirements based on level-1 requirements. However, such configuration may affect your services.

- **Background**

  This section describes how a rule works, possible security risks if the rule is not configured, and default configuration of the component version (if involved).

 Copyright © Huawei Technologies Co., Ltd.

- **Impact**

  This section describes impact on services if the rule is executed, for example, whether the service performance will be affected.

- **How to check**

  This section provides the method of checking the rule item. You will find verified check commands.

- **How to fix**

  The section provides a method of hardening the rule. You will find verified commands for security hardening.

- **Reference**

  This section provides the reference source of the rule.

1.3 Rule Statisticss

Level 1 Rules	68
Level 2 Rules	63
Total	131

 Copyright © Huawei Technologies Co., Ltd.

2 Rules

- Top of the window
- Bottom of the window

2.1 C.CS.FOUNDATION.G_1 Identity and Access Management (IAM)

2.1.1 C.CS.FOUNDATION.G_1.R_1 Ensuring that AK/SK Are Disabled for Administrator Account

Level: Level 1

Background:

The administrator has IAM user management permissions, which cover a wide range of operations. You need to disable the AK/SK for the administrator to prevent security risks caused by AK/SK leakage.

Impact:

The administrator account cannot use the AK/SK credentials.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. Hover over the username in the upper right and choose **My Credentials** from the drop-down list.
3. In the navigation pane on the left, choose **Access Keys**.
4. Check whether "No data available." is displayed in the access key list.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.

 Copyright © Huawei Technologies Co., Ltd.

2. Hover over the username in the upper right and choose **My Credentials** from the drop-down list.
3. Choose **Access Keys** in the navigation pane, and click **Delete** in the row that contains the target access key.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.2 C.CS.FOUNDATION.G_1.R_2 Enabling MFA for Administrator Account

Level: Level 1

Background:

Virtual multi-factor authentication (MFA) is an authentication method that requires users to install an MFA application (such as an authenticator) on their smart devices and bind the application to their accounts as a virtual MFA device. When users log in to the console or perform a critical operation, they need to enter a 6-digit code generated by the virtual MFA device. MFA devices can be hardware- or software-based. Currently, software-based virtual MFA devices are supported. MFA must be enabled for users to log in to the management console.

Impact:

A 6-digit verification code is required for logins after MFA is enabled. Enabling MFA has no other impacts on services.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. Choose **Users** in the navigation pane, and click **Security Settings** in the row that contains a user with administrator permissions.
3. Check whether **Bound** is displayed next to **Virtual MFA Device**.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation page on the left, choose **Security Settings**. Then, click the **Critical Operations** tab and click **Bind** next to **Virtual MFA Device**.
3. Set up the MFA application by scanning the QR code or entering the secret key.
4. Open the authenticator app on your mobile phone and view the verification code. The code is automatically updated every 30 seconds.
5. On the **Bind Virtual MFA Device** page, enter two consecutive verification codes and click **OK**.

The preceding steps apply to users who have upgraded their Huawei Cloud accounts to a Huawei ID. If you have not upgraded your Huawei Cloud account to a HUAWEI ID, click **Bind** to go to the **Account & security** page of the HUAWEI ID account center, and associate an MFA device with your HUAWEI ID as instructed.

 Copyright © Huawei Technologies Co., Ltd.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.3 C.CS.FOUNDATION.G_1.R_3 Ensuring that No IAM Users Created in Admin User Group

Level: Level 2

Background:

The default user **admin** has operation permissions for all cloud service resources. It is insecure if all users belong to the **admin** user group or share the same administrator account. To control the access of cloud resources by users or applications, customers can use Identity and Access Management (IAM) to create IAM users for their employees or applications.

Impact: None.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Users**.
3. Check whether there are users other than the enterprise administrator.
4. In the navigation pane on the left, choose **User Groups**.
5. Check whether there are user groups (other than the **admin** group) that contain at least one user.

How to fix:

1. Log in to the management console as the administrator, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **User Groups**. On the displayed page, click admin to go to its details page.
3. On the displayed details page, select the **Users** tab and delete users other than the administrator.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.4 C.CS.FOUNDATION.G_1.R_4 Ensuring that the Minimum Password Length Specified in IAM password Policy Is Not Less Than 8

Level: Level 1

Background: Password Policy

A strong password policy that meets the following requirements for IAM users is recommended:

Contains at least 8 characters.

 Copyright © Huawei Technologies Co., Ltd.

Impact: None.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. On the displayed page, click the **Password Policy** tab, and check whether the policy meets the minimum requirements.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. In the displayed dialog box, click **Password Policy** and configure the password policy as required.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.5 C.CS.FOUNDATION.G_1.R_5 Ensuring that the IAM Password Policy Meets Password Strength Requirements

Level: Level 1

Background:

A strong password policy that meets the following requirements for IAM users is recommended:

- Contain three or four of the following character types: uppercase letters, lowercase letters, digits, and special characters.
- Restrict consecutive identical characters (set **Max. Number of Consecutive Identical Characters** to **1**)

Impact: None.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. On the displayed page on the left, click the **Password Policy** tab, and check whether the policy contains the preceding or stricter requirements.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.

 Copyright © Huawei Technologies Co., Ltd.

3. In the displayed dialog box, click **Password Policy** and configure the password policy as required.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.6 C.CS.FOUNDATION.G_1.R_6 Ensuring that IAM Password Policies Forbid Password Reuse

Level: Level 1

Background:

A strong password policy that meets the following requirements for IAM users is recommended:

Cannot use any of the three recently used passwords.

Impact: None.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. On the displayed page on the left, click the **Password Policy** tab, and check whether the policy contains the preceding or stricter requirements.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. In the displayed dialog box, click **Password Policy** and configure the password policy as required.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.7 C.CS.FOUNDATION.G_1.R_7 Ensuring that the IAM Passwords Must Be Changed At Least Once Every 180 Days or Less

Level: Level 1

Background:

The password validity period policy of IAM users must be set. It is recommended that the policy meet the following requirements:

After the password expires, the system forces the user to change the password. (The password validity period should be set to 180 days or shorter.)

Impact: None.

 Copyright © Huawei Technologies Co., Ltd.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. On the displayed page on the left, click the **Password Policy** tab, and check whether the policy meets the minimum requirements.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. In the displayed dialog box, click **Password Policy** and configure the password validity policy as required.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.8 C.CS.FOUNDATION.G_1.R_8 Ensuring that the Minimum Password Age Is Set

Level: Level 2

Background:

The minimum password age for IAM users must be set. It is recommended that the policy meet the following requirements:

A password can be changed only after it is used for a specified time. (The minimum password age should be set to 5 minutes.)

Impact: None.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. On the displayed page on the left, click the **Password Policy** tab, and check whether the policy meets the minimum requirements.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. On the displayed page, click **Password Policy** and configure the **Minimum Password Age**.

Reference:

 Copyright © Huawei Technologies Co., Ltd.

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.9 C.CS.FOUNDATION.G_1.R_9 Enabling Login Protection

Level: Level 2

Background:

To improve account security and prevent phishing attacks and password leakage, the administrator can enable login protection on the **Account Security Settings** page. When users log in to the console, they need to verify their identities by virtual MFA, SMS, or email in addition to their passwords.

Impact: None.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Account Security Settings**.
3. On the displayed page, click the **Critical Operations** tab.
4. Check whether **Login Protection** is **Enabled**.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane, choose **Security Settings**.
3. On the displayed page, click the **Critical Operations** tab, click **Enable** next to **Login Protection**, select **Enable** and a verification method, and click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.10 C.CS.FOUNDATION.G_1.R_10 Enabling User Operation Protection

Level: Level 1

Background:

To improve account security and secure access to cloud services, the administrator can enable operation protection in IAM. When the account administrator or users created using the account perform a critical operation, such as deleting an Elastic Cloud Server (ECS) and unbinding an Elastic IP (EIP), on the console, they need to verify their identities again by virtual MFA device, SMS, or email.

Impact: None.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.

 Copyright © Huawei Technologies Co., Ltd.

2. In the navigation pane on the left, choose **Account Security Settings**.
3. On the displayed page, click the **Critical Operations** tab.
4. Check whether **Operation Protection** is **Enabled**.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. On the displayed page, click the **Critical Operations** tab, click **Enable** next to **Login Protection**, select **Enable** and a verification method, and click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.11 C.CS.FOUNDATION.G_1.R_11 Enabling Access Key Management

Level: Level 1

Background:

To ensure the security of your account and resources, you need to enable access key management. This option is disabled by default. After you enable this option, only the administrator can create, enable, disable, or delete access keys of IAM users.

Impact: None.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. Click the **Critical Operations** tab, and check whether **Access Key Management** is enabled.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. Click the **Critical Operations** tab, and enable **Access Key Management**.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

 Copyright © Huawei Technologies Co., Ltd.

2.1.12 C.CS.FOUNDATION.G_1.R_12 Avoiding Setting Access Keys for Users with Console Passwords When Setting Initial IAM Users

Level: Level 2

Background:

To improve account resource security, you are advised not to set access keys for IAM users who have console passwords when setting initial IAM users.

Impact:

When a user is created, no access key is created for the user who has the console password.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Users**.
3. Click **Security Settings** in the **Operation** column of each user.
4. View the user whose **Access Type** is set to **Management console access**. The access key of the user is displayed at the bottom of the page. Check whether the user has an access key.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Users**.
3. Click **Security Settings** in the **Operation** column of each user. The user details page is displayed.
4. View the user whose **Access Type** is set to **Management console access**. The access key of the user is displayed at the bottom of the page. Delete unnecessary access keys.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.13 C.CS.FOUNDATION.G_1.R_13 Ensuring that Only One Active Access Key Is Available for an IAM User

Level: Level 2

Background:

To improve account resource security, you are advised to assign only one active access key to an IAM user.

Impact:

Only one access key is available for a user.

 Copyright © Huawei Technologies Co., Ltd.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose Users.
3. Click **Security Settings** in the **Operation** column of each user. The user details page is displayed.
4. The access keys of the user are displayed at the bottom of the user details page. Check whether the user has only one enabled access key.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose Users.
3. Click **Security Settings** in the **Operation** column of each user. The user details page is displayed.
4. The access keys of the user are displayed at the bottom of the user details page. If there are two enabled access keys, disable or delete one of them.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.14 C.CS.FOUNDATION.G_1.R_14 Ensuring that No IAM Policy Is Created to Allow the *:* Permissions

Level: Level 1

Background:

To improve account resource security, do not create an IAM policy that allows the *:* management permission.

Impact:

IAM custom policies do not contain the *:* management permissions.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Permissions** > **Policies/Roles**. The IAM permission list page is displayed.
3. On the page displayed, filter by **Custom policy** and click the policy name to view the policy details.
4. On the policy details page, select **JSON** for **Policy View** and check whether the policy content contains *:*.

How to fix:

 Copyright © Huawei Technologies Co., Ltd.

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Permissions** > **Policies/Roles**. The IAM permission list page is displayed.
3. On the page displayed, filter by **Custom policy** and click the policy name to view the policy details.
4. On the policy details page, select **JSON** for **Policy View** and modify the policy whose content contains *:* to a specific path.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.15 C.CS.FOUNDATION.G_1.R_15 Configuring a Login Authentication Policy

Level: Level 1

Background:

The administrator can set a log authentication policy that covers **Session Timeout**, **Account Lockout**, **Account Disabling**, **Recent Login Information**, and **Custom Information**.

1. **Session Timeout**: Set a session timeout that will apply if users do not perform any operations within a specific period. The timeout ranges from 15 minutes to 24 hours, and the default timeout is **1 hour**.
2. **Account Lockout**: Set a duration to lock users out if a specific number of unsuccessful login attempts are reached within a certain period. You can set the account lockout duration, maximum number of unsuccessful login attempts before the account is locked, and time for resetting the account lockout counter.
   - Lockout duration: The value ranges from 15 to 30 minutes, and the default value is **15 minutes**.
   - Maximum number of unsuccessful login attempts: The value ranges from 3 to 10, and the default value is **5**.
   - Time for resetting the account lockout counter: The value ranges from 15 to 60 minutes, and the default value is **15 minutes**.
3. **Account Disabling**: Set a validity period to disable IAM users if they have not accessed HUAWEI CLOUD using the console or APIs within a certain period. This option is disabled by default. The validity period ranges from 1 to 240 days. If this option is enabled, the setting will take effect only for IAM users created using the account. If an IAM user is disabled, the user can request the administrator to enable their account again.
4. **Recent Login Information**: Configure whether to display the previous login information after users log in. If incorrect login information is displayed on the Login Verification page, users should change their passwords immediately. This option is disabled by default and can be enabled by the administrator.
5. **Custom Information**: Set custom information that will be displayed upon successful login. For example, enter the word **Welcome**. No information is displayed by default, and the administrator can set custom information that will be displayed. You and all the IAM users created using your account will see the same information upon successful login.

 Copyright © Huawei Technologies Co., Ltd.

Impact: None.

How to check:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. On the displayed page, click the **Login Authentication Policy** tab, and check whether **Session Timeout** and **Account Lockout** are configured, whether **Account Disabling** and **Recent Login Information** are enabled, and whether **Custom Information** is set.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. On the displayed page, click the **Login Authentication Policy** tab, and configure **Session Timeout**, **Account Lockout**, **Account Disabling**, **Recent Login Information**, and **Custom Information**, respectively.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.1.16 C.CS.FOUNDATION.G_1.R_16 Configuring an ACL

Level: Level 1

Background:

The administrator can set an access control list (ACL) to allow user access only from specified IP address ranges, IPv4 CIDR blocks, or VPC endpoints.

1. **IP Address Ranges**: Specify IP address ranges from 0.0.0.0 to 255.255.255.255 to allow access to HUAWEI CLOUD. The default value is **0.0.0.0–255.255.255.255**. If this parameter is left blank or the default value is used, IAM users can access HUAWEI CLOUD from anywhere.
2. **IPv4 CIDR Blocks**: Specify IPv4 CIDR blocks to allow access to HUAWEI CLOUD. For example, **10.10.10.10/32**.
3. **VPC Endpoints**: You can configure this parameter only on the **API Access** tab. You can allow access to Huawei Cloud APIs only from the VPC endpoint with the specified ID, for example, **0ccad098-b8f4-495a-9b10-613e2a5exxxx**.

Access type:

1. **Console Access**: The ACL will take effect only for IAM users who are created using your account and have permissions to access the console.
2. **API Access**: The ACL will take effect only for IAM users and controls their API access through API Gateway. The ACL will take effect 2 hours after you complete the configuration.

Impact: None.

How to check:

 Copyright © Huawei Technologies Co., Ltd.

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane on the left, choose **Security Settings**.
3. On the displayed page, click the **ACL** tab, and check whether **IP Address Ranges** and **IPv4 CIDR Blocks** have been configured.

How to fix:

1. Log in to the management console using the administrator account, hover over the username in the upper right, and choose **Identity and Access Management** from the drop-down list.
2. In the navigation pane, choose **Security Settings**.
3. On the displayed page, click the **ACL** tab, and configure **IP Address Ranges** and **IPv4 CIDR Blocks**, respectively.

Reference:

https://support.huaweicloud.com/intl/en-us/function-iam/index.html

2.2 C.CS.FOUNDATION.G_2 Logging and Monitoring

2.2.1 C.CS.FOUNDATION.G_2.R_1 Enabling CTS

Level: Level 1

Background:

Before using Cloud Trace Service (CTS), you need to enable it, and a tracker will be automatically created. The tracker identifies and associates with all cloud services you are using, and records all operations on the services. CTS collects, stores, and queries resource operation records. You can use these records to perform security analysis, track resource changes, audit compliance, and locate faults.

Impact: None.

How to check:

1. Log in to the management console.
2. Choose **Service List** > **Management & Governance** > **Cloud Trace Service**.
3. In the navigation pane on the left, choose **Trace List** and check whether there is any data.
4. In the navigation pane on the left, choose **Trackers** and check whether management tracker **system** is enabled.

How to fix:

1. Log in to the management console.
2. Hover on the upper left to display **Service List**. Under **Management & Governance**, click **Cloud Trace Service**.
3. On the displayed authorization page, click **Enable and Authorize**. CTS displays traces generated in the last seven days. To store traces for a long time, you can transfer them to Object Storage Service (OBS).

 Copyright © Huawei Technologies Co., Ltd.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-cts/cts_03_5107.html

2.2.2 C.CS.FOUNDATION.G_2.R_2 Enabling the Key Event Notifications in CTS

Level: Level 1

Background:

Key operations include high-risk operations (such as restarting VMs and changing security configurations), cost-sensitive operations (such as creating and deleting high-priced resources), and service-sensitive operations (such as changing network configurations). The following lists the key operation items of some cloud services.

- IAM: createUser, deleteUser, createAgency, and DeleteAgency
- ECS: rebootServer, updateSecurityGroup, removeSecurityGroup, and more
- VPC: modifySecurityGroup
- CTS: updateTracker, deleteTracker, and more
- OBS: setBucketAcl, setBucketPolicy, and more

After the key event notification is enabled, CTS sends notifications about these key operations to related subscribers through Simple Message Notification (SMN). This function is triggered by CTS, and notifications are sent by SMN.

You need to enable the key event notifications in CTS. You are advised to set the operation type to Custom (including deletion, creation, and login). When some key operations are recorded, CTS can send notifications to subscribers in real time through SMN. This function is triggered by CTS, and notifications are sent by SMN. For example, if the operation type is set to Root Login, a notification is sent when an enterprise administrator has a login event. If the operation type is set to CTS change, a notification is sent when the CTS tracker changes.

Impact: None.

How to check:

1. Log in to the management console.
2. Hover on the upper left to display **Service List**. Under **Management & Governance**, click **Cloud Trace Service**.
3. In the navigation pane on the left, choose **Key Event Notifications** and check whether a notification in the normal state exists in the **Notification Name** column.

How to fix:

1. Log in to the management console.
2. Hover on the upper left to display **Service List**. Under **Management & Governance**, click **Cloud Trace Service**.
3. In the navigation pane on the left, choose **Key Event Notifications**.
4. Click **Create Key Event Notification** in the upper right corner of the page. On the displayed page, specify required parameters.
5. Configure basic settings.
6. Configure key operations and users.

 Copyright © Huawei Technologies Co., Ltd.

Notification Name: Root Login (or any suitable name for your organization)
Operation Type: Custom
Operation List:
Service: IAM
Resource: user
Operation: login
User type: specified user
User list:
User group: **admin**
User: <Username of your enterprise administrator >

Notification Name: CTS change (or any suitable name for your organization)
Operation Type: Custom
Operation List:
Service: CTS
Resource: Tracker
Operations: updateTracker and deleteTracker
User type: All users

7. Configure an SMN topic.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-cts/cts_01_0009.html

2.2.3 C.CS.FOUNDATION.G_2.R_3 Ensuring that Log Retention Duration in LTS Meets Requirements

Level: Level 1

Background:

After the log data of hosts and cloud services is reported to LTS, the log data is automatically deleted after the default log retention duration expires. Therefore, you need to configure the log retention duration based on service requirements.

Impact:

A longer log storage duration requires more costs.

How to check:

1. Log in to the management console.
2. Hover on the upper left to display **Service List**. Under **Management & Governance**, click **Log Tank Service**.
3. In the navigation pane on the left, choose **Log Management**.
4. In the log group list, locate the target log group, click **Modify** in the **Operation** column, and check whether the log storage duration meets the requirements.

How to fix:

 Copyright © Huawei Technologies Co., Ltd.

1. Log in to the LTS console and choose **Log Management** in the navigation pane on the left.
2. In the log group list, locate the target log group and click **Modify** in the **Operation** column.
3. Modify **Log Retention Duration** based on service requirements.
4. Click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-lts/lts_04_0003.html

2.2.4 C.CS.FOUNDATION.G_2.R_4 Enabling LTS Log Transfer

Level: Level 1

Background:

After the log data of hosts and cloud services is reported to LTS, the log data is automatically deleted after the default log retention duration expires. If you want to store logs for a longer period, you need to configure log transfer in LTS. LTS can dump logs to the following cloud services:

- OBS: OBS is suitable for long-term storage.
- Data Ingestion Service (DIS): DIS provides long-term log storage and rich big data analysis capabilities.

Impact:

Before configuring log transfer, you need to configure the storage space of the target service.

How to check:

1. Log in to the management console.
2. Hover on the upper left to display **Service List**. Under **Management & Governance**, click **Log Tank Service**.
3. In the navigation pane on the left, choose **Log Transfer**.
4. In the Transfer Destination area on the right, check whether the status of OBS and DIS is normal.

How to fix:

1. Log in to the LTS console and choose **Log Transfer** in the navigation pane on the left.
2. Click **Configure Log Transfer** in the upper right corner.
3. On the displayed page, configure the log transfer parameters.
4. Click **OK**. When the log transfer status changes to **Normal**, the transfer task is created.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-lts/lts_04_0011.html

2.2.5 C.CS.FOUNDATION.G_2.R_5 Enabling VPC Flow Logs

Level: Level 2

 Copyright © Huawei Technologies Co., Ltd.

Background:

VPC flow logs record information about traffic going to and from VPCs. You can use flow logs to monitor network traffic, analyze network attacks, and determine whether security groups and firewall rules need to be changed. If you want to know the traffic details of NICs in a VPC, you can view flow logs about the NICs through LTS.

Impact:

The log storage space increases, which incurs extra costs.

How to check:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **VPC Flow Logs**, and check whether a VPC flow log exists.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **VPC Flow Logs**.
4. In the upper right corner, click **Create VPC Flow Log**. On the displayed dialog box, configure parameters as prompted.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-vpc/FlowLog_0002.html

2.2.6 C.CS.FOUNDATION.G_2.R_6 Enabling RDS Database Audit

Level: Level 2

Background:

If you enable SQL audit, all SQL operations will be logged for your download and query. SQL audit is disabled by default. Enabling this function may affect the database performance.

Impact:

The log storage space increases, which incurs extra costs.

How to check:

1. Log in to the management console.
2. Choose **Databases** > **Relational Database Service**.
3. On the **Instances** page, click the instance name.
4. In the navigation pane on the left, choose **SQL Audits**. On the displayed page, click **Set SQL Audit** and check whether **Audit Log** is enabled.

How to fix:

1. Log in to the management console.
2. Choose **Databases** > **Relational Database Service**.

 Copyright © Huawei Technologies Co., Ltd.

3. On the **Instances** page, click the instance name.
4. In the navigation pane on the left, choose **SQL Audits**. On the displayed page, click **Set SQL Audit**. In the displayed dialog box, configure the required parameters and click **OK**. Audit logs are retained for 7 days by default but can be retained from 1 to 732 days if needed.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_sql_auditing_log.html

2.2.7 C.CS.FOUNDATION.G_2.R_7 Enabling ECS Logs in LTS

Level: Level 2

Background:

ICAgent collects logs from hosts based on your specified collection rules, and packages and sends the collected log data to LTS on a log stream basis. You can view logs on the LTS console in real time.

Impact:

The log storage space increases, which incurs extra costs.

How to check:

1. Log in to the management console.
2. Hover on the upper left to display **Service List**. Under **Management & Governance**, click **Log Tank Service**. In the navigation pane on the left, choose **Log Management**.
3. In the navigation pane on the left, choose **Log Ingestion** > **Elastic Cloud Server (ECS)** and check whether the host access information, log group, and log stream are configured.

How to fix:

1. Log in to the management console.
2. Hover on the upper left to display **Service List**. Under **Management & Governance**, click **Log Tank Service**. In the navigation pane on the left, choose **Log Management**.
3. Click **Create Log Group**. In the displayed dialog box, enter a name and click **OK**.
4. Click the name of the created log group. Click **Create Log Stream**. In the displayed dialog box, enter a name and click **OK**.
5. Installing ICAgent
6. Log in to the LTS console, choose **Log Management**, and click the name of a log group.
7. In the log stream list, click the name of a log stream.
8. In the navigation pane on the left, choose **Log Ingestion** > **Elastic Cloud Server (ECS)**. Then, configure the collection path and other parameters as prompted.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-lts/lts_04_1031.html

 Copyright © Huawei Technologies Co., Ltd.

2.2.8 C.CS.FOUNDATION.G_2.R_8 Enabling ELB Access Logs

Level: Level 2

Background:

ELB logs details of HTTP and HTTPS requests, such as URIs, client IP addresses and ports, and status codes. You can use these logs for auditing. You can also search for logs using time and keywords and use a variety of SQL aggregation functions to analyze requests in a specified period to learn about the website visit frequency.

Impact:

The log storage space increases, which incurs extra costs.

How to check:

1. Log in to the management console.
2. Hover on the upper left to display **Service List**. Under **Networking**, click **Elastic Load Balance**. On the displayed page, locate the load balancer and click its name.
3. On the **Access Logs** tab page, check whether access logging is enabled and whether a log group and a log stream are configured.

How to fix:

1. Log in to the management console.
2. Hover on the upper left to display **Service List**. Under **Management & Governance**, click **Log Tank Service**. In the navigation pane on the left, choose **Log Management**.
3. Click **Create Log Group**. In the displayed dialog box, enter a name and click **OK**.
4. Click the name of the created log group. Click **Create Log Stream**. In the displayed dialog box, enter a name and click **OK**.
5. Hover on the upper left to display **Service List**. Under **Networking**, click **Elastic Load Balance**. On the displayed page, locate the load balancer and click its name.
6. On the **Access Logs** tab page, click **Configure Access Log**. In the displayed dialog box, enable access logging and select the created log group and log stream.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-elb/en-us_topic_0150301848.html

2.2.9 C.CS.FOUNDATION.G_2.R_9 Enabling WAF Logs

Level: Level 1

Background:

Users can authorize WAF to access LTS so that all attack and access logs can be collected in Log Tank Service (LTS). With LTS, users can perform real-time decision analysis, device O&M management, and service trend analysis in a timely and efficient manner. Enabling LTS for WAF does not affect WAF performance.

 Copyright © Huawei Technologies Co., Ltd.

Impact:

The log storage space increases, which incurs extra costs.

How to check:

1. Log in to the management console.
2. In the service list, choose **Security & Compliance** > **Web Application Firewall**.
3. In the navigation pane on the left, choose **Events**.
4. Select the **Log Settings** tab.
5. Check whether the log function is enabled, whether the log group is configured, and whether log streams for attack and access logs are configured.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Security & Compliance** > **Web Application Firewall**.
3. In the navigation pane on the left, choose **Events**.
4. Select the **Log Settings** tab, enable LTS, and set a log group and log stream.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-waf/waf_01_0172.html

2.2.10 C.CS.FOUNDATION.G_2.R_10 Enabling Logging for OBS Buckets

Level: Level 1

Background:

You can enable OBS logging to facilitate bucket analysis or auditing as required. With access logs, a bucket owner can deeply analyze the property, type, or trend of requests. When logging is enabled for a bucket, OBS automatically logs access requests to the bucket and generates and writes log files into a specific bucket.

Impact:

OBS storage space must be configured in advance.

How to check:

1. Log in to the management console.
2. Choose **Storage** > **Object Storage Service**.
3. In the navigation pane, choose **Object Storage**.
4. Click the name of the target bucket to go to the bucket **Overview** page. In the **Basic Configurations** area, check whether **Logging** is in the **Configured** state.

How to fix:

1. Log in to the management console.
2. Choose **Storage** > **Object Storage Service**.
3. In the navigation pane, choose **Object Storage**.
4. In the bucket list, click the bucket to be operated. The **Overview** page of the bucket is displayed.

 Copyright © Huawei Technologies Co., Ltd.

5. In the **Basic Configurations** area, click **Logging**. The **Logging** dialog box is displayed.
6. Select **Enable** and configure parameters as prompted.

Reference:

https://support.huaweicloud.com/intl/en-us/ugobs-obs/obs_41_0046.html

2.2.11 C.CS.FOUNDATION.G_2.R_11 Enabling FunctionGraph Logging

Level: Level 2

Background:

You can enable FunctionGraph logging to facilitate analysis or audit as required. By accessing logs, the function owner can analyze the function execution process and quickly locate faults.

Impact:

The log storage space increases, which incurs extra costs.

How to check:

1. Log in to the management console.
2. Choose **Compute** > **FunctionGraph**.
3. In the navigation pane, choose **Functions** > **Function List**.
4. Click a function, choose **Configuration** > **Log**, and check whether the parameter **Collect Logs** is configured.

How to fix:

1. Log in to the management console.
2. Choose **Compute** > **FunctionGraph**.
3. In the navigation pane, choose **Functions** > **Function List**.
4. Click a function, choose **Configuration** > **Log**, and enable and configure the **Collect Logs** parameter.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-functiongraph/functiongraph_01_1841.html

2.2.12 C.CS.FOUNDATION.G_2.R_12 Enabling the CFW Log Management Capability

Level: Level 1

Background:

You can record attack event logs, access control logs, and traffic logs to Log Tank Service (LTS) and use these logs to quickly and efficiently perform real-time decision analysis, device O&M, and service trend analysis.

Impact:

 Copyright © Huawei Technologies Co., Ltd.

The log storage space increases, which incurs extra costs.

How to check:

1. Log in to the management console.
2. Select a region.
3. Choose **Security Compliance** > **Cloud Firewall** from the service list.
4. In the navigation pane on the left, choose **Log Audit** > **Log Management**.
5. Check whether log management is enabled.

How to fix:

1. Log in to the management console.
2. Select a region in the upper part of the page.
3. Choose **Security Compliance** > **Cloud Firewall** from the service list.
4. In the navigation pane on the left, choose **Log Audit** > **Log Management**. On the displayed page, enable the log management function.
5. Create a log group and log stream. For details, see Creating Log Groups and Log Streams.
6. Select a created log group or log stream. Click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-cfw/cfw_01_0141.html

2.2.13 C.CS.FOUNDATION.G_2.R_13 Enabling DBSS Database Audit

Level: Level 2

Background:

The database audit function should be enabled for databases. The database audit function of Database Security Service (DBSS) provides the audit function in bypass mode. It records user access to the database in real time, generates fine-grained audit reports, and sends real-time alarms for risky operations and attacks, helping users locate internal violations and improper operations in the database.

Impact: None.

How to check:

1. Log in to the management console.
2. Select a region in the upper part of the page.
3. In the service list, choose **Security & Compliance** > **Database Security Service**.
4. On the database audit page, choose **Instances**. Check whether the status of the database audit instance is **Running** and whether the number of associated databases is **0**.

How to fix:

1. Log in to the management console.
2. Select a region in the upper part of the page.

 Copyright © Huawei Technologies Co., Ltd.

3. In the service list, choose **Security & Compliance** > **Database Security Service**.
4. Add a database: Click **Databases** on the left and click **Add Database** on the right. In the displayed dialog box, set the database information. A database whose **Audit Status** is **Disabled** will be added to the database list.
5. Add an agent. Log in to the DBSS management console. In the **Agent** column of a database, click **Add**. In the **Add** dialog box, configure parameters and click **OK**.
6. Add a security group rule. To avoid connectivity issues, add an inbound rule in the security group of the database audit instance.
7. Download and then install the agent on the database or application based on the add mode you chose.
8. Enable database audit. On the **Databases** page, select an instance from the **Instance** drop-down list.
9. In the database list, click **Enable** in the **Operation** column of the database you want to audit.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-dbss/dbss_01_0117.html

2.2.14 C.CS.FOUNDATION.G_2.R_14 Enabling DBSS Database Audit Alarm Notifications

Level: Level 1

Background:

After configuring alarm notifications, you can receive DBSS alarms on database risks. If this function is not enabled, you have to log in to the management console to view alarms.

Impact: None.

How to check:

1. Log in to the management console. In the upper part of the displayed page, select a region.
2. Choose **Security & Compliance** > **Database Security Service**.
3. In the navigation tree on the left, choose **Database Audit** > **Settings**.
4. Select an instance. Click the **Alarm Notifications** tab.
5. Check whether **Alarm Notifications** is enabled in the **Global Settings** dialog box.

How to fix:

1. Log in to the management console. In the upper part of the displayed page, select a region.
2. Choose **Security & Compliance** > **Database Security Service**.
3. In the navigation tree on the left, choose **Databases Audit** > **Settings**.
4. Select an instance. Click the **Alarm Notifications** tab.
5. Set alarm notifications and click **Apply**.

 Copyright © Huawei Technologies Co., Ltd.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-dbss/dbss_01_0356.html

2.2.15 C.CS.FOUNDATION.G_2.R_15 Enabling Log File Integrity Verification

Level: Level 1

Background:

When dumping audit logs to OBS, you can enable file verification to ensure the integrity of audit files and prevent files from being tampered with.

Impact: None.

How to check:

1. Log in to the management console.
2. Select a region.
3. In the navigation pane on the left, choose **Cloud Trace Service** > **Trackers**. The tracker management page is displayed.
4. Select the tracker to be checked and view its details.
5. Check whether the file verification function is enabled.

How to fix:

1. Log in to the management console.
2. Select a region in the upper part of the page.
3. In the navigation pane on the left, choose **Cloud Trace Service** > **Trackers**. The tracker list page is displayed.
4. Select the tracker to be repaired and click **Configure** in the **Operation** column.
5. In the **Configure Transfer** step, enable the **Verify Trace File** function.
6. Save the configurations.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-cts/cts_03_5106.html

2.2.16 C.CS.FOUNDATION.G_2.R_16 Enabling Encrypted Storage of Log Files

Level: Level 2

Background:

When dumping audit logs to OBS, you can configure encrypted storage to prevent unauthorized access to files.

Impact:

If the KMS key used for encryption is disabled, scheduled for deletion, or deleted, your data cannot be accessed any more.

How to check:

 Copyright © Huawei Technologies Co., Ltd.

1. Log in to the management console.
2. Select a region.
3. In the navigation pane on the left, choose **Cloud Trace Service** > **Trackers**. The tracker management page is displayed.
4. Click the **system** tracker to go to the details page.
5. The **Encrypt Trace File** function is disabled.

How to fix:

1. Log in to the management console.
2. Select a region in the upper part of the page.
3. In the navigation pane on the left, choose **Cloud Trace Service** > **Trackers**. The tracker management page is displayed.
4. Select the **system** tracker to be repaired and click **Configure** in the **Operation** column.
5. In the **Configure Transfer** step, enable the **Encrypt Trace File** function, and select an encryption key.
6. Save the configurations.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-cts/cts_03_5106.html

2.2.17 C.CS.FOUNDATION.G_2.R_17 Setting OBS Bucket for Storing Logs to Not Publicly Readable

Level: Level 1

Background:

Setting the bucket for storing audit logs to not publicly readable prevents unauthorized access to audit logs.

Impact: None.

How to check:

1. Log in to the management console.
2. Select a region.
3. In the navigation pane on the left, choose **Cloud Trace Service** > **Trackers**. The tracker management page is displayed.
4. Select the tracker to be checked and click the bucket name in the **Storage** column. The bucket overview page is displayed.
5. In the navigation pane on the left, choose **Permissions** > **Bucket ACLs**.
6. Check whether **Public Permissions** is set to **Private**.

How to fix:

1. Log in to the management console.
2. Select a region in the upper part of the page.
3. In the navigation pane on the left, choose **Cloud Trace Service** > **Trackers**. The tracker management page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

4. Select the tracker to be checked and click the bucket name in the **Storage** column. The bucket overview page is displayed.
5. In the navigation pane on the left, choose **Permissions** > **Bucket ACLs**.
6. In the **Public Permissions** area, click **Private**.
7. Confirm the configurations.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-cts/cts_03_5106.html

2.3 C.CS.FOUNDATION.G_3 VMs and Containers

2.3.1 C.CS.FOUNDATION.G_3_1 Elastic Cloud Server (ECS)

2.3.1.1 C.CS.FOUNDATION.G_3_1.R_1 Using a Key Pair to Securely Log In to BMS

Level: Level 2

Background:

Key pairs are a set of security credentials for identity authentication when you remotely log in to ECSs.

A key pair consists of a public key and a private key. Key Pair Service (KPS) stores the public key and you store the private key. If you have imported a public key into a Linux ECS, you can use the corresponding private key to log in to the ECS without a password.

Therefore, you do not need to worry about password interception, cracking, or leakage.

Impact: None.

How to check:

1. Log in to the management console.
2. In the service list, choose **Compute** > **Elastic Cloud Server**.
3. In the navigation pane on the left, choose **Key Pair**. On the displayed page, check whether there are key pairs.
4. In the service list, choose **Compute** > **Elastic Cloud Server**.
5. On the ECS page, click an ECS name to go to the ECS details page.
6. On the **Basic Information** tab page, check whether the key pair information is displayed in the ECS information area.

How to fix:

During ECS creation:

1. Log in to the management console.
2. In the service list, choose **Compute** > **Elastic Cloud Server**.
3. In the navigation pane on the left, choose **Key Pair**. On the displayed page, click **Create Key Pair**, enter a name, and click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

4. A dialog box is displayed, indicating that the private key has been downloaded. The file name is the specified key pair name with a suffix of .pem. Keep the private key file secure, and click **OK** in the displayed dialog box.
5. In the **Advanced Settings** step of purchasing ECS, select **Key Pair** for **Login Mode**, select the created key pair from the **Key Pair** drop-down list, and select **I acknowledge that I have obtained private key file xxx.pem and that without this file I will not be able to log in to my ECS**.

After ECS creation:

1. Log in to the management console.
2. In the upper left corner, select a region and project.
3. In the navigation pane on the left, choose **Security & Compliance** > **Data Encryption Workshop**. The **Key Management Service** will be displayed.
4. In the navigation pane on the left, click **Key Pair Service**.
5. Click **ECS List** to view ECSs.
6. Click **Bind** in the row of an ECS to open the **Bind Key Pair** dialog box.
   - If the ECS is shut down, a dialog box will be displayed.
   - If the ECS is running, you need to provide the **root** password.
7. Select a new key pair from the drop-down list box of **New Key Pair**.
8. The default port number is **22** and can be modified.
9. You can enable or disable the password login mode as required. By default, the password login mode is disabled.
10. Select **I have read and agree to the Key Pair Service Disclaimer**.
11. Click **OK**.
    - If the ECS is not shut down, use the **root** password to bind the key pair. It takes about 30 seconds to complete.
    - If the ECS is shut down, the binding operation may take about five minutes.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-dew/dew_01_0033.html

2.3.1.2 C.CS.FOUNDATION.G_3_1.R_2 Setting Firewall Policies in ECS to Restrict the Accesses to Metadata

Level: Level 1

Background:

ECS metadata contains basic ECS information on the cloud platform, such as the cloud service ID, host name, and network information. It may also contain sensitive information. The multi-user design of GuestOS causes a large metadata access scope, the SSRF vulnerability of tenant APPs may cause metadata leakage.

You can configure firewall policies in ECS to restrict the accesses to metadata and mitigate metadata leakage risks.

Impact:

Metadata access is restricted. Non-administrator users will fail to access metadata.

How to check:

 Copyright © Huawei Technologies Co., Ltd.

1. Log in to the ECS as a common user (not user **root** or **Administrator**).
2. If you use Linux, run the curl command to access 169.254.169.254. If you use Windows, use a browser to access 169.254.169.254. If you can use a common user to access 169.254.169.254, the metadata access scope is too large.

How to fix:

1. If you use Windows and need to assign permissions only to the administrator to access custom data, enable the firewall as an administrator and run the following commands in PowerShell:

```
PS C:\>$RejectPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("Everyone")
PS C:\>$RejectPrincipalSID =
$RejectPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\>$ExceptPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("Administrator")
PS C:\>$ExceptPrincipalSID =
$ExceptPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\>$PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptPrincipalSID)(A;;CC;;;$RejectPrincipalSID)"
PS C:\>New-NetFirewallRule -DisplayName "Reject metadata service for $($RejectPrincipal.Value),
exception: $($ExceptPrincipal.Value)" -Action block -Direction out -Protocol TCP -RemoteAddress
169.254.169.254 -LocalUser $PrincipalSDDL
```

2. If you use Linux and need to assign permissions only to user **root** to access custom data, run the following command as user **root**:

```
iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner ! --uid-owner root --
jump REJECT
```

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-ecs/ecs_03_0166.html

2.3.1.3 C.CS.FOUNDATION.G_3_1.R_3 Updating the Password Reset Plug-in in ECS to the Latest Version

Level: Level 1

Background:

ECS provides the one-click password resetting function. If you have installed the password reset plug-in, you can reset the password with a few clicks when your ECS password is lost or expires.

Updating the password reset plug-in ensures that vulnerabilities are fixed in a timely manner.

Impact: None.

How to check:

Check whether the plug-in of the latest version is installed.

- Run the following command to check the plug-in version in Linux servers:

  cat /CloudrResetPwdAgent/depend/jre/release | grep -i VERSION
- To check the plug-in version in Windows servers, perform the following steps:

  Open the **C:\CloudResetPwdAgent\depend\jre\release** file.

  If **JAVA_VERSION="1.8.0_362"** is not found in the **release** file or there are no release files, the password reset plug-in is not updated to the latest version.

How to fix:

 Copyright © Huawei Technologies Co., Ltd.

Upgrade the password reset plug-in to the latest version. (Skip this step if the plug-in is not installed.)

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-ecs/ecs_03_1007.html

2.3.1.4 C.CS.FOUNDATION.G_3_1.R_4 Enabling Encryption for Private Images

Level: Level 2

Background:

Image encryption supports encrypting private images. When creating an ECS, if you select an encrypted image, the system disk of the created ECS automatically has encryption enabled, implementing system disk encryption.

Impact: None.

How to check:

1. Log in to the management console.
2. Choose **Compute** > **Image Management Service** from the service list.
3. Click the **Private Images** tab. On the private image list page, check whether the value of **Encryption** field of the private image is **Yes**.

How to fix:

You can create an encrypted image using an external image file or an encrypted ECS.

1. Create an encrypted image using an external image file.

   When you register the external image file as a private image, select **KMS encryption** and select a key. For details, see Creating a Windows System Disk Image from an External Image File or Creating a Linux System Disk Image from an External Image File.
2. Create an encrypted image using an encrypted ECS.

   When you use an ECS to create a private image, if the system disk of the ECS is encrypted, the private image created using the ECS is also encrypted. The key used for encrypting the image must be the same as that used for encrypting the system disk. For details, see Creating a System Disk Image from a Windows Server and Creating a System Disk Image from a Linux ECS.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-ims/ims_01_0328.html

2.3.2 C.CS.FOUNDATION.G_3_2 Bare Metal Server (BMS)

2.3.2.1 C.CS.FOUNDATION.G_3_2.R_1 Using a Key Pair to Securely Log In to BMS

Level: Level 2

Background:

 Copyright © Huawei Technologies Co., Ltd.

Key pairs are a set of security credentials for identity authentication when you remotely log in to ECSs.

A key pair consists of a public key and a private key. Key Pair Service (KPS) stores the public key and you store the private key. If you have imported a public key into a Linux ECS, you can use the corresponding private key to log in to the ECS without a password.

Therefore, you do not need to worry about password interception, cracking, or leakage.

Impact: None.

How to check:

1. Log in to the management console.
2. In the service list, choose **Compute** > **Bare Metal Server**.
3. In the navigation pane on the left, choose **Key Pair**. On the displayed page, check whether there are key pairs.
4. In the service list, choose **Compute** > **Bare Metal Server**.
5. On the BMS page, click a BMS name to go to its details page.
6. Check whether key pair information is displayed.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Compute** > **Bare Metal Server**.
3. In the navigation pane on the left, choose **Key Pair**. On the displayed page, click **Create Key Pair**, enter a name, and click **OK**.
4. A dialog box is displayed, indicating that the private key has been downloaded. The file name is the specified key pair name with a suffix of .pem. Keep the private key file secure, and click **OK** in the displayed dialog box.
5. In the **Advanced Settings** step of purchasing BMS, select **Key Pair** for **Login Mode**, select the created key pair from the **Key Pair** drop-down list, and select **I acknowledge that I have obtained private key file xxx.pem and that without this file I will not be able to log in to my BMS**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-bms/bms_01_0015.html

2.3.2.2 C.CS.FOUNDATION.G_3_2.R_2 Setting Firewall Policies in BMS to Restrict the Accesses to Metadata

Level: Level 1

Background:

BMS metadata contains basic BMS information on the cloud platform, such as the cloud service ID, host name, and network information. It may also contain sensitive information. The multi-user design of GuestOS causes a large metadata access scope, the SSRF vulnerability of tenant APPs may cause metadata leakage.

You can configure firewall policies in BMS to restrict the accesses to metadata and mitigate metadata leakage risks.

Impact:

 Copyright © Huawei Technologies Co., Ltd.

Metadata access is restricted. Non-administrator users will fail to access metadata.

How to check:

1. Log in to the BMS as a common user (not user **root** or **Administrator**).
2. If you use Linux, run the curl command to access 169.254.169.254. If you use Windows, use a browser to access 169.254.169.254. If you can use a common user to access 169.254.169.254, the metadata access scope is too large.

How to fix:

1. If you use Windows and need to assign permissions only to the administrator to access custom data, enable the firewall as an administrator and run the following commands in PowerShell:

```
PS C:\>$RejectPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("Everyone")
PS C:\>$RejectPrincipalSID =
$RejectPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\>$ExceptPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("Administrator")
PS C:\>$ExceptPrincipalSID =
$ExceptPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\>$PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptPrincipalSID)(A;;CC;;;$RejectPrincipalSID)"
PS C:\>New-NetFirewallRule -DisplayName "Reject metadata service for $($RejectPrincipal.Value),
exception: $($ExceptPrincipal.Value)" -Action block -Direction out -Protocol TCP -RemoteAddress
169.254.169.254 -LocalUser $PrincipalSDDL
```

2. If you use Linux and need to assign permissions only to user **root** to access custom data, run the following command as user **root**:

```
iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner ! --uid-owner root --
jump REJECT
```

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-bms/bms_01_0040.html

2.3.2.3 C.CS.FOUNDATION.G_3_2.R_3 Updating the Password Reset Plug-in in BMS to the Latest Version

Level: Level 1

Background:

BMS provides the one-click password resetting function. If you have installed the password reset plug-in, you can reset the password with a few clicks when your BMS password is lost or expires.

Updating the password reset plug-in ensures that vulnerabilities are fixed in a timely manner.

Impact: None.

How to check:

Check whether the plug-in of the latest version is installed.

- Run the following command to check the plug-in version in Linux servers:
  cat /CloudrResetPwdAgent/depend/jre/release | grep -i VERSION
- To check the plug-in version in Windows servers, perform the following steps:
  Open the **C:\CloudResetPwdAgent\depend\jre\release** file.

 Copyright © Huawei Technologies Co., Ltd.

If **JAVA_VERSION="1.8.0_362"** is not found in the **release** file or there are no release files, the password reset plug-in is not updated to the latest version.

How to fix:

Upgrade the password reset plug-in to the latest version. If the plug-in is not installed, skip this step. For details, see Installing the One-Click Password Reset Plugin.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-bms/bms_01_0030.html

2.3.3 C.CS.FOUNDATION.G_3_3 Cloud Container Engine (CCE)

2.3.3.1 C.CS.FOUNDATION.G_3_3.R_1 Disabling the Kubernetes Cluster Versions that has Reached EOS

Level: Level 1

Background:

After the cluster version EOS, CCE does not support the creation of new clusters or provide technical support including new feature updates, vulnerability or issue fixes, new patches, work order guidance, and online checks for the EOS cluster version. Pay attention to the Kubernetes version policies in the CCE console bulletin or CCE official documentation. Upgrade the cluster by referring to the Cluster Upgrade before the cluster lifecycle ends.

Impact:

Some compatibility issues exist between different Kubernetes versions. Before upgrading a cluster, tenants may need to adapt to the applications. Upgrading a cluster is a high-risk operation. Before upgrading a cluster, you need to fully verify the cluster in the production environment.

How to check:

On the CCE console, view the version information of the existing clusters. Check whether the cluster version is in the EOS by referring to Kubernetes Version Policies.

How to fix:

If a Kubernetes cluster is in the EOS state, upgrade it by referring to Cluster Upgrade.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-cce/cce_bestpractice_0317.html

2.3.3.2 C.CS.FOUNDATION.G_3_3.R_2 Enabling LTS and Collecting Container Logs

Level: Level 2

Background:

Log Tank Service (LTS) collects log data from hosts and cloud services. By processing massive log volumes efficiently, securely, and in real time, LTS provides insights for you to optimize the availability and performance of cloud services and

 Copyright © Huawei Technologies Co., Ltd.

applications. It also helps you efficiently perform real-time decision-making, device O&M, and service trend analysis.

You are advised to collect container logs in a unified manner (including standard container output, log files in containers, node log files, and Kubernetes events) and report them to LTS.

Impact:

The cloud-native log collection plug-in must be installed in the tenant's cluster. After LTS is enabled, you will be billed if the log data exceeds the LTS free quota.

How to check:

On the cluster management page of the CCE console, select a cluster and choose **Log Center** on the left to check whether the **Log Collection and Management** function is enabled. After the function is enabled, you can filter and view logs on the **Container Logs** tab page.

How to fix:

Enable the log collection function and configure log collection policies as required. The log collection policies must cover standard container output, container file logs, and node file logs.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-cce/cce_10_0555.html

2.3.3.3 C.CS.FOUNDATION.G_3_3.R_3 Enabling the Container Security Edition of HSS

Level: Level 2

Background:

Host Security Service (HSS) is designed to protect server workloads in hybrid clouds and multi-cloud data centers. It protects servers and containers and prevents web pages from malicious modifications. You are advised to enable HSS to protect the **Node** node in the CCE cluster and the containers on it.

Impact:

You will be charged for enabling the Container Edition of HSS. You need to install the HSS agent on each node of the cluster and that will consume a small amount of CPU and memory.

How to check:

On the HSS console, choose **Asset Management** > **Containers & Quota** and click **Container Nodes**. On the **Node List** tab page, view the protection status of containers. If the status is **Protected**, the protection has been enabled.

How to fix:

On the HSS console, choose **Asset Management** > **Containers & Quota** and click **Container Nodes**. On the **Node List** tab page, enable protection for servers whose **Protection Status** is **Unprotected**. Tenants can enable protection in batches.

Reference:

https://support.huaweicloud.com/intl/en-us/productdesc-hss2.0/hss_01_0136.html

 Copyright © Huawei Technologies Co., Ltd.

https://support.huaweicloud.com/intl/en-us/bestpractice-cce/cce_bestpractice_0317.html

2.3.3.4 C.CS.FOUNDATION.G_3_3.R_4 Handling Vulnerabilities Released on the CCE Official Website in a Timely Manner

Level: Level 1

Background:

You need to pay attention to and handle the vulnerabilities released by CCE in a timely manner. CCE fixes high-risk vulnerabilities within one month after the Kubernetes community detects them and releases fixing solutions. The fixing policies are the same as those of the community. Before the vulnerabilities are completely fixed, you can refer to the mitigations provided by CCE to minimize the impact of the vulnerabilities.

Impact:

Fixing or mitigating vulnerabilities may require cluster version upgrading and node resetting.

How to check:

Determine whether your clusters are affected by referring to the method provided in the official vulnerability notice.

How to fix:

Fix or mitigate vulnerabilities by referring to the official vulnerability notice.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-cce/cce_bestpractice_0317.html

2.3.3.5 C.CS.FOUNDATION.G_3_3.R_5 Protecting the Cluster API Server

Level: Level 1

Background:

Kubernetes APIs have access control capabilities, but some CVE vulnerabilities without access control occasionally exist. To prevent attackers from probing Kubernetes API versions, you are advised not to bind EIPs to clusters unless necessary to avoid attacks. If an EIP must be bound, properly configure the firewall or security group rules to restrict access of unnecessary ports and IP addresses.

Impact:

Kubernetes clusters cannot be accessed from the public network and can be accessed only from the VPC.

How to check:

On the cluster management page of the CCE console, select a cluster and check whether there are public IP addresses in the connection information area.

How to fix:

On the cluster management page of the CCE console, select a cluster and unbind the public IP address from the cluster in the connection information area.

 Copyright © Huawei Technologies Co., Ltd.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-cce/cce_bestpractice_0318.html

2.3.3.6 C.CS.FOUNDATION.G_3_3.R_6 Preventing Cluster Nodes from Being Exposed to Public Networks

Level: Level 1

Background:

After a node is exposed to the public network, attackers can attack nodes and further control the cluster through the Internet.

Do not bind an EIP to a cluster node unless necessary to reduce the attack surface. If an EIP must be bound, properly configure the firewall or security group rules to restrict access of unnecessary ports and IP addresses.

You may have configured the **kubeconfig.json** file on a node in your cluster. kubectl can use the certificate and private key in this file to control the entire cluster. You are advised to delete unnecessary files from the **/root/.kube** directory on the node to prevent malicious use.

rm -rf /root/.kube

Impact:

Cluster nodes cannot be accessed from the public network and can be accessed only from the VPC.

How to check:

On the cluster management page of the CCE console, select a cluster and click **Node Management** in the left pane. On the **Nodes** tab page, check whether there are public IP address in the **IP Address** column.

How to fix:

If the **IP Address** column contains public IP addresses, click the node name to go to the node details page, click the **EIP** tab, and unbind the EIP.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-cce/cce_bestpractice_0318.html

2.3.3.7 C.CS.FOUNDATION.G_3_3.R_7 Hardening the Security Group Rules of the VPC Where the Kubernetes Cluster Resides

Level: Level 1

Background:

CCE is a universal container platform. Its default security group rules apply to common scenarios. Based on security requirements, you can harden the security group rules set for CCE clusters on the **Security Groups** page of **Network Console**.

Impact:

 Copyright © Huawei Technologies Co., Ltd.

If security group rules are incorrectly configured, network connectivity problems may occur and services will be affected.

How to check:

When a cluster is created, a security group is automatically created for the master node and worker node, separately. The security group name of the master node is *{Cluster name}*-**cce-control-***{Random ID}*, and the security group name of the worker node is *{Cluster name}*-**cce-node-***{Random ID}*. If a CCE Turbo cluster is used, an additional ENI security group named *{Cluster name}*-**cce-eni-***{Random ID}* will be created. In the **Security Group** area on the left of the ECS console, select the corresponding security group and check whether the inbound rules meet expectations. You are advised to disable port 22 in the inbound direction of the security group on the **Node** node and enable port 5443 in the inbound direction of the security group on the **Master** node only for the VPC network segments, container network segments, and network segments of the hosting grid control plane.

How to fix:

Enable inbound and outbound rules as required.

Reference:

https://support.huaweicloud.com/intl/en-us/cce_faq/cce_faq_00265.html

https://support.huaweicloud.com/intl/en-us/bestpractice-cce/cce_bestpractice_0318.html

2.3.3.8 C.CS.FOUNDATION.G_3_3.R_8 Forbidding Containers to Obtain Host Machine Metadata

Level: Level 2

Background:

If tenants use CCE clusters as shared resource pools to build advanced services and allow end users of advanced services to create uncontrollable container workloads in the clusters, you need to restrict the access to metadata on hosts.

Impact:

Container applications will be restricted to access the metadata of the host where the application is located. Improper security hardening may affect the password change on the ECS console. Therefore, risk assessment and verification must be performed before the rectification.

How to check:

Log in to each node in the cluster and run the following commands in any container to access the **userdata** and **metadata** interfaces of OpenStack to check whether the requests are intercepted:

```
curl 169.254.169.254/openstack/latest/meta_data.json
curl 169.254.169.254/openstack/latest/user_data
```

How to fix:

Perform security hardening as required by referring to section "Forbidding Containers to Obtain Host Metadata" in Node Security Configuration.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-cce/cce_bestpractice_0318.html

2.3.3.9 C.CS.FOUNDATION.G_3_3.R_9 Restricting the Access of Containers to the Management Plane

Level: Level 2

Background:

If service containers on a node do not need to access **kube-apiserver**, you are advised to disable container network traffic on the node from accessing **kube-apiserver**.

Impact:

The service containers cannot access **kube-apiserver**. You need to evaluate hardening risks based on service scenarios.

How to check:

Log in to each node in the cluster and run the following command in any container to check whether the request is intercepted:

```
curl -k https://{Private_API_server_IP}:5443
```

How to fix:

Perform security hardening as required by referring to section "Restricting the Access of Containers to the Management Plane" in Container Security Configuration.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-cce/cce_bestpractice_0319.html

2.4 C.CS.FOUNDATION.G_4 Network

2.4.1 C.CS.FOUNDATION.G_4.R_1 Disabling Internet Access over SSH

Level: Level 1

Background:

The SSH protocol is mainly used to remotely connect to and manage hosts. The default port number is **22**. The SSH protocol is an easy target for resource scanning and brute force cracking in network attacks. When you configure the network ACL rule or security groups for VPC subnets, do not configure SSH port rules whose source IP address is **0.0.0.0/0** or **::/0**. If necessary, you need to configure specific source IP addresses based on the whitelist.

Impact:

After ACL rules are configured, only source IP addresses in the whitelist can remotely access the preceding ports on the target host.

How to check:

 Copyright © Huawei Technologies Co., Ltd.

1. Log in to the management console.
2. In the service list, choose **Networking** > **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate and click the target network ACL to view its details.
5. Switch to the **Inbound Rules** tab, check whether there is an SSH protocol rule whose source IP address is **0.0.0.0/0** or **::/0**, and whether the source IP address of the default port **22** is valid.
6. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
7. Locate the row that contains the target security group, click **Manage Rule** in the **Operation** column, and click **Inbound Rules**.
8. Switch to the **Inbound Rules** tab, check whether there is an SSH protocol rule whose source IP address is **0.0.0.0/0** or **::/0**, and whether the source IP address of the default port **22** is valid.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate and click the target network ACL to view its details.
5. In the **Inbound Rules** tab, locate the target rule, click **Modify** in the **Operation** column, configure the parameters as prompted, and set the source IP address to a specific IP address.
6. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
7. Locate the row that contains the target security group, click **Manage Rule** in the **Operation** column, and click **Inbound Rules**.
8. Switch to the **Inbound Rules** tab, configure the parameters as prompted, and set the source IP address to a specific IP address.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-vpc/acl_0002.html

https://support.huaweicloud.com/intl/en-us/usermanual-vpc/en-us_topic_0081124350.html

2.4.2 C.CS.FOUNDATION.G_4.R_2 Disabling Internet Access over RDP

Level: Level 1

Background:

The RDP protocol is mainly used to remotely connect to and manage hosts. The default port number is **3389**. The RDP protocol is an easy target for resource scanning and brute force cracking in network attacks. When you configure the network ACL rule or security groups for VPC subnets, do not configure RDP port rules whose source IP address is **0.0.0.0/0** or **::/0**. If necessary, you need to configure specific source IP addresses based on the whitelist.

Impact:

 Copyright © Huawei Technologies Co., Ltd.

After ACL rules are configured, only source IP addresses in the whitelist can remotely access the preceding ports on the target host.

How to check:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate and click the target network ACL to view its details.
5. Switch to the **Inbound Rules** tab, check whether there is an SSH protocol rule whose source IP address is **0.0.0.0/0** or **::/0**, and whether the source IP address of the default port **3389** is valid.
6. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
7. Locate the row that contains the target security group, click **Manage Rule** in the **Operation** column, and click **Inbound Rules**.
8. Switch to the **Inbound Rules** tab, check whether there is an SSH protocol rule whose source IP address is **0.0.0.0/0** or **::/0**, and whether the source IP address of the default port **3389** is valid.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate and click the target network ACL to view its details.
5. In the **Inbound Rules** tab, locate the target rule, click **Modify** in the **Operation** column, configure the parameters as prompted, and set the source IP address to a specific IP address.
6. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
7. Locate the row that contains the target security group, click **Manage Rule** in the **Operation** column, and click **Inbound Rules**.
8. Switch to the **Inbound Rules** tab, configure the parameters as prompted, and set the source IP address to a specific IP address.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-vpc/acl_0002.html

https://support.huaweicloud.com/intl/en-us/usermanual-vpc/en-us_topic_0081124350.html

2.4.3 C.CS.FOUNDATION.G_4.R_3 Disabling Access to Remote Management Ports and High-Risk Ports over the Source IP Address 0.0.0.0/0 for Subnet ACL

Level: Level 1

Background:

When configuring the network ACL rule for a VPC subnet, the remote management ports and high-risk ports should not be added to the inbound rule. If these ports are required by services, enable them to the smallest extent. If the source IP address is

 Copyright © Huawei Technologies Co., Ltd.

0.0.0.0/0 or **::/0**, the mask of the public IP address is less than **32**, and the mask of the internal IP address is less than **24**, the minimum access control principle is not met.

High-risk ports include **20**, **21**, **135**, **137**, **138**, **139**, **445**, **389**, **593**, and **1025**.

Remote management ports include **23**, **177**, **513**, **4899**, **6000** to **6063**, **5900**, and **5901**.

Impact:

After ACL rules are configured, only source IP addresses in the whitelist can remotely access the preceding ports on the target host.

How to check:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate and click the target network ACL to view its details.
5. In the **Inbound Rules** tab, check whether any rules allow traffic on high-risk or remote management ports.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
4. Locate and click the target network ACL to view its details.
5. In the **Inbound Rules** tab, locate the target rule, click **Modify** in the **Operation** column, configure the parameters as prompted, and set the protocol port.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-vpc/acl_0002.html

2.4.4 C.CS.FOUNDATION.G_4.R_4 Disabling Access to Remote Management Ports and High-Risk Ports over the Source IP Address 0.0.0.0/0 for Security Groups

Level: Level 1

Background:

When configuring the security group rule for a VPC, the remote management ports and high-risk ports should not be added to the inbound rule. If these ports are required by services, enable them to the smallest extent. If the source IP address is **0.0.0.0/0** or **::/0**, the mask of the public IP address is less than **32**, and the mask of the internal IP address is less than **24**, the minimum access control principle is not met.

High-risk ports include **20**, **21**, **135**, **137**, **138**, **139**, **445**, **389**, **593**, and **1025**.

Remote management ports include **23**, **177**, **513**, **4899**, **6000** to **6063**, **5900**, and **5901**.

 Copyright © Huawei Technologies Co., Ltd.

Impact:

After ACL rules are configured, only source IP addresses in the whitelist can remotely access the preceding ports on the target host.

How to check:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. Locate the row that contains the target security group, click **Manage Rule** in the **Operation** column, and click **Inbound Rules**.
5. In the **Inbound Rules** tab, check whether any rules allow traffic on high-risk or remote management ports.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. Locate the row that contains the target security group, click **Manage Rule** in the **Operation** column, and click **Inbound Rules**.
5. In the **Inbound Rules** tab, configure the protocols and ports as prompted.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-vpc/en-us_topic_0081124350.html

2.4.5 C.CS.FOUNDATION.G_4.R_5 Ensuring the Principle of Least Privilege over VPC Peering Connections

Level: Level 2

Background:

A VPC peering connection is a network connection between two VPCs. The routes configured for a VPC peering connection must meet the principle of least privilege. The destination of both the local and peer routes should be a subnet of the minimum size.

Impact: None

How to check:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Virtual Private Cloud**. The **Network Console** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud** > **VPC Peering Connections**. Check whether the configurations are required for the services.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Virtual Private Cloud**. The **Network Console** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

3. In the navigation pane, choose **Virtual Private Cloud** > **VPC Peering Connections**.
4. On the displayed page, locate the target peering connection, and click **Modify** or **Delete** in the **Operation** column.
5. To create a new one, click **Create Peering Connection**, and configure the parameters as prompted.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-vpc/en-us_topic_0046655036.html

2.4.6 C.CS.FOUNDATION.G_4.R_6 Enabling Access Control for ELB Listeners

Level: Level 2

Background:

ELB users can add a whitelist or blacklist to specify IP addresses that are allowed or denied to access a listener. An IP address whitelist allows only specified IP addresses to access the listener. An IP address blacklist blocks only specified IP addresses from access the listener.

Whitelists and blacklists do not conflict with inbound security group rules. Whitelists define the IP addresses that are allowed to access the listeners, while blacklists specify the IP addresses that are denied to access the listeners. Inbound security group rules control access to backend servers by specifying the protocol, ports, and IP addresses.

Access control does not restrict the ping command. You can still ping backend servers from the restricted IP addresses.

To ping the IP address of a shared load balancer, you need to add a listener and associate a backend server to it.

To ping the IP address of a dedicated load balancer, you only need to add a listener to it.

Impact:

If the IP address set in the whitelist or blacklist is incorrectly configured, the load balancer listener cannot be accessed from related IP addresses, which may cause access restriction.

How to check:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Elastic Load Balance**.
3. Locate and click the load balancer to go to the listener management tab.
4. Check whether an access control policy is configured for each listener.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Networking** > **Elastic Load Balance**.
3. Locate and click the load balancer to go to the listener management tab.

 Copyright © Huawei Technologies Co., Ltd.

4. You can configure access control for a listener in either of the following ways:
   - In the **Listeners** tab, locate the listener and click **Configure** in the **Access Control** column.
   - Click the target listener to go to the basic information page. Click **Configure** on the right of **Access Control**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-elb/elb_03_0003.html

2.5 C.CS.FOUNDATION.G_5 Storage

2.5.1 C.CS.FOUNDATION.G_5_1 Object Storage Service (OBS)

2.5.1.1 C.CS.FOUNDATION.G_5_1.R_1 Using OBS Server to Encrypt Stored Objects

Level: Level 2

Background:

With server-side encryption enabled, OBS encrypts a user's object as ciphertext before storing it on the server.

Impact:

Once server-side encryption is enabled, data read and write performance will be affected to some extent.

How to check:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the bucket to be operated. In the navigation pane on the left, choose **Overview**.
3. In the **Basic Configurations** area, check whether **Default Encryption** is in the **Configured** state.

How to fix:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the bucket to be operated. In the navigation pane on the left, choose **Overview**.
3. In the **Basic Configurations** area, click **Default Encryption**. The **Default Encryption** dialog box is displayed.
4. Select **Enable**.
5. Select **SSE-KMS** or **SSE-OBS**.
6. If **SSE-KMS** is selected, the available encryption algorithms include AES256 and SM4. The encryption key **obs/default** is selected by default. You can also click **Create KMS Key** to create a custom key on the DEW console, and choose the created key from the drop-down list.

 Copyright © Huawei Technologies Co., Ltd.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-obs/obs_03_0088.html

2.5.1.2 C.CS.FOUNDATION.G_5_1.R_2 Disabling Anonymous Access

Level: Level 1

Background:

Disabling open access over anonymous users can protect data from being disclosed. This function is not required for static websites where open access is required.

Impact:

Once anonymous access is disabled, services that need to be opened to all users, such as static website, are affected. Determine whether to enable this function based on your service requirement.

How to check:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, locate the target bucket, and view the policy resolution result.
3. Click the target bucket and choose **Permissions** > **Bucket ACLs**. Check whether permission **Public Read** or **Public Read and Write** is granted to anonymous users in the **Public Permissions** area.

How to fix:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the navigation pane on the left, choose **Permissions** > **Bucket Policy**. On the displayed page, click **Edit**, and deselect **All accounts**.
3. In the navigation pane on the left, choose **Permissions** > **Bucket ACLs**, Set **Public Permissions** to **Private**, click **Edit**, and cancel the ACL permissions granted by the anonymous users.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-obs/obs_03_0142.html

2.5.1.3 C.CS.FOUNDATION.G_5_1.R_3 Using OBS Temporary Data Sharing to Share Specified Data

Level: Level 2

Background:

If you need to share the objects, that is, files or folders, stored in OBS with other users, you can use temporary data sharing to generate a sharing URL, which will become invalid after the specified validity period expires.

Impact:

You need to specify a validity period. Once expired, the sharing URL cannot be used to access OBS data.

How to check:

 Copyright © Huawei Technologies Co., Ltd.

A temporary URL consists of the access domain name and the temporary authentication information of a file. The following shows an example:

https://bucketname.obs.regionID.myhuaweicloud.com:443/image.png?AccessKeyId=*xxx*&Expires=*xxx*&response-content-disposition=*xxx*&x-obs-security-token=*xxx*&Signature=*xxx*

The temporary authentication information includes the **AccessKeyId**, **Expires**, **x-obs-security-token**, and **Signature** parameters. **AccessKeyId**, **x-obs-security-token**, and **Signature** are used for authentication. The **Expires** parameter specifies the validity period of the authentication.

How to fix:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket, select the object to be shared, click **Share**, set a validity period, and copy the sharing URL.

Reference:

https://support.huaweicloud.com/intl/en-us/perms-cfg-obs/obs_40_0009.html

2.5.1.4 C.CS.FOUNDATION.G_5_1.R_4 Controlling Permissions of OBS Resources Using Both VPC Endpoint and OBS Bucket Policies

Level: Level 2

Background:

You can set a VPC endpoint policy to restrict servers in a VPC, such as ECS, CCE, and BMS, to access specific resources in OBS. You can also set a bucket policy to restrict servers in a specified VPC to access buckets in OBS. In this way, access control with both VPC endpoint and bucket policies is implemented.

Impact: None

How to check:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket, check whether VPC rules are configured for the bucket policy on the **Permissions** page.
3. In the service list, choose **Networking** > **Virtual Private Cloud**.
4. Locate the target VPC endpoint node, click its ID, and check whether bucket rules are configured.

How to fix:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the navigation pane on the left, choose **Permissions** > **Bucket Policy**. Click **Edit** on the displayed page and configure the VPC rules.
3. In the service list, choose **Networking** > **Virtual Private Cloud**.
4. Locate the target VPC endpoint node and click its ID. Click **Edit** and configure the bucket rules.

Reference:

 Copyright © Huawei Technologies Co., Ltd.

https://support.huaweicloud.com/intl/en-us/usermanual-obs/obs_03_0142.html

2.5.1.5 C.CS.FOUNDATION.G_5_1.R_5 Using Bucket Policies to Restrict Access to OBS Buckets Using HTTPS

Level: Level 1

Background:

The SecureTransport condition in the bucket policy specifies that HTTPS must be used to perform operations on the bucket, ensuring transmission security during data upload and download.

Impact: None

How to check:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket. On the **Permissions** page, check whether **SecureTransport** is set to **True**.

How to fix:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the navigation pane on the left, choose **Permissions** > **Bucket Policy**. Click **Edit** on the displayed page and set **SecureTransport** to **True**.

Reference:

https://support.huaweicloud.com/intl/en-us/perms-cfg-obs/obs_40_0041.html

2.5.1.6 C.CS.FOUNDATION.G_5_1.R_6 Enabling Versioning

Level: Level 2

Background:

With OBS versioning, multiple versions of an object can be retained in a bucket, enhancing quick recovery capability in data exception scenarios.

Impact: None

How to check:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket. The **Objects** page is displayed.
3. In the navigation pane on the left, choose **Overview**.
4. In the **Basic Configurations** area, check whether **Versioning** is enabled.

How to fix:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket. The **Objects** page is displayed.
3. In the navigation pane on the left, choose **Overview**.

 Copyright © Huawei Technologies Co., Ltd.

4. In the **Basic Configurations** area, click **Versioning**.
5. In the displayed dialog box, select **Enable**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-obs/obs_03_0327.html

2.5.1.7 C.CS.FOUNDATION.G_5_1.R_7 Enabling WORM in Compliance Scenarios

Level: Level 2

Background:

OBS provides the write once read many (WORM) function, that is, data can be written once and read multiple times. This ensures that data of a specified object version cannot be overwritten or deleted within a specified period of time.

Impact:

Versioning must be enabled to enable WORM.

How to check:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket. The **Objects** page is displayed.
3. In the navigation pane on the left, choose **Overview**.
4. In the **Basic Configurations** area, check whether **WORM Retention** is set to **Configured**. The options include **Not supported**, **Not configured**, and **Configured**.

How to fix:

Not configured

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket. The **Objects** page is displayed.
3. In the navigation pane on the left, choose **Overview**.
4. In the **Basic Configurations** area, click **WORM Retention**. The **Configure WORM Retention** dialog box is displayed.
5. Choose **Configure** and specify a default retention period. The default retention mode is **Compliance**.

Not supported

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the navigation pane on the left, choose **Dashboard**.
3. Click **Create Bucket** to create a bucket.
4. Configure the parameters and enable WORM. You can set whether WORM is supported only when creating a bucket. Once created, whether WORM is supported cannot be modified.
5. Upload the objects to the bucket and click the target bucket in the bucket list. The **Objects** page is displayed.

 Copyright © Huawei Technologies Co., Ltd.

6. In the navigation pane on the left, choose **Overview**.
7. In the **Basic Configurations** area, click **WORM Retention**. The **Configure WORM Retention** dialog box is displayed.
8. Choose **Configure** and specify a default retention period. The default retention mode is **Compliance**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-obs/obs_03_0718.html

2.5.1.8 C.CS.FOUNDATION.G_5_1.R_8 Avoiding Creating Public Objects in a Private Bucket

Level: Level 1

Background:

Do not grant the public read permission on objects to anonymous users in OBS buckets. This prevents objects from being opened to all users and avoids object data breach.

Impact: None

How to check:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket. The **Objects** page is displayed.
3. In the object list, click the target object to view its details.
4. In the **Public Permissions** area, check whether **Public Read** is enabled.
5. In the **User Permissions** area, check whether the read permission for object access is granted to anonymous users and whether read and write permissions are granted for ACL access.

How to fix:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket. The **Objects** page is displayed.
3. In the object list, click the target object to view its details.
4. In the **Public Permissions** area, select **Private**.
5. In the **User Permissions** area, click the permission of anonymous users, and click **Edit**.
6. Grant the read permission for object access and grant read and write permissions for ACL access.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-obs/en-us_topic_0045853821.html

2.5.1.9 C.CS.FOUNDATION.G_5_1.R_9 Enabling URL Validation

Level: Level 2

Background:

 Copyright © Huawei Technologies Co., Ltd.

Enable OBS URL validation, so that user data cannot be stolen by others.

Impact: None

How to check:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket. The **Objects** page is displayed.
3. In the navigation pane on the left, choose **Overview**.
4. In the **Basic Configurations** area, click **URL Validation**. The **URL Validation** page is displayed.
5. Check **Whitelisted Referers** and **Blacklisted Referers**.

How to fix:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket. The **Objects** page is displayed.
3. In the navigation pane on the left, choose **Overview**.
4. In the **Basic Configurations** area, click **URL Validation**. The **URL Validation** page is displayed.
5. Click the edit button next to the text box of **Whitelisted Referers** or **Blacklisted Referers**, and enter the referers.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-obs/obs_03_0341.html

2.5.1.10 C.CS.FOUNDATION.G_5_1.R_10 Using a User-Defined Domain Name in Scenarios Where OBS Objects Need to Be Previewed Online

Level: Level 2

Background:

Based on security and compliance requirements, Huawei Cloud OBS forbids online preview of objects in a bucket using the default domain name of OBS. That is, when you use the preceding domain name to access objects (such as videos, images, and web pages) in the bucket from a browser, the object content is not displayed but downloaded as attachments. If you want to preview OBS objects online, use a user-defined domain name.

Impact: None

How to check:

Enter http://*User-defined domain name*/*Object access path* in the browser and check whether the file can be previewed online.

How to fix:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket. In the navigation pane on the left, choose **Domain Name Mgmt**.

 Copyright © Huawei Technologies Co., Ltd.

3. Click **Configure User Domain Name** in the upper part. In the displayed dialog box, enter the domain name in the **User Domain Name** text box.
4. Click **OK**. If the domain name is not resolved, manually resolve CNAME, and click **OK** again.
5. Configure a CNAME record on the DNS, and map the user-defined domain name to the domain name of the bucket.
6. Share http://*User-defined domain name*/*Object access path* with other users for them to preview the object.

Reference:

https://support.huaweicloud.com/intl/en-us/obs_faq/obs_03_0087.html

2.5.1.11 C.CS.FOUNDATION.G_5_1.R_11 Enabling Cross-Region Replication

Level: Level 2

Background:

The cross-region replication function provides users with the cross-region data disaster recovery capability.

Impact: None

How to check:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket. In the navigation pane on the left, choose **Cross-Region Replication**, and check whether a cross-region replication rule is configured.

How to fix:

1. Log in to the management console, and choose **Storage** > **Object Storage Service** from the service list.
2. In the bucket list, click the target bucket. In the navigation pane on the left, choose **Cross-Region Replication**.
3. Click **Create Rule** and select **I have read and agree to the disclaimer.** The **Create Cross-Region Replication Rule** dialog box is displayed.
4. Configure the parameters and click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-obs/obs_03_0003.html

2.5.2 C.CS.FOUNDATION.G_5_2 Elastic Volume Service (EVS)

2.5.2.1 C.CS.FOUNDATION.G_5_2.R_1 Ensuring that EVS Encryption Is Enabled

Level: Level 2

Background:

EVS encryption protects your static data. EVS encryption ensures that data is automatically encrypted when it is written from servers to EVS and is decrypted when it is read from EVS.

Impact:

If the KMS key used by EVS encryption is disabled, scheduled to be deleted, or deleted, the data in your encrypted EVS cannot be accessed.

How to check:

1. Log in to the management console and choose **Storage** > **Elastic Volume Service** from the service list.
2. In the disk list, set **Encrypted** to **No** in the search and filter text box to check whether there are non-encrypted disks.

How to fix:

Whether an EVS disk is encrypted cannot be modified after being purchased. You can enable encryption when creating an EVS disk.

1. Log in to the management console and choose **Storage** > **Elastic Volume Service** from the service list.
2. Click **Buy Disk** in the upper right corner.
3. Click **More**.
4. Enable **Encryption**. If EVS is not granted to access your keys, the **Create Agency** dialog box will be displayed. You need to grant EVS the permission to access KMS keys.
5. On the displayed dialog box, select a key from the drop-down list.

Reference:

https://support.huaweicloud.com/intl/en-us/productdesc-evs/evs_01_0001.html

https://support.huaweicloud.com/intl/en-us/qs-evs/en-us_topic_0021738346.html

2.5.3 C.CS.FOUNDATION.G_5_3 Scalable File Service (SFS)

2.5.3.1 C.CS.FOUNDATION.G_5_3.R_1 Ensuring that the SFS Turbo File System Encryption Is Enabled

Level: Level 2

Background:

SFS Turbo file system encryption protects your static data. SFS Turbo file system encryption ensures that data is automatically encrypted when it is written from your applications to SFS Turbo file system and is decrypted when it is read from SFS Turbo file system.

Impact:

If the KMS key used by SFS Turbo file system encryption is disabled, scheduled to be deleted, or deleted, the data in your encrypted SFS Turbo file system encryption cannot be accessed.

How to check:

 Copyright © Huawei Technologies Co., Ltd.

1. Log in to the management console, and choose **Storage** > **Scalable File Service** from the service list.
2. On the **File Systems** page, set **Encrypted** to **No** in the search and filter text box to check whether there are non-encrypted file systems.

How to fix:

Whether an SFS Turbo file system is encrypted cannot be modified after being purchased. You can enable encryption when creating an SFS Turbo file system.

1. Log in to the management console, and choose **Storage** > **Scalable File Service** from the service list.
2. Click **Create File System** in the upper right corner.
3. Click **Advanced Settings**.
4. Enable **KMS encryption**.
5. On the displayed dialog box, select a key from the drop-down list.

Reference:

https://support.huaweicloud.com/intl/en-us/productdesc-sfs/sfs_01_0006.html

https://support.huaweicloud.com/intl/en-us/qs-sfs/en-us_topic_0034428727.html

2.5.4 C.CS.FOUNDATION.G_5_4 Cloud Backup and Recovery (CBR)

2.5.4.1 C.CS.FOUNDATION.G_5_4.R_1 Selecting an Encryption Disk for EVS that Carries the Backup Data

Level: Level 2

Background:

The CBR backup disk can be an encrypted disk. You cannot manually encrypt or cancel encrypting backups.

Impact: None

How to check:

1. Log in to the CBR console.
   - Log in to the management console.
   - Click  in the upper left corner to select a region.
2. Click  and choose **Storage** > **Cloud Backup and Recovery**.
3. In the navigation pane on the left, choose **Cloud Disk Backups**. Click a vault in the **Vaults** tab to view its information.
4. Select a bound disk to check whether the backup disk is encrypted.

How to fix:

1. Log in to the CBR console.
   - Log in to the management console.

- Click  in the upper left corner to select a region.
- Click  and choose **Storage** > **Cloud Backup and Recovery**.

2. In the navigation pane on the left, choose **Cloud Disk Backups**. Click **Buy Disk Backup Vault** in the upper right corner and select an encrypted disk.
3. Click **Next** and complete the payment as prompted.

Reference:

https://support.huaweicloud.com/intl/en-us/qs-cbr/cbr_02_0004.html

2.5.4.2 C.CS.FOUNDATION.G_5_4.R_2 Enabling Re-confirmation for Deleting Backup Data

Level: Level 2

Background:

To prevent backup data from being deleted by mistake, enable the re-confirmation mechanism.

Impact: None

How to check:

1. Log in to the CBR console.
   - Log in to the management console.
   - Click  in the upper left corner to select a region.
   - Click  and choose **Storage** > **Cloud Backup and Recovery**.
2. Hover the mouse over the username in the upper right corner and click **Security Settings**.
3. On the displayed page, click the **Critical Operations** tab, and check whether **Operation Protection** is enabled.

How to fix:

1. Log in to the CBR console.
   - Log in to the management console.
   - Click  in the upper left corner to select a region.
   - Click  and choose **Storage** > **Cloud Backup and Recovery**.
2. Hover the mouse over the username in the upper right corner and click **Security Settings**.
3. On the displayed page, click the **Critical Operations** tab, locate **Operation Protection**, and click **Enable**
4. **Self-verification** is selected by default. Click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/iam_faq/iam_01_0213.html

 Copyright © Huawei Technologies Co., Ltd.

2.5.4.3 C.CS.FOUNDATION.G_5_4.R_3 Enabling Cross-Region Backup Replication

Level: Level 2

Background:

Cross-region replication is more secure and reliable.

Impact:

To enable cross-region replication, a CBR vault needs to be configured in the target region.

How to check:

1. Log in to the CBR console.
   - Log in to the management console.
   - Click  in the upper left corner and select the target region.
   - Click  and choose **Storage** > **Cloud Backup and Recovery**.
2. Click the **Backups** tab and set the filter criteria to the backup name to view backup details.

How to fix:

1. Log in to the CBR console.
   - Log in to the management console.
   - Click  in the upper left corner to select a region.
   - Click  and choose **Storage** > **Cloud Backup and Recovery**.
2. Click the **Backups** tab and locate the backups corresponding to the vault and server.
3. Locate the target backup, click **More** > **Create Replica** in the **Operation** column, configure the parameters in the displayed dialog box, and click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-cbr/cbr_03_0018.html

2.5.4.4 C.CS.FOUNDATION.G_5_4.R_4 Enabling Forcible Backup

Level: Level 2

Background:

Enabling forcible backup can protect the security and accuracy of user data to the greatest extent and ensures service security.

Impact:

To enable forcible backup, a CBR vault needs to be configured.

How to check:

1. Log in to the IAM console.

2. In the navigation pane on the left, choose **User Groups**, click the target user group, and check authorization records in the **Permissions** tab.

How to fix:

1. Log in to the IAM console.
2. In the navigation pane on the left, choose **Permissions** > **Policies/Roles**, and click **Create Custom Policy** in the upper right corner.
3. Enter a policy name, set **Policy View** to **JSON**, and create forcible backup policies for ECS, EVS, and SFS Turbo. The following shows an example of the policy content for creating forcible backup policies for EVS and CBR.
   - Create a forcible backup policy for EVS.

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "evs:volumes:create"
            ],
            "Condition": {
                "Null": {
                    "cbr:VaultId": [
                        "true"
                    ]
                }
            }
        }
    ]
}
```

   - Enable a backup policy.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": ["cbr:policies:create"],
      "Condition": {
          "Bool": {
              "cbr:EnabledPolicy": "false"
          }
      }
    }
  ]
}
```

   - Modify the backup policy and ensure that the policy cannot be disabled.

```
{
"Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": ["cbr:policies:update"],
      "Condition": {
```

 Copyright © Huawei Technologies Co., Ltd.

```
            "Bool": {
                "cbr:EnabledPolicy": "false"
            }
        }
    }
]
}
```

- To create a vault, a backup policy must be bound.

```
{
 "Version": "5.0",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "cbr:vaults:create"
            ],
            "Condition": {
                "Null": {
                    "cbr:PolicyId": [
                        "true"
                    ]
                }
            }
        }
    ]
}
```

4. Attach the policy to a user group. Users in the group then inherit the permissions defined in the policy.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-iam/iam_01_0605.html

2.6 C.CS.FOUNDATION.G_6 Databases

2.6.1 C.CS.FOUNDATION.G_6_1 RDS for MySQL

2.6.1.1 C.CS.FOUNDATION.G_6_1.R_1 Enabling Encrypted Communication

Level: Level 1

Background:

If TLS encrypted connections are not enabled, data is transmitted in plaintext between the MySQL client and server, which is vulnerable to eavesdropping, tampering, and man-in-the-middle attacks. If you are connected to the MySQL server through an insecure network such as the Internet, it is important to enable the TLS encrypted connection.

Impact: None.

How to check:

 Copyright © Huawei Technologies Co., Ltd.

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. In the upper left corner of the page, click  and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance.
5. In the **Basic Information** area, check whether SSL is enabled.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. In the upper left corner of the page, click  and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance.
5. On the **Basic Information** page, enable SSL in the **DB Information** area.
6. In the displayed dialog box, click **Yes**.
7. In the **Basic Information** area, view the results.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_mysql_0001.html

2.6.1.2 C.CS.FOUNDATION.G_6_1.R_2 Do Not Use the Default Port

Level: Level 1

Background:

The default port of MySQL is 3306. The default port is easy to be listened. You are advised to use a non-default port.

Impact: None.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. In the upper left corner of the page, click  and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance.
5. In **Connection Information** area on **Basic Information** page, you can view the database port.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. In the upper left corner of the page, click  and choose **Databases** > **Relational Database Service**.

4. On the **Instances** page, click the instance.
5. In the **Connection Information** area on the **Basic Information** page, click **Change** next to the **Database Port** field.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_change_database_port.html

2.6.1.3 C.CS.FOUNDATION.G_6_1.R_3 Enabling Transparent Data Encryption

Level: Level 2

Background:

Real-time I/O encryption and decryption are performed on data files. Data is encrypted before being written to disks and is decrypted before being read from disks to memory. This effectively protects databases security.

Impact:

When TDE is enabled, the instance is not restarted, but the CPU usage increases significantly.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the target DB instance.
5. In the DB Information area, check whether TDE is enabled.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the target DB instance.
5. In the DB Information area, click the switch in the TDE field to enable TDE.
6. In the displayed dialog box, click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_05_0031.html

2.6.1.4 C.CS.FOUNDATION.G_6_1.R_4 Update the Database Version to the Latest Version

Level: Level 1

Background:

When a new CVE vulnerability is released in the MySQL community, the impact of the vulnerability will be analyzed in a timely manner and the patch release plan will be determined based on the impact of the vulnerability. You are advised to upgrade the system and repair the vulnerability in a timely manner to prevent vulnerabilities from affecting data security.

Impact:

During the upgrade, instances will be restarted and services will be interrupted. Therefore, you are advised to perform the upgrade during off-peak hours.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. On the **Basic Information** page, view the latest DB version next to the **DB Engine Version** field under **DB Information**.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. In the **DB Information** area on the **Basic Information** page, click **Upgrade Minor Version** next to the **DB Engine Version** field.
6. In the displayed dialog box, select a scheduled time and click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_05_0041.html

2.6.1.5 C.CS.FOUNDATION.G_6_1.R_5 Do Not Bind an EIP to Access RDS for MySQL Through Internet

Level: Level 1

Background:

Do not deploy RDS for MySQL on the internet or DMZ. Deploy RDS for MySQL on the internal network of company and use routers or firewalls to protect RDS for MySQL, do not bind an EIP to access RDS for MySQL through internet. Unauthorized access and DDoS attacks are prevented.

Impact: None.

How to check:

Log in to the management console, go to the instance details page, choose connection & security and check whether an EIP is bound.

 Copyright © Huawei Technologies Co., Ltd.

How to fix:

Unbind the EIP and use the internal network.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_05_0033.html

2.6.1.6 C.CS.FOUNDATION.G_6_1.R_6 Configuring Proper Security Group Rules

Level: Level 1

Background:

A security group is a logical group that have the same security protection requirements in a VPC to ensure database security and stability.

Impact: None.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the Instances page, click the DB instance or read replica.
5. In the Connection Information area on the Basic Information page, locate the target security group in the **Security Group** field.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the Instances page, click the DB instance or read replica.
5. In the **Connection Information** area on the **Basic Information** page, click  in the **Security Group** field.
6. Click  to submit the change.
7. To cancel the change, click .
8. Click  in the upper right corner on the **Basic Information** page to view the result of the change. This process takes about 1 to 3 minutes.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_08_0003.html

 Copyright © Huawei Technologies Co., Ltd.

2.6.1.7 C.CS.FOUNDATION.G_6_1.R_7 Enabling the Database Audit Logs

Level: Level 2

Background:

The audit feature records all database activities. You can view the audit logs to perform security assessments and pinpoint problem causes, thereby enhancing system operational efficiency.

Impact:

Enabling this feature may lead to higher disk space consumption and potential performance impacts. You are advised to manage the types of audited objects to reduce the number of audit logs.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. In the upper left corner of the page, choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. In the navigation pane on the left, choose **SQL Audits**. On the displayed page, click **Set SQL Audit** above the list. In the displayed dialog box, check whether the **Audit Log** is enabled.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. In the upper left corner of the page, choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. In the navigation pane on the left, choose **SQL Audits**. On the displayed page, click **Set SQL Audit** above the list. In the displayed dialog box, enable or disable the audit log. Audit logs can be retained from 1 to 732 days and are retained for 7 days by default.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_sql_auditing_log.html

2.6.2 C.CS.FOUNDATION.G_6_2 Document Database Service (DDS)

2.6.2.1 C.CS.FOUNDATION.G_6_2.R_1 Enabling Encrypted Communication

Level: Level 1

Background:

If TLS encrypted connections are not enabled, data is transmitted in plaintext between the MongoDB client and server, which is vulnerable to eavesdropping, tampering, and man-in-the-middle attacks. If you are connected to the MongoDB server through an insecure network such as the Internet, you are advised to enable TLS encrypted connections.

Impact: None.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. On the **Instances** page, click the target DB instance.
5. In the **Basic Information** area, check whether SSL is enabled.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. On the **Instances** page, click the target DB instance.
5. On the **Basic Information** page, enable SSL in the **DB Information** area.
6. In the displayed dialog box, click **Yes**.
7. In the **Basic Information** area, view the results.
8. After SSL is enabled, click  next to **SSL** to download an SSL certificate.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-dds/dds_03_0074.htm

2.6.2.2 C.CS.FOUNDATION.G_6_2.R_2 Limiting the Maximum Number of Connections

Level: Level 2

Background:

If the number of MongoDB connections is too large, too many server resources are consumed. The OPS (query, insert, update, and delete) responds slowly. In addition, you need to set the maximum number of connections based on the OS. Ensure that this maximum connections do not exceed the maximum number of threads; otherwise, the setting will be ineffective. You can set the maximum number of connections to prevent DoS attacks and make full use of system resources, achieving the optimal OPS response capability.

Impact: None.

How to check:

1. Log in to the management console.

2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. In the navigation pane on the left, choose **Instances**. On the displayed page, locate the instance whose parameters you want to export and click its name.
5. Click **Parameters** in the navigation pane on the left. On the displayed page, check the value of **net.maxIncomingConnections** as required. It indicates the maximum number of concurrent connections that mongos or mongod can accept. This parameter depends on the instance specifications. The default value varies according to the instance specifications.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. In the navigation pane on the left, choose **Instances**. On the displayed page, locate the instance whose parameters you want to export and click its name.
5. In the navigation pane on the left, choose **Parameters**. On the displayed page, modify parameters as required.
6. Modify the **net.maxIncomingConnections** parameter based on the instance type.
7. Change the maximum number of connections based on the value range of **net.maxIncomingConnections**. This parameter depends on the instance specifications. The default value varies according to the instance specifications.
8. After parameters are modified, click **Change History**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-dds/dds_01_0052.html

2.6.2.3 C.CS.FOUNDATION.G_6_2.R_3 Disabling the Script Running Function

Level: Level 2

Background:

If the **javascriptEnabled** feature is enabled, the feature option is **security.javascriptEnabled**. JavaScript can be run on the mongod server, which poses security risks. If the **javascriptEnabled** feature is disabled, the **mapreduce** and **group** commands cannot be used. If your application does not require operations such as **mapreduce**, you are advised to disable **javascriptEnabled**.

Impact:

If services involve operations such as **mapreduce** and **group**, services will be affected.

How to check:

1. Log in to the management console.

 Copyright © Huawei Technologies Co., Ltd.

2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. In the navigation pane on the left, choose **Instances**. On the displayed page, click the target DB instance.
5. In the navigation pane on the left, choose Parameters. On the displayed page, check the value of **security.javascriptEnabled** as required.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. In the navigation pane on the left, choose **Instances**. On the displayed page, locate the instance whose parameters you want to export and click its name.
5. In the navigation pane on the left, choose **Parameters**. On the displayed page, modify parameters as required.
6. Modify the **security.javascriptEnabled** parameter based on the instance type.
7. After parameters are modified, click **Change History**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-dds/dds_01_0052.html

2.6.2.4 C.CS.FOUNDATION.G_6_2.R_4 Enabling the Database Audit Logs

Level: Level 2

Background:

The audit feature records all database activities. You can view the audit logs to perform security assessments and pinpoint problem causes, thereby enhancing system operational efficiency.

Impact:

Enabling this feature may lead to higher disk space consumption and potential performance impacts. You are advised to manage the types of audited objects to reduce the number of audit logs.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. On the **Instances** page, click the target DB instance.
5. In the navigation pane on the left, click **Audit Logs**.

 Copyright © Huawei Technologies Co., Ltd.

6. On the **Audit Logs** page, click **Set Audit Policy**.
7. On the displayed page, check whether the audit policy is enabled.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. On the **Instances** page, click the target DB instance.
5. In the navigation pane on the left, click **Audit Logs**.
6. On the **Audit Logs** page, click **Set Audit Policy**.
7. On the displayed page, click .
8. Configure required parameters and click **OK** to enable the audit policy.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-dds/dds_03_0067.html

2.6.2.5 C.CS.FOUNDATION.G_6_4.R_7 Enabling the Backup Function and Configuring a Backup Policy

Level: Level 2

Background:

DDS instances support automatic backup and manual backup. You can periodically back up the database. If the database is faulty or data is damaged, you can use the backup files to restore the database, ensuring data reliability.

Impact: None.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. On the **Instances** page, click the instance name.
5. In the navigation pane on the left, choose **Backups & Restorations**.
6. On the **Backups & Restorations** page, check whether backup policy is enabled.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.

4. On the **Instances** page, click the instance name.
5. In the navigation pane on the left, choose **Backups & Restorations**.
6. On the **Backups & Restorations** page, click **Set Backup Policy**. If you want to enable the automated backup policy, click . Once enabled, the backup policy can be modified.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-dds/en-us_topic_backup_restore.html

2.6.2.6 C.CS.FOUNDATION.G_6_2.R_6 Setting Second-Level Monitoring and Alarm Rules

Level: Level 2

Background:

DDS monitors instances by default. When a metric value exceeds the threshold, an alarm is generated. The system automatically sends an alarm notification through SMN, helping you learn about the running status of DDS DB instances in a timely manner.

Impact: None.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. On the **Instances** page, click the target instance name.
5. In the navigation pane on the left, choose **Advanced O&M**.
6. On the displayed page, click the **Real-Time Monitoring** tab and check whether **Monitoring by Seconds** is enabled.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. On the **Instances** page, click the target instance name.
5. In the navigation pane on the left, choose **Advanced O&M**.
6. On the displayed page, click the **Real-Time Monitoring** tab and click  next to **Monitoring by Seconds**.
7. In the displayed dialog box, select a collection period and click **Yes**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-dds/dds_03_0090.html

2.6.2.7 C.CS.FOUNDATION.G_6_2.R_7 Do Not Use the Default Port

Level: Level 1

Background:

The default port of MongoDB is 27017. The default port is easy to be listened, which poses security risks. You are advised to use a non-default port.

Impact: None.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. On the **Instances** page, click the instance name.
5. In the **Network Information** area on the **Basic Information** page, check whether the database port is 27017.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. On the **Instances** page, click the instance name.
5. In the **Network Information** area on the **Basic Information** page, click  in the **Database Port** field to change the database port.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-dds/dds_03_change_database_port.html

2.6.2.8 C.CS.FOUNDATION.G_6_2.R_8 Patch Upgrade

Level: Level 1

Background:

DDS supports patch upgrades to add new functions, fix bugs, and improve security and performance.

Impact: None.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.

4. On the Instances page, locate the instance you want to upgrade and check whether **Upgrade Minor Version** is displayed in the **DB Engine Version** column.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Document Database Service**.
4. On the **Instances** page, locate the instance you want to upgrade and click **Upgrade Minor Version** in the **DB Engine Version** column.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-dds/dds_03_0211.html

2.6.2.9 C.CS.FOUNDATION.G_6_2.R_9 Enabling Disk Encryption

Level: Level 2

Background:

Enabling disk encryption improves data security but slightly affects database read and write performance.

Impact:

If disk encryption is enabled, the database read and write performance will be slightly affected.

How to check:

1. Log in to the management console.
2. In the upper left corner of the management console, specify Region and Project.
3. Choose **Databases** > **Document Database Service**.
4. On the **Instances** page, click the instance name.
5. On the instance details page, check whether the storage space is encrypted.

How to fix:

After a DB instance is created, the disk encryption status cannot be changed. Enable disk encryption when you need to create a DB instance. Procedure:

1. Log in to the management console.
2. In the upper left corner of the management console, specify Region and Project.
3. Choose **Databases** > **Document Database Service**.
4. On the buy instance page, select disk encryption, enter and select instance information, and click **Buy Now**.

Reference:

https://support.huaweicloud.com/intl/en-us/qs-dds/dds_02_0063.html

 Copyright © Huawei Technologies Co., Ltd.

2.6.3 C.CS.FOUNDATION.G_6_3 RDS for PostgreSQL

2.6.3.1 C.CS.FOUNDATION.G_6_3.R_1 Configuring Proper Security Group Rules

Level: Level 1

Background:

A security group is a logical group that have the same security protection requirements in a VPC to ensure database security and stability.

Impact: None.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the target primary DB instance or read replica.
5. In the Connection Information area on the Basic Information page, locate the target security group in the **Security Group** field.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the target primary DB instance or read replica.
5. In the **Connection Information** area on the **Basic Information** page, click  in the **Security Group** field.
6. Click  to submit the change.
7. To cancel the change, click .
8. Click  in the upper right corner on the **Basic Information** page to view the result of the change. This process takes about 1 to 3 minutes.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_09_0026.html

2.6.3.2 C.CS.FOUNDATION.G_6_3.R_2 Enabling the Backup Function and Configuring a Backup Policy

Level: Level 1

Background:

You can periodically back up the database. If the database is faulty or data is damaged, you can use the backup files to restore the database, ensuring data reliability.

Impact: None.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page, choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. On the **Backups & Restorations** page, click **Intra-Region Backup Policies**. Viewing the configured backup policy

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page, choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. On the **Backups & Restorations** page, click **Intra-Region Backup Policies**.
6. On the displayed page, if you want to enable the automated backup policy, click . Once enabled, the backup policy can be modified.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_09_0027.html

2.6.3.3 C.CS.FOUNDATION.G_6_2.R_4 Enabling the Database Audit Logs

Level: Level 2

Background:

Use PostgreSQL Audit Extension (pgAudit) and RDS for PostgreSQL DB instances to record all user operations on the database. By viewing audit logs, you can perform database audit and analyze root causes of faults, improving system O&M efficiency.

Impact:

Enabling this feature may lead to higher disk space consumption and potential performance impacts. You are advised to manage the types of audited objects to reduce the number of audit logs.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.

3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. In the navigation pane, choose **Plugins**. click **Loaded shared_preload_libraries parameter values** in the upper right corner, and check whether the parameter value contains **pgaudit**.
6. On the **Plugins** page, search for the **pgaudit** and check whether the plugin is installed.
7. In the navigation pane on the left, choose **SQL Audits**. On the displayed page, click **Set SQL Audit** above the list.
8. Check whether the audit log function is enabled.
9. In the navigation pane on the left, choose **Parameters** and check whether the value of **pgaudit.log** is NONE.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. In the navigation pane, choose **Plugins**. click **Loaded shared_preload_libraries parameter values** in the upper right corner, and add **pgaudit** to the parameter value.
6. On the **Plugins** page, search for the **pgaudit** and click install in the **Operation** column.
7. In the navigation pane on the left, choose **SQL Audits**. On the displayed page, click **Set SQL Audit** above the list.
8. Click  to enable the audit log function. Set the retaining days for storing SQL audit logs and click **OK** to save the settings. Audit logs are retained for 7 days by default but can be retained from 1 to 732 days if needed.
9. In the navigation pane on the left, choose **Parameters** and change the value of **pgaudit.log** to **DDL**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_09_0063.html

2.6.3.4 C.CS.FOUNDATION.G_6_3.R_4 Do Not Use the Default Port

Level: Level 1

Background:

The default port of PostgreSQL is 5432. The default port is easy to be listened, which poses security risks. You are advised to use a non-default port.

Impact: None.

How to check:

1. Log in to the management console.

2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the DB instance name.
5. In the **Connection Information** area on the **Basic Information** page, view the port on the **Database Port field**.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the DB instance name.
5. In the **Connection Information** area on the **Basic Information** page, click **Change** next to the **Database Port** field.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_pg_change_database_port.html

2.6.3.5 C.CS.FOUNDATION.G_6_3.R_5 Configuring the Timeout for Client Authentication

Level: Level 1

Background:

The **authentication_timeout** parameter specifies the maximum duration allowed for client authentication, in seconds. This prevents the client from occupying connection channels for a long period of time. The default value is 60s.

Impact:

If the authentication is not complete within the specified time, the connection is forcibly disconnected.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. In the navigation pane on the left, choose **Parameters**. On the displayed page, view the value of **authentication_timeout**.

How to fix:

1. Log in to the management console.

 Copyright © Huawei Technologies Co., Ltd.

2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. In the navigation pane on the left, choose **Parameters**. On the displayed page, modify the **authentication_timeout** parameter.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_pg_configuration.html

2.6.3.6 C.CS.FOUNDATION.G_6_3.R_6 Restricting IP Addresses for Connecting to the Database

Level: Level 2

Background:

If no restriction is set on the IP address for connecting to the database, the entire network can be accessed, which increases the attack surface.

Impact:

If services use floating IP addresses to achieve high availability, the scenarios where floating IP addresses are used will be affected.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. In the navigation pane, choose **Accounts** and click **pg_hba Modifications**. Check whether 0.0.0.0/0 can be accessed. You are advised to configure the network segment used by services.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. In the navigation pane, choose **Accounts** and click **pg_hba Modifications**. Configure the network segment used by the service to access the database.
6. The default rule can be modified or deleted. New rules can be manually added. After the operation is complete, click **Submit** above the list. In the displayed dialog box, click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_pg_05_0027.html

2.6.3.7 C.CS.FOUNDATION.G_6_3.R_7 Enabling Log Recording for User Logins

Level: Level 2

Background:

To ensure database security and traceability, all operations of login users are recorded for security audit. The **log_connections** records the authentication logs of each connection attempt to the server and the logs of user logout. When important data is lost due to attacks or misoperations of internal employees, the login IP address can be located in a timely manner.

Impact: None.

How to check:

Check whether the database parameters **log_connections** and **log_disconnections** are enabled.

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. In the navigation pane on the left, choose **Parameters**. On the displayed page, check whether the **log_connections** and **log_disconnections** parameters are enabled.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the instance name.
5. In the navigation pane on the left, choose **Parameters**. On the displayed page, modify the **log_connections** and **log_disconnections** parameters.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_pg_configuration.html

2.6.3.8 C.CS.FOUNDATION.G_6_3.R_8 Update the Database Version to the Latest Version

Level: Level 1

Background:

PostgreSQL community edition 9.5, 9.6, or 10 has reached EOL and is no longer maintained. The EOS notice has been released for PostgreSQL 9.5 or 9.6 on the

 Copyright © Huawei Technologies Co., Ltd.

cloud. Earlier versions may have vulnerabilities. Run the software of the latest version can protect the system from certain attacks.

Impact: None.

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the target DB instance.
5. In the **DB Information** area on the **Basic Information** page, view the current database version in the **DB Engine Version** field.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **Relational Database Service**.
4. On the **Instances** page, click the target DB instance.
5. In the **DB Information** area on the **Basic Information** page, click **Upgrade Minor Version** next to the **DB Engine Version** field.
6. If you want to perform a cross-major version upgrade, click the target DB instance name in the DB instance list to switch to the **Basic Information** page.
7. In the navigation pane on the left, choose **Major Version Upgrade**.

Reference:

https://support.huaweicloud.com/intl/en-us/bulletin-rds/rds_bulletin_0008.html

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_pg_05_0003.html

https://support.huaweicloud.com/intl/en-us/usermanual-rds/rds_pg_05_0004.html

2.6.4 C.CS.FOUNDATION.G_6_4 GaussDB

2.6.4.1 C.CS.FOUNDATION.G_6_4.R_1 Configuring Maximum Number of Concurrent Database Connections

Level: Level 2

Background:

If the number of GaussDB connections is excessive, it can lead to high resource consumption on the server, resulting in sluggish operation responses. To address this, consider setting the maximum number of GaussDB connections based on the operating system environment. Ensure that this maximum value does not exceed the maximum number of threads supported by the operating system; otherwise, the setting will be ineffective. By configuring the maximum connections appropriately, you can mitigate the risk of Denial-of-Service (DoS) attacks and optimize system resource utilization for optimal operational response capabilities.

 Copyright © Huawei Technologies Co., Ltd.

Impact: None

How to check:

1. Connect to the database.
2. Run the **SHOW max_connections** command to check the maximum number of global session connections.
3. Run the **SHOW max_inner_tool_connections** command to check the maximum number of concurrent connections to the database.
4. Run the **SHOW sysadmin_reserved_connections** command to check the minimum number of connections reserved by the administrator.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **GaussDB**. The GaussDB console is displayed.
4. On the **Instances** page, click the name of the target instance to go to the **Basic Information** page.
5. In the navigation pane on the left, click **Parameters**. On the displayed page, modify parameters.
6. If the parameters cannot be modified on the console, evaluate the risks in advance and contact customer service for modification.

Reference source:

https://support.huaweicloud.com/intl/en-us/bestpractice-gaussdb/gaussdb_practice_0037.html

2.6.4.2 C.CS.FOUNDATION.G_6_4.R_2 Security Authentication Configuration

Level: Level 1

Background:

To enhance user experience and safeguard accounts against unauthorized access, GaussDB implements a limit on login attempts and a lockout duration following failed login attempts.

Impact: None

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **GaussDB**. The GaussDB console is displayed.
4. On the **Instances** page, click the target instance.
5. In the navigation tree on the left, choose **Parameters** and view **failed_login_attempts** to view the number of global retry times.

 Copyright © Huawei Technologies Co., Ltd.

6. Connect to the database.
7. Run the **SHOW failed_login_times** command to check the global lockout duration.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **GaussDB**. The GaussDB console is displayed.
4. On the **Instances** page, click the name of the target instance to go to the **Basic Information** page.
5. In the navigation pane on the left, click **Parameters**. On the displayed page, modify parameters.
6. If the parameters cannot be modified on the console, evaluate the risks in advance and contact customer service for modification.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-gaussdb/gaussdb_practice_0038.html

2.6.4.3 C.CS.FOUNDATION.G_6_4.R_3 User Password Security

Level 1

Background:

User passwords are stored in the system catalog **pg_authid**. To prevent password leakage, GaussDB encrypts user passwords before storing them. The encryption algorithm is determined by the configuration parameter **password_encryption_type**.

The password of a GaussDB database user has a validity period. You can set the **password_notify_time** parameter to remind the user to change the password. To change the password validity period, you can change the value of **password_effect_time**.

Impact: None

Check method:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **GaussDB**. The GaussDB console is displayed.
4. On the **Instances** page, click the target instance.
5. In the left-side navigation pane, click **Parameters** to verify the **password_encryption_type**, which determines the encryption method used for database passwords.
6. Connect to the database.
7. Run the **SHOW password_policy** command to check the password complexity configuration.

 Copyright © Huawei Technologies Co., Ltd.

8. Run the **SHOW password_notify_time** command to check the maximum number of global session connections.
9. Run the **SHOW password_effect_time** command to check the password validity period.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **GaussDB**. The GaussDB console is displayed.
4. On the **Instances** page, click the name of the target instance to go to the **Basic Information** page.
5. In the navigation pane on the left, click **Parameters**. On the displayed page, modify parameters.
6. If the parameters cannot be modified on the console, evaluate the risks in advance and contact customer service for modification.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-gaussdb/gaussdb_practice_0039.html

2.6.4.4 C.CS.FOUNDATION.G_6_4.R_4 Permission Management

Level: Level 2

Background:

To prohibit PUBLIC users from obtaining the CREATE permission, as it allows any database account create tables and other objects in PUBLIC mode, it is important to restrict the PUBLIC permission.

Impact: None

How to check:

1. Connect to the database.
2. Run the **SELECT CAST(has_schema_privilege('public','public','CREATE') AS TEXT)** command. If the command output is **true**, the problem needs to be fixed.

How to fix:

Run the **REVOKE CREATE ON SCHEMA public FROM PUBLIC;** command to fix the problem.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-gaussdb/gaussdb_practice_0040.html

2.6.4.5 C.CS.FOUNDATION.G_6_4.R_5 Enabling the Database Audit Logging Function

Level: Level 2

 Copyright © Huawei Technologies Co., Ltd.

Background:

The audit feature records all database activities. You can view the audit logs to perform security assessments and pinpoint problem causes, thereby enhancing system operational efficiency.

Impact:

Enabling this feature may lead to higher disk space consumption and potential performance impacts. It is advisable to manage the types of audited objects to minimize the volume of audit logs generated.

How to check:

1. Connect to the database.
2. Run the **SHOW audit_enabled** command to check whether the database audit function is enabled.

How to fix:

Run the modification statement to modify the parameter.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-gaussdb/gaussdb_practice_0041.html

2.6.4.6 C.CS.FOUNDATION.G_6_4.R_6 WAL Archiving Configuration

Level: Level 2

Background:

Write Ahead Log (WAL) is also called Xlog.

Impact: None

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **GaussDB**. The GaussDB console is displayed.
4. On the **Instances** page, click the name of the target instance to go to the **Basic Information** page.
5. In the navigation tree on the left, choose **Parameters** and check the value of **wal_level**, which determines the WAL level.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **GaussDB**. The GaussDB console is displayed.
4. On the **Instances** page, click the name of the target instance to go to the **Basic Information** page.

 Copyright © Huawei Technologies Co., Ltd.

5. In the navigation pane on the left, click **Parameters**. On the displayed page, modify parameters.
6. If the parameters cannot be modified on the console, evaluate the risks in advance and contact customer service for modification.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-gaussdb/gaussdb_practice_0042.html

2.6.4.7 C.CS.FOUNDATION.G_6_4.R_7 Enabling the Backup Function and Configuring a Backup Policy

Level: Level 2

Background:

GaussDB provides high availability, but if a primary database or a table in it is maliciously or mistakenly deleted, data in the standby database will also be deleted. You can only restore the deleted data from backups.

Impact: None

How to check:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **GaussDB**. The GaussDB console is displayed.
4. On the **Instances** page, click the target instance.

How to fix:

1. Log in to the management console.
2. Click  in the upper left corner and select a region and a project.
3. Click  in the upper left corner of the page and choose **Databases** > **GaussDB**. The GaussDB console is displayed.
4. On the **Instances** page, click the target instance.
5. In the navigation pane, choose **Backups**. On the displayed page, click **Modify Backup Policy**. You can view the configured backup policy. To modify the backup policy, adjust the parameter values.
6. Modify the instance-level backup policy as prompted.

   Instance-level full backup policy

   - **Retention Period (days)**: This parameter defines the duration for retaining automated backups. A longer period enhances data reliability. Adjust this setting based on your needs. The initial default is set to **7 days**. Full backups are retained till the retention period expires. However, even if the retention period has expired, the most recent backup will be retained.
   - Extending the retention period improves data reliability. You can extend the retention period as needed.

 Copyright © Huawei Technologies Co., Ltd.

- If you shorten the retention period, the new backup policy takes effect for existing backups. Any automated backups (including full and incremental backups) that have expired will be automatically deleted. Manual backups will not be automatically deleted but you can delete them manually.

Policy for automatically deleting full backups

To ensure data integrity, even after the retention period expires, the most recent backup will be retained, for example,

If **Backup Cycle** was set to **Monday** and **Tuesday** and the **Retention Period** was set to **2**:

- The full backup generated on Monday will be automatically deleted on Thursday. The reasons are as follows:

  The backup generated on Monday expires on Wednesday, but it is the last backup, so it will be retained until a new backup expires. The next backup will be generated on Tuesday and will expire on Thursday. So the full backup generated on Monday will not be automatically deleted until Thursday.
- A full backup generated on Tuesday will be automatically deleted on the following Wednesday. The reasons are as follows:

  The backup generated on Tuesday will expire on Thursday, but as it is the last backup, so it will be retained until a new backup expires. The next backup will be generated on the following Monday and will expire on the following Wednesday. So the full backup generated on Tuesday will not be automatically deleted until the following Wednesday.
- **Backup flow control**: controls the speed at which backup data is uploaded to OBS during backup. The default value is 75 MB/s. The value 0 indicates that the speed is not limited.
- **Enable standby server backup**: If standby server backup is enabled, full backup and differential backup are performed on the server of the standby DN.
- **Time window**: An hour within 24 hours, such as 01:00-02:00 or 12:00-13:00. The backup time is in UTC format. If the DST or standard time is switched, the backup time segment changes with the time zone.
- **Backup Cycle**: Select at least one day as required.

Note:

The backup retention period is from 1 to 732 days. To extend the retention period, contact customer service. Automated backups can be retained for up to 2,562 days.

The backup time window is an hour. You are advised to select off-peak hours based on service requirements. While the default setting encompasses all backup cycles, these can be customized. Ensure that the schedule includes at least one day per week.

A full backup is immediately triggered after a DB instance is created. Then, a full backup or differential backup is performed based on the time window and backup cycle you specified. We recommend that you set the automated backup time window Full backup is performed during this period.

Differential backup policy

- **Backup Cycle**: Select the backup cycle for performing a differential backup. 30 minutes is used by default.
- **Prefetch Pages**: Set the number of prefetch pages from the modified pages in the disk table file during a differential backup. The default value is **64**.

 Copyright © Huawei Technologies Co., Ltd.

When modified pages are adjacent (for example, with a bulk data load), you can set this parameter to a large value. When modified pages are scattered (for example, random update), you can set this parameter to a small value. If this parameter is set to a large value, the occupied I/O increases. In this case, other services are affected and the database performance deteriorates.

- **Shard Size**: Backup files generated during full and differential backups are split based on the shard size. The value range is from 0 to 1024, but it must be a multiple of 4. The default value is **4**. **0** indicates that the size is not limited.

7. Click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-gaussdb/gaussdb_practice_0043.html

2.7 C.CS.FOUNDATION.G_7 Enterprise Intelligence

2.7.1 C.CS.FOUNDATION.G_7_1 AI Development Platform ModelArts

2.7.1.1 C.CS.FOUNDATION.G_7_1.R_1 Using the IP Address Whitelist to Access the Notebook

Level: Level 2

Background:

Notebook instances can be accessed directly via SSH and authenticated using keypair authentication. For enhanced security, you are advised to establish an IP address whitelist to limit access to the instance exclusively to approved endpoints.

Impact:

After this function is enabled, only whitelisted IP addresses access the notebook instances.

How to check:

1. Log in to the ModelArts management console. In the navigation pane on the left, choose **DevEnviron** > **Notebook**.
2. In the notebook instance list, go to the notebook instance details page and check whether the whitelist is configured.

How to fix:

1. Log in to the ModelArts management console. In the navigation pane on the left, choose **DevEnviron** > **Notebook**.
2. In the notebook instance list, go to the notebook instance details page and modify the whitelist configuration.

 Copyright © Huawei Technologies Co., Ltd.



Reference:

https://support.huaweicloud.com/intl/en-us/devtool-modelarts/modelarts_05_0369.html

2.7.1.2 C.CS.FOUNDATION.G_7_1.R_2 Using Dedicated Resource Pools

Level: Level 2

Background:

For optimal performance and security in the production environments for training, inference, and development, you are advised to use a dedicated resource pool. This ensures access to exclusive computing resources and enhances resource isolation.

Impact:

Using dedicated resource pools increases costs.

How to check:

On the **Resource Pools** page, check whether the resource pool type is dedicated resource pool.

How to fix:

Both public and dedicated resource pools are available for you to select when ModelArts is used for full-process AI development.

Public resource pools: provide large-scale public computing clusters, which are allocated based on job parameter settings. Resources are isolated by job. Public resource pools are billed based on resource flavors, service duration, and the number of instances, regardless of tasks (training, deployment, or development) for which the pools are used. Public resource pools are available by default. You can select a public resource pool during AI development.

Dedicated resource pools provide dedicated compute resources, which can be used for notebook instances, training jobs, and model deployment. The resources provided in a dedicated resource pool are exclusive, featuring higher resource efficiency than a public resource pool.

To use a dedicated resource pool, buy one and select it during AI development.

Reference:

https://support.huaweicloud.com/intl/en-us/resmgmt-modelarts/resmgmt-modelarts_0003.html

 Copyright © Huawei Technologies Co., Ltd.

2.7.1.3 C.CS.FOUNDATION.G_7_1.R_3 Running a Custom Image as a Non-root User

Level: Level 2

Background:

You can create a Dockerfile for a custom image and then push it to SWR. To enhance permission control, it is recommended that you explicitly define the default running user as **root** when customizing an image. This helps reduce security risks during container running.

Impact:

When a non-root user is used to run services, there may be situations where permissions are insufficient.

How to check:

Check whether the **USER** field in the Dockfile file is defined as a non-root user. If yes, the container runs as a non-root user.

How to fix:

The **USER** field in Dockerfile displays a non-root user.

Reference:

https://support.huaweicloud.com/intl/en-us/docker-modelarts/develop-modelarts-0097.html

2.7.1.4 C.CS.FOUNDATION.G_7_1.R_4 Using Independent Agencies for Different Sub-users

Level: Level 2

Background:

To use ModelArts resources, ensure you obtain agency authorization from the user. For better permission control over sub-users, you are advised to grant agency permissions to each sub-user individually on the ModelArts global configuration page. Avoid sharing the same agency credential with multiple sub-users.

Impact: None

How to check:

Check whether permissions are granted to **All Users** in the ModelArts global configuration. If yes, assign the permissions individually to different sub-users.

How to fix:

It is recommended that tenants assign agency permissions to sub-users individually in the global configuration page of ModelArts.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-modelarts/modelarts_24_0085.html

 Copyright © Huawei Technologies Co., Ltd.

2.7.1.5 C.CS.FOUNDATION.G_7_1.R_5 Enabling "Strict Mode"

Level 1

Background:

When using ModelArts resources, you need to assign different agencies to different sub-users to achieve minimum authorization.

Impact:

After enabling the strict mode, you need grant permissions to different sub-users individually. If the original configuration granted permissions to all users, enable this mode. However, exercise caution: if permissions are not thoroughly checked, functions may be affected after permission reduction.

How to check:

Check whether **Strict Mode** is enabled in **Global Configuration** on the console. If yes, only the **Disable Strict Mode** button is displayed on the page.

How to fix:

Enable **Strict Mode** in **Global Configuration** on the console.

Reference:

https://support.huaweicloud.com/intl/en-us/bestpractice-modelarts/modelarts_24_0085.html

2.7.2 C.CS.FOUNDATION.G_7_2 MapReduce Service (MRS)

2.7.2.1 C.CS.FOUNDATION.G_7_2.R_1 Enabling Kerberos Authentication

Level 1

Background:

MRS cluster components utilize Kerberos authentication. When Kerberos authentication is enabled, users can access component resources only after being authenticated. However, if Kerberos authentication is disabled, authentication and authorization are not required for accessing MRS components, which introduces risks to the cluster.

Impact:

After this function is enabled, users have to complete the Kerberos authentication to access MRS components.

How to check:

Log in to the MRS management page and check whether Kerberos authentication is enabled on the **Overview** page of the cluster.

How to fix:

Kerberos authentication mode for an MRS cluster is immutable once configured. Therefore, enabling Kerberos authentication (which is enabled by default) needs to be performed during the purchase of an MRS cluster. For details about how to enable

 Copyright © Huawei Technologies Co., Ltd.

Kerberos authentication when purchasing a cluster, visit https://support.huaweicloud.com/intl/en-us/qs-mrs/mrs_09_0010.html.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-mrs/mrs_01_0419.html

2.7.2.2 C.CS.FOUNDATION.G_7_2.R_2 Separate Deployment of Management, Control, and Data Nodes

Level: Level 2

Background:

The common deployment templates for an MRS cluster include management and control co-deployment, management and control separate deployment, and data separate deployment. To isolate data nodes from management and control nodes, it is advisable to use the management and control separate deployment and data separate deployment modes.

Impact:

Compared with co-deployment of management and control nodes, you need to purchase more nodes for the MRS cluster.

How to check:

1. Log in to MRS Manager.
2. On the **Nodes** page of the cluster, check whether there are **Core** nodes.
3. If yes, it is the data separate deployment mode.
4. Check whether the number of master nodes is greater than 5. If yes, it is the management and control separate deployment mode.

How to fix:

Use instance migration to implement the management and control separate deployment.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-mrs/mrs_01_0121.html

2.7.2.3 C.CS.FOUNDATION.G_7_2.R_3 EIP Security Group Management and Control

Level: Level 1

Background:

You can bind an Elastic IP (EIP) to an MRS cluster. Once the EIP is bound and the security group is enabled, you can use the EIP to access the FusionInsight Manager management page of the MRS cluster or log in to a node in the MRS cluster via SSH. To ensure security, properly manage and control security groups. Avoid allowing untrusted IP addresses to access MRS clusters. Additionally, carefully control the port range for allowed IP addresses and avoid directly enabling all ports

Impact:

Only the IP addresses configured in the security group can access the cluster nodes.

 Copyright © Huawei Technologies Co., Ltd.

How to check:

Check whether an EIP is bound to the cluster. If yes, check whether the IP addresses in the security group of the EIP are trusted and whether the enabled ports are proper.

How to fix:

Delete insecure security group configurations.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-ecs/en-us_topic_0030878383.html

2.7.3 C.CS.FOUNDATION.G_7_3 GaussDB(DWS)

2.7.3.1 C.CS.FOUNDATION.G_7_3.R_1 Enabling Cluster Data Encryption

Level: Level 2

Background:

GaussDB(DWS) can enable database encryption for clusters to protect static data and avoid security issues such as database cracking.

Impact:

After enabling this function, there is a slight performance deterioration. Specifically, the AES algorithm experiences only a minor deterioration, while the SM4 algorithm suffers a significant deterioration.

How to check:

1. Log in to the GaussDB(DWS) management console.
2. In the navigation pane on the left, choose **Clusters**.
3. On the **Clusters** page, click the name of a cluster to go to the **Cluster Details** page. In the **Data Encryption Information** area, view the database encryption information.

Parameter	Description
Key Name	Indicates the database encryption key of the cluster when **Encrypt DataStore** is enabled.
Last Key Rotation Time	Indicates the time when the last encryption key is rotated when **Encrypt DataStore** is enabled.

How to fix:

Enable database encryption during cluster creation.

Reference:

https://support.huaweicloud.com/intl/en-us/mgtg-dws/dws_01_0019.html

2.7.3.2 C.CS.FOUNDATION.G_7_3.R_2 Enabling Audit Logging on the GaussDB(DWS) Management Console

Level: Level 2

Background:

GaussDB(DWS) uses Cloud Trace Service (CTS) to record mission-critical operations performed on the GaussDB(DWS) management console, such as cluster creation, snapshot creation, cluster scale-out, and cluster restart. The logs can be used in purposes such as security analysis, compliance audit, resource tracing, and fault locating. After this function is enabled, console operations can be audited and faults can be located.

Impact:

Audit logs occupy some storage space, slightly affecting performance.

How to check:

Check whether CTS traces GaussDB(DWS) logs.

How to fix:

1. Log in to the management console, choose **Service List** > **Management & Governance** > **Cloud Trace Service**. The CTS management console is displayed.
2. In the navigation pane on the left, choose **Tracker List**.
3. Enable CTS.
4. If you are a first-time CTS user and do not have any created trackers in the tracker list, enable CTS first. For details, see Enabling CTS in the *Cloud Trace Service Getting Started*.
5. If you have enabled CTS, the system has automatically created a management tracker. Only one management tracker can be created and it cannot be deleted. You can also create a data tracker. For details, see Creating a Tracker in the *Cloud Trace Service User Guide*.

Reference:

https://support.huaweicloud.com/intl/en-us/mgtg-dws/dws_01_0118.html

2.7.3.3 C.CS.FOUNDATION.G_7_3.R_3 Enabling GaussDB(DWS) Audit Logs

Level: Level 2

Background:

GaussDB(DWS) supports database operation audit logs, which operate independently of the audit on the management plane. These logs record the operations performed by each user within the database. It is recommended that you enable the operation log recording function as needed. This will facilitate historical data tracing and enhance data security.

Impact:

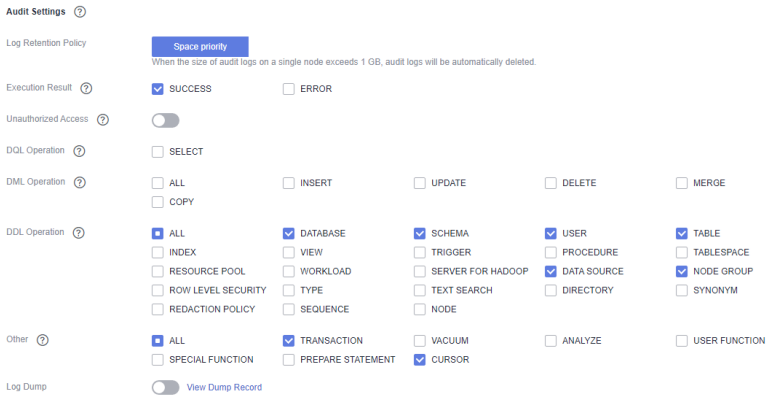
When the number of concurrent requests is large, the performance may be slightly affected.

How to check:

1. Log in to the GaussDB(DWS) management console.
2. Choose **Clusters**.
3. In the cluster list, click the name of a cluster. Choose Security.

 Copyright © Huawei Technologies Co., Ltd.

4. In the **Audit Configuration** area, verify whether the audit log function is enabled. If neither the execution result nor the specific operation is selected, the audit log function is not enabled.



How to fix:

In the **Audit Configuration** area, configure audit logs.

Reference:

https://support.huaweicloud.com/intl/en-us/mgtg-dws/dws_01_0075.html

2.7.3.4 C.CS.FOUNDATION.G_7_3.R_4 Enabling Audit Log Dumping for a GaussDB(DWS) Database

Level: Level 2

Background:

Database audit logs in GaussDB(DWS) capture details about connections and user activities within the database. The audit logs help monitor the database to ensure security, rectify faults, or locate historical operations. By default, audit log information is stored within the database. To enhance data protection and accessibility, consider dumping audit logs to OBS (Object Storage Service). This ensures that audit logs are backed up and easily accessible when needed.

Impact:

OBS storage space must be prepared in advance.

How to check:

1. In the cluster list, click the name of the cluster for which you want to enable audit log dump. In the navigation pane, choose **Security Settings**.
2. In the **Audit Settings** area, enable the audit log dump function.
3.  indicates that the function is enabled.  indicates that the function is disabled.

How to fix:

After configuring the OBS dump directory, apply the configuration.

Reference:

 Copyright © Huawei Technologies Co., Ltd.

https://support.huaweicloud.com/intl/en-us/mgtg-dws/dws_01_0142.html

2.7.3.5 C.CS.FOUNDATION.G_7_3.R_5 Enabling Rights Separation on GaussDB(DWS)

Level: Level 2

Background:

By default, the administrator specified when you create a GaussDB(DWS) cluster is the database system administrator. The administrator can create other users and view the audit logs of the database. That is, separation of permissions is disabled.

GaussDB(DWS) supports role-based separation of permissions. In this way, different roles have different permissions and cluster data can be better protected.

Impact:

Administrators are classified into system administrators, security administrators, and audit administrators.

How to check:

1. On the **Security Settings** page, view the rights separation settings.
2.  indicates that **Rights Separation** is enabled. After rights separation is enabled, set the usernames and passwords of the security administrator and audit administrator. The two users can be used to connect to the database and perform database-related operations.
3.  indicates that **Rights Separation** is disabled. This function is disabled by default.

How to fix:

On the **Security Settings** page, configure rights separation.

Reference:

https://support.huaweicloud.com/intl/en-us/mgtg-dws/dws_01_0074.html

2.7.3.6 C.CS.FOUNDATION.G_7_3.R_6 Enabling SSL Encrypted Transmission

Level: Level 1

Background:

SSL (Secure Sockets Layer) is a robust security protocol that facilitates bidirectional authentication between the server and client. It achieves this through the use of digital signatures and digital certificates, ensuring secure data transmission. Enabling SSL is strongly recommended.

Impact:

You need to configure certificates and other SSL parameters.

How to check:

1. Log in to the GaussDB(DWS) management console.

 Copyright © Huawei Technologies Co., Ltd.

2. In the navigation pane, choose **Clusters**.
3. In the cluster list, click a cluster name. On the page displayed, click the **Security Settings** tab. By default, **Configuration Status** is **Synchronized**, which indicates that the latest database result is displayed.
4.  indicates SSL is enabled. Set **require_ssl=1**, indicating that the server requires SSL connection.
5.  : indicates SSL is disabled. Set **require_ssl=0**, indicating that the server does not require SSL connection. By default, SSL connection is disabled.

How to fix:

Enable mandatory SSL connection.

Reference:

https://support.huaweicloud.com/intl/en-us/mgtg-dws/dws_01_0038.html

2.8 C.CS.FOUNDATION.G_8 Security

2.8.1 C.CS.FOUNDATION.G_8.R_1 Enabling WAF

Level: Level 1

Background:

For users with web-based businesses, it is required to enable the Web Application Firewall (WAF) service. Once enabled, all public traffic to the website will first go through WAF. Malicious traffic will be detected and filtered by WAF, while normal traffic will be returned to the source IP, ensuring the safety, stability, and availability of the source IP.

Impact: None

How to check:

1. Log in to the management console.
2. In the service list, choose **Security & Compliance** > **Web Application Firewall**.
3. Check whether WAF is enabled.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Security & Compliance** > **Web Application Firewall**.
3. Click **Buy WAF**. On the displayed page, select a cloud mode, edition, expansion packages, and required duration.
4. Add a domain name to WAF. In the navigation pane on the left, choose **Website Settings**. In the upper left corner of the domain name list, click **Add Website**. Select **Cloud Mode** for the deployment mode. On the displayed page, set **Domain Name** (you can also choose to quickly add a domain on the cloud), and set the parameters for the domain information, origin server settings, and advanced settings areas as prompted.

 Copyright © Huawei Technologies Co., Ltd.

5. Connect a domain name to WAF. Complete steps such as **Whitelist WAF**, **Test WAF**, **Modify Retrieval Proxy Address**.
6. Enable WAF. Locate the row containing the desired domain name and change the working mode to **Enabled** in the **Mode** column.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-waf/waf_01_0324.html

2.8.2 C.CS.FOUNDATION.G_8.R_2 Configuring a Geolocation Access Rule in WAF

Level: Level 1

Background:

Geolocation access control rules in WAF enable users to restrict source IP addresses from a specific country or region to access the protected website.

Impact:

If the source IP address of the request traffic is identified by WAF as coming from a specified country or region, it may be blocked.

How to check:

1. Log in to the management console.
2. In the service list, choose **Security & Compliance** > **Web Application Firewall**.
3. In the navigation pane on the left, choose **Policies**. On the displayed page, click the name of the policy you want to modify.
4. On the displayed page, check whether there is a rule in the **Geolocation Access Control** area and whether the rule is **Enabled**.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Security & Compliance** > **Web Application Firewall**.
3. In the navigation pane on the left, choose **Policies**. On the displayed page, click the name of the policy you want to modify. In the **Geolocation Access Control** area, users can change **Status** as needed and click **Customize Rule** to go to the page for configuring geolocation access control rules.
4. In the upper left corner of the **Geolocation Access Control** page, click **Add Rule**. In the displayed dialog box, add a geolocation access control rule.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-waf/waf_01_0013.html

2.8.3 C.CS.FOUNDATION.G_8.R_3 Configuring the WAF Back-to-Source IP Addresses (Origin Server Deployed on ECSs)

Level: Level 1

Background:

 Copyright © Huawei Technologies Co., Ltd.

A back-to-source IP address is an IP address used by WAF to forward client requests to origin servers. To origin servers, all web requests come from WAF and all source IP addresses are WAF back-to-source IP addresses. The real client IP address is encapsulated into the HTTP X-Forwarded-For (XFF) header field. If no ELB is configured between WAF and origin servers, users need to configure ECSs housing web services to allow only WAF back-to-source IP addresses.

Impact:

Service traffic can only be transmitted to ECSs through WAF.

How to check:

1. Log in to the management console.
2. In the **Service List**, choose **Security & Compliance** > **Web Application Firewall**. In the navigation pane on the left, click **Website Settings** page and obtain WAF back-to-source IP addresses.
3. In the **Service List**, choose **Compute** > **Elastic Cloud Server**. In the ECS instance list, select the ECS housing the origin server and check the inbound rule of the security group.
4. Check whether only WAF back-to-source IP addresses are allowed to access the ECSs that work as origin servers.

How to fix:

1. Log in to the management console.
2. Choose **Security& Compliance** > **Web Application Firewall**. In the navigation pane on the left, choose **Website Settings**.
3. On the right of the website list, click the **WAF Back-to-Source IP Addresses** link.
4. In the displayed dialog box, click **Copy** to copy all the addresses.
5. Choose **Compute** > **Elastic Cloud Server**. In the **Name/ID** column of the target ECS, click the ECS name to go to the details page.
6. Select the **Security Groups** tab, expand all security groups, and click **Manage Rule** in the upper right corner of the target security group.
7. Click the **Inbound Rules** tab and click **Add Rule**. In the displayed **Add Inbound Rule** dialog box, add rules to allow all inbound traffic from WAF back-to-source IP addresses.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-waf/waf_01_0325.html

2.8.4 C.CS.FOUNDATION.G_8.R_4 Configuring the WAF Back-to-Source IP Addresses (Origin Server Deployed on ELBs)

Level: Level 1

Background:

A back-to-source IP address is an IP address used by WAF to forward client requests to origin servers. To origin servers, all web requests come from WAF and all source IP addresses are WAF back-to-source IP addresses. The real client IP address is encapsulated into the HTTP X-Forwarded-For (XFF) header field. If ELB is

 Copyright © Huawei Technologies Co., Ltd.

configured between WAF and origin servers, configure the ELB load balancer to allow only WAF back-to-source IP addresses.

Impact:

Service traffic can only be transmitted to ELBs through WAF.

How to check:

1. Log in to the management console.
2. In the **Service List**, choose **Security& Compliance** > **Web Application Firewall**. In the navigation pane on the left, click **Website Settings** page and obtain WAF back-to-source IP addresses.
3. In the upper left corner of the page, hover on **Service List**. Choose **Networking** > **Elastic Load Balance Elastic**. In the load balancer list, click the name of the corresponding listener.
4. On the **Basic Information** tab of each listener, check whether its **Access Control** is set to **Whitelist**.

How to fix:

1. Log in to the management console.
2. Choose **Security& Compliance** > **Web Application Firewall**. In the navigation pane on the left, choose **Website Settings**.
3. On the right of the website list, click the **WAF Back-to-Source IP Addresses** link.
4. In the displayed dialog box, click **Copy** to copy all the addresses.
5. In the upper left corner of the page, hover on **Service List**. Choose **Networking** > **Elastic Load Balance Elastic**. In the load balancer list, click the name of the corresponding listener.
6. In the displayed dialog box, select **Whitelist** for **Access Control**.
   - If no such an IP address group exists, click **Create IP Address Group** and add the back-to-source IP addresses to the IP address group you are creating.
   - Select the IP address group created in 6.a from the **IP Address Group** drop-down list.
7. Click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-waf/waf_01_0325.html

2.8.5 C.CS.FOUNDATION.G_8.R_5 Enabling WAF Basic Web Protection Block Mode

Level: Level 1

Background:

Basic web protection has two modes: **Block** and **Log only**. In **Log only** mode, WAF logs attacks only. In **Block** mode, WAF blocks and records every attack detected.

Impact:

 Copyright © Huawei Technologies Co., Ltd.

Normal traffic to the protected website may be mistakenly blocked due to matching with the built-in rules of WAF. You need to configure a global whitelist to adapt to the built-in rules.

How to check:

1. Log in to the management console.
2. In the service list, choose **Security & Compliance** > **Web Application Firewall**.
3. In the navigation pane on the left, choose **Website Settings**.
4. Locate the row containing the target domain name, and check whether the content of **Basic Web Protection** in the **Policy** column is **Enabled (Block)**.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Security & Compliance** > **Web Application Firewall**.
3. In the navigation pane on the left, choose **Website Settings**.
4. Locate the row containing the target domain name. In the **Policy** column, click **Configure Policy**. On the displayed page, in the **Basic Web Protection** configuration area, select **Block** for **Mode**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-waf/waf_01_0008.html

2.8.6 C.CS.FOUNDATION.G_8.R_6 Enabling Alarm Notifications for WAF Events

Level: Level 1

Background:

Once this function is enabled, WAF sends users SMS or email notifications if an attack is detected.

Impact: None

How to check:

1. Log in to the management console.
2. In the service list, choose **Security & Compliance** > **Web Application Firewall**.
3. In the navigation pane, choose **Instance Management** > **Notifications**.
4. On the displayed page, select a notification and check whether its **Status** is **Enabled**.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Security & Compliance** > **Web Application Firewall**.
3. In the navigation pane, choose **Instance Management** > **Notifications**.
4. On the displayed page, click **Create**. In the displayed dialog box, set alarm notification parameters.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-waf/waf_01_0019.html

 Copyright © Huawei Technologies Co., Ltd.

2.8.7 C.CS.FOUNDATION.G_8.R_7 Enabling HSS (Basic/Professional/Enterprise/Premium Edition)

Level: Level 1

Background:

Host Security Service (HSS) should be installed and enabled for servers, such as Elastic Cloud Server (ECS) and Bare Metal Server (BMS), to comprehensively identify and manage server assets, monitor risks in servers in real time, and prevent unauthorized intrusions, helping enterprises enhance server security.

Impact: None

How to check:

1. Log in to the management console.
2. In the service list, choose **Security & Compliance** > **Host Security Service**.
3. In the navigation pane, choose **Dashboard**.
4. On the displayed page, check whether the number of unprotected servers is 0.

How to fix:

1. Log in to the management console.
2. In the upper left corner, select a region. In the service list, choose **Security & Compliance** > **Host Security Service**.
3. Click **Buy HSS** in the upper right corner. Set **Billing Mode** to **Yearly/Monthly**, select an edition (edition differences), select an enterprise project, select a required duration, enter a server quota, and click **Next**.
4. Once the purchase is successful, return to the HSS console and choose **Asset Management** > **Servers & Quota**. On the displayed page, click **Disable** to filter the servers that are not protected. Select a server whose **Agent Status** is **Not installed**, click **Install Agent**, and enter the ECS password. Once the installation is successful, the agent status is **Online**.
5. Click **Enable**. On the displayed page, select **Yearly/Monthly** for **Billing Mode**, select the edition purchased in step 3, and select the purchased quota.
6. Click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-hss2.0/hss_01_0230.html

2.8.8 C.CS.FOUNDATION.G_8.R_8 Enabling Ransomware Prevention (Premium/Container/WTP)

Level: Level 2

Background:

After infiltrating a server, ransomware encrypts the server's data and demands payment in exchange for decryption. This can lead to service interruptions, data leaks, or loss, and even if the ransom is paid, the server owner may not be able to recover all losses. Therefore, ransomware is one of the biggest challenges in network security today. HSS provides static and dynamic ransomware prevention and

 Copyright © Huawei Technologies Co., Ltd.

regularly back up server data to help you resist ransomware and reduce the risk of business losses.

Impact: None

How to check:

1. Log in to the management console.
2. In the upper left corner, select a region. In the service list, choose **Security & Compliance** > **Host Security Service**.
3. In the navigation pane on the left, choose **Prevention** > **Ransomware Prevention**.
4. On the displayed page, check whether **Vault Binding Status** and **Ransomware Prevention Status** of the server for which you want to enable ransomware prevention are **Enabled**.

How to fix:

1. Log in to the management console.
2. In the upper left corner, select a region. In the service list, choose **Security & Compliance** > **Host Security Service**.
3. In the navigation pane on the left, choose **Prevention** > **Ransomware Prevention**.
4. On the displayed page, select the server for which you want to enable ransomware prevention.
5. Click **Enable Backup**, select the name of the vault to be associated, and click **OK**.
6. Click **Enable Ransomware Prevention**. In the displayed dialog box, confirm the server information, select a prevention policy, and click **OK**.
7. If the **Ransomware Prevention Status** of the server changes to **Enabled**, ransomware protection is enabled successfully.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-hss2.0/hss_01_0348.html

2.8.9 C.CS.FOUNDATION.G_8.R_9 Enabling the HSS Web Tamper Protection Edition

Level: Level 1

Background:

The HSS Web Tamper Protection (WTP) edition should be enabled to protect websites from Trojans, illegal URLs, viruses, and tampering.

Impact:

Files in protected directories can only be modified by configuring privileged processes.

How to check:

1. Log in to the management console.
2. In the service list, choose **Security & Compliance** > **Host Security Service**.

 Copyright © Huawei Technologies Co., Ltd.

3. In the navigation pane on the left, choose **Prevention** > **Web Tamper Protection**.
4. Check whether the numbers of protected servers and protected directories are 0.

How to fix:

1. Log in to the management console.
2. In the service list, choose **Security & Compliance** > **Host Security Service**.
3. Click **Buy HSS** in the upper right corner. Set **Billing Mode** to **Yearly/Monthly**, select **Web Tamper Protection** for **Edition**, select an enterprise project, select a required duration, enter a server quota, and click **Next**.
4. On the displayed page, select the servers you want to protect (note that the agent must be installed in advance. See Installing an Agent), choose the target quota, and click **Add and Enable Protection**.
5. On the displayed page, select a protected server and click **Configure Protection**.
6. On the displayed page, add directories you want to protect. For details, see Adding a Protected Directory.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-hss2.0/hss_01_0214.html

2.8.10 C.CS.FOUNDATION.G_8.R_10 Enabling CFW

Level: Level 1

Background:

If you have services accessible to the Internet through Elastic IP (EIP), you are advised to enable CFW. After CFW is enabled, all public network traffic destined for the EIP will go to CFW first. CFW detects and blocks malicious attack traffic, and then routes only the legitimate traffic to the service server, keeping the server secure, stable, and reliable.

Impact: None

How to check:

1. Log in to the management console.
2. Select a region.
3. Click **Service List** and choose **Security & Compliance** > **Cloud Firewall**.
4. In the navigation pane on the left, choose **Assets** > **EIPs**. The EIP list is displayed.
5. Check whether protection is enabled.

How to fix:

1. Log in to the management console.
2. Select a region.
3. Click **Service List** and choose **Security & Compliance** > **Cloud Firewall**.
4. In the navigation pane on the left, choose **Assets** > **EIPs**. The EIP list is displayed.

 Copyright © Huawei Technologies Co., Ltd.

5. (Optional) Manually update the EIP list. Click **Synchronize EIP** in the upper right corner of the page to import your EIP information.
6. Enable EIP protection.
7. Enable protection for a single EIP. In the row of the EIP, click **Enable Protection** in the **Operation** column.
8. Enable protection for multiple EIPs. Select the EIPs to be protected and click **Enable Protection** above the table.
9. On the page that is displayed, confirm the information and click **Bind and Enable** Protection. The **Protection Status** column in the **Operation** column is **Protected**.
10. In the navigation pane, choose **Access Control** > **Access Policies**.
11. Click **Add Rule**. Enter new protection information. For details, see Adding a Protection Rule.
12. Click **OK** to complete the security policy configuration.
13. In the navigation pane, choose **Attack Defense** > **Intrusion Prevention**.
14. Select a **Protection Mode** based on the service scenario. For details, see Configuring Intrusion Prevention Policies.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-cfw/cfw_01_0031.html

2.8.11 C.CS.FOUNDATION.G_8.R_11 Enabling CFW Alarm Notification

Level: Level 2

Background:

You can create alarm rules to monitor log exceptions in real-time. If a log meets the preset rules, you will receive an alarm notification via SMS or email.

Impact: None

How to check:

1. Log in to the management console.
2. Select a region.
3. Click **Service List** and choose **Security & Compliance** > **Cloud Firewall**.
4. In the navigation pane, choose **System Management** > **Notifications**.
5. Check whether the **Attack alarm** notification item is enabled.

How to fix:

1. Log in to the management console.
2. Select a region.
3. Click **Service List** and choose **Security & Compliance** > **Cloud Firewall**.
4. In the navigation pane, choose **System Management** > **Notifications**.
5. Locate the row that contains **Attack alarm**, click **Edit** in the **Operation** column, and set notification parameters.
6. After confirming that the information is correct, enable the **Attack alarm** notification in the **Status** column.

 Copyright © Huawei Technologies Co., Ltd.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-cfw/cfw_01_0166.html

2.8.12 C.CS.FOUNDATION.G_8.R_12 Enabling Automatic Notification of SecMaster High-Risk Alarms

Level: Level 1

Background:

Enable automatic notification of high-risk alarms of the SecMaster. When a high-risk alarm is detected, you can receive an email or SMS notification in a timely manner to quickly handle and respond to the alarm.

Impact: None

How to check:

1. Log in to the management console.
2. Click **Service List** and choose **Security & Compliance** > **SecMaster**.
3. Choose **Workspaces** > **Management**. Check whether a workspace exists.
4. Click the workspace name to access the console. Choose **Security Orchestration** > **Playbooks** > **Playbooks** and check whether **Automatic notification of high-risk alerts** is **Enabled**.

How to fix:

1. Log in to the management console.
2. Choose **Service List** > **Management & Governance** > **Simple Message Notification**.
3. Choose **Topic Management** > **Topics**. In the upper right corner of the page, click **Create Topic**. In the displayed dialog box, set topic name to **SOAR-High-risk-alarm-Notification** and display name to SecMaster high risk alert notification, and click **OK**.
4. Choose **Topic Management** and subscriptions. In the upper right corner of the page, click **Add Subscription**, select the topic name in the previous step, and configure the protocol and subscription endpoint as required to receive real-time notifications of high-risk alarms.
5. Click **Service List** and choose **Security & Compliance** > **SecMaster**.
6. Choose **Workspaces** > **Management**. Find the workspace to be operated (or create a workspace for the first time).
7. Click the workspace name to access the workspace console. Choose **Security Orchestration** > **Playbooks**.
8. Find the **Automatic notification of high-risk alerts**, click **Enable**, select **v1**, and click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-secmaster/secmaster_01_0061.html

 Copyright © Huawei Technologies Co., Ltd.

2.8.13 C.CS.FOUNDATION.G_8.R_13 Enabling CBH and Multi-Factor Authentication

Level: Level 1

Background:

Cloud Bastion Host (CBH) can monitor the usage of the CBH system, monitor O&M activities of each managed resource, and identify suspicious O&M actions in real time. This protects resources and data from being accessed without authorization or damaged by external or internal users. CBH reports alarms to customers, who can then more easily handle or audit O&M issues in a timely, centralized manner. To further secure user accounts in CBH, users can enable multi-factor authentication (MFA) included in CBH. After MFA is enabled, multi-factor authentication is required every time when a user logs in to the CBH system through a web browser or an SSH client. MFA methods: SMS, mobile OTP, USB keys, and dynamic token.

Impact: None

How to check:

1. Log in to the management console.
2. Click **Service List** and choose **Security & Compliance** > **Cloud Bastion Host**. On the displayed page, buy a CBH instance.
3. Log in to the CBH system using a web browser as the CBH administrator.
4. In the navigation pane on the left, choose **User** > **User**. On the displayed user list page, select the target user, view its details, and check whether multi-factor authentication is enabled for the user.

How to fix:

1. Log in to the management console.
2. Click **Service List** and choose **Security & Compliance** > **Cloud Bastion Host**.
3. Log in to the CBH system using a web browser as the CBH administrator.
4. In the navigation pane on the left, choose **User** > **User**. On the displayed user list page, select a user, click **Manage** in the **Operation** column. In the displayed dialog box, click **Edit** in the **User Setting** area. On the displayed **Edit User setting** page, enable **Multifactor Verification**.

Reference:

https://support.huaweicloud.com/intl/en-us/qs-cbh/cbh_06_0002.html

2.8.14 C.CS.FOUNDATION.G_8.R_14 Enabling DEW's Secret Hosting

Level: Level 1

Background:

The secret hosting feature of Data Encryption Workshop (DEW) enables unified management, retrieval, and secure storage of various types of secrets, such as database passwords, server passwords, SSH keys, and access keys.

Impact: None

 Copyright © Huawei Technologies Co., Ltd.

How to check:

1. Log in to the management console.
2. Click **Service List** and choose **Security & Compliance** > **Data Encryption Workshop**.
3. In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.
4. Check whether the secret is hosted and whether its status is **Enabled**.

How to fix:

1. Log in to the management console.
2. Click **Service List** and choose **Security & Compliance** > **Data Encryption Workshop**.
3. In the navigation pane on the left, choose **Cloud Secret Management Service** > **Secrets**.
4. On the displayed page, click **Create Secret**. In the displayed dialog box, set related parameters.
5. Click **Next**. If an RDS secret is hosted, you can set the rotation period.
6. Click **Next**. Confirm the secret information and click **OK**.

Reference:

https://support.huaweicloud.com/intl/en-us/usermanual-dew/dew_01_9993.html

 Copyright © Huawei Technologies Co., Ltd.

3 Summary

This document provides guidance for you to check and implement the security configuration baseline for Huawei Cloud services, helping you improve your cloud environment's security defense capabilities.

This document is for reference only and does not have any legal effect or constitute legal advice. It is also not a basis for guaranteeing that any customer's cloud environment is secure. You should evaluate your own use of cloud services and supplement or trim this security configuration baseline guide based on your actual needs.

 Copyright © Huawei Technologies Co., Ltd.

4 Change History

Date	Version	Description
April 2024	2.0	Routine update
August 2021	1.0	This issue is the first official release.

 Copyright © Huawei Technologies Co., Ltd.