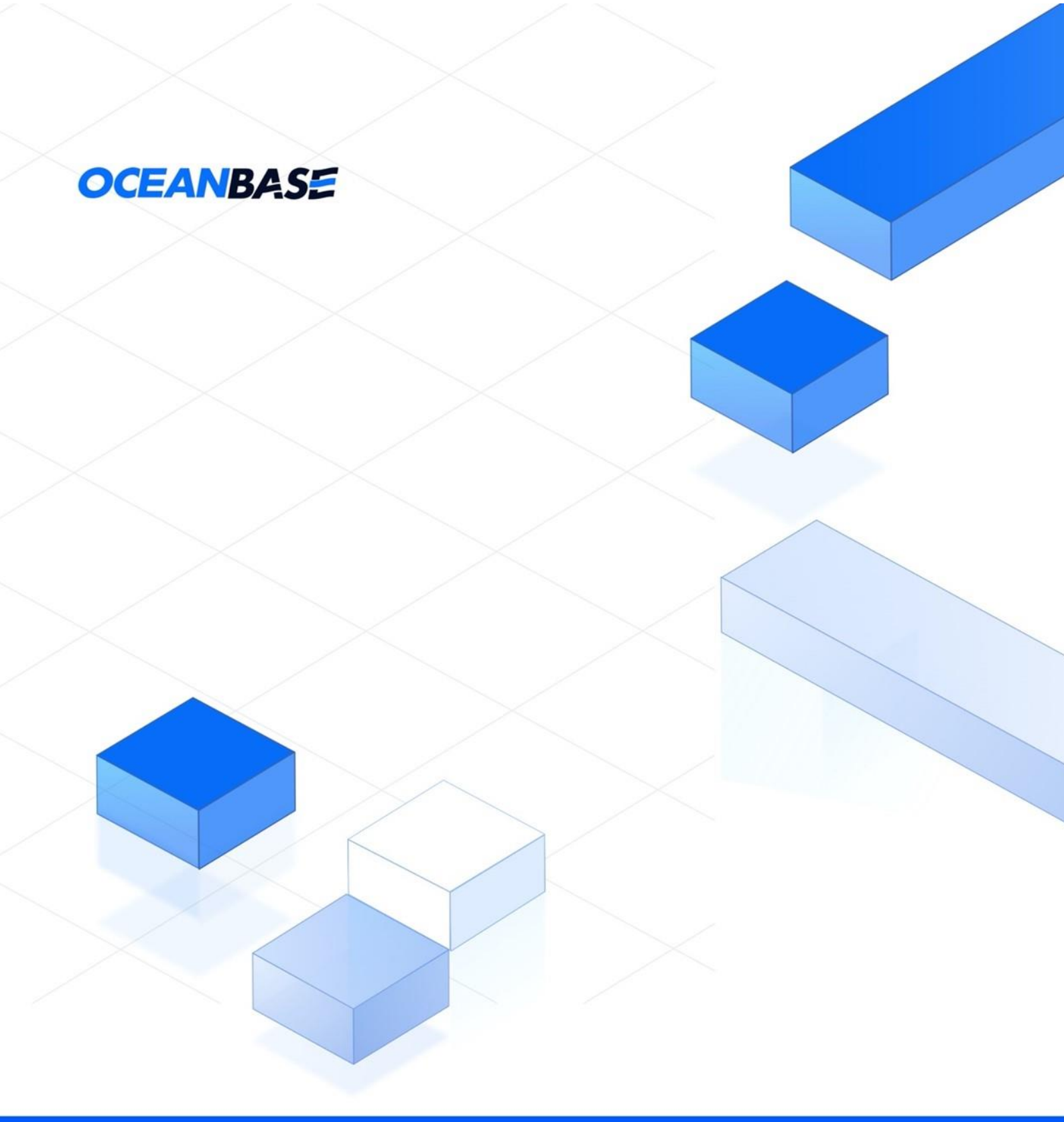


OceanBase Cloud Shared Responsibility Model

Version V1.0

Dec 1, 2025

Preface

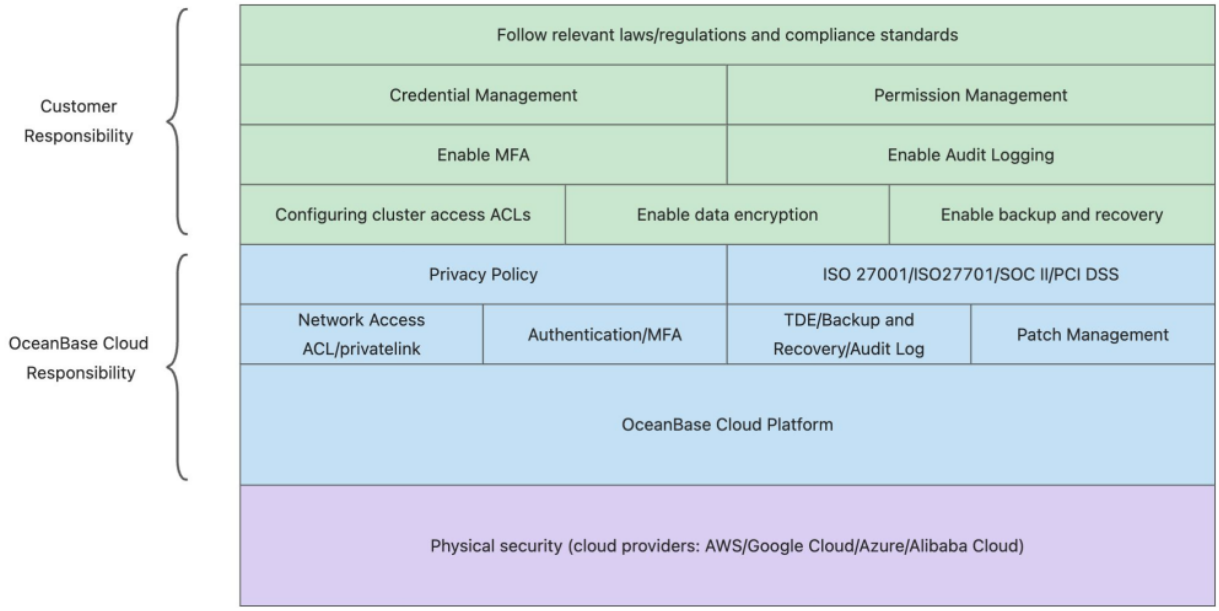
> This document provides an overview of OceanBase Cloud's shared responsibility model. For a detailed understanding of OceanBase Cloud's security mechanisms, please refer to the official OceanBase Cloud documentation. OceanBase Cloud is committed to working with you to build a secure cloud data infrastructure.

OceanBase Cloud is a fully managed Database-as-a-Service (DBaaS) built on the distributed architecture of OceanBase Database. By using OceanBase Cloud, you can easily deploy and manage your OceanBase database cluster and enjoy a flexible and efficient data management experience.

In the data era, we not only face rapidly changing business needs but also must address increasingly complex security threats. The security and compliance of DBaaS services are a shared responsibility between customers and cloud service providers. OceanBase cloud is dedicated to helping customers focus on application development and business needs, and reducing their operational burden. Before using OceanBase Cloud services, customers should understand their security responsibilities and have a full understanding of the security features provided by OceanBase Cloud to build a data environment that is both efficient and secure.

1. Large diagram of the shared responsibility model

As shown in the diagram below, OceanBase, based on a shared responsibility model, works hand-in-hand with customers through multi-layered security mechanisms to address potential security challenges:



OceanBase Cloud is responsible for the underlying platform security.

- OceanBase Cloud is responsible for protecting the security of infrastructure from the SaaS control console to the underlying hosts and networks, and provides necessary security features to customers.

Customers are responsible for securing their data and configurations within the service.

- As cloud service users, customers are responsible for managing the internal resources and configurations of the SaaS service and fulfilling their security management responsibilities for the SaaS service, including but not limited to：
    - Manage accounts, credentials, and permissions used to access OceanBase Cloud resources.
    - Choose a suitable cloud service provider and its geographical location based on your own business needs to deploy your database cluster.

- Configure strict network access control lists (ACLs) to restrict connection requests to only specific IP addresses or subnets.
- Enable multi-factor authentication (MFA) to prevent unauthorized login attempts；
- Configure the audit log recording policy.
- .....

2. Shared responsibility model breakdown

Technology Domain	OceanBase Cloud Responsibility	Customer Responsibility
Privacy	OceanBase Cloud will provide transparency in the collection and processing of customer personal information, such as providing the OceanBase Cloud Privacy Policy, a list of subprocessors and affiliates, and will process customer-provided personal information in accordance with the OceanBase Cloud Privacy Policy.	Customers should manage their data in accordance with the relevant laws and regulations of their location.
Compliance	The OceanBase Cloud platform has passed multiple compliance certifications, such as ISO 27001, SOC2, and PCI DSS, and therefore can serve as a data foundation to support customers' compliance requirements.	Customers should comply with relevant compliance requirements and enable and configure the security features of OceanBase Cloud.
Data Security	OceanBase Cloud supports TDE-based encryption for cluster static data. OceanBase Cloud supports TLS-based encryption for cluster data transmission. OceanBase Cloud supports database operation audit logs. OceanBase Cloud supports backup and recovery.	Customers should set the minimum TLS version to ensure strong encryption during transmission and avoid security risks introduced by outdated protocols and cipher suites. TDE static data encryption is not enabled by default; customers should enable it as needed based on their business requirements. The audit log function is not enabled by default; customers should enable

		it as needed based on their business requirements. When using backup and recovery, customers should configure appropriate backup strategies based on their actual business scenarios. When using remote backup, customers should comply with relevant regulations to avoid compliance risks such as cross-border data transfer.
Identity Security	OceanBase Cloud supports management console access logs. OceanBase Cloud supports management console MFA. OceanBase Cloud supports authentication for cluster access. OceanBase Cloud supports cluster access logs.	Customers should properly safeguard their console and database access credentials and rotate them periodically. Customers should enable cluster access audit logs and audit cluster access behavior regularly. Customers should enable MFA for console accounts to restrict unauthorized access.
Network Security	OceanBase Cloud is highly integrated with cloud service provider networks, for example, it supports private links. OceanBase Cloud provides network access control capabilities, supporting tenant-level network ACLs.	Customers should use features such as private links to access the database cluster from the cloud service provider's internal network, avoiding exposure of the cluster access endpoints to the public network. Customers should configure network ACLs for the cluster to restrict

		unauthorized access from illegal network segments.
Host Security	OceanBase Cloud is responsible for host security, such as managing and updating critical security patches for the operating system.	Not involved.
Cloud Infrastructure Security	The physical security of OceanBase Cloud's underlying infrastructure is guaranteed by the cloud service provider.	Customers should choose appropriate cloud service providers and availability zones to meet their business needs and compliance requirements.