In today's digital landscape, securing cloud environments is more crucial than ever. This involves protecting sensitive data through robust encryption, implementing Zero Trust Security principles, and managing access with Identity and Access Management (IAM) solutions. Together, these strategies form a comprehensive approach to safeguarding your cloud infrastructure from emerging threats and ensuring your data remains secure.

* **Data Encryption**
  + [**Securing Ends with Data Encryption for the Cloud**](https://www.alibabacloud.com/blog/597403?utm_content=g_1000396717)

The article discusses the significance of data encryption in protecting sensitive and private data for businesses, particularly in cloud-native environments. It highlights the importance of implementing zero-trust security measures with hybrid and multi-cloud architectures to secure data both at rest and in transit. The piece emphasizes the role of data encryption in safeguarding against cyberattacks, which can cause substantial damage to any industry.

* + [**Data encryption**](https://www.alibabacloud.com/help/oss/security-and-compliance/data-encryption-2?utm_content=g_1000396718)

Alibaba Cloud's Object Storage Service (OSS) offers robust data protection through server-side and client-side encryption, complemented by encryption in transit via HTTPS over SSL/TLS. Server-side encryption safeguards data at rest using either KMS-managed keys (SSE-KMS), where Key Management Service (KMS) encrypts and decrypts data using customer master keys (CMKs), or OSS-managed keys (SSE-OSS), where OSS handles key generation and management. SSE-KMS is ideal for high-volume encryption tasks due to its efficiency and cost-effectiveness, while SSE-OSS suits bulk object encryption. KMS ensures key privacy, integrity, and availability, facilitating custom encryption function development. Client-side encryption allows users to encrypt objects locally before uploading, maintaining control over CMK integrity and validity. Two CMK types are supported: KMS-managed and customer-managed.

* + [**Transparent data encryption**](https://www.alibabacloud.com/help/polardb/polardb-for-postgresql/tde?utm_content=g_1000396719)

This topic describes transparent data encryption (TDE), which encryps data at rest, safeguarding sensitive database files on disks against potential attackers. It is available for PolarDB for PostgreSQL clusters running specific engine versions. TDE allows authenticated users to access encrypted data without modifying application code or configurations for decryption, preventing unauthorized access to sensitive information in tablespace, disks, and database backups.

* + [**Data Encryption In Transit**](https://www.alibabacloud.com/help/well-architected/latest/data-transmission-encryption?utm_content=g_1000396720)

Alibaba Cloud's KMS offers various encryption keys: Default Keys are exclusive for cloud service server encryption; Software Keys support both cloud service and application client encryption, while Hardware Keys are suitable for financial-grade data encryption, supporting national cryptographic algorithms. Software key encryption is recommended for most application scenarios.

* + [**Data Encryption at Rest**](https://www.alibabacloud.com/help/well-architected/latest/data-encryption-at-rest?utm_content=g_1000396721)

To ensure data security when stored on the cloud, enterprises should encrypt static data, particularly in ECS cloud disks, OSS, RDS, and cloud databases. Alibaba Cloud offers disk storage encryption services with key management through its Key Management Service (KMS). The storage encryption feature employs 256-bit encryption (AES256) to safeguard sensitive data. A list of cloud services supporting server-integrated static data encryption and their respective encryption procedures is available. Users can utilize the complimentary default key provided by Alibaba Cloud for server encryption or opt for a custom Bring Your Own Key (BYOK) method for enhanced data protection. For BYOK implementation, refer to the guide on importing key material into a symmetric key.

* **Zero Trust Security:** 
  + [**Overview of zero trust security**](https://www.alibabacloud.com/help/asm/user-guide/overview-of-zero-trust-security?utm_content=g_1000396722)

Zero Trust is a security model that denies implicit trust within and beyond network boundaries. Alibaba Cloud's Service Mesh (ASM) implements Zero Trust security for cloud-native applications by integrating authentication and authorization features, previously coded within applications, providing out-of-the-box configuration and immediate policy updates. The microservices architecture, while scalable and agile, increases security risks due to its distributed nature. Traditional network perimeter security is insufficient; hence, internal network communication must also be secured, making Zero Trust crucial.

* + [**Zero-Trust Security Practice of Nacos**](https://www.alibabacloud.com/blog/601298?utm_content=g_1000396723)

Nacos, a dynamic naming and configuration service, is pivotal for managing sensitive data in complex modern systems. Common security risks include exposing Nacos to the internet without proper authentication, leading to vulnerabilities and potential cyber-attacks. To mitigate these risks, Nacos adopts zero-trust security principles, focusing on identity management, authentication, access control, transmission security, and continuous behavior monitoring.

* **IAM**
  + [**A New Chapter in Modernizing Security with Cloud-Native Technologies: Identity Management**](https://www.alibabacloud.com/blog/596394?utm_content=g_1000396724)

The summary of the article discusses the importance of the human element in cybersecurity, emphasizing that humans are both the core strength and potential vulnerability in security systems. Identity and Access Management (IAM) is seen as a key component of zero-trust strategies, with cloud-native IAM services gaining prominence. These services offer seamless deployment and ease of use, providing comprehensive cybersecurity controls and network isolation measures. Cloud service providers like Alibaba Cloud facilitate a secure transition to the cloud for their customers, offering integrated security capabilities and real-time monitoring. The principle of least privilege (PoLP) is advocated, assigning different privilege settings to user accounts based on their functional requirements. Internal abnormal behavior detection systems are recommended to identify and prevent unauthorized actions, as demonstrated by the Weimob incident. Establishing effective baseline security policies requires an organization's strong and independent security team.

* + [**Set up an Identity and Access Management (IAM) System on Alibaba Cloud**](https://www.alibabacloud.com/blog/598608?utm_content=g_1000396725)

The article outlines the setup of an Identity and Access Management (IAM) system using Keycloak on Alibaba Cloud. Keycloak, an open-source IAM solution, facilitates Single Sign-On (SSO), user registration, and user federation, supporting protocols like SAML 2.0, OAuth 2.0, and OpenID Connect. For deployment on Alibaba Cloud, an ECS instance with sufficient resources is required, and Keycloak can run on any OS supporting Java. After installing Java, the Keycloak server distribution is downloaded, uploaded, and extracted on the ECS instance. An admin user is created, and the server is started in standalone mode. Key tasks include setting up realms, clients, and users. Realms manage objects like users and applications; clients request authentication, often for securing applications; and users are managed through the Keycloak console or RESTful APIs. Testing involves verifying user authentication and integration with Keycloak IAM interfaces from an application client using Python and the python-keycloak library. Further enhancements include configuring comprehensive authentication flows and deploying Keycloak in a cluster for higher availability and fault tolerance, ideally connected to a reliable, scalable database like Alibaba Cloud ApsaraDB RDS for MySQL.

* + [**Set Application Provisioning Scope**](https://www.alibabacloud.com/help/idaas/eiam/developer-reference/api-eiam-2021-12-01-setapplicationprovisioningscope?utm_content=g_1000396726)

This summary outlines the process of setting the account synchronization scope for applications within Identity as a Service (IDaaS) Employee IAM (EIAM). Developers can invoke the DeveloperAPI within the same scope to manage and query accounts. It's recommended to use OpenAPI Explorer for easier operation and automatic signature calculation. Key request parameters include InstanceId and ApplicationId, while OrganizationalUnitIds is optional. The response includes the requestId. JSON format is used for successful responses. Error codes are documented separately. Recent changes include updates to the API description, request parameters, and response structure as of March 28, 2024.

* + [**Get Application Provisioning Scope**](https://www.alibabacloud.com/help/idaas/eiam/developer-reference/api-eiam-2021-12-01-getapplicationprovisioningscope?utm_content=g_1000396727)

The API operation queries the account synchronization scope for applications in Identity as a Service (IDaaS) Employee IAM (EIAM), aligning with the scope where developers can call DeveloperAPI for account management. For ease of use, debugging is recommended through OpenAPI Explorer, which automatically handles signature calculations. No authorization information is disclosed in the API. Request parameters include InstanceId and ApplicationId, both required for identifying the specific instance and application. Response parameters consist of requestId for tracking requests and ApplicationProvisioningScope detailing the synchronization scope, including a list of authorized organizational units.