bamboocloud

Bamboocloud Privileged Access Management System

Product Whitepaper

Information in this document is subject to change without prior notice.

Trademark

Shenzhen Bamboocloud Technology Co., Ltd.

Headquarters address: 40F, Building A2, Creative City, Liuxian Avenue, Nanshan District, Shenzhen, Guangdong, China

Official website: en.bamboocloud.com

Telephone: 0755-86117880

Table of contents

1 Basic concepts

Privileged Access Management (PAM)

Privileged access management is a security solution designed to manage and monitor privileged accounts and their permissions. Privileged accounts typically have elevated access to critical systems and sensitive data, such as system administrators or root accounts. Therefore, the compromise or misuse of privileged accounts can pose severe security risks.

The primary objective of PAM is to centralize the management and monitoring of privileged accounts, ensuring that only authorized users can access necessary resources with minimal privileges, while also meeting compliance requirements.

Host Privilege

Host privileges refer to the access and administrative permissions for infrastructure resources, such as servers, network devices, and databases. Privileged accounts with these permissions can perform high-risk operations such as system maintenance, command execution, and configuration changes.

Since these operations directly impact the secure functioning of enterprise IT infrastructure, strict privilege management and behavior monitoring mechanisms are undoubtedly required.

Connection Privilege

Connection privileges refer to the permissions granted to service accounts used by entities such as applications, middleware, and servers to access resources like databases, primarily used for system-to-system communications and data transmission. Such privileged accounts are often authenticated using credentials stored in configuration files or code, while this static configuration approach can introduce significant security vulnerabilities.

Connection privileges typically involve access to core data resources and are used continuously during system operation, making their security management essential for preventing data breaches and protecting enterprises’ core assets.

Application Privilege

Application privileges refer to the administrative permissions within application systems. Privileged accounts with these permissions (such as super administrators or regular administrators) can perform critical operations such as user management, system configuration, and permission assignment.

To ensure compliance and secure application operations, organizations must implement robust privilege hierarchies and effective mechanisms for managing application privileges.

2 Background

According to the recent Data Breach Investigation Reports (DBIR), privilege abuse attacks have been steadily increasing and now rank as the fifth leading cause of data breaches—following social engineering attacks, web application attacks, system intrusions, and human errors.

This alarming trend underscores the critical importance of privileged accounts in information security frameworks and highlights the need for organizations to reassess and strengthen their privileged access management strategies.

In this context, establishing a real-name system to manage privileged account users and their activities, maintaining robust security for critical assets, and ensuring business continuity and stability have become significant challenges.

To address these challenges, it is necessary for enterprises to take multi-faceted control measures as follows:

- Strict verification and registration of privileged identities to ensure authenticity and traceability
- Strong authentication mechanisms to enhance access security
- Fine-grained and dynamic permission allocation to ensure each account is granted only the minimum privileges necessary to perform its tasks
- Comprehensive audit logging to record and analyze all privileged account activities for timely detection and response to potential security risks

3 Product overview

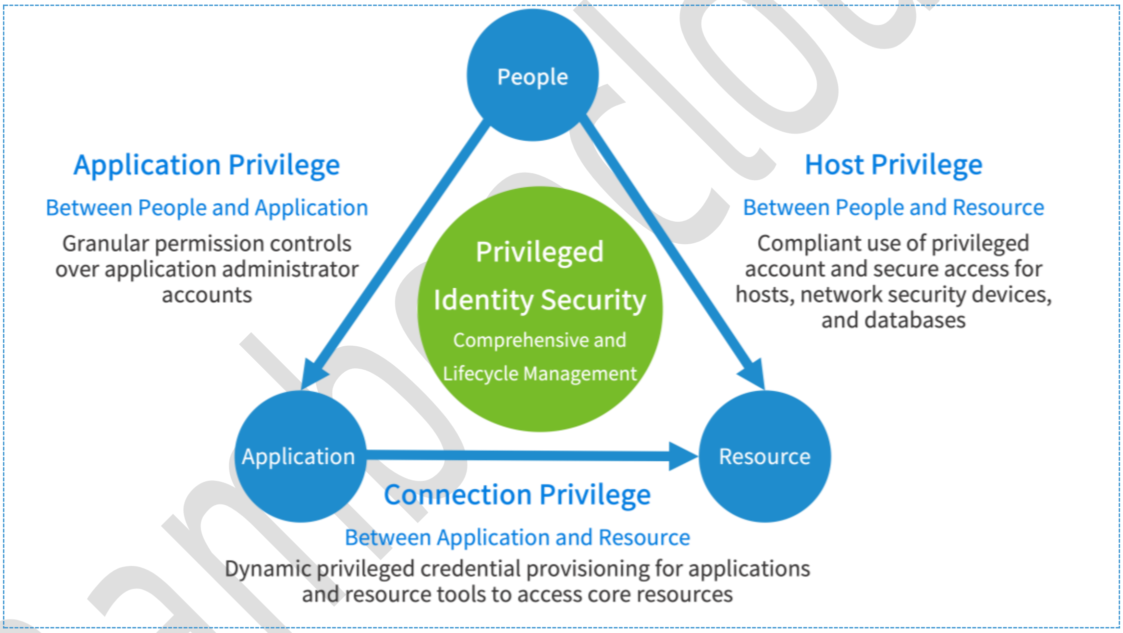
The Bamboocloud Privileged Access Management System addresses common challenges in managing privileged accounts, such as handling large volumes of accounts, inefficient decentralized management, lack of real-name authentication, and unclear accountability. By strengthening security controls over user and resource access, the platform enables comprehensive, centralized, and efficient management of privileged accounts.

The platform's core framework is built around the full lifecycle of privileged access management, which includes initial account discovery, credential request and approval, precise authorization, periodic credential rotation, and account deprovisioning. It ensures on-demand privilege allocation, precise command control, and effectively mitigates the risks of privilege abuse. This guarantees security and compliance in the management and operations of enterprise digital infrastructures.

4 Product architecture

4. 1 Business architecture

The platform focuses on three key areas: host privilege management, connection privilege management, and application privilege management. It aims to establish a comprehensive privileged identity governance framework centered around privileged access management and grounded in the management of user and application identities.


People
Application Privilege
Between People and Application
Granular permission controls over application administrator accounts
Host Privilege
Between People and Resource
Compliant use of privileged account and secure access for hosts, network security devices, and databases
Privileged Identity Security
Comprehensive and Lifecycle Management
Application
Resource
Connection Privilege
Between Application and Resource
Dynamic privileged credential provisioning for applications and resource tools to access core resources

Host privilege management

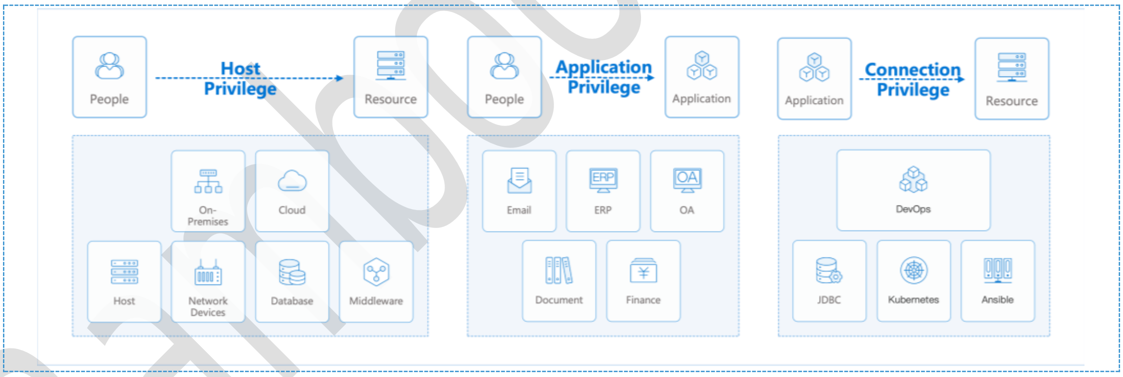
The platform provides security control capabilities for four types of infrastructure resources — hosts, network devices, databases, and middleware. These capabilities include account and password security management, resource permission management, operational security management, and activity auditing.

Application privilege management

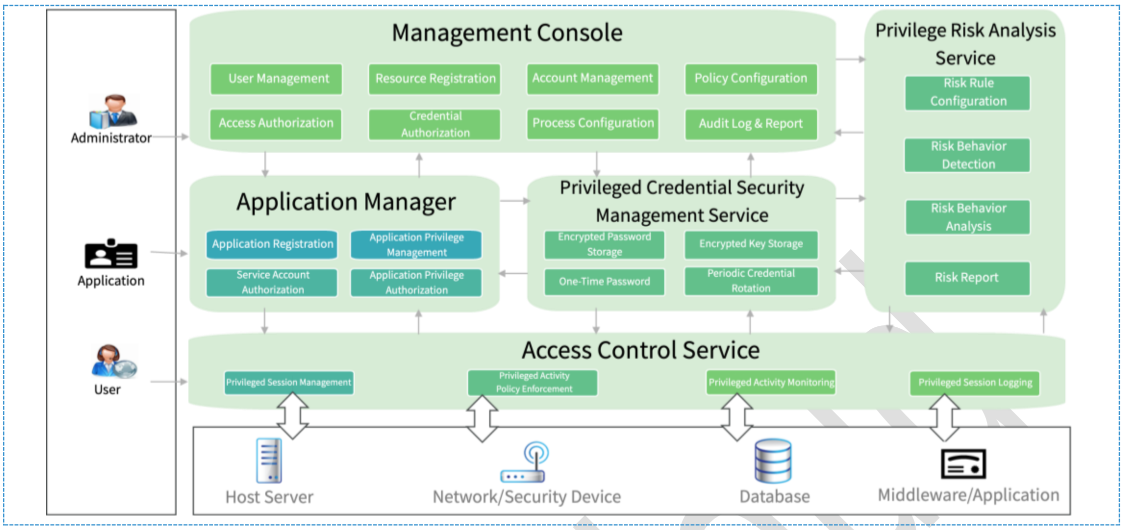
The platform addresses the security management needs of privileged administrative accounts for application systems (such as super administrators or regular administrators). It offers a dedicated management entry point and enables fine-grained control over operations personnel through secondary authorization.

Connection privilege management

The platform meets the security requirements of privileged service accounts used by applications. Through embedded privilege management services within applications, it replaces hard-coded configurations with real-time dynamic account and password provisioning for applications. Combined with data encryption and application identity authentication, the platform ensures secure and compliant use of service accounts with connection privileges.



4. 2 System architecture



The Bamboocloud Privileged Access Management System is composed of the following components: the management console, application manager, privileged credential security management service, access control service, and privilege risk analysis service.

Management console

Provide essential management functions, including identity and authentication management, resource and account registration and management, centralized permission control of privileged accounts, and logging and auditing of privileged account activities.

Application manager

Centralize the management of application privileges and connection privileges with on-demand privilege requests and allocation. By centrally managing service accounts, eliminate hard-coded credentials and achieves dynamic provisioning of privileged credentials for applications.

Privileged credential security management service

Manage the security of all credential information within the system. Offer centralized, high-strength encrypted storage for user credentials, resource account passwords, and keys, along with features such as credential rotation and one-time password mechanisms.

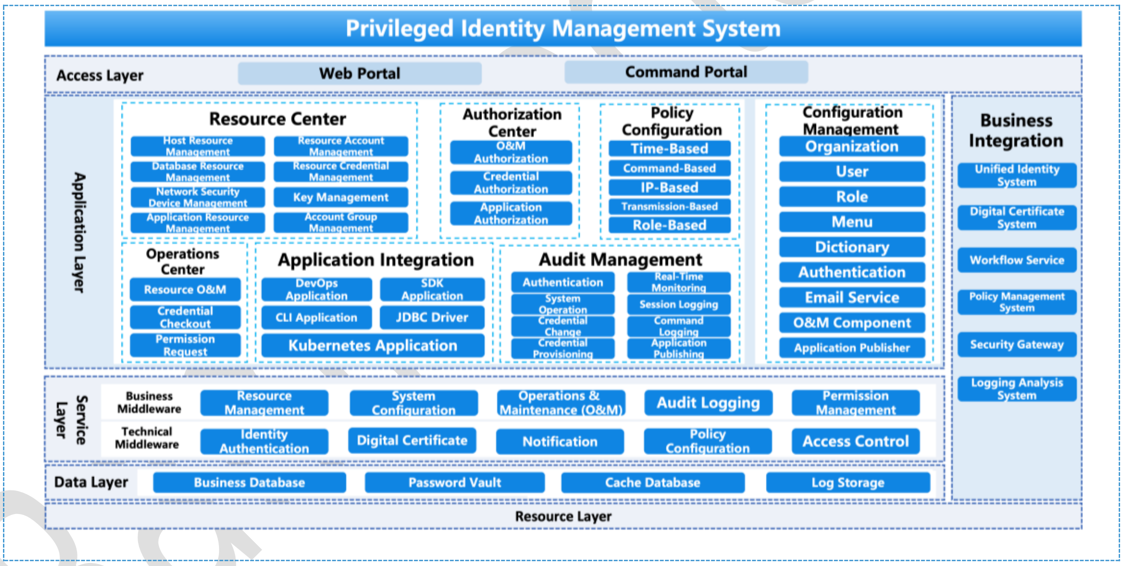
Access control service

Act as an access protocol agent for secure operations and maintenance, providing centralized privileged session management, privileged activity policy enforcement, and session logging and monitoring.

Privilege risk analysis service

Provide real-time risk analysis and alerts throughout the lifecycle of privileged accounts.

4. 3 Functional architecture



Access layer

- **Web portal**: Provide an intuitive visual interface for various enterprise users to access system functions via web browsers.
- **Command portal**: Provide a command line interface (CLI) for operations and maintenance personnel to efficiently access and manage enterprise assets.

Application layer

- **Resource center**: Serve as the foundation of the platform for centralized management of various resources (such as hosts and databases), related resource accounts, credentials, and keys to ensure secure and well-organized resource data.
- **Authorization center**: Define user permissions for resources managed by the resource center through maintenance and operations-based, credentials-based, and application-based authorization to ensure legitimate and compliant resource access.
- **Policy configuration**: Establish a rules framework for system access and operations. Through policies based on time, command, IP address, and other dimensions, refine and restrict user access to and operations on resources under varying conditions, thereby improving overall system security.
- **Configuration management**: Manage configurations for organizations, users, and roles, as well as settings for authentication and email services, to ensure a well-structured and smoothly operating running environment.
- **Operations center**: Focus on routine resource management, including resource operations and maintenance, credential checkouts, and permission requests, to ensure resource availability and business continuity.
- **Application integration**: Provide multiple integration methods including DevOps and CLI to enhance system compatibility with diverse business scenarios and improve system practicality.
- **Audit management**: Oversee business security through comprehensive authentication and operation monitoring. Through real-time monitoring and detailed logging of sessions and commands, enable robust audit trails to promptly identify and address potential security issues and abnormal activities.

Service Layer

- **Business middleware**: Provide foundational services for resources and system configurations to ensure normal business operations.
- **Technical middleware**: Provide services such as identity authentication and digital certificates to facilitate business management.

Data layer

Store data and resources via services including business databases, password vaults, cache databases, message queues, and log storage.

Business integration

Support integration with unified identity systems, digital certificate systems, and other platforms for flexible functionality expansion.

5 System requirements

Item	Description
Server	**Operating system**: ● Mainstream Unix systems, such as IBM AIX, HP-UX, Oracle Solaris, and SCO UNIX. ● Mainstream Linux systems, such as Red Hat, CentOS, SUSE, and Debian.
	CPU: x86 and ARM processors.
Database	Mainstream databases, such as MySQL, Oracle, DM, KingbaseES, and Shentong.
Middleware	Mainstream middleware used as application servers, such as TongWeb, Tomcat, WebLogic, and WebSphere.

6 Use scenarios

Scenario	Description
Privileged account discovery and extraction	The platform follows the "centralize first, then control" principle. It provides account discovery capabilities for various types of resources and monitors privileged accounts on managed resources to identify new accounts, dormant accounts, and orphan accounts.
Privileged credential management	As automated credential management (such as passwords and SSH keys) is the core of privileged account management, the platform supports configuring distinct password security policies for different types of systems, ensuring compliance with password requirements such as high complexity, single-use, and regular rotation.
Break glass mechanism	The platform implements encrypted credential storage and regularly backs up the latest credential data to a secure storage area. Administrators can decrypt and view account credentials using data decryption tools in emergency scenarios.
Single sign-on resource access	Once authenticated on the platform, the operational personnel can access authorized resources without step-up authentication. The platform supports various client-side maintenance tools and maintains users' familiar workflows.

Scenario	Description
Step-up authentication for sensitive resources	Multi-factor authentication policies can be configured for high-security resources. Once such policies are implemented, the operational personnel must complete step-up authentication—such as entering an SMS verification code—to access these resources.
Vault mode	For high-security resources, the platform supports security review processes for various operational scenarios with either single or dual control approval modes. Authorization can be verified through methods such as one-time passwords (OTPs), email verification codes, or workflow-based approvals.

7 Core capabilities

7.1 Compliant privileged account management

Through centralized control over privileged accounts for devices and applications, the platform conducts regular compliance checks on account permissions and credential health. In doing so, it proactively identifies and addresses orphan accounts, unauthorized access, dormant accounts, and accounts with passwords that have remained unchanged for extended periods, thereby mitigating security risks.

Additionally, the platform detects weak passwords to prevent security breaches caused by poor password strength and ensure regulatory compliance.

7.2 Fine-grained permission management

With the RBAC (role-based access control) mechanism, the platform enables granular permission management down to menu items and button-level functions through security administrators.

It supports multi-dimensional policy configuration and lifecycle management for role-based permissions, ensuring precise control over permission assignment, revocation, and validity periods. The integrated temporary permission elevation system, complemented by real-time permission synchronization and dynamic updates enabled by the microservices architecture, allows users to initiate time-bound elevation requests.

The platform implements the principle of least privilege and comprehensive audit trails, maintaining security boundaries for core business operations while accommodating agile business needs,

7. 3 Credential masking

The platform employs credential masking technology to conceal account and password information during client logins. By dynamically managing resource connections at the request layer, it automatically maps user identities to resource accounts. This approach prevents users from storing actual credentials locally and circumventing the system.

Furthermore, by avoiding plain-text credential input, the platform reduces the risk of credential leaks and secures asset operations and maintenance.

7. 4 One-time password for privileged account

To address security demands in complex network environments and for highly sensitive assets, the platform offers one-time password protection for privileged accounts.

Under this mechanism, the system automatically rotates passwords based on account usage, ensuring that each password is valid for a single use only. This prevents unauthorized access even if passwords are compromised.

7. 5 Privileged credential provisioning

The platform provides account and credential provisioning services for applications accessing other applications, as well as for applications accessing foundational services and resources. Common scenarios include provisioning database access credentials for applications and resource credentials used by CI/CD pipelines within DevOps tools.

Through centralized management of privileged service accounts and credentials, the platform eliminates hard-coded credentials and implements dynamic credential provisioning, enhancing both business security and operational flexibility.

7. 6 Cross-region, multi-data-center architecture

The platform centralizes the management of assets distributed across different geographic regions using a standalone access control module. This facilitates centralized privileged access management in multi-data-center architectures, as well as hybrid cloud environments encompassing both on-premises and cloud-based assets.

Regardless of network complexity, the platform enforces standardized access control policies and audit mechanisms to ensure continuity, consistency, and compliance in privileged account management.

By effectively addressing various privileged access challenges in multi-cloud deployments and interconnected data centers, the platform enables organizations to establish a secure, efficient, and scalable privileged access management system.

8 Core advantages

- **Compliant lifecycle management**: Manage privileged accounts throughout their entire lifecycle, including discovery, registration, provisioning, request handling, revocation, and deletion.
- **Secure password synchronization**: Implement a script-free, interactive password rotation mechanism. Newly generated passwords are synchronized instantly and securely stored in the vault, ensuring immediate usability without any intermediate states. All transmissions are encrypted to minimize the risk of password interception.
- **Automated credential management**: Centralize the management of privileged credentials such as passwords, keys, and access tokens; support automated credential rotation with customizable password policies and rotation schedules, ensuring that credentials are securely managed in real time.
- **Secure credential vault**: Store all privileged credentials in a centralized vault with dedicated encryption keys to ensure confidentiality and security.
- **Dual-control approval**: Enforce a dual-review process for tasks such as system data queries, configuration changes, and other high-sensitive operations, preventing unauthorized access and safeguarding operational security.
- **Application service account management**: Manage service accounts and their credentials used in configuration files, JDBC (Java database connectivity) connections, DevOps tools, Docker, and other virtualization and automation systems; enable dynamic credential provisioning to eliminate hard-coded risks.
- **Least privilege access**: Implement temporary, need-based permission allocation with automatic revocation; provide granular permission

controls based on protocol, command, time, and IP address to optimize both security and efficiency.

- **Multi-factor single sign-on**: Enable end-to-end multi-factor single sign-on from client endpoints to operational service components and target resources, improving user experience while strengthening identity authentication security.
- **Automated workflow**: Streamline privileged identity lifecycle management with multi-level approval workflows and customizable request templates, ensuring compliance for every activity.
- **Standardized system integration**: Provide standardized APIs for seamless integration with mainstream workflow platforms, asset management, vulnerability management, and automation tools to simplify inter-system collaboration and enterprise-wide system interoperability. Supported systems include CMDB (configuration management database), ITSM (IT service management), and SIEM (security information and event management).
- **High scalability and customization**: The microservices architecture on which the platform is built ensures high scalability and customization to meet specific privileged access management needs.

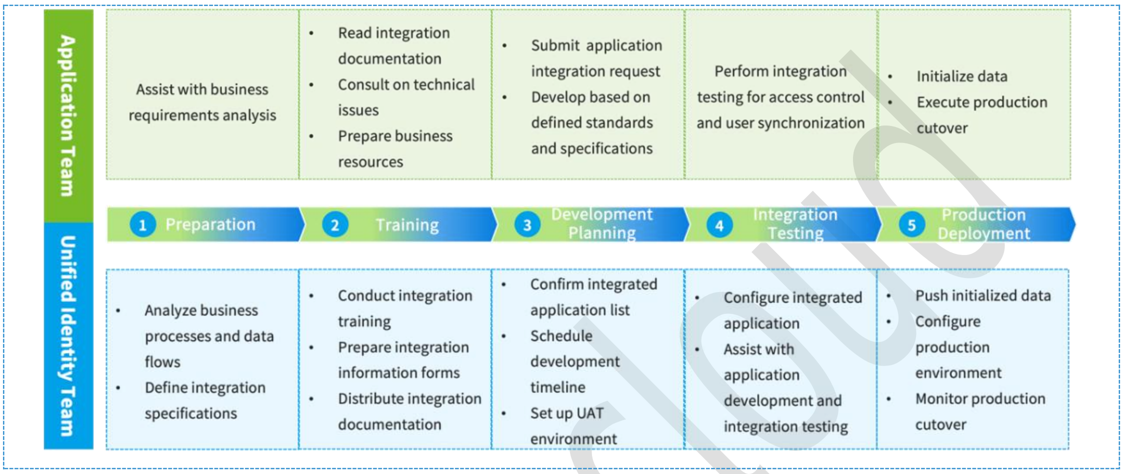
9 Feature overview

Feature	Description
Multi-protocol compatibility	Support maintenance, operations, and activity auditing through various protocols, such as Telnet, SSH, SFTP, RDP, X11 (X Window System), VNC, HTTP/HTTPS, JDBC, and ODBC.
Multi-resource compatibility	● Compatible with Windows systems (all versions), mainstream Unix systems (such as IBM AIX, HP-UX, Oracle Solaris, SCO UNIX, FreeBSD), mainstream Linux systems (such as Red Hat, SUSE, and Debian), and mainframe systems (such as AS/400 and OS/390). ● Compatible with various network and security devices from vendors such as Huawei, H3C, Cisco, and Juniper. ● Compatible with mainstream databases, such as MySQL, PostgreSQL, DM, KingbaseES, and Vastbase. **Note**: Customization can be completed within an agreed-upon time frame.
Multi-maintenance tool compatibility	● Compatible with common client-side maintenance tools, such as CMD, NetTerm, SecureCRT, XShell, CuteFTP, Remote Desktop, MobaXterm, and WinSCP. ● Provide a web-based interface for resource operations and maintenance. ● Support quick integration with specific Windows maintenance tools.

Feature	Description
Multi-authentication method support	Support multiple authentication methods, such as static passwords, Active Directory, OTP, and extensions for other methods.
Concurrent processing performance (standard single node)	● Character-oriented protocol: Support up to 500 concurrent sessions. ● Graphics protocol: Support up to 50 concurrent sessions.
Audit storage optimization	● Character-oriented protocol: Generate no more than 500 KB of audit logs per hour. ● Graphics protocol: Generate no more than 20 MB of audit logs per hour.
HA and load balancing	● Support HA (high availability) and load balancing modes. ● Support quick configuration via the web console.
Rapid deployment	● No agent or plugin installation is required on target resources. ● No additional client software installation is required for end users.
Distributed deployment	Support a hierarchical node architecture, where upper-level nodes can manage and supervise the operations and data of data of lower-level nodes.

10 Product deployment

10. 1 Implementation process



	1 Preparation	2 Training	3 Development Planning	4 Integration Testing	5 Production Deployment
Application Team	Assist with business requirements analysis	• Read integration documentation • Consult on technical issues • Prepare business resources	• Submit application integration request • Develop based on defined standards and specifications	Perform integration testing for access control and user synchronization	• Initialize data • Execute production cutover
Unified Identity Team	• Analyze business processes and data flows • Define integration specifications	• Conduct integration training • Prepare integration information forms • Distribute integration documentation	• Confirm integrated application list • Schedule development timeline • Set up UAT environment	• Configure integrated application • Assist with application development and integration testing	• Push initialized data • Configure production environment • Monitor production cutover

10. 2 Deployment features

The Bamboocloud Privileged Access Management System features streamlined and efficient deployment that enables rapid implementation without disrupting the existing infrastructure environment.

The platform requires no installation of client-side software, agents, or plugins on managed assets, nor does it make any configuration changes to target assets. For service account management, only minimal modifications are needed on the application side for fast integration and account takeover.

The platform adopts a "bypass access, single entry point" design. Devices can be centrally managed once connected to any available network port in the data center, without altering the existing network infrastructure and topology. With centralized device management combined with features such as identity mapping and password synchronization, the platform significantly reduces the credential management burden for device administrators.

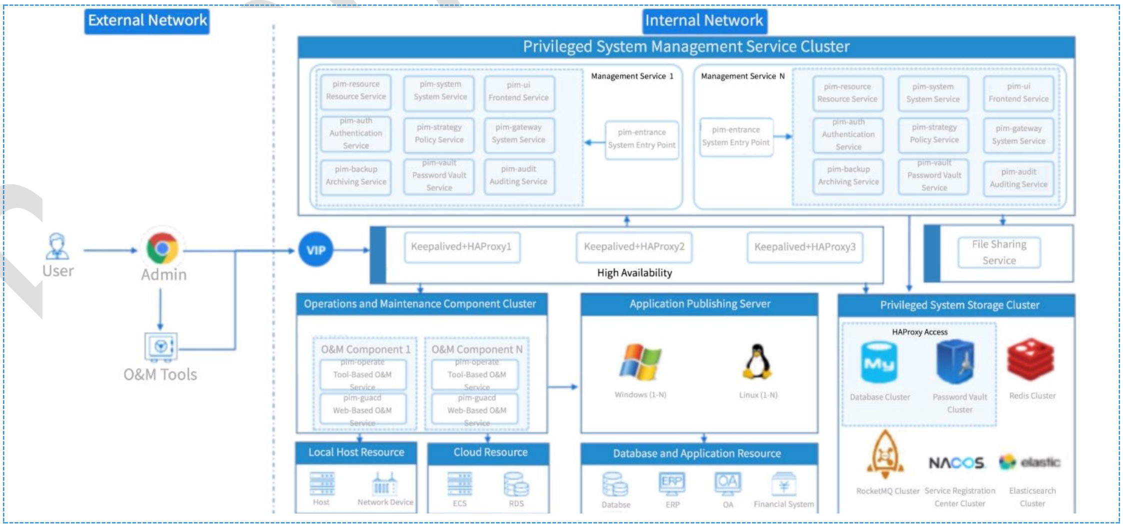
10. 3 Deployment architecture

The Bamboocloud Privileged Access Management System employs a distributed cluster deployment architecture. Through multi-node collaboration and load balancing, the system ensures high availability, performance, and scalability.

The platform is built upon a microservices architecture where all functional components support containerized deployment and flexible scaling based on business needs.

High availability is achieved through the integration of Keepalived for failover and HAProxy for intelligent load balancing, enhancing the load handling and disaster recovery capabilities of each sub-service to ensure overall system stability and reliability.

The platform's deployment architecture consists of four core components: the privileged system management service cluster, the operations and maintenance component cluster, the application publishing server, and the privileged system storage cluster.


External Network
Internal Network
Privileged System Management Service Cluster
pim-resource Resource Service
pim-system System Service
pim-ui Frontend Service
pim-auth Authentication Service
pim-strategy Policy Service
pim-gateway System Service
pim-backup Archiving Service
pim-vault Password Vault Service
pim-audit Auditing Service
Management Service 1
pim-entrance System Entry Point
Management Service N
pim-entrance System Entry Point
pim-resource Resource Service
pim-system System Service
pim-ui Frontend Service
pim-auth Authentication Service
pim-strategy Policy Service
pim-gateway System Service
pim-backup Archiving Service
pim-vault Password Vault Service
pim-audit Auditing Service
User
Admin
O&M Tools
VIP
Keepalived+HAProxy1
Keepalived+HAProxy2
Keepalived+HAProxy3
High Availability
File Sharing Service
Operations and Maintenance Component Cluster
O&M Component 1
pim-operate Tool-Based O&M Service
pim-guacd Web-Based O&M Service
O&M Component N
pim-operate Tool-Based O&M Service
pim-guacd Web-Based O&M Service
Application Publishing Server
Windows (1-N)
Linux (1-N)
Privileged System Storage Cluster
HAProxy Access
Database Cluster
Password Vault Cluster
Redis Cluster
RocketMQ Cluster
NACOS
Service Registration Center Cluster
elastic
Elasticsearch Cluster
Local Host Resource
Host
Network Device
Cloud Resource
ECS
RDS
Database and Application Resource
Databse
ERP
OA
Financial System

Privileged system management service cluster

This cluster is built on a microservices architecture, comprising several microservice components such as pim-resource, pim-system, pim-audit, and pim-auth, which provide services such as resource management, system operations, auditing, and authentication.

Operations and maintenance component cluster

This cluster Includes tool-based maintenance and web-based maintenance services. It supports distributed deployment across different regional subnets, enabling the platform to manage resources within specific subnets.

Application publishing server

This component facilitates secure access to database and application resources. It supports both Windows and Linux application publishing services and can be deployed independently as needed.

Privileged system storage cluster

This cluster is responsible for storing data and resources. It includes the database cluster, the password vault cluster, the Redis cluster, the Elasticsearch cluster, the Nacos cluster for service registration and discovery, and the RocketMQ cluster for message middleware.

11 Abbreviations

AD	Active Directory
CLI	Command Line Interface
CMDB	Configuration Management Database
DBIR	Data Breach Investigations Reports
DevOps	Development and Operations
HA	High Availability
IT	Information Technology
ITSM	IT Service Management
JDBC	Java Database Connectivity
OTP	One-Time Password
PAM	Privileged Access Management
RBAC	Role-Based Access Control
RSA	Rivest-Shamir-Adleman
SIEM	Security Information and Event Management
UAT	User Acceptance Testing