ModelArts

Security and Compliance

Issue	01
Date	2026-11-25



HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are the property 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.

The 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/intl/en-us/

Contents

1 Shared Responsibilities..... 1
2 Identity Authentication and Access Control..... 3
3 Audit and Logging..... 5
4 Service Resilience..... 7
5 Security Boundaries..... 9

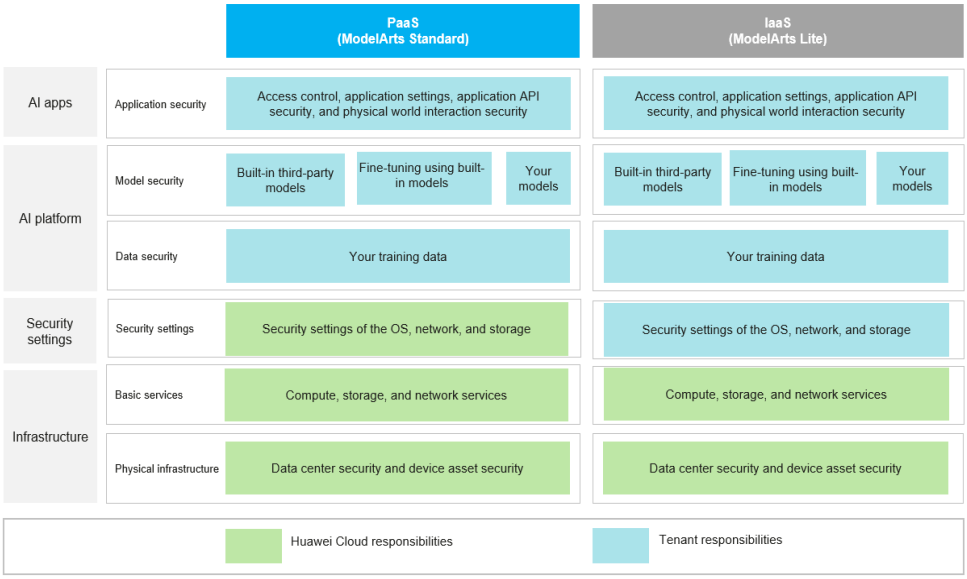
 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

1 Shared Responsibilities

Huawei Cloud ensures that its dedication to cybersecurity will always take precedence over commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 1-1 Huawei Cloud shared security responsibility model



In the preceding model, different responsibilities are assigned at different layers.

- **AI applications**: You can build diverse AI applications like OCR, NLP, or large language models. You need to secure their application's API connections. For applications linked to physical devices, such as smart machines, consider their

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

real-world safety impacts. You bear full responsibility for ensuring this security.

- **AI platform**: The platform refers to ModelArts. It uses models and training data sourced from open communities or supplied by you. You handle your own security measures.
- **Security configuration**: The security configuration and management depends on the resource mode. For ModelArts dedicated resource pools, **Huawei Cloud** handles resources and ensures security. For Lite resources, you manage resources, configure services, and maintain security.
- **Infrastructure**: **Huawei Cloud** data centers manage the security of essential services like compute, storage, network, and their physical infrastructure across all resource modes.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

2 Identity Authentication and Access Control

Identity Authentication

You can use ModelArts services through the console, APIs, or SDKs. Essentially, access requests are sent through ModelArts REST APIs.

ModelArts APIs can be accessed upon successful authentication. Requests sent through the console can be authenticated using tokens, and requests for calling APIs can be authenticated using tokens or AK/SK. For details, see **Authentication**.

Access Control

ModelArts allows you to configure fine-grained permissions for refined management of resources and permissions. To do so, ModelArts provides IAM permission control, agency authorization, and workspace.

- IAM permission control

  To use ModelArts functions, you need to grant permissions through IAM. For example, if you need to create a training job on ModelArts, you must have the **modelarts:trainJob:create** permission.

  If no fine-grained authorization policy is configured for a user created by the administrator, the user has all permissions of ModelArts by default. To control user permissions, the administrator needs to add the user to a user group on IAM and configure fine-grained authorization policies for the user group. In this way, the user obtains the permissions defined in the policies before performing operations on cloud service resources. During policy-based authorization, the administrator can select the authorization scope based on ModelArts resource types. For details about resource permissions, see **Permissions Policies and Supported Actions**.

- Agency authorization

  ModelArts needs to access other services for AI computing. For example, ModelArts needs to access OBS to read your data for training. To ensure security, ModelArts requires your authorization before accessing any cloud services, which is the agency. Then, you can perform AI computing tasks on ModelArts.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

ModelArts does not save your token authentication credentials. Before performing operations on your resources (such as OBS buckets) in a backend job, you are required to explicitly authorize ModelArts through an IAM agency. ModelArts will use the agency to obtain a temporary authentication credential for performing operations on your resources. For details, see **Configuring Agency Authorization for ModelArts with One Click**.

- Workspace

  Workspace allows customers who have enabled **enterprise projects** to divide their resources into multiple logically isolated spaces and control access to different spaces.

  After workspace is enabled, a default workspace is created. All resources you have created are in this workspace. A workspace is like a ModelArts twin. You can switch between workspaces in the upper left corner of the ModelArts console. Jobs in different workspaces do not affect each other. ModelArts allows you to create multiple workspaces to develop algorithms and manage and deploy models for different service objectives. In this way, the development outputs of different applications are managed in different workspaces for use.

Remote Access Management

When you use a local IDE to remotely access the ModelArts notebook development environment through SSH, the key pair is required for authentication.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

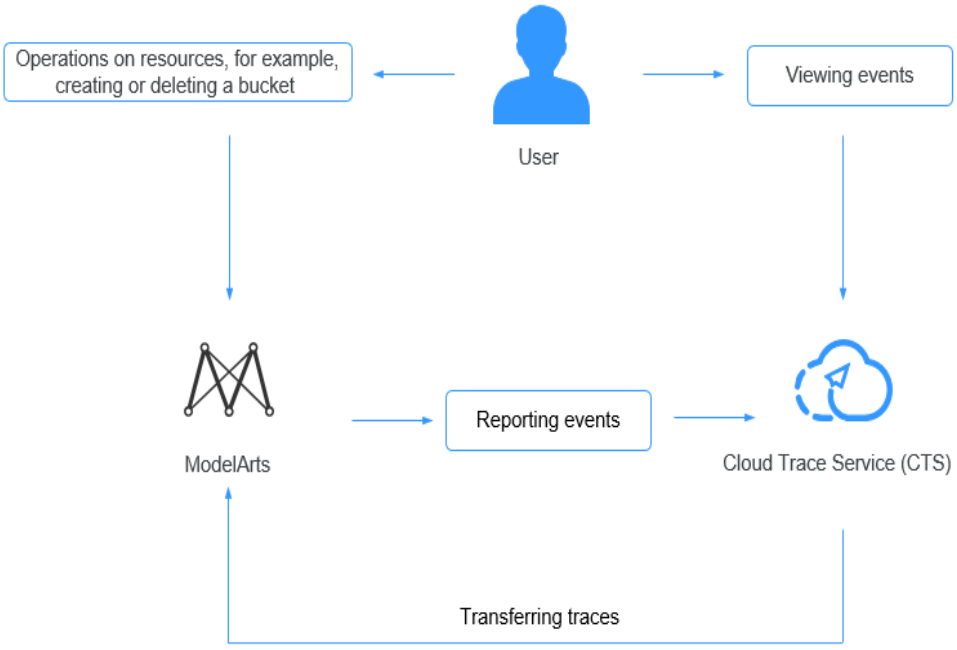
3 Audit and Logging

Auditing

Cloud Trace Service (CTS) records operations on the cloud resources in your account. You can use the logs generated by CTS to perform security analysis, trace resource changes, audit compliance, and locate faults.

After you enable CTS and configure a trace task, CTS can record management and data traces of ModelArts for auditing.

Figure 3-1 CTS



For details about how to enable and configure CTS, see **Enabling CTS**.

For details about the ModelArts events that can be traced by CTS, see the user guide of each module, for example, **Using CTS to Audit Dedicated Resource Pool and Lite Cluster Operations** for resource management.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Log

You can enable ModelArts logging for analysis or audit. After CTS is enabled, CTS starts recording operations on ModelArts. The CTS management console stores the last seven days of operation records. This section describes how to view operation records of the last seven days on the CTS console.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

4 Service Resilience

Resilience refers to security resilience of cloud services after attacks, excluding reliability and availability. This chapter describes ModelArts capabilities of defense and detection against intrusions, defense against jitter, proper use of domain names, and content security detection.

Security Suite and Cloud Bastion Host for Enhanced Defense and Detection Against Intrusions

The security suites ModelArts deployed at the host, application, network, and data layers can timely detect security intrusions.

- ModelArts uses web secure components to prevent web security risks from web applications deployed on it and uses WAF for security protection.
- Host Security Service (HSS) products have been deployed on all hosts that carry ModelArts services. These products include but not limited to Huawei-developed HSS and Compute Security Platform (CSP).
- Vulnerability Scan Service (VSS) has been deployed on ModelArts and performs routine scanning to quickly detect and fix vulnerabilities.
- ModelArts performs security O&M on cloud resources through a security management platform.
- Situation Awareness (SA) has been deployed on ModelArts to understand security situation, query attack histories, and promptly detect compliance risks and respond to threat alarms.
- Advanced Anti-DDoS (AAD) has been deployed on the EIPs that carry key ModelArts services to prevent traffic storms.
- Database Security Service (DBSS) has been deployed on ModelArts databases that store important data.

Jitter Prevention and Emergency Response and Restoration Policies Against Attacks

ModelArts isolates resources of different tenants, so that attacks on a tenant's resources will not affect others' resources.

- ModelArts provides dedicated resource pools that are physically isolated, so that attacks on a tenant's resources will not affect others' resources.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

- ModelArts defines and maintains its performance specifications to defend attacks, for example, by configuring API rate limits.
- ModelArts provides alarm reporting and self-protection against attacks.
- ModelArts detects abnormal service behavior, for example, by detecting abnormal operations platform data and integrating security logs.
- ModelArts provides risk control and emergency response against attacks. For example, ModelArts quickly identifies malicious tenants and malicious IP addresses.
- ModelArts quickly restores services after traffic attacks stop.

Secure Domain Name Usage and Tenant Content Security Policies

ModelArts domain names meet certain security requirements to avoid compliance risks and phishing attacks.

Domain names visible to tenants: domain names accessible to tenants, which require more attention to security and compliance.

Domain names invisible to tenants: Domain names used for internal communication between Huawei Cloud services, where external users cannot access the corresponding authoritative DNS servers; or Internet-restricted domain names that are accessible only to Huawei employees, partners, and contractors in yellow and green zones through Huawei's office network (that is, these domain names are not accessible from the Internet).

- Huawei Cloud base domains are used securely and are not directly assigned to tenants.
- Externally registered and ICP-filed domain names are not used by Huawei Cloud services to call each other on the intranet.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

5 Security Boundaries

The shared responsibility model for cloud services is a collaborative framework in which both the cloud service provider and the cloud service customer jointly assume responsibility for cloud service security and compliance. This model is designed to ensure the overall security, reliability, and trustworthiness of cloud services.

Under the shared responsibility model, each party has clearly defined obligations. The cloud service provider is responsible for managing the underlying cloud infrastructure, delivering secure hardware and software resources, and ensuring the availability of the cloud infrastructure. Cloud service customers are responsible for protecting their data and applications while complying with related compliance requirements.

The providers are responsible for the services and functions and should:

- Establish and maintain secure infrastructure, including networks, servers, and storage devices.
- Provide reliable underlying platforms to ensure runtime security.
- Provide identity authentication and access control to ensure that only authorized users can access the cloud services and tenants are isolated from each other.
- Provide reliable backup and disaster recovery to prevent data loss caused by hardware faults or natural disasters.
- Provide transparent security monitoring and incident response services, timely security updates, and vulnerability patches.

The customers should:

- Encrypt data and applications for confidentiality and integrity.
- Ensure timely security updates and vulnerability fixes for model-related software.
- Comply with relevant compliance requirements, such as GDPR, HIPAA, and PCI DSS.
- Implement proper access control to ensure that only authorized users can access and manage resources such as online services.
- Monitor and report any abnormal activity and take actions in a timely manner.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

Inference Deployment Security Responsibilities

- Providers
  - Fix the patches related to underlying ECSs.
  - Upgrade the K8S and fix vulnerabilities.
  - Operate VM OS lifecycle maintenance.
  - Ensure the security and compliance of the ModelArts inference platform.
  - Improve the security of containerized application services.
  - Upgrade the model runtime environment and fix vulnerabilities periodically.
- Customers
  - Authorize resource use and control access.
  - Ensure the security of applications, its supply chain, and dependencies by security scanning, auditing, and access verification.
  - Minimize permissions and limit credential delivery.
  - Ensure the security of models (custom images, OBS models, and dependencies) during runtime.
  - Update and fix vulnerabilities in a timely manner.
  - Securely store sensitive data such as credentials.

Best Practices for Inference Deployment Security

- External service authorization

  ModelArts inference requires authorization from other cloud services. You can grant only the required permissions based on your needs. For example, you can grant access permission on an OBS bucket to a tenant for model management.
- Internal resource authorization

  ModelArts inference supports fine-grained permission control. You can configure the permissions for users based on the actual needs to restrict the permissions on some resources.
- Model management

  To decouple models from images and protect model assets, you can dynamically import models from trainings or OBS. You need to upgrade the dependency packages of models, and fix vulnerabilities in open-source or third-party packages. Sensitive information related to models needs to be decoupled and configured during real-time service deployment. Select the runtime environment recommended by ModelArts. The earlier environments may have security vulnerabilities.

  You can select open trusted images when creating models using a container image, for example, images from OpenEuler and Ubuntu. Create non-root users rather than root users to run an image. Only the security package required during the runtime is installed in the image. Downsize the image and upgrade the installation package to the latest vulnerability-free version. Decouple sensitive information from images during service deployment. Ensure that it is not hardcoded in the Dockerfile directly. Perform security scanning on images periodically and install patches to fix vulnerabilities. To facilitate alarm reporting and fault rectification, add health check interface

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.

and ensure that the service status can be returned properly. To ensure the service data security, use HTTPS transmission streams and reliable encryption suites for containers.

- Model deployment

  To prevent services from being overloaded or wasted, set proper compute node specifications during deployment. Avoid listening on other ports within the container. If internal local access is required, bind those ports to **localhost**. Do not directly transfer sensitive information through environment variables. Encrypt sensitive information with encryption component before data transmission.

  App authentication key is an access credential for real-time services. You must keep the app key properly.

ModelArts Security Hardening

ModelArts secures its platform and user services by applying security enhancements to both public pools and dedicated pools. These measures include:

- SSH access restriction: By default, containers are prevented from accessing port 22.
- Host NFS service access restriction: By default, containers are blocked from accessing ports 20048 and 2049.
- Kubernetes API Server access restriction: By default, containers are blocked from accessing port 10250.
- VXLAN protocol port restriction: By default, containers are blocked from accessing port 4789.
- OpenStack management address access restriction: By default, containers are blocked from accessing 169.254.169.254.

 Copyright © Huawei Cloud Computing Technologies Co., Ltd.