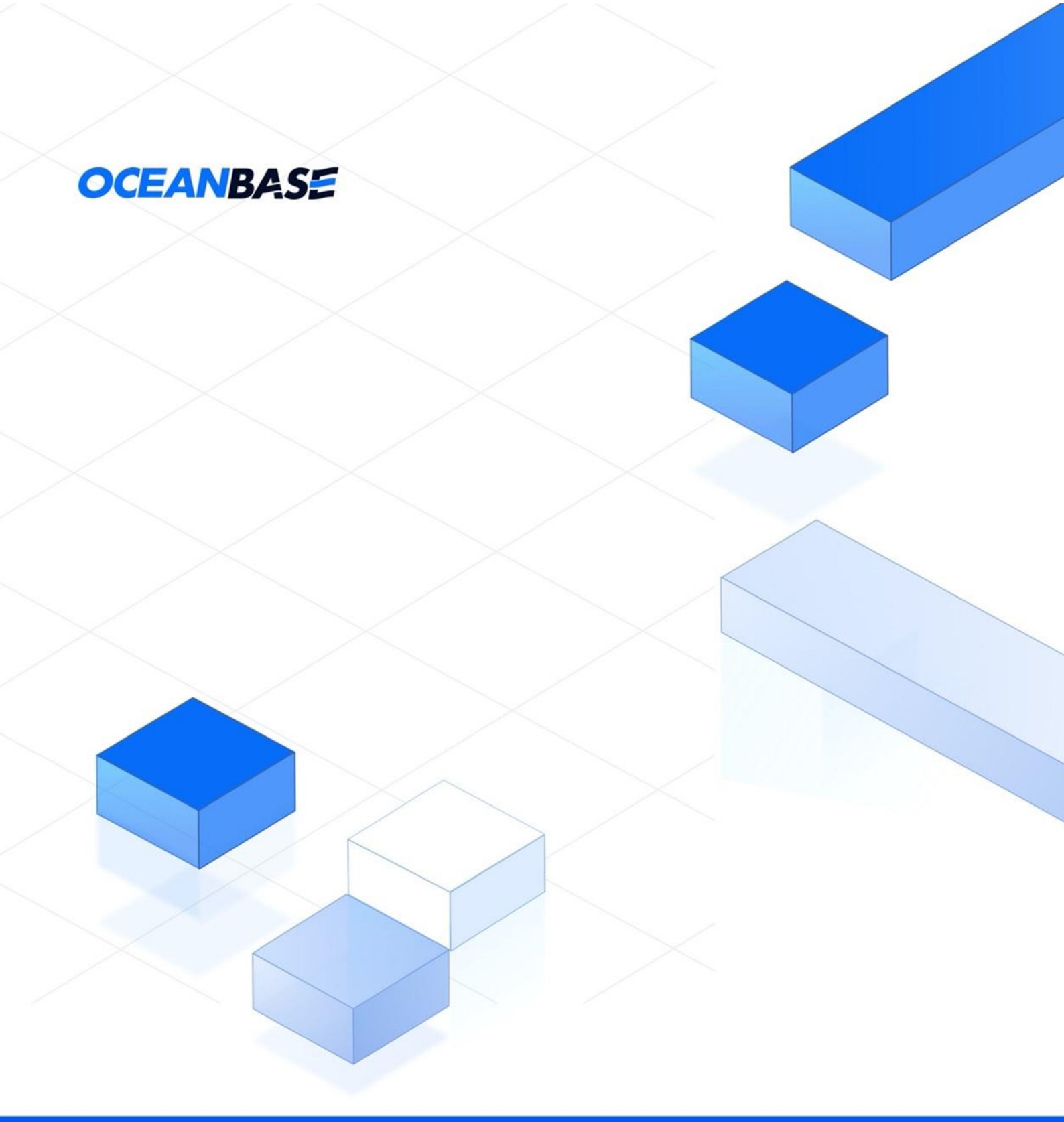


OceanBase Cloud Security Whitepaper

Version V1.0

Dec 1, 2025

Preface

In the wave of digital transformation, as data becomes a core asset driving business innovation and decision-making, its security is increasingly important. Databases are the infrastructure carrying core enterprise data, and their security directly determines the stability of an enterprise's digital assets. Especially in cloud architectures, where data migrates from local, closed environments to the open, shared cloud, building a comprehensive, multi-layered security protection system has become a critical challenge that enterprises must overcome when migrating to the cloud.

Addressing this challenge requires both continuous improvement in technical architecture and security capabilities from cloud database service providers, and proactive action from enterprise users in areas such as access control and data governance. Only through collaboration between vendors and users can a truly robust security defense for cloud databases be established. As a pioneer in the cloud database field, OceanBase Cloud has always considered security a core issue in technological development. Through years of technological accumulation and practical verification, we have built a multi-layered, comprehensive security protection system covering the entire product lifecycle, providing enterprises with a reliable cloud data foundation.

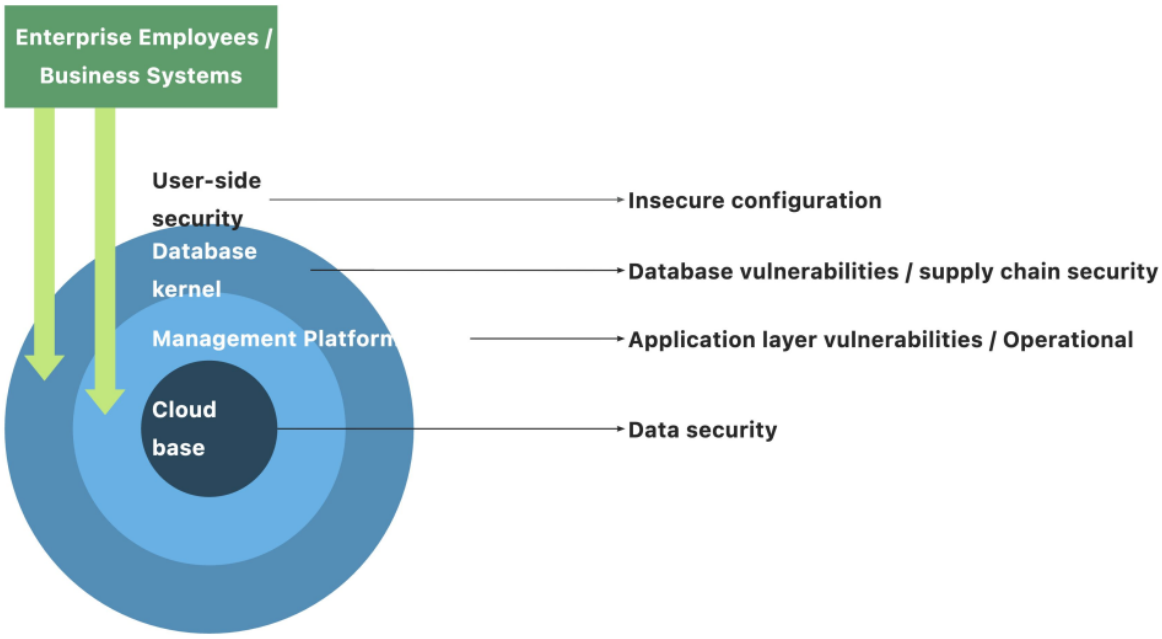
This white paper aims to systematically explain OceanBase Cloud's understanding of cloud database security and comprehensively demonstrate the core capabilities of its security system. We look forward to working with our users to jointly build a secure, efficient, and self-controllable cloud data ecosystem, safeguarding enterprise data migration to the cloud.

This white paper contains the following chapters：

- Chapter 1: Cloud Database Security Challenges: This chapter will briefly introduce the security threats and challenges faced by cloud databases
- Chapter 2: Security Protection System: This chapter will provide an overview of the security protection system for OceanBase Cloud Databases
- Chapter 3: Product Security Features: This chapter will introduce you to the security features supported by OceanBase Cloud Database
- Chapter 4: Multi-Cloud Security Capabilities: This chapter will introduce you to the multi-cloud security capabilities and advantages of OceanBase Cloud Database
- Chapter 5: Shared Responsibility Model: This chapter will guide you through understanding the shared responsibility model of OceanBase Cloud Database

- Chapter 6: Compliance Qualifications: This chapter will help you quickly understand the compliance qualifications of OceanBase Cloud Database

1. Cloud Database Security Challenges



1.1. Cloud Base Security

After databases are migrated to the cloud, the data storage medium changes from a company's private, exclusive physical media to shared storage resources provided by cloud service providers. This shared model increases the possibility of data leakage, tampering, or misuse.

Data isolation challenges

Cloud database instances typically run on shared virtualization infrastructure (such as virtual machines, containers, and shared storage). If the isolation mechanism of a cloud database is flawed, malicious attackers may be able to breach the isolation mechanism and compromise user data security.

Data erasure challenge

Businesses may temporarily upload sensitive data (such as financial information and intellectual property) to the cloud for processing or analysis due to business needs. After the task is completed, the data must be thoroughly erased to eliminate potential risks. However, if the cloud database lacks the ability to completely erase data, it may lead to the leakage of sensitive data.

Data sovereignty and compliance risks

Data sovereignty refers to the fact that the physical storage location and jurisdiction of data are bound by the laws of the jurisdiction in which it is located. If users need to deploy their businesses globally, cloud databases should offer flexible deployment location options and help mitigate related compliance risks:

1. Regional compliance conflicts: Different countries/regions have significantly different requirements for data storage and cross-border transfers (e.g., EU GDPR, China's Data Security Law). If data storage locations do not comply with local regulations, it may result in hefty fines or business disruptions.

2. Mandatory data localization: Some countries require that certain types of data (such as citizens' personal information) must be stored within their borders. If a cloud database does not provide localized nodes, it may directly lead to business non-compliance.

3. Cross-border data flow restrictions: Cloud databases, by clearly defining data flow directions, prevent accidental data transmission to restricted areas due to cross-regional data synchronization.

1.2. Management Platform Security

Cloud databases provide instance services to all tenants through an internet-facing management platform. This management platform is essentially a typical internet system consisting of a "front-end website + back-end service + operation and maintenance management," and therefore faces the same security challenges as internet applications.

Application security vulnerabilities

The management and control platform is extremely complex. If the vendor's technical capabilities are insufficient, there is a high possibility of serious application-layer security vulnerabilities, such as allowing third parties or hackers to maliciously manipulate tenant instances without authorization, leading to catastrophic consequences.

Operation and maintenance security risks

If the operation and maintenance security management of the control platform is not implemented maturely or in a standardized manner, it may lead to security problems：

1. Operations and maintenance channel leakage: If the access control platform's access channel to the database is not properly managed, it may be abused by unauthorized individuals, leading to the leakage of sensitive data.

2. Insider Risk: Incomplete audit logs on the control platform could lead to user data leakage or tampering if insiders act maliciously or negligently.

3. Reliance on third-party tools: Monitoring, backup, and other tools used by the management platform may indirectly expose user data, and it is necessary to ensure that they comply with data security policies.

Cross-cloud security risks

The management and control platform is built on multiple clouds, which means it needs to directly address the security risks brought about by cross-cloud environments, such as...

1. Cloud service providers have different service configurations, and it is necessary to follow the corresponding security best practices. Inappropriate or conflicting configurations may introduce security risks

2. It is necessary to ensure end-to-end security of cross-cloud call links to prevent attackers from using this to breach the originally isolated cloud environment boundaries, or even to amplify the impact of attacks by exploiting the trust relationships between cross-cloud services

1.3. Database Security

Databases are complex systems and inevitably contain security vulnerabilities. In traditional networks, databases reside in the core business network segment, making them difficult for attackers to access. However, cloud databases, in order to support flexible business needs, may expose database access ports to the public internet, which exacerbates the potential risks of security vulnerabilities.

Database protocol vulnerability

During the development of databases, design and implementation flaws may introduce security vulnerabilities. For cloud databases, users may expose their database services to the public internet. If there are no network ACL restrictions and the database has protocol-level vulnerabilities, these vulnerabilities could be exploited, leading to service unavailability, data leaks, and other security risks.

Supply chain security risks

Databases inevitably rely on third-party components, and vulnerabilities in these components can compromise database security. If cloud database service providers lack the technical capabilities and security controls, the risks associated with third-party components may accumulate over time, potentially leading to the introduction of components with backdoors and resulting in major security incidents.

1.4. User-side Security

If user-side R&D and operations personnel fail to use cloud databases securely, it could also lead to significant security risks. Such issues exist in traditional network environments, but in open, shared cloud environments, these risks may be amplified.

Clear data transmission

In traditional on-premises deployments, databases and clients typically communicate via the enterprise intranet, a relatively closed network environment with a relatively low risk of clear data transmission. However, in cloud environments, data transmission paths may traverse shared links in cloud infrastructure (such as virtualized network devices or public internet channels). If transmitted in clear mode, this poses a risk of data leakage.

Identity credential management

Users need to manage a large number of authentication credentials when using cloud databases, including accounts on the cloud management console and accounts within the database. If relevant personnel lack security awareness and configure weak passwords or use generic passwords, the account and password system may be compromised by malicious attackers, leading to serious security incidents such as access control breaches and data leaks.

Inadequate access control

Users of cloud databases may face complex access control issues. These include managing maintenance and auditing permissions on the management platform, assigning control permissions to multiple business units within an enterprise, resolving complex personnel authorization relationships between business units, managing permissions within the database instance, ensuring proper isolation between different business units, and controlling network access permissions for the database. Improper access control configuration can lead to excessive privileges for internal personnel, or even unauthorized access and other security problems.

2. Security Protection System

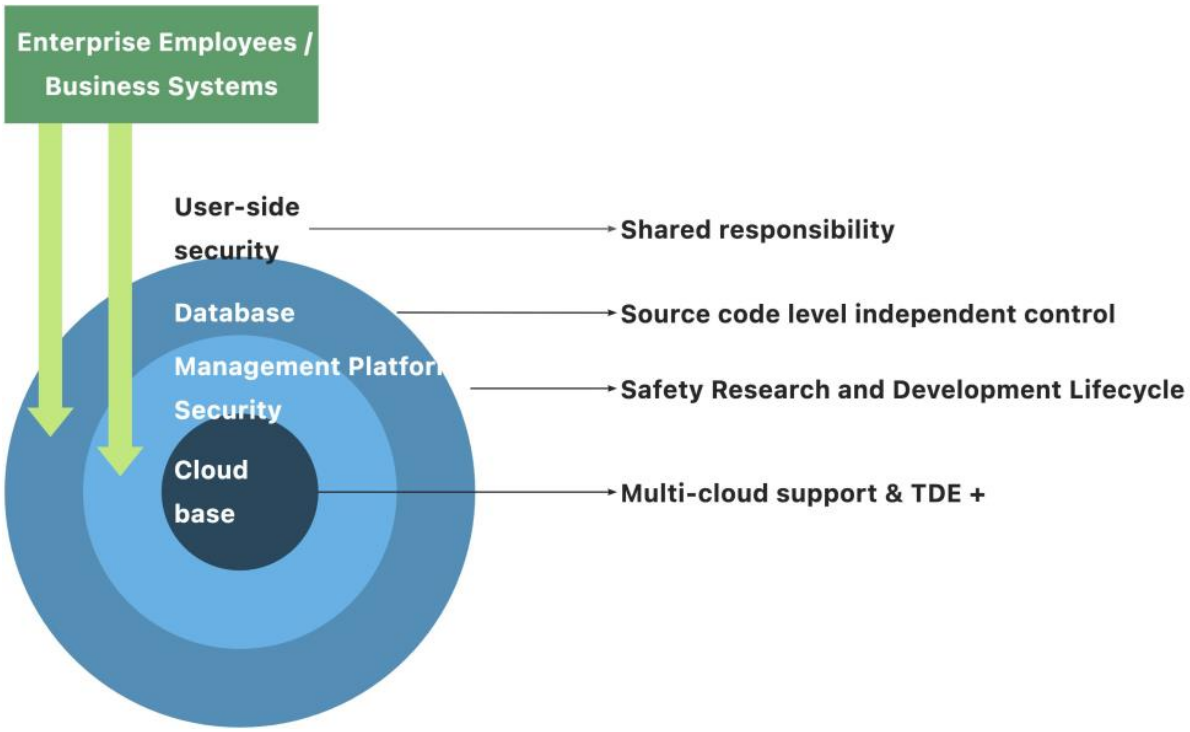
2.1. Cloud Database Security Objectives

Before explaining OceanBase Cloud's security protection system, it's necessary to first clarify the core objectives of cloud database security. There's a fundamental consensus in the security field: no system can achieve absolute security. Therefore, the goal of cloud database security construction is not to pursue an unattainable "zero risk.".

Looking back at the development of databases, migrating databases to the cloud is an inevitable trend in technological evolution, and its value lies in three dimensions: economy (reducing hardware investment and operation and maintenance costs), flexibility (achieving elastic scaling of resources), and openness (building an interconnected service ecosystem). The underlying support for these advantages comes precisely from the open and shared technical characteristics of cloud computing. However, while this openness creates value, it also brings new security challenges. Problems that do not exist or have limited impact in traditional closed environments are introduced and amplified in the cloud, becoming security threats and challenges to cloud databases.

The value of security lies in safeguarding the ever-evolving technologies and business models. Therefore, we believe that the goal of cloud database security is to address the security issues that arise during the cloud migration process, enabling cloud databases to achieve a level of security comparable to or even higher than that of traditional databases.

2.2. Multi-level Security Protection System



2.2.1. Multi-cloud Support & BYOK

OceanBase Cloud database is built on mainstream public clouds (currently supporting AWS, GCP, Alibaba Cloud, Tencent Cloud, and Huawei Cloud). OceanBase Cloud's underlying data isolation and data erasure capabilities are guaranteed by the public cloud service providers. OceanBase Cloud supports deployment of clusters in multiple international and regional locations globally, allowing users to choose suitable cloud service providers and regions to meet compliance requirements for business data sovereignty. Furthermore, OceanBase Cloud supports TDE transparent encryption and BYOK (Bring Your Own Key) capabilities. After enabling TDE and completing root key escrow, users can ensure that all data stored on disk is encrypted, and root key access behavior is auditable, further guaranteeing user data security.

2.2.2. Safety Research and Development Lifecycle (SDLC)

OceanBase Cloud's cloud database development process adheres to a complete security development lifecycle, with security involvement at every stage: requirements gathering, design, development, testing, and release. OceanBase Cloud values communication and collaboration with the security community, regularly conducting crowdsourced testing projects and continuously receiving threat intelligence and security vulnerabilities contributed by white-hat security researchers.

Security risks discovered internally and externally are handled in a closed-loop manner by the security team, ensuring the security and reliability of the product throughout its entire lifecycle. Furthermore, OceanBase Cloud has strict access control and behavior auditing for access to the product's production environment. Internal technical personnel have only limited access permissions, and during online fault handling, access to user business tenants requires user authorization.

2.2.3. Source Code Level Independent Control

OceanBase Cloud's cloud database uses the OceanBase database kernel, with all code independently developed. All upstream third-party components are open-source, giving OceanBase full source-code control over the database kernel. OceanBase Cloud development process incorporated industry-leading source-code-level security solutions and supply chain threat intelligence. All kernel code changes and component version changes undergo security scanning, ensuring a high level of supply chain security for the product.

2.2.4. Shared Responsibility Model

Ensuring the security of OceanBase Cloud databases requires a collaborative effort between users and us. OceanBase Cloud provides security capabilities such as multi-factor authentication, a multi-level authentication system, transparent encryption, audit logs, network ACLs, and backup and recovery to help customers build secure data infrastructure. In subsequent chapters, we will introduce OceanBase Cloud's shared responsibility model to help users understand the areas they need to focus on for secure use of OceanBase Cloud. We will also release OceanBase Cloud security best practices in the future, providing users with more detailed security guidance for using OceanBase Cloud.

3. Product Security Features

3.1. Certification

3.1.1. Cryptography Policy

OceanBase Cloud Control Console employs an account-password-based authentication method. To address inherent risks such as weak passwords, password leaks, and brute-force attacks, the product strictly adheres to international compliance standards such as Cybersecurity Classified Protection, ISO 27001, and PCI DSS, and has established a robust password strategy. First, OceanBase Cloud Control Console verifies password strength when users set their passwords, requiring them to contain a combination of uppercase and lowercase letters, numbers, and special symbols, and to be at least 8 characters long, to mitigate the risk of weak passwords. Second, the control console notifies users to rotate their passwords every 90 days and prohibits the repetition of the last 5 passwords to reduce the risk of password leaks. This mechanism complies with the dynamic password update requirements of standards such as PCI DSS. Furthermore, OceanBase Cloud Control Console has built-in anti-brute-force capabilities; when an account is detected to have failed login attempts exceeding a certain limit, the account will be locked to prevent malicious brute-force attacks.

3.1.2. Multi-factor Authentication

Multi-Factor Authentication (MFA) effectively enhances the OceanBase Cloud management platform's ability to resist attacks such as credential stuffing and account scanning by combining two or more independent verification factors. Credential stuffing attacks reuse leaked account passwords from other platforms, while account scanning attacks use automated tools to mass-produce common accounts and weak passwords. Both pose a persistent threat to management platforms exposed to the public internet. MFA effectively reduces the risk of account hijacking through a dual verification mechanism of knowledge factors (such as user passwords) and possession factors (such as time-synchronized one-time passwords, TOTPs).

Specifically, OceanBase Cloud uses the TOTP protocol to implement holding factor verification. When a user first enables MFA, they can scan a QR code generated by the server using an authentication application that supports the TOTP protocol (such as Google Authenticator) to complete the initial negotiation of the encrypted shared key. Afterward, the user's device and the server maintain time synchronization via the NTP protocol, independently calculating and generating a 6-digit dynamic verification code every 30 seconds based on the preset shared key and the current timestamp using

the HMAC-SHA algorithm. Upon login, the user must sequentially enter their account password (knowledge factor) and the currently valid dynamic verification code (holding factor). The server verifies the validity of the dynamic verification code using a preset time error window (e.g., ±1 minute). Even if an attacker intercepts historical passwords or network traffic, they cannot reverse-engineer a valid verification code due to the lack of the shared key. This mechanism, through the short validity period (valid only for 30 seconds) and unpredictability of dynamic passwords, constructs a dual technical barrier against credential stuffing and account scanning attacks.

3.2. Authentication

3.2.1. Control Console Access Control System

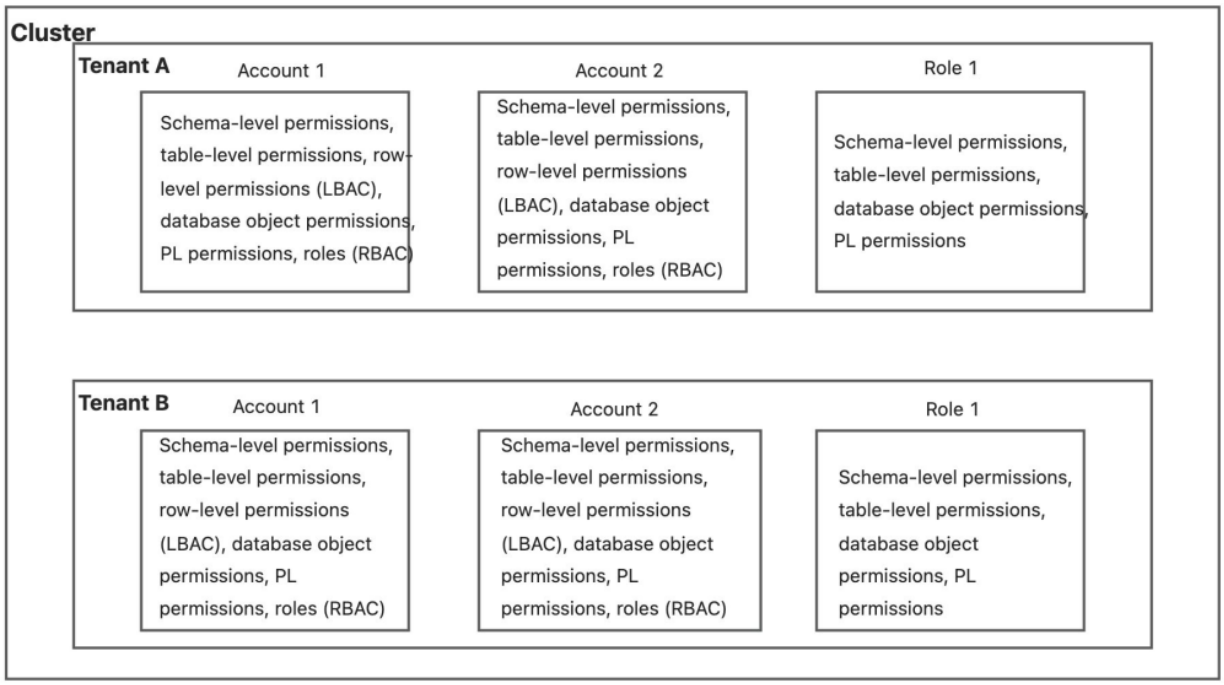
As a cloud database management platform, OceanBase Cloud needs to meet the permission management requirements of enterprises for database operation and maintenance. For example, how to assign management permissions to multiple business units within an enterprise, how to ensure isolation between different business units, and how to resolve complex personnel authorization relationships between business units. To address this, OceanBase Cloud has designed a four level permission management system: "Organization, Project, Member, Role," constructing a refined business isolation and permission control mechanism.

This system uses the organization as the top level unit, pre-setting roles such as organization administrator (the sole owner with the highest authority) and expense administrator within the organization to separate resource and financial management. Secondly, it uses projects as business units, supporting cross-project affiliation for members. Each project independently manages cluster resources and operational permissions. Project owners can assign roles such as project administrator and instance administrator, ensuring strict isolation between resource operations and business boundaries. Members, as the carriers of permissions, achieve dynamic mapping and on-demand allocation of "member-role-permission" by binding roles within the organization or project (e.g., instance administrators have read-write permissions for instances, while project members only have read-only permissions). For example, the expense administrator role only has access to the expense center, while instance administrators have operational permissions for instances within the project.

This hierarchical design not only satisfies the need for fine-grained access control in multi-service parallel scenarios, but also reduces user authorization and maintenance costs through a role-based access control (RBAC) model. Furthermore, the resource logical isolation mechanism between organizations and projects ensures that data and operations between different business units are not visible to each other, further strengthening enterprise-level security control capabilities.

3.2.2. Cluster Access Control

OceanBase Cloud leverages the OceanBase distributed database to achieve cluster-level access control. OceanBase natively supports multi-tenancy and implements tenant-level data and resource isolation, effectively enabling data isolation across multiple application scenarios. OceanBase is compatible with both MySQL and Oracle permission models and supports role-based and tag-based access control models, as well as permission management about PL. The OceanBase Cloud management console encapsulates the database kernel's permission management capabilities, allowing users to easily implement common permission configuration requirements, such as implementing a three-tiered account system.



3.3. encryption

3.3.1. Encrypted Transmission

In traditional database applications, network communication between the client and the database typically occurs via an intranet connection, with external network access relying on dedicated network tunnels such as VPNs. Security primarily depends on physical network isolation and dedicated encrypted tunnels. However, in cloud database environments, data transmission paths may traverse shared links within the cloud infrastructure, posing a risk of data packet eavesdropping and tampering. Furthermore, cloud platforms often allow database instances to be bound to public IP addresses. DBAs, for convenience, may directly access the database via the public network for daily

management. In this case, client-database communication will directly pass through the public network, further amplifying the security risks during data transmission. OceanBase Cloud cloud databases utilize SSL/TLS encryption technology to ensure secure communication between the client and server. Users can easily enable SSL encryption in the management console, with the system automatically generating certificates and supporting configuration of mandatory SSL connections to ensure the confidentiality and integrity of data transmission. OceanBase Cloud also provides a certificate rotation mechanism, allowing users to manually refresh or set automatic certificate renewal cycles to avoid risks caused by expired or leaked certificates.

3.3.2. Static Encryption

In cloud database environments, data is more vulnerable to leakage due to the reliance on shared infrastructure of public clouds for computation, table data storage, and backup. Therefore, encryption technology becomes a core means of ensuring data security. OceanBase Cloud supports Transparent Data Encryption (TDE), where the database kernel automatically encrypts static data on the storage medium, providing seamless data protection for users. Even if the underlying service is attacked or the storage medium is illegally accessed, attackers can only obtain ciphertext data that cannot be deciphered. OceanBase Cloud's encryption system employs a two-level key architecture, storing data keys in encrypted form. This ensures the security of the keys themselves while supporting an efficient key rotation mechanism, further reducing the risk of key leakage. Furthermore, the system is compatible with mainstream international encryption algorithms such as AES128, AES192, and AES256.

3.4. audit

3.4.1. Console Auditing

Auditing capabilities are a crucial component of enterprise security capabilities. OceanBase Cloud provides auditing capabilities for historical operation events on the console, comprehensively recording user actions performed in the management interface, covering critical events such as account permission modifications, cluster configuration changes, tenant resource adjustments, database object management, and database login behavior. Each audit log records the event type, operation details, execution time, user, and execution result (success/failure) in a standardized format, and the audit logs are highly reliable and tamper-proof. Furthermore, leveraging the permission system of the OceanBase Cloud management console, access permissions for audit logs are restricted for different roles, ensuring the isolation and security of audit information. Authorized administrators can quickly filter audit logs in the management console by multiple dimensions such

as time range, operation object, and execution result, meeting the requirements of internal audit forensics and external compliance reviews.

3.4.2. SQL Auditing

OceanBase Cloud also provides tenant-level SQL auditing capabilities, enabling precise monitoring of specific operations (such as DDL structure changes, sensitive table DML operations, and permission granting statements) through predefined rules. It automatically parses the syntax tree during SQL execution, extracting metadata such as the operation object, the number of affected rows, the executing user, and the client IP, generating audit logs independent of the transaction state (retaining traces even after transaction rollback). This allows for end-to-end monitoring of database DML/DDL operations, permission changes, and other behaviors.

OceanBase Cloud management console provides real-time retrieval and one-click export capabilities for SQL audit logs. To balance storage costs and audit requirements, OceanBase innovatively adopts a hot-cold tiered storage strategy, optimizing resource costs while ensuring the availability of audit data. SQL execution records support storage for up to 720 days. Users can configure the hot storage duration, retaining SQL audit logs that require frequent analysis in the short term, meeting the needs of rapid troubleshooting and analysis in daily operations and avoiding performance degradation caused by full log retrieval. After the log storage time exceeds the hot storage duration, OceanBase Cloud automatically converts the SQL audit logs to cold storage, retaining complete records while reducing storage overhead. This is suitable for low-frequency access scenarios such as compliance auditing and traceability evidence collection, reducing long-term storage costs.

4. Multi-cloud Security Capabilities

4.1. CSPM & CMDB

To address the configuration differences and potential security risks across cloud service providers in multi-cloud environments, OceanBase Cloud has independently developed two core systems: the Cloud Security Posture Management (CSPM) platform and the Configuration Management Database (CMDB). Based on industry best security practices, this solution achieves comprehensive security posture awareness and risk control in complex multi-cloud environments, effectively safeguarding cloud infrastructure and data assets.

OceanBase Cloud's self-developed CSPM system features asset discovery and classification, continuous security monitoring, and intelligent risk identification. Through automated detection technology, it achieves real-time discovery and intelligent classification of OceanBase Cloud multi-cloud assets, establishing a complete asset inventory. A real-time monitoring mechanism provides 24/7 uninterrupted security monitoring of all OceanBase Cloud environments, ensuring continuous visibility of the security posture. Based on preset security baselines, it periodically performs deep security checks to accurately identify security risks, including but not limited to high-risk port openings on cloud hosts and improper permission configurations.

On the other hand, the OceanBase Cloud CMDB system addresses the unique asset management challenges of multi-cloud environments by implementing unified configuration management, intelligent topology visualization, and other security features. The OceanBase Cloud CMDB system uses a structured data model to store various cloud resource configuration attributes, covering key security elements such as network configuration parameters, storage configurations, and access control policies. Simultaneously, it constructs a multi-cloud network topology map through automated discovery technology, intuitively presenting the relationships between resources and data flows, providing a visual analysis foundation for architecture risk assessment.

4.2. Cross-cloud Data Security

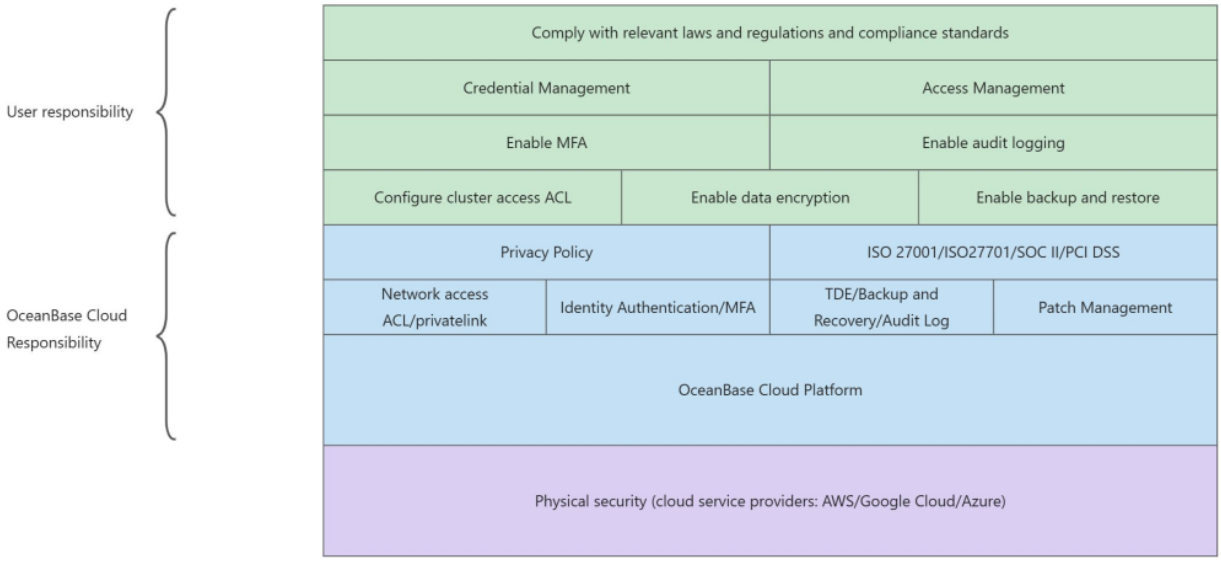
Some OceanBase Cloud product features involve cross-cloud data transmission and storage, such as cross-cloud primary/standby databases and cross-cloud bidirectional synchronization based on OMS. To ensure the security of cross-cloud data itself and compliance security, OceanBase Cloud has independently developed cross-cloud tunneling technology based on TLS and network access

control, ensuring end-to-end data encryption and security throughout the entire cross-cloud communication chain.

Currently, OceanBase Cloud has launched services in 27 countries/regions, allowing users to choose the region for data storage as needed, ensuring compliance and data security requirements are met. Furthermore, as an independent third-party platform, OceanBase Cloud supports flexible selection among multiple cloud vendors and supports TDE transparent encryption and BYOK (Bring Your Own Key) capabilities. After enabling TDE and completing root key hosting, users can ensure that all data stored on disk is encrypted, and root key access behavior is auditable, further guaranteeing user data security.

5. Shared Responsibility Model

Ensuring the security of cloud database services is a shared responsibility between cloud service providers and customers. OceanBase Cloud is committed to maximizing this responsibility, helping customers focus on application development and business needs while reducing their operational burden. OceanBase Cloud takes full responsibility for the security construction of infrastructure, from hosts and networks to the cloud database management platform, building a multi-layered protection system covering the cloud foundation, management platform, and database. Meanwhile, customers need to focus on internal security management, including but not limited to: rationally planning the deployment areas of database clusters to meet data sovereignty requirements, strictly implementing account credentials and access control, enabling multi-factor authentication, finely configuring network access control policies, and enabling audit log monitoring. We recommend that users, based on a full understanding of the security capabilities provided by OceanBase Cloud, implement security practices tailored to their own business needs to jointly create a secure, reliable, and efficient cloud database environment.



OceanBase Cloud database is responsible for the security of the service itself

OceanBase Cloud's cloud database is responsible for protecting the security of infrastructure from the cloud service control console to the underlying hosts and networks, and provides necessary security features to customers.

The client is responsible for "internal security of the service"

As cloud service users, customers are responsible for managing the internal resources and configurations of the cloud service and fulfilling their security management responsibilities for the cloud service, including but not limited to..：

- Manage accounts, credentials, and permissions used to access OceanBase Cloud cloud database 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；
- Enable audit logging and configure audit policies；

6. Compliance Qualifications

6.1. ISO 27001

ISO 27001 specifies best practices for the establishment and implementation of Information Security Management Systems (ISMS). OceanBase has implemented comprehensive management of its physical security, network security, and data security. OceanBase invited the British Standards Institution (BSI) to audit its information security management system and received certification.

6.2. ISO 27701

ISO 27701 is a management system for privacy data protection, serving as a guide for establishing, implementing, maintaining, and continually improving a Privacy Information Management System (PIMS). As the data controller, OceanBase complies with relevant laws and regulations regarding the collection, use, and storage of personally identifiable information (PII). As the data processor, OceanBase assists its clients in processing PII information. OceanBase provides a range of security capabilities to ensure the security of PII information and defines the responsibilities of OceanBase and its clients regarding data processing. OceanBase invited the British Standards Institution (BSI) to audit its Privacy Information Management System and received certification.

6.3. PCI DSS

PCI DSS is an information security standard developed by the PCI Standards Security Committee, applicable to companies that transmit, store, and process cardholder data. OceanBase invites Atsec as a third-party audit firm annually to conduct an audit of its security governance. Following the audit, OceanBase Cloud database is deemed compliant with the PCI DSS standard, making it a PCI DSS-certified service provider. Therefore, if you need PCI DSS certification, after using OceanBase Cloud database service, you can submit an AOC report for OceanBase Cloud database to the testing organization, which can simplify database testing.

6.4. SOC2

The Standard Operating Procedure (SOC) was developed by the American Institute of Certified Public Accountants (AICPA) and covers five aspects: security, availability, confidentiality, integrity, and privacy. Its purpose is to ensure that service providers can securely manage data and protect user privacy and interests. OceanBase Cloud database annually invites Ernst & Young as a third-party

audit firm to assess its corporate governance, security capabilities, and operational processes, and provides a Type II SOC report on the security, availability, and confidentiality of OceanBase Cloud Cloud Database.