数据加密服务

产品介绍

文档版本 42

发布日期 2024-12-06

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 什么是数据加密服务

数据加密服务

数据是企业的核心资产，每个企业都有自己的核心敏感数据。这些数据都需要被加密，从而保护它们不会被他人窃取。

数据加密服务（Data Encryption Workshop, DEW）是一个综合的云上数据加密服务。它提供密钥管理（KMS）、凭据管理（CSMS）、密钥对管理（KPS）、专属加密(DHSM）、云平台密码系统服务（CPCS）五个微服务，安全可靠地为您解决数据安全、密钥安全、密钥管理复杂等问题。其密钥由硬件安全模块（Hardware Security Module，HSM） 保护，并与多个华为云服务集成。您也可以借此服务开发自己的加密应用。

表 1-1 服务介绍

名称	定义	更多信息
密钥管理服务 （Key Management Service, KMS）	密钥管理是一种安全、可靠、简单易用的密钥托管服务，帮助您轻松创建和管理密钥，保护密钥的安全。 KMS通过使用硬件安全模块（Hardware Security Module，HSM）保护密钥安全，HSM模块满足FIPS 140-2 Level 3安全要求。帮助用户轻松创建和管理密钥，所有的用户密钥都由HSM中的根密钥保护，避免密钥泄露。	密钥概述
云凭据管理服务 （Cloud Secret Management Service，CSMS）	凭据管理是一种安全、可靠、简单易用的凭据托管服务。 用户或应用程序通过凭据管理服务，创建、检索、更新、删除凭据，轻松实现对敏感凭据的全生命周期和统一管理，有效避免程序硬编码或明文配置等问题导致的敏感信息泄密以及权限失控带来的业务风险。	创建凭据

名称	定义	更多信息
密钥对管理服务（Key Pair Service, KPS）	密钥对管理是一种安全、可靠、简单易用的SSH密钥对托管服务，帮助用户集中管理SSH密钥对，保护SSH密钥对的安全。 KPS是利用HSM产生的硬件真随机数来生成密钥对，并提供了一套完善和可靠的密钥对的管理方案，帮助用户轻松创建、导入和管理SSH密钥对。生成的SSH密钥对的公钥文件均保存在KPS中，私钥文件由用户自己下载保存在本地，从而保障了SSH密钥对的私有性和安全性。	创建密钥对
专属加密（Dedicated Hardware Security Module，Dedicated HSM）	专属加密是一种云上数据加密的服务，可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。 Dedicated HSM为您提供经国家密码管理局检测认证的加密硬件，帮助您保护弹性云服务器上数据的安全性和完整性，满足监管合规要求。同时，用户能够对专属加密实例生成的密钥进行安全可靠的管理，也能使用多种加密算法来对数据进行可靠的加解密运算。	专属加密
密码系统服务（Cloud Platform Cryptosystem Service，CPCS）	云平台密码系统服务，提供专属的密码服务以及服务集群化部署能力。具备密码服务集群的全生命周期管理的能力，包括自动化部署与释放、集群弹性伸缩、集群调用的应用级隔离等，同时提供简单的应用管理、物理环境信息以及管理制度导入功能，并对各类能力进行集中监控、配置等，帮助租户快速通过密评。	-

2 基本概念

本文解释了数据加密服务（Data Encryption Workshop, DEW）的基本术语概念，帮助您正确理解和使用DEW。

表 2-1 通用加密术语

名称	定义	更多信息
对称密钥加密	对称密钥加密又称专用密钥加密。信息的发送方和接收方使用相同密钥去加密和解密数据。 优点：加密和解密速度快。 缺点：每对密钥需保持唯一性，所以用户量大时密钥管理困难。 适用场景：加密大量数据。	**密钥概述**
非对称密钥加密	非对称密钥加密又称公开密钥加密。它需要使用一对密钥来分别完成加密和解密的操作，一个公开发布，即公开密钥，另一个由用户自己秘密保存，即私用密钥。 优点：加密和解密使用密钥不同，所以安全性高。 缺点：加密和解密速度较慢。 适用场景：对敏感信息加密。	**密钥概述**
国密	国密即国家密码局认定的国产密码算法。其中包括对称加密算法、椭圆曲线非对称加密算法、摘要算法。包括 SM2、SM4 等。 SM1为对称加密算法，加密强度为128位，采用硬件实现。 SM2为非对称加密算法，其加密强度为256位。 SM3为密码摘要算法，消息分组长度为 512 位，摘要值长度为 256 位。 SM4为对称加密算法，加密强度为128位。	-

名称	定义	更多信息
HMAC算法（Hash-based Message Authentication Code，HMAC）	HMAC算法是一种基于密钥的消息认证码算法。HMAC算法使用信息与密钥结合，使用哈希函数对结果进行加密，由此实现对信息完整性的保护以及信息验证。	-
数字签名	数字签名（Digital Signature）又称公钥数字签名，通常用于验证消息的真实性和完整性。发送方通过私钥对信息加密签名后发送给接收方，接收方通过公钥进行解密验签，通过信息对比保障电子文件的安全性，达到预防篡改、伪装的目的。	-

表 2-2 密钥管理服务术语

名称	定义	更多信息
硬件安全模块（Hardware Security Module，HSM）	硬件安全模块是一种用于保护和管理强认证系统所使用的密钥同时提供相关密码学操作的计算机硬件设备。	-
用户主密钥（Customer Master Key，CMK）	用户主密钥是用户或云服务通过密钥管理创建的密钥，是一种密钥加密密钥，主要用于加密并保护数据加密密钥。一个用户主密钥可以加密多个数据加密密钥。 用户主密钥分为自定义密钥和默认密钥。	**什么是用户主密钥?**
默认密钥（Default Key）	默认密钥是对象存储服务（Object Storage Service，OBS）等其他云服务自动通过密钥管理为用户创建的用户主密钥，其别名后缀为“/default”。	**什么是默认密钥?**
密钥材料（Key Material）	密钥材料是密码运算操作的重要输入之一，与密钥ID、基本元数据共同组成用户主密钥（Customer Master Key，CMK）。	-
信封加密（Envelope Encryption）	信封加密是一种加密手段，将加密数据的数据密钥封入信封中存储、传递和使用，不再使用用户主密钥直接加解密数据。	**信封加密方式有什么优势?**
数据加密密钥（Data Encrypt Key，DEK）	数据加密密钥是用于加密数据的密钥。	**什么是数据加密密钥?**
HYOK（Hold Your Own Key，HYOK）	用户可以完全控制其密钥，密钥始终归用户所有。	**专属密钥库**

表 2-3 SSH 密钥对术语

名称	定义	更多信息
SSH密钥对	SSH密钥对是一种用于加密和验证网络连接的安全协议。它由两个部分组成：私钥和公钥。 • 私钥是一个加密的文件，只有持有者可以访问它。 • 公钥是一个非加密的文件，可以与任何人共享。当一个用户想要连接到另一个用户的计算机时，可以使用公钥来加密消息，并使用私钥来解密消息。 这种加密方式比传统的密码验证更安全，因为私钥只有持有者可以访问，而公钥可以在不暴露私钥的情况下共享。	**密钥对管理**
私有密钥对	私有密钥对是仅支持当前账号查看或使用的密钥对。	**创建密钥对**
账号密钥对	账号密钥对是支持本账号下所有用户查看或使用的密钥对。	**升级密钥对**

3 密钥管理

3.1 功能特性

密钥管理，即密钥管理服务（Key Management Service, KMS），是一种安全、可靠、简单易用的密钥托管服务，帮助您轻松创建和管理密钥，保护密钥的安全。

KMS通过使用硬件安全模块HSM（Hardware Security Module, HSM）保护密钥的安全，所有的用户密钥都由HSM中的根密钥保护，避免密钥泄露。并且HSM模块满足FIPS 140-2 Level 3安全要求。

KMS对密钥的所有操作都会进行访问控制及日志跟踪，提供所有密钥的使用记录，满足审计和合规性要求。

功能介绍

表 3-1 密钥管理

功能	服务内容
密钥全生命周期管理	• 创建、查看、启用、禁用、计划删除、取消删除自定义密钥 • 修改自定义密钥的别名和描述
用户自带密钥	导入密钥、删除密钥材料
小数据加解密	在线工具加解密小数据
签名验签	消息或消息摘要的签名、签名验证 **说明** 仅支持通过API调用。
密钥标签	添加、搜索、编辑、删除标签
密钥轮换	开启、修改、关闭密钥轮换周期
密钥授权	创建、撤销、查询授权

功能	服务内容
	退役授权 **说明** 仅支持通过API调用。
密钥区域性	跨区域创建副本密钥
云服务加密	对象存储服务OBS加密
	云硬盘服务EVS加密
	镜像服务IMS加密
	弹性文件服务SFS加密（SFS文件系统加密）
	弹性文件服务SFS加密（SFS Turbo文件系统加密）
	云数据库RDS（MySQL、PostgreSQL、SQL Server引擎）加密
	文档数据库服务DDS加密
	数据仓库服务DWS加密
数据加密密钥管理	创建、加密、解密数据加密密钥 **说明** 仅支持通过API调用。
生成硬件真随机数	生成512bit的随机数，为加密系统提供基于硬件真随机数的密钥材料和加密参数 **说明** 仅支持通过API调用。
消息认证码	生成、验证消息认证码 **说明** 仅支持通过API调用。
密钥库管理	创建、禁用、删除密钥库

KMS 支持的密钥算法

KMS创建的对称密钥使用的是AES、SM4加解密算法。KMS创建的非对称密钥支持RSA、ECC、SM2算法。

表 3-2 KMS 支持的密钥算法类型

密钥类型	算法类型	密钥规格	说明	适用场景
对称密钥	AES	AES_256	AES对称密钥	• 数据的加解密 • 加解密数据密钥 **说明** 小量数据的加解密可通过控制台在线工具进行。 大量数据的加解密需要调用API接口进行。
对称密钥	SM4	SM4	国密SM4对称密钥	• 数据的加解密 • 加解密数据密钥
摘要密钥	SHA	• HMAC_256 • HMAC_384 • HMAC_512	摘要密钥	• 数据防篡改 • 数据完整性校验
摘要密钥	SM3	HMAC_SM3	国密SM3摘要密钥	• 数据防篡改 • 数据完整性校验
非对称密钥	RSA	• RSA_2048 • RSA_3072 • RSA_4096	RSA非对称密钥	• 数字签名和验签 • 数据的加解密 **说明** 非对称密钥适用于签名和验签场景，加密数据效率不高，加解密数据推荐使用对称密钥。
	ECC	• EC_P256 • EC_P384	椭圆曲线密码，使用NIST推荐的椭圆曲线	数字签名和验签
非对称密钥	SM2	SM2	国密SM2非对称密钥	• 数字签名和验签 • 小量数据的加解密

通过外部导入的密钥支持的密钥包装加解密算法如**表3-3**所示。

表 3-3 密钥包装算法说明

密钥包装算法	说明	设置
RSAES_OAEP_SHA_256	具有“SHA-256”哈希函数的OAEP的RSA加密算法。	请您根据自己的HSM功能选择加密算法。 如果您的HSM支持“RSAES_OAEP_SHA_256”加密算法，推荐使用“RSAES_OAEP_SHA_256”加密密钥材料。 **须知** “RSAES_OAEP_SHA_1”加密算法已经不再安全，请谨慎选择。
RSAES_OAEP_SHA_1	具有“SHA-1”哈希函数的OAEP的RSA加密算法。	
SM2_ENCRYPT	国密推荐的SM2椭圆曲线公钥密码算法。	请在支持国密的局点使用SM2加密算法。

专属密钥库

KMS通过专属密钥库支持HYOK功能，帮助用户完全自主可控名下的用户主密钥，用户主密钥不脱离加密机，并且密码运算完全在加密机中完成。与默认密钥库不同，用户可以通过专属加密集群随时对密钥进行全生命周期管理。

专属加密实例基础版、铂金版（国内）均支持HYOK功能。

说明

HYOK（Hold Your Own Key）是指用户可以完全控制其密钥，密钥始终归用户所有。

专属密钥库操作可参见**激活集群**以及**创建密钥库**。专属密钥库支持的算法类型如**表 专属密钥库的密钥算法类型**所示。

表 3-4 专属密钥库的密钥算法类型

密钥类型	算法类型	密钥规格	说明	适用场景
对称密钥	AES	AES_256	AES对称密钥	• 数据的加解密 • 加解密数据密钥 **说明** 小量数据的加解密可通过控制台在线工具进行。 大量数据的加解密需要调用API接口进行。
对称密钥	SM4	SM4	国密SM4对称密钥	• 数据的加解密 • 加解密数据密钥

密钥类型	算法类型	密钥规格	说明	适用场景
非对称密钥	RSA	• RSA_2048 • RSA_3072 • RSA_4096	RSA非对称密钥	• 数字签名和验签 • 数据的加解密 **说明** 非对称密钥适用于签名和验签场景，加密数据效率不高，加解密数据推荐使用对称密钥。
	ECC	• EC_P256 • EC_P384	椭圆曲线密码，使用NIST推荐的椭圆曲线	数字签名和验签
非对称密钥	SM2	SM2	国密SM2非对称密钥	• 数字签名和验签 • 小量数据的加解密

密钥区域性

KMS通过密钥区域性，实现密钥跨区域使用。每组用户主密钥与副本密钥具有相同的密钥材料，因此可以实现单区域的加密数据在不同区域进行解密，解决因跨区导致的无法解密。

您可以独立管理多个区域的密钥，副本密钥同样支持创建密钥别名、启用、禁用、标签、授权、在线加解密。副本密钥的轮换无法自主设置，需按照主密钥的轮换设置进行同步轮换。

密钥区域性原理如**图 密钥区域性**所示。

图 3-1 密钥区域性

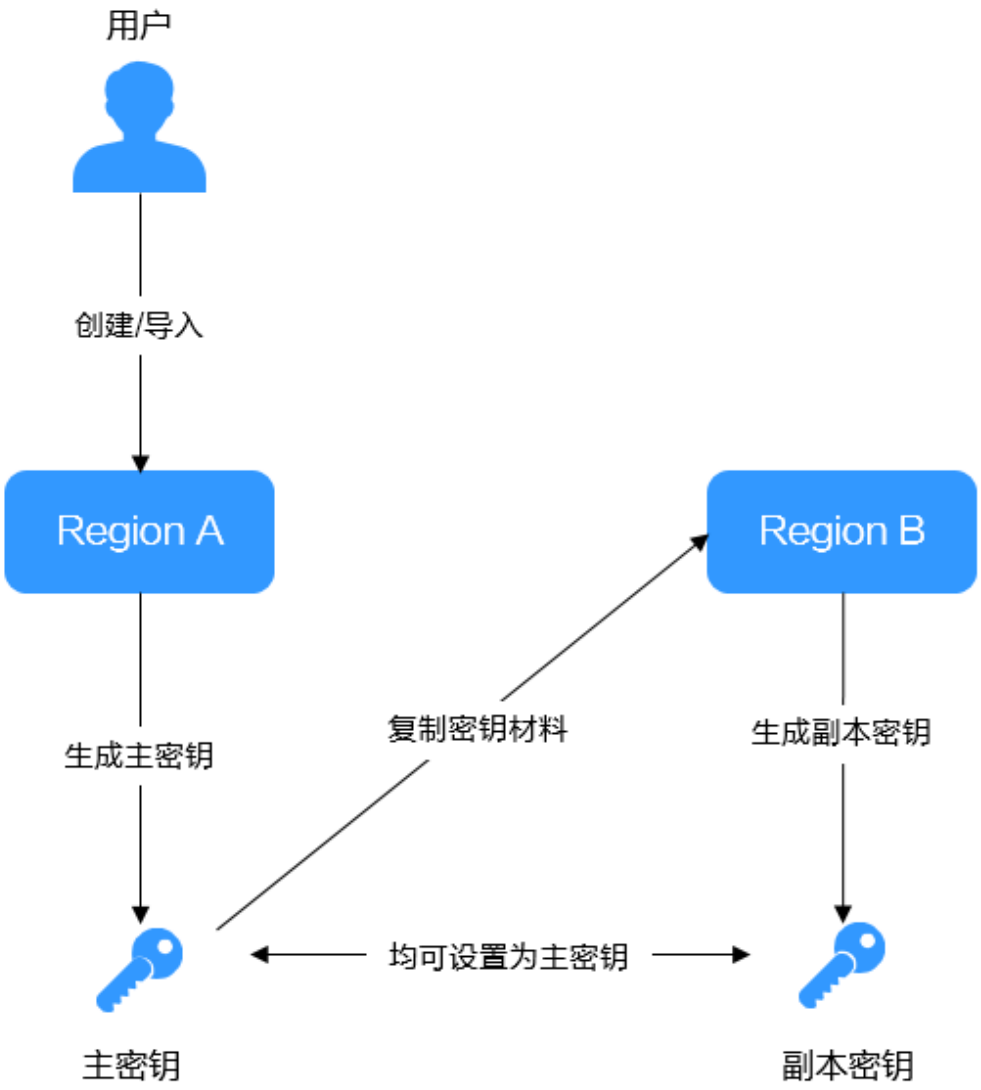


表 3-5 密钥区域性使用场景

使用场景	说明
灾备场景	如果密钥所在区域出现欠费资源冻结或异常无法处理数据解密，替换使用另一区域中的副本密钥进行正常数据处理，保证业务不中断。
跨区域签名验签	如果由于业务需要，客户业务处于不同区域，可通过不同区域密钥实现签名验签解密，提升业务对接高效性。

3.2 产品优势

服务集成广泛

- 与OBS、EVS、IMS等服务集成，用户可以通过KMS管理这些服务的密钥，还可以通过KMS API完成用户本地数据的加解密。
- 与CTS服务集成，用户可以通过CTS服务查看近期KMS的操作记录。
- 与CES服务集成，用户可以通过CES服务查看密钥计费请求次数。

合规遵循

密钥由经过安全认证的第三方硬件安全模块（HSM）产生，对密钥的关键操作都会进行访问控制及日志跟踪，符合中国和国际法律合规的要求。

高易用性

无需购买硬件加密设备，通过控制台或者API的方式实现密钥易用、易管理。

3.3 使用场景

前提条件

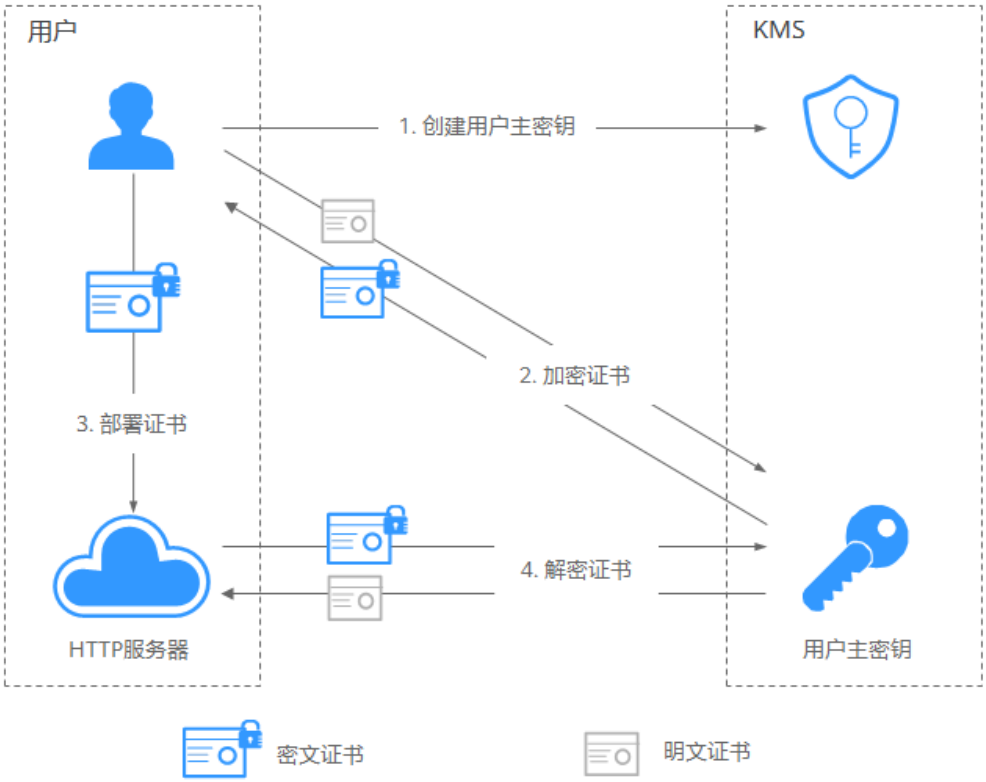
本章节涉及的“自定义密钥”均为“对称密钥”。对称密钥和非对称密钥的介绍，请参见**密钥概述**章节。

小数据加解密

当您有少量数据（例如：密码、证书、电话号码等）需要加解密时，用户可以通过KMS界面使用在线工具加解密数据，或者调用KMS的API接口使用指定的用户主密钥直接加密、解密数据。当前支持不大于4KB的小数据加解密。

以保护服务器HTTPS证书为例，采用调用KMS的API接口方式进行说明，如**图3-2**所示。

图 3-2 保护服务器 HTTPS 证书



流程说明如下：

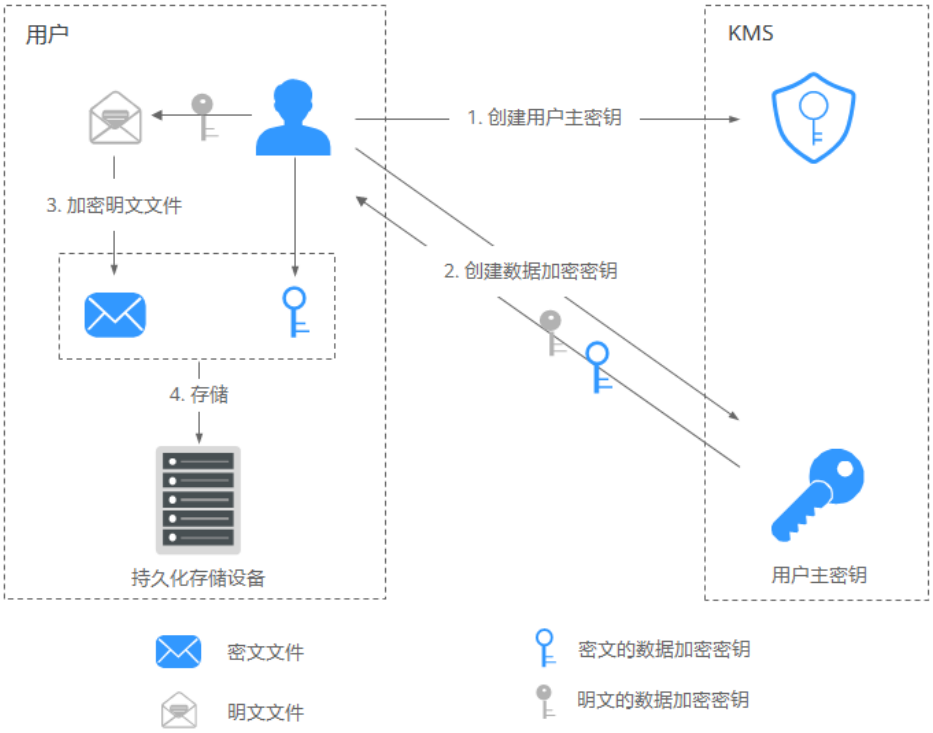
1. 用户需要在KMS中创建一个用户主密钥。
2. 用户调用KMS的“encrypt-data”接口，使用指定的用户主密钥将明文证书加密为密文证书。
3. 用户在服务器上部署密文证书。
4. 当服务器需要使用证书时，调用KMS的“decrypt-data”接口，将密文证书解密为明文证书。

大量数据加解密

当您有大量数据（例如：照片、视频或者数据库文件等）需要加解密时，用户可采用信封加密方式加解密数据，无需通过网络传输大量数据即可完成数据加解密。

- 加密本地文件流程，如图3-3所示。

图 3-3 加密本地文件



流程说明如下：

a. 用户需要在KMS中创建一个用户主密钥。

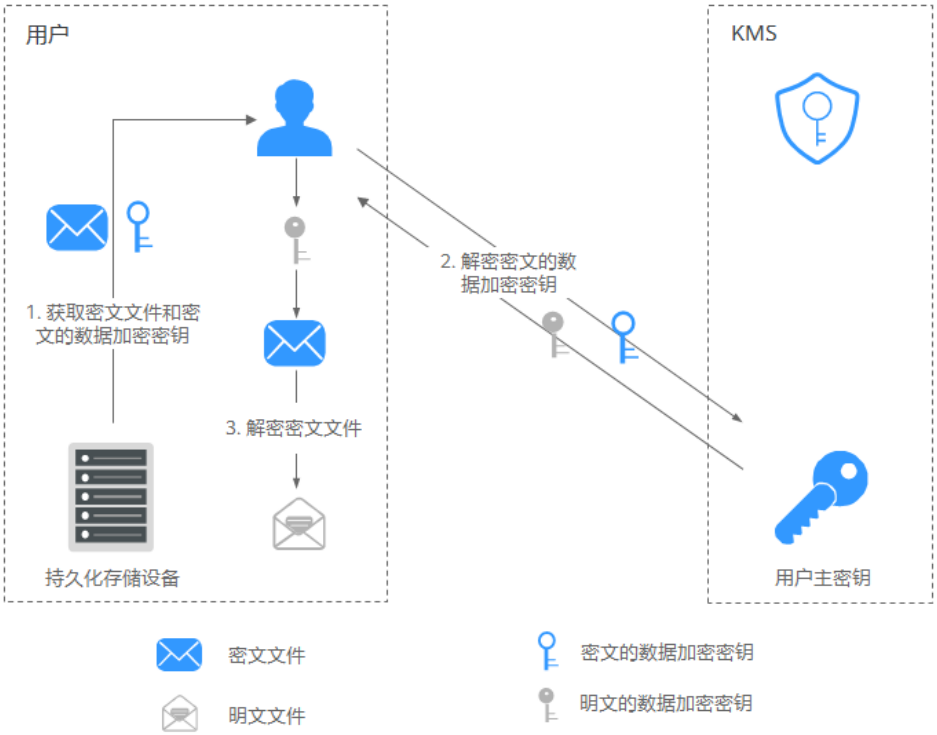
b. 用户调用KMS的“create-datakey”接口创建数据加密密钥。用户得到一个明文的数据加密密钥和一个密文的数据加密密钥。其中**密文的数据加密密钥**是由指定的**自定义密钥**加密**明文的数据加密密钥**生成的。

c. 用户使用明文的数据加密密钥来加密明文文件，生成密文文件。

d. 用户将密文的数据加密密钥和密文文件一同存储到持久化存储设备或服务中。

- 解密本地文件流程，如图3-4所示。

图 3-4 解密本地文件



流程说明如下：

a. 用户从持久化存储设备或服务中读取密文的数据加密密钥和密文文件。

b. 用户调用KMS的“decrypt-datakey”接口，使用对应的用户主密钥（即生成密文的数据加密密钥时所使用的用户主密钥）来解密密文的数据加密密钥，取得明文的数据加密密钥。

   如果对应的用户主密钥被误删除，会导致解密失败。因此，需要妥善管理好用户主密钥。

c. 用户使用明文的数据加密密钥来解密密文文件。

相关链接

相关文档	文档链接
最佳实践	• 小数据加解密，请参见**加解密小数据**。 • 大量数据加解密，请参见**加解密大量数据**。
API示例	• 小数据加解密，请参见**加解密小数据**。 • 大量数据加解密，请参见**加解密大数据**。

相关文档	文档链接
代码示例	• 小数据加解密，请参见**加解密小数据**。 • 大量数据加解密，请参见**加解密大数据**。

3.4 如何使用

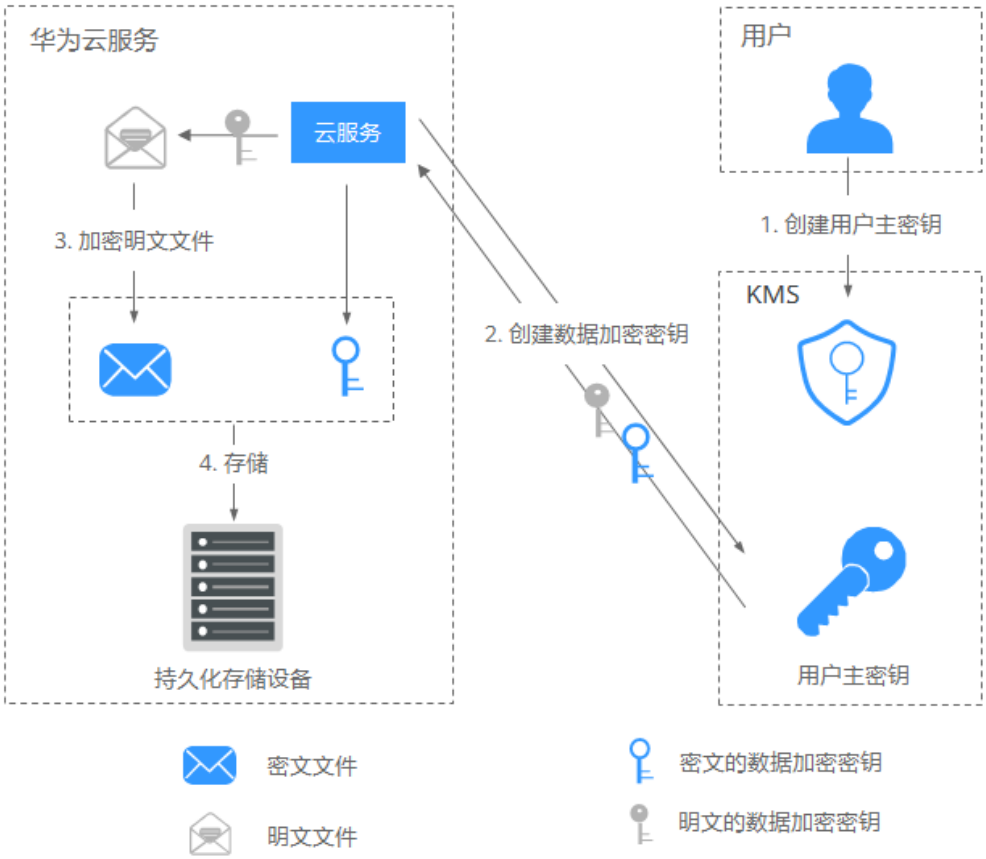
前提条件

本章节涉及的“自定义密钥”均为“对称密钥”。对称密钥和非对称密钥的介绍，请参见**密钥概述**章节。

与华为云服务配合使用

华为云服务基于信封加密技术，通过调用KMS的接口来加密云服务资源。由用户管理自己的自定义密钥，华为云服务在拥有用户授权的情况下，使用用户指定的自定义密钥对数据进行加密。

图 3-5 华为云服务使用 KMS 加密原理



加密流程说明如下：

1. 用户需要在KMS中创建一个自定义密钥。
2. 华为云服务调用KMS的“create-datakey”接口创建数据加密密钥。得到一个明文的数据加密密钥和一个密文的数据加密密钥。

   说明

   密文的数据加密密钥是由指定的用户主密钥加密明文的数据加密密钥生成的。
3. 华为云服务使用明文的数据加密密钥来加密明文文件，得到密文文件。
4. 华为云服务将密文的数据加密密钥和密文文件一同存储到持久化存储设备或服务中。

说明

用户通过华为云服务下载数据时，华为云服务通过KMS指定的自定义密钥对密文的数据加密密钥进行解密，并使用解密得到的明文的数据加密密钥来解密密文数据，然后将解密后的明文数据提供给用户下载。

表 3-6 使用 KMS 加密的云服务列表

服务名称	如何使用
对象存储服务	对象存储服务支持普通方式和服务端加密方式上传和下载对象。当用户使用服务端加密方式上传对象时，数据会在服务端加密成密文后安全地存储在对象存储服务中；用户下载加密对象时，存储的密文会先在服务端解密为明文，再提供给用户。对象存储服务支持KMS托管密钥的服务端加密方式（即SSE-KMS加密方式），该加密方式是通过KMS提供密钥的方式进行服务端加密。 用户如何使用对象存储服务的SSE-KMS加密方式上传对象，具体操作请参见《对象存储服务控制台指南》。
云硬盘	在创建云硬盘时，用户启用云硬盘的加密功能，系统将使用用户主密钥产生的数据密钥对磁盘进行加密，则在使用该云硬盘时，存储到云硬盘的数据将会自动加密。 用户如何使用云硬盘加密功能，具体操作请参见《云硬盘用户指南》。
镜像服务	用户通过外部镜像文件创建私有镜像时，可启用私有镜像加密功能，选择KMS提供的用户主密钥对镜像进行加密。 用户如何使用镜像服务的私有镜像加密功能，具体操作请参见《镜像服务用户指南》。
弹性文件服务	用户通过弹性文件服务创建文件系统时，选择KMS提供的用户主密钥对文件系统进行加密，当使用该文件系统时，存储到文件系统的文件将会自动加密。 用户如何使用弹性文件服务的文件系统加密功能，具体操作请参见《弹性文件服务用户指南》。
云数据库RDS	在购买数据库实例时，用户启用数据库实例的磁盘加密功能，选择KMS提供的用户主密钥对数据库实例的磁盘进行加密，选择磁盘加密后会提高数据的安全性。 用户如何使用云数据库RDS的磁盘加密功能，具体操作请参见《云数据库RDS用户指南》。

服务名称	如何使用
文档数据库服务	在购买文档数据库实例时，用户启用文档数据库实例的磁盘加密功能，选择KMS提供的用户主密钥对文档数据库实例的磁盘进行加密，选择磁盘加密后会提高数据的安全性。 用户如何使用文档数据库的磁盘加密功能，具体操作请参见**《文档数据库服务用户指南》**。

与用户的应用程序配合使用

当您的应用程序需要对明文数据进行加密时，可通过调用KMS的接口来创建数据加密密钥，再使用数据加密密钥将明文数据进行加密，得到密文数据并进行存储。同时，用户的应用程序调用KMS的接口创建对应用户主密钥，对数据加密密钥进行加密，得到密文的数据加密密钥并进行存储。

基于信封加密技术，用户主密钥存储在KMS中，用户的应用程序只存储密文的数据加密密钥，仅在需要使用时调用KMS解密数据加密密钥。

加密流程说明如下：

1. 应用程序调用KMS的“create-key”接口创建一个自定义密钥。
2. 应用程序调用KMS的“create-datakey”接口创建数据加密密钥。得到一个明文的数据加密密钥和一个密文的数据加密密钥。

   说明

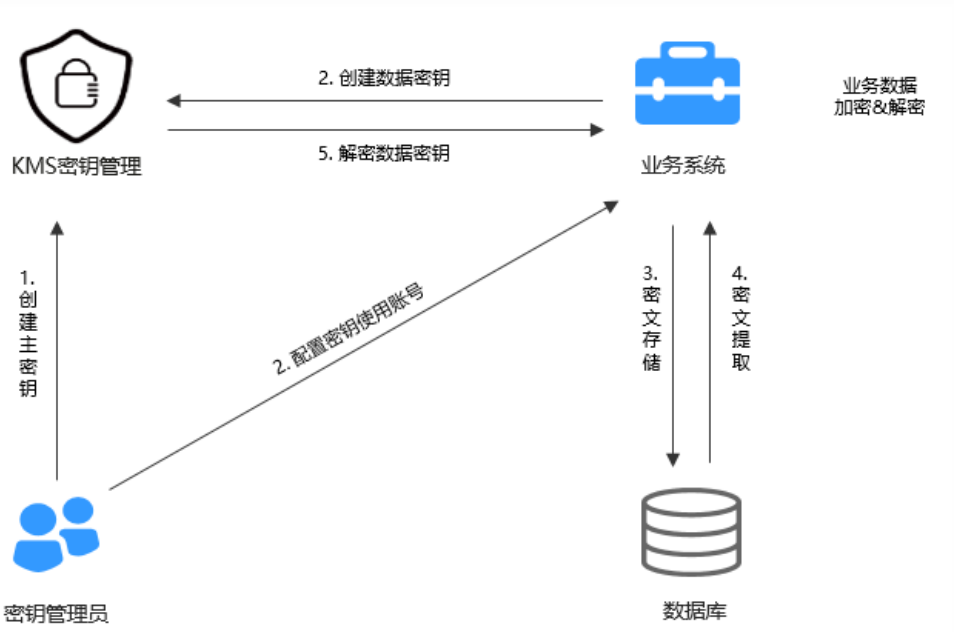
   密文的数据加密密钥是由**1**创建的用户主密钥加密明文的数据加密密钥生成的。
3. 应用程序使用明文的数据加密密钥来加密明文文件，生成密文文件。
4. 应用程序将密文的数据加密密钥和密文文件一同存储到持久化存储设备或服务中。

具体操作请参见**《数据加密服务API参考》**。

3.5 场景示例

应用自集成 KMS

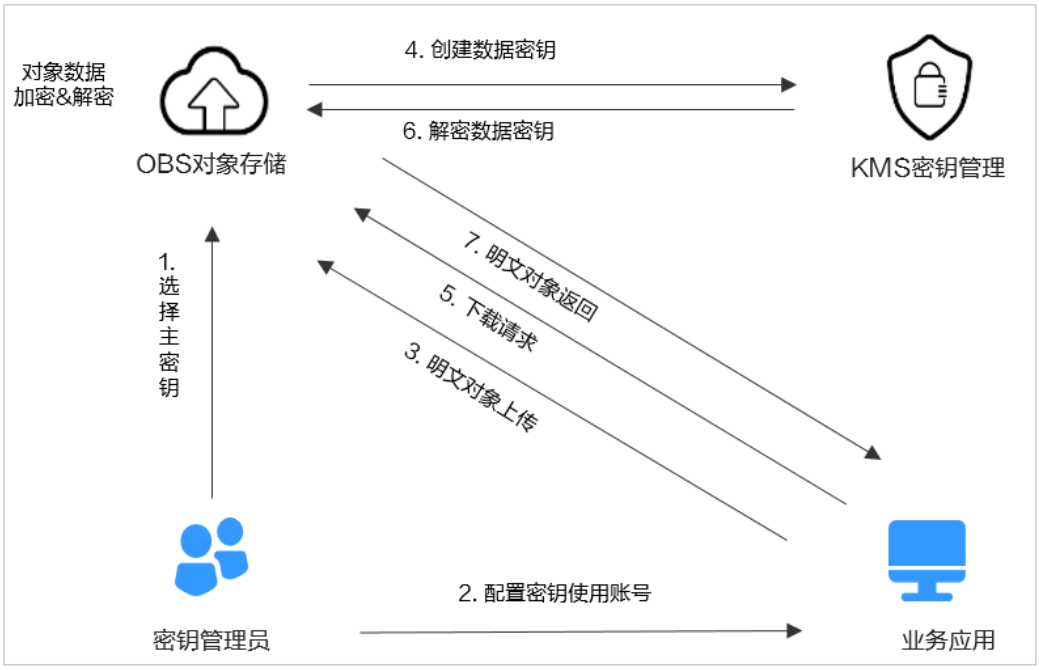
图 3-6 应用自集成 KMS 原理



- 用户使用KMS密钥管理对业务系统进行数据的加密与解密，需使用集成SDK，具体请参见**SDK概述**。
- 用户在业务系统中使用KMS密钥管理时，可灵活调用API实现更多功能，例如**签名数据**、**验证签名**等。

云服务集成 KMS 加解密

图 3-7 云服务集成 KMS 原理



- 用户在使用KMS加解密功能时，无需额外开发，具体操作可参见**使用KMS加密的云服务**。
- 针对大量数据的加解密场景，操作可参见**加解密大量数据**。

3.6 使用 KMS 加密的云服务

3.6.1 OBS 服务端加密

- 用户使用OBS（Object Storage Service，OBS）服务端加密方式上传时，可以选择“SEE-KMS加密”，从而使用KMS提供的密钥来加密上传的文件，如**图3-8**所示。更多信息请参见**《对象存储服务控制台指南》**。

图 3-8 OBS 服务端加密

可供选择的用户主密钥包含以下两种：

- KMS为使用OBS的用户创建一个默认密钥“obs/default”。
- 用户通过KMS界面创建的自定义密钥。

说明

SM4加密算法仅支持华北-乌兰察布一区域。

- 用户也可以通过调用OBS API接口，选择服务端加密SSE-KMS方式（SSE-KMS方式是指OBS使用KMS提供的密钥进行服务端加密）上传文件，详情请参考**《对象存储服务API参考》**。

3.6.2 EVS 服务端加密

- 用户创建磁盘时，可以选择“高级配置 > 加密”，使用KMS提供的密钥来加密磁盘上的数据，如**图3-9**所示。更多信息请参见。

说明

当用户需要使用磁盘加密功能时，需要授权云硬盘访问密钥管理。如果用户有授权资格，则可直接授权。如果权限不足，需先联系Security Administrator权限用户添加Security Administrator权限，然后重新操作。详细信息请参见。

图 3-9 EVS 服务端加密

可供选择的用户主密钥包含以下两种：

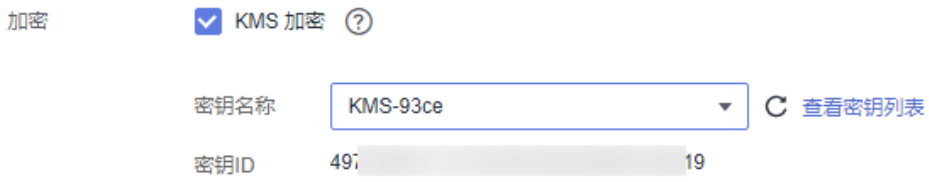
- KMS为使用EVS（Elastic Volume Service，EVS）的用户创建一个默认密钥“evs/default”。
- 用户通过KMS界面创建的自定义密钥。

- 用户也可以通过调用EVS API接口创建加密磁盘，详情请参考《云硬盘API参考》。

3.6.3 IMS 服务端加密

- 用户使用OBS桶中已上传的外部镜像文件创建私有镜像时，可以选择“KMS加密”，使用KMS提供的密钥来加密镜像，如图3-10所示，更多信息请参见 。

图 3-10 IMS 服务端加密



可供选择的用户主密钥包含以下两种：

- KMS为使用IMS（Image Management Service，IMS）的用户创建一个默认密钥“ims/default”。
- 用户通过KMS界面创建的自定义密钥。

- 用户也可以通过调用IMS API接口创建加密镜像，详情请参考《镜像服务API参考》。

3.6.4 SFS 服务端加密

- 用户通过弹性文件服务（Scalable File Service，SFS）创建文件系统时，可以选择“KMS加密”，使用KMS提供的密钥来加密文件系统，如图3-11所示。更多信息请参见《弹性文件服务用户指南》。

图 3-11 SFS 服务端加密

用户可选择通过KMS界面创建的自定义密钥进行加密。

- 用户也可以通过调用SFS API接口创建加密的文件系统，详情请参考《弹性文件服务API参考》。

3.6.5 RDS 服务端加密

- 用户在通过云数据库（Relational Database Service，RDS）购买数据库实例时，可以选择“磁盘加密”，使用KMS提供的密钥来加密数据库实例的磁盘，更多信息请参见《云数据库RDS用户指南》。

图 3-12 RDS 服务端加密

用户可选择通过KMS界面创建的自定义密钥进行加密。

- 用户也可以通过调用RDS API接口购买加密数据库实例，详情请参考《云数据库RDS API参考》。

3.6.6 DDS 服务端加密

- 用户在通过文档数据库服务（Document Database Service，DDS）购买文档数据库实例选择自定义购买时，可以选择“磁盘加密”，使用KMS提供的密钥来加密文档数据库实例的磁盘，更多信息请参见《文档数据库服务用户指南》。

图 3-13 DDS 服务端加密

用户可选择通过KMS界面创建的自定义密钥进行加密。

- 用户也可以通过调用DDS API接口购买加密数据库实例，详情请参考《 文档数据库API参考 》。

4 凭据管理

4.1 功能特性

凭据管理，即云凭据管理服务（Cloud Secret Management Service，CSMS），是一种安全、可靠、简单易用的凭据托管服务。用户或应用程序通过凭据管理服务，创建、检索、更新、删除凭据，轻松实现对敏感凭据的全生命周期的统一管理，有效避免程序硬编码或明文配置等问题导致的敏感信息泄露以及权限失控带来的业务风险。

凭据统一管理

应用系统中存在大量的敏感凭据信息，且分散到不同业务部门及系统，管理混乱，缺乏集中管理工具。

通过凭据管理服务对敏感凭据进行统一的存储、检索、使用等全生命周期管控。

解决方案说明如下：

1. 用户或管理员对应用敏感凭据进行收集。
2. 将收集的敏感凭据上传托管到凭据管理服务。
3. 通过IAM细粒度功能，对每个凭据的访问和使用配置对应的权限策略。

凭据安全检索

应用程序访问数据库或其他服务时，需要提供如密码、令牌、证书、SSH 密钥、API 密钥等各种类型的凭据信息进行身份校验，通常是直接使用明文方式将上述凭据嵌入在应用程序的配置文件中。该场景存在凭据信息硬编码、明文存储易泄露和安全性较低等风险问题。

通过凭据管理服务，用户可以将代码中的硬编码替换为对API 的调用，以便用编程的方式动态查询凭据，由于该凭据中不包含敏感信息，保证凭据不被泄露。

解决方案说明如下：

应用读取配置时，调用凭据管理服务API检索读取凭据（代替硬编码和明文凭据）。

轮换凭据和密钥

为提升系统安全性，需要对敏感凭据进行定期更新。凭据轮换时要求对目标凭据具备依赖性的应用或配置同步更新，多应用系统凭据更新容易遗漏，可能带来业务中断风险。

通过凭据管理服务，提供凭据多版本管理，应用节点通过API/SDK调用实现应用层凭据安全轮换。

解决方案说明如下：

1. 管理员通过凭据管理控制台或API接口新增凭据版本，更新目标凭据内容。
2. 应用节点通过调用API/SDK 获取最新凭据版本，或指定版本状态的凭据，实现全量或灰度的凭据轮换。
3. 定期重复**步骤1**和**步骤2**实现凭据定期轮转。
4. 加密密钥开启密钥轮换，提高存储安全性。

凭据事件通知

用户为凭据对象订阅关联事件后，当事件为启用状态且基础事件类型在凭据对象上触发时，通过消息通知服务（SMN）对应事件通知会发送至事件指定的通知主题上。基础事件类型包括：凭据新版本创建，凭据版本过期，凭据删除，凭据轮转。配置事件通知后，用户可以通过函数工作流服务(FunctionGraph)中基于事件驱动的托管函数来自动化轮转凭据。

解决方案说明如下：

1.管理员通过凭据管理服务的事件通知控制台或者调用API接口新增事件。

2.创建或更新凭据时，关联订阅所需的事件对象。

3.用户在凭据状态发生改变时收到事件通知消息，并可在函数工作流服务(FunctionGraph)中配置函数，来实现凭据自动更新或轮转等功能。

凭据管理基本功能

表 4-1 凭据管理基本功能

功能	服务内容
凭据全生命周期管理	• 创建、查看、定时删除、取消删除凭据 • 修改凭据的加密密钥和描述信息
凭据版本管理	• 创建、查看凭据版本 • 查看凭据值 • 凭据版本到期设置
凭据版本状态管理	更新、查询、删除凭据版本状态
凭据标签管理	添加、搜索、编辑、删除标签
凭据事件管理	• 创建、查看、删除事件 • 修改凭据事件类型

功能	服务内容
凭据通知管理	查看变更事件类型、事件名称、凭据名称

4.2 产品优势

凭据加密保护

凭据通过集成KMS进行加密存储，加密密钥基于第三方认证的硬件安全模块（HSM）来生成和保护。凭据检索时，通过 TLS 安全传输到服务器本地。

凭据安全检索

使用CSMS服务，将应用程序代码中的硬编码凭据替换为对凭据的API调用，以便以编程方式动态检索和管理凭据，实现凭据安全管理。同时对分散在各个应用程序中的敏感凭据统一集中管理，降低暴露风险。

凭据集中管控

与IAM集成，通过身份、权限管理确保只有授权用户可以检索或修改凭据，与CTS集成，持续监控对凭据的操作访问。有效防范对敏感信息的非法访问和泄漏。

凭据变更通知

通过与SMN服务集成，凭据基础事件变化及时通知，并通过函数工作流服务(FunctionGraph)配置函数，实现凭据自动更新或轮转等功能。

凭据安全调用

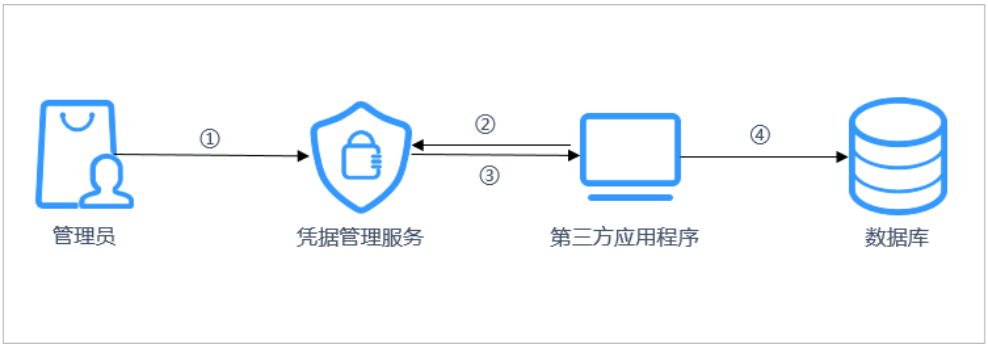
与CCE集成，通过CCE插件允许用户将凭据挂载至业务Pod内，从而将敏感信息与集群环境解耦，有效避免程序硬编码或明文配置等问题导致的敏感信息泄密。

4.3 使用场景

以最基础的数据库用户名及密码管理为示例，为您介绍凭据管理服务基本的使用场景。

使用场景：管理员角色负责存入、更新凭据值的操作，使用者通过第三方应用服务获取所需的凭据值，具体使用流程如图4-1所示。

图 4-1 凭据登录流程



流程说明如下：

步骤1 您首先需要在凭据管理服务中使用**控制台**或者API创建一个凭据，用来存储数据库的相关信息（例如：数据库地址、端口、密码）。

步骤2 当您使用应用程序访问数据库时，凭据管理服务会去查询管理员通过步骤1所创建的凭据内存储的内容。

步骤3 凭据管理服务检索并解密凭据密文，将凭据中保存的信息通过凭据管理API安全地返回到应用程序中。

步骤4 应用程序获取到解密后的凭据明文信息，使用这些安全的信息访问数据库。

----结束

5 密钥对管理

5.1 功能特性

密钥对管理，即密钥对管理服务（Key Pair Service，KPS），是一种安全、可靠、简单易用的SSH密钥对托管服务，帮助用户集中管理SSH密钥对，保护SSH密钥对的安全。

SSH密钥对，简称为密钥对，是为用户提供的远程登录Linux云服务器的认证方式，是一种区别于传统的用户名和密码登录的认证方式。

密钥对是通过加密算法生成的一对密钥，包含一个公钥和一个私钥，公钥自动保存在KPS中，私钥由用户保存在本地。用户也可以根据自己的需要将私钥托管在KPS中，由KPS统一管理。如果用户将公钥配置在Linux云服务器中，则可以使用私钥登录Linux云服务器，而不需要输入密码。由于密钥对可以让用户无需输入密码登录到Linux云服务器，因此，可以防止由于密码被拦截、破解造成的账户密码泄露，从而提高Linux云服务器的安全性。

功能介绍

用户可通过密钥对管理界面或接口，对密钥对进行以下操作：

- 创建、导入、查看、删除密钥对
- 重置、替换、绑定、解绑密钥对
- 托管、导入、导出、清除私钥

KPS 支持的密码算法

- 通过管理控制台创建的SSH密钥对支持的加解密算法为：
  - SSH-ED25519
  - ECDSA-SHA2-NISTP256
  - ECDSA-SHA2-NISTP384
  - ECDSA-SHA2-NISTP521
  - SSH_RSA有效长度为：2048，3072，4096
- 通过外部导入的SSH密钥对支持的加解密算法为：
  - SSH-DSS

- SSH-ED25519
- ECDSA-SHA2-NISTP256
- ECDSA-SHA2-NISTP384
- ECDSA-SHA2-NISTP521
- SSH_RSA有效长度为：2048，3072，4096

5.2 产品优势

- 登录安全增强

  无需密码登录到Linux云服务器，可以有效防止密码被拦截、破解造成的账户密码泄露，从而提高Linux云服务器的安全性。
- 合规遵循

  对密钥对的所有操作都会进行访问控制及日志跟踪，符合中国和国际法律合规的要求。

5.3 使用场景

用户在购买弹性云服务器（Elastic Cloud Server，简称ECS）时，选择密钥对管理服务（Key Pair Service, KPS）提供的SSH密钥对对登录弹性云服务器的用户进行身份认证，或者通过提供的密钥对获取Windows操作系统弹性云服务器的登录密码。

登录 Linux 操作系统的弹性云服务器

如果用户购买的是Linux操作系统的弹性云服务器，可以选择“密钥对方式”登录，详细信息请参见**《弹性云服务器用户指南》**。

购买弹性云服务器时，可供选择的密钥对包含以下两种：

- 用户通过云服务器控制台界面创建或者导入密钥对。
- 用户通过密钥对管理服务（Key Pair Service, KPS）界面创建或者导入密钥对。

两种密钥对没有区别，只是导入的渠道不同。

获取 Windows 操作系统弹性云服务器的登录密码

如果用户购买的是Windows操作系统的弹性云服务器，需要使用密钥对的私钥获取登录密码，详细信息请参见**《弹性云服务器用户指南》**。

购买弹性云服务器时，可供选择的密钥对包含以下两种：

- 用户通过云服务器控制台界面创建或者导入密钥对。
- 用户通过密钥对管理服务（Key Pair Service, KPS）界面创建或者导入密钥对。

两种密钥对没有区别，只是导入的渠道不同。

6 专属加密

6.1 图解专属加密

6.2 功能特性

专属加密（Dedicated Hardware Security Module，Dedicated HSM）是一种云上数据加密的服务，可处理加解密、签名、验签、产生密钥和密钥安全存储等操作。

Dedicated HSM为您提供经国家密码管理局检测认证的加密硬件，帮助您保护弹性云服务器上数据的安全性与完整性，满足FIPS 140-2安全要求。同时，您能够对专属加密实例生成的密钥进行安全可靠的管理，也能使用多种加密算法来对数据进行可靠的加解密运算。

功能介绍

Dedicated HSM提供以下功能：

- 生成、存储、导入、导出和管理加密密钥（包括对称密钥和非对称密钥）。
- 使用对称和非对称算法加密和解密数据。
- 使用加密哈希函数计算消息摘要和基于哈希的消息身份验证代码。
- 对数据进行加密签名（包括代码签名）并验证签名。
- 以加密方式生成安全随机数据。

Dedicated HSM 支持的密码算法

支持国密算法以及部分国际通用密码算法，满足用户各种加密算法需求。

表 6-1 Dedicated HSM 支持的密码算法

加密算法分类	通用密码算法	国密算法
对称密码算法	AES	SM1、SM4、SM7
非对称密码算法	RSA（1024-4096）	SM2
摘要算法	SHA1、SHA256、SHA384	SM3

Dedicated HSM 支持的密码机类型

表 6-2 Dedicated HSM 支持的密码机类型

密码机类型	功能	适用场景
服务器密码机	• 数据加密/解密 • 数据签名/验签 • 数据摘要 • 支持MAC的生成和验证	满足各种行业应用中的基础密码运算需求，比如身份认证、数据保护、SSL密钥和运算卸载等。

密码机类型	功能	适用场景
金融密码机	• 支持PIN码的生成/加密/转换/验证 • 支持MAC生成及验证 • 支持CVV生成及验证 • 支持TAC生成及验证 • 支持常用Racal指令集 • 支持PBOC3.0常用指令集	满足金融领域密码运算需求，比如发卡系统、POS系统等。
签名验证服务器	• 签名/验签 • 编码/解码数字信封 • 编码/解码带签名的数字信封 • 证书验证	满足签名业务相关需求，比如CA系统、证书验证、大量数据的加密传输和身份认证。

6.3 产品优势

- 云上使用

  Dedicated HSM旨在满足用户将线下加密设备能力转移到云上的要求，降低运维成本。

- 弹性扩容

  灵活调整专属加密的数量，满足不同业务的加解密运算要求。

- 安全管理

  专属加密实例设备管理与内容（敏感信息）管理权限分离，用户作为设备使用者完全控制密钥的产生、存储和访问授权，Dedicated HSM只负责监控和管理设备及其相关网络设施。即使Dedicated HSM的运维人员也无法获取到用户的密钥。

- 权限认证
  - 敏感指令支持分类授权控制，有效防止越权行为。
  - 支持用户名口令认证、数字证书认证等多种权限认证方式。

- 可靠性
  - 基于国家密码局认证或FIPS 140-2第3级验证的硬件加密机，对高安全性要求的用户提供高性能专属加密服务。
  - 专属加密实例之间独享加密芯片，即使部分硬件芯片损坏也不影响使用。
  - 基于加密机的备份能力提供可靠的备份和托管加密机数据的方案。

- 安全合规

  Dedicated HSM为您提供经国家密码管理局检测认证的专属加密实例，帮助您保护弹性云服务器上数据的安全性和隐私性要求，满足监管合规要求。

- 应用广泛

  Dedicated HSM可提供认证合规的金融加密机、服务器加密机以及签名验签服务器等，灵活支撑用户业务场景。

6.4 使用场景

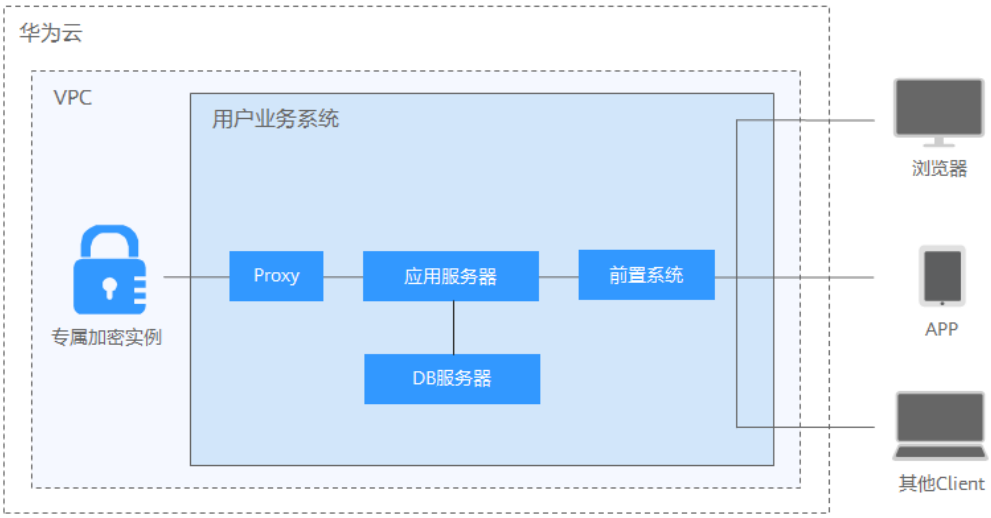
如果用户购买了专属加密实例，可通过Dedicated HSM提供的**Ukey**初始化并管控专属加密实例。用户作为设备使用者完全控制密钥的产生、存储和访问授权。

用户可通过专属加密实例加密用户业务系统（包含敏感数据加密、金融支付加密以及电子票据加密等），帮助用户加密企业自身的敏感数据（如合同、交易、流水等）以及企业用户的敏感数据（用户身份证号码、手机号码等），以防止黑客攻破网络、拖库导致数据泄露、内部用户非法访问或篡改数据等风险。

说明

用户需要将专属加密实例和业务系统部署在同一个VPC内，并选择合适的安全组规则。如果您对此有疑问，请咨询客服人员。

图 6-1 产品架构



敏感数据加密

应用领域：政府公共事业、互联网企业、包含大量敏感信息的系统应用。

数据是企业的核心资产，每个企业都有自己的核心敏感数据。通过专属加密服务对敏感数据进行完整性校验和加密存储，有效防止敏感数据被窃取、篡改，权限被非法获取。

金融支付

应用领域：交通卡支付、电商支付、各种预付费卡支付等系统应用

保证支付数据在传输和存储过程中的完整性、保密性和支付身份的认证、支付过程的不可否认性。

验伪

应用领域：交通、制造、医疗。

保证电子合同、电子发票、电子保单、电子病例在传输、存储过程中的保密性和完整性。

6.5 版本说明

专属加密提供标准版、铂金版（国内）专属加密实例，具体服务内容如表6-3所示。

说明

带*条目根据不同型号设备略有不同，请联系客服进行确认。

表 6-3 专属加密

功能	服务内容	标准版-虚拟共享	铂金版（国内）-单用户独占
独享芯片加密	用户独享云端密码芯片资源，实现用户密钥硬件隔离的同时保障业务性能	支持	支持
全业务支持	支持金融支付、身份认证、数字签名等应用安全，满足各种重要系统对于数据安全性的严苛要求	支持	支持
弹性扩展	可根据您的业务需要弹性地增加和缩减密码运算资源	支持	支持
高可靠	后端硬件设备可以HA双机（主-备）部署，实现高可靠（需订购2个实例实现）	支持	支持
兼容性	提供与实体密码设备相同的功能与接口，方便向云端迁移，具体支持： PKCS#11接口，CSP接口，JCE接口，GM/T 0018-2012 SDF接口等	支持	支持
机框、电源独占	用户独享硬件加密机机框、电源资源	不支持	支持
网络独占	用户独享硬件加密机网络带宽、接口资源	不支持	支持
FIPS 140-2认证	采用符合 FIPS 140-2 第 3 级标准的 HSM 上生成和使用加密密钥	不支持	不支持
通用算法	对称算法	AES	AES
	非对称算法	RSA（1024，4096）*	RSA（1024，4096）*

功能	服务内容	标准版-虚拟共享	铂金版（国内）-单用户独占
	摘要算法	SHA1、SHA256、SHA384	SHA1、SHA256、SHA384
国密算法	对称算法	SM1、SM4、SM7 *	SM1、SM4、SM7 *
	非对称算法	SM2	SM2
	摘要算法	SM3	SM3
通用算法性能	RSA2048验签运算性能	3,500 TPS	40,000 TPS
	RSA2048签名运算性能	400 TPS	4,000 TPS
国密算法性能	SM1加密运算性能	600 TPS	15,000 TPS
	SM2签名运算性能	3,000 TPS	80,000 TPS
	SM2验签运算性能	2,000 TPS	15,000 TPS
	SM4加密运算性能	4000~35000Tps*	35000~40000Tps*
	SM4解密运算性能	4000~30000Tps*	35000~40000Tps*
	SM7算法性能	1000Tps*	1000Tps*
数据通讯	TCP/IP 最大并发连接	64	2,048

7 云平台密码系统服务

7.1 什么是云平台密码系统服务

云平台密码系统服务（Cloud Platform Cryptosystem Service, CPCS），提供专属的密码服务以及服务集群化部署能力。

具备密码服务集群的全生命周期管理的能力，包括自动化部署与释放、集群弹性伸缩、集群调用的应用级隔离等，并对各类能力进行集中监控、配置等，帮助租户快速通过密评。

主要包含以下密码服务：加解密服务、签名验签服务、密钥管理服务、时间戳服务、协同签名服务、动态令牌服务、数据库加密服务、文件加密服务、电子签章服务、SSL VPN服务。

7.2 功能特性

资源总览

通过控制台集中展示租户密码服务资源使用情况，动态监控密码服务集群的核心API调用情况。

专属密码服务

提供密码服务集群的全自动化部署与生命周期管理。

表 7-1 专属密码集群基本功能

功能	服务内容
集群全生命周期管理	• 创建、查看、删除集群。 • 集群实例弹性伸缩
集群实例管理	• 创建、查看、删除集群实例。 • 启用、禁用集群实例

功能	服务内容
集群应用管理	● 绑定、解绑应用
集群访问管理	● 为集群授权、解除授权访问密钥

应用管理

提供应用管理功能，租户记录自身业务所在的网络地址以及描述信息后，通过CPCS提供的专属网络隔离能力、访问密钥动态管理能力，可以减少安全风险，保护资源的安全性、机密性。通过绑定集群打通网络访问，使用访问密钥管理，可以对访问权限进行集中管控，通过身份认证以获取访问的授权，进行1对1访问。

7.3 产品优势

自动化部署

CPCS服务实现密码服务集群自动化部署，并且实现快速弹性伸缩。

集群隔离

- 租户级隔离
- VPC级隔离
- 应用级隔离

态势感知

动态监控密码服务资源使用情况、密码能力调用情况、集群实例健康状态检查等。

加密场景

专属加密集群支持多加密场景选择，可以通过不同加密需求选择对应密码服务类型。

- 加解密服务
- 签名验签服务
- 密钥管理服务
- 时间戳服务
- 协同签名服务
- 动态令牌服务
- 数据库加密服务
- 文件加密服务
- 电子签章服务
- SSL_VPN服务

7.4 应用场景

密码服务能力

- 网络安全访问
  通过集群完成公网访问的验证与接入，确保数据安全性。
- 应用部署上云
  通过VPC以及子网信息，将应用部署上云，通过与集群联动，实现应用级隔离访问。

8 安全

8.1 责任共担

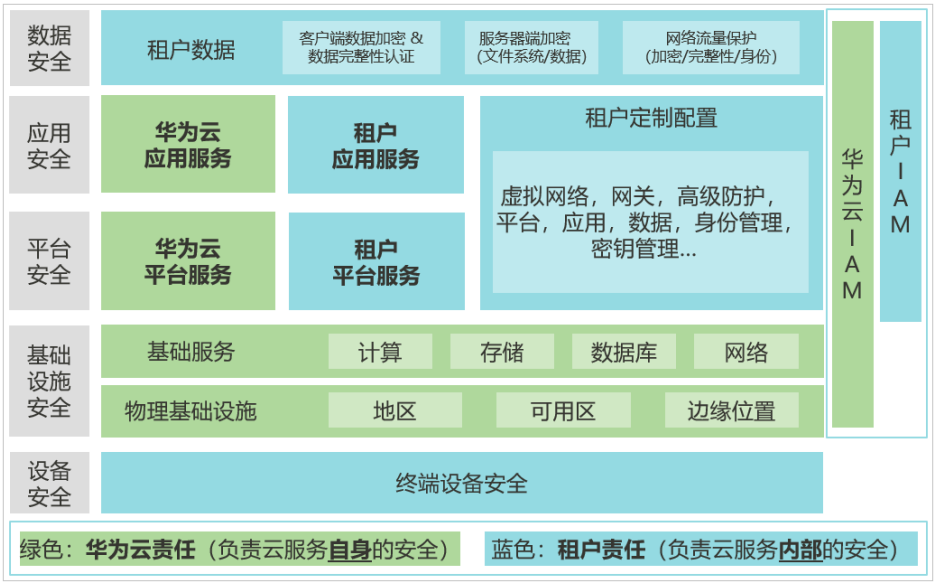
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图8-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 8-1 华为云安全责任共担模型



8.2 资产识别与管理

DEW服务涉及的用户核心资产及管理方式详见下表：

资产所属的子服务	资产名称	资产管理方式
密钥管理KMS	用户密钥	用户密钥使用硬件加密机保护。
凭据管理CSMS	用户凭据	用户凭据使用硬件加密机保护。
密钥对管理KPS	密钥对	密钥对使用硬件加密机保护。
专属加密DHSM	专属加密实例	专属加密实例的操作权限完全交给用户控制，密码机硬件由华为云数据中心机房进行统一管理。

8.3 身份认证与访问控制

身份认证

用户访问DEW的方式有多种，包括DEW控制台、API、SDK，无论访问方式封装成何种形式，其本质都是通过DEW提供的REST风格的API接口进行请求。

DEW的接口支持多种认证请求，以AK/SK举例：经过认证的请求总是需要包含一个签名值，该签名值以请求者的访问密钥（AK/SK）作为加密因子，结合请求体携带的特定信息计算而成。通过访问密钥（AK/SK）认证方式进行认证鉴权，即使用Access Key ID（AK）/Secret Access Key（SK）加密的方法来验证某个请求发送者身份。详情请参见**认证鉴权**。

访问控制

- DEW支持通过统一身份认证服务（Identity and Access Management，IAM）实现精细化的访问控制。默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作，请参见**权限管理**。
- 针对KMS子服务，还另外提供了在KMS页面配置授权功能。用户可以为其他IAM用户或账号创建授权，授予其使用自身的用户主密钥（CMK）的权限，一个用户主密钥下最多可创建100个授权，请参见**KMS管理授权**。

8.4 数据保护技术

DEW通过多种数据保护手段和特性，保障存储在DEW中数据安全可靠。

数据保护手段	简要说明	详细介绍
传输加密（HTTPS）	DEW支持HTTPS传输协议，为数据传输的安全性提供保证。	**如何构造HTTPS协议请求**
密钥管理	用户密钥材料的管理和存储采用硬件加密机进行保护，避免密钥泄露。	**密钥管理功能特性**
信封加密	对于大量数据加解密场景，DEW提供信封加密方式来保护应用系统中敏感数据的安全，加密数据的数据密钥随信封进行存储、传递和使用。	**加解密大量数据**
密钥轮换机制	当广泛重复地使用加密密钥，势必对加密密钥的安全造成风险。DEW支持用户定期密钥轮换，更改原有的密钥材料，以符合加密最佳实践的要求。	**密钥轮换概述**
凭据管理	DEW提供凭据的全生命周期管理和安全便捷的应用接入方式，帮助您降低硬编码方式带来的凭据泄露风险，提升数据及资产的安全性。	**凭据管理功能特性**
密钥导入	用户在向KMS服务导入密钥材料时，支持RSAES_OAEP_SHA_256和SM2_ENCRYPT这2种密钥包装算法进行加密保护。	**导入密钥材料**

8.5 审计与日志

云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等应用场景。

CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

CTS支持追踪数据加密服务相关的操作事件，请参见**审计日志**。

8.6 服务韧性

DEW服务采用故障隔离、数据备份、流量控制等多种方式提高服务韧性，保证用户数据安全。

故障隔离

- DEW采用region间隔离设计，可以确保任何一个region的故障不会影响其它region的DEW服务。
- DEW的基础设施包括服务器和加密机等采用AZ级容灾设计，任何一个AZ的故障不会影响DEW服务的可用性，DEW服务将自动屏蔽发生故障的AZ并将流量切换到其它AZ，实现业务的平滑调度。
- DEW的基础设施包括服务器和加密机等采用集群设计，任何一个服务器或加密机的可用性问题不会影响DEW服务的可用性。

数据备份

DEW的密钥在多台加密机中进行复制，可以确保任何一台加密机的故障不会导致密钥的丢失。同时，DEW的数据（非敏感数据）在多个服务器和数据库实例间进行复制，并实时备份以确保数据不会丢失。

流量控制

DEW服务能够达到99.95%的可用性SLA，同时为单个用户提供较高的API调用配额。当单个用户的API调用量达到配额后，DEW服务会限制该用户后续的API调用，从而保障服务的可用性。

8.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 8-2 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 8-3 资源中心

销售许可证&软件著作权证书

另外，华为云还提供了以下销售许可证及软件著作权证书，供用户下载和参考。具体请查看**合规资质证书**。

图 8-4 销售许可证&软件著作权证书

9 DEW 权限管理

如果您需要对华为云上购买的数据加密服务（DEW）资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为账号中给员工创建IAM用户，并使用策略来控制员工对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望开发人员拥有数据加密服务（DEW）的使用权限，但是不希望开发人员拥有删除DEW等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用DEW，但是不允许删除DEW的权限策略，控制开发人员对云资源的使用范围。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用DEW的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

DEW 权限

默认情况下，KMS管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

DEW部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京1）对应的项目（cn-north-1）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问DEW时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对DEW服务，KMS管理员能够控制IAM

用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，权限的最小粒度为API授权项（action）。DEW支持的API授权项请参见**DEW权限及授权项**。

如**表 KMS系统策略**、**表 KPS系统策略**、**表 CSMS系统策略**所示，包括了DEW的所有系统权限。

表 9-1 KMS 系统策略

系统角色/策略名称	描述	类别	依赖关系
KMS Administrator	密钥管理服务(KMS)管理员，拥有该服务下的所有权限。	系统角色	无
KMS CMKFullAccess	密钥管理服务(KMS)的加密密钥所有权限。拥有该权限的用户可以完成基于策略授权的所有操作。	系统策略	无
KMS CMKReadOnlyAccess	密钥管理服务(KMS)的加密密钥只读权限。拥有该权限的用户可以完成基于策略授权的所有操作。	系统策略	无

表 9-2 KPS 系统策略

系统角色/策略名称	描述	类别	依赖关系
DEW KeypairFullAccess	数据加密服务中密钥对管理服务(KPS)的所有权限。拥有该权限的用户可以完成基于策略授权的所有操作。	系统策略	无
DEW KeypairReadOnlyAccess	数据加密服务中密钥对管理服务(KPS)的查看权限。拥有该权限的用户仅能查看密钥对管理服务(KPS)数据。	系统策略	无

表 9-3 CSMS 系统策略

系统角色/策略名称	描述	类别	依赖关系
CSMS FullAccess	数据加密服务中凭据管理服务(CSMS)的所有权限。拥有该权限的用户可以完成基于策略授权的所有操作。	系统策略	无
CSMS ReadOnlyAccess	数据加密服务中凭据管理服务(CSMS)的只读权限。拥有该权限的用户可以完成基于策略授权的所有操作。	系统策略	无

说明

DEW KeypairFullAccess、DEW KeypairReadOnlyAccess策略用于进行企业项目授权时，对个人用户授权后无法生效。

如果个人用户需使用企业项目授权，需将个人用户加入用户组，对用户组整体进行授权后，该个人用户才能正常使用企业项目。

表9-4列出了DEW常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 9-4 常用操作与 KMS 系统权限的关系

操作	KMS Administrator	KMS CMKFullAccess
创建密钥	√	√
启用密钥	√	√
禁用密钥	√	√
计划删除密钥	√	√
取消计划删除密钥	√	√
修改密钥别名	√	√
修改密钥描述	√	√
创建随机数	√	√
创建数据密钥	√	√
创建不含明文数据密钥	√	√
加密数据密钥	√	√
解密数据密钥	√	√
获取密钥导入参数	√	√
导入密钥材料	√	√
删除密钥材料	√	√
创建授权	√	√
撤销授权	√	√
退役授权	√	√
查询授权列表	√	√
查询可退役授权列表	√	√
加密数据	√	√
解密数据	√	√
签名消息	√	√

操作	KMS Administrator	KMS CMKFullAccess
验证签名	√	√
开启密钥轮换	√	√
修改密钥轮换周期	√	√
关闭密钥轮换	√	√
查询密钥轮换状态	√	√
查询密钥实例	√	√
查询密钥标签	√	√
查询项目标签	√	√
批量添加删除密钥标签	√	√
添加密钥标签	√	√
删除密钥标签	√	√
查询密钥列表	√	√
查询密钥信息	√	√
查询公钥信息	√	√
查询实例数	√	√
查询配额	√	√
查询密钥对列表	x	x
创建或导入密钥对	x	x
查询密钥对	x	x
删除密钥对	x	x
更新密钥对描述	x	x
绑定密钥对	x	x
解绑密钥对	x	x
查询绑定任务信息	x	x
查询失败的任务	x	x
删除所有失败的任务	x	x
删除失败的任务	x	x
查询正在处理的任务	x	x

相关链接

- IAM产品介绍
- 创建用户组、用户并授予DEW权限
- 权限支持的授权项

10 如何访问

公有云提供了Web化的服务管理平台，即管理控制台管理方式和基于HTTPS请求的API（Application Programming Interface）管理方式。

- 管理控制台方式

  如果用户已注册公有云，可直接登录管理控制台，单击管理控制台左上角的，选择区域或项目后，单击页面左侧的，选择“安全与合规 > 数据加密服务”。

- API方式

  用户可通过接口方式访问数据加密服务，具体操作请参见《数据加密服务API参考》。

11 与其他云服务的关系

与对象存储服务的关系

对象存储服务（Object Storage Service，OBS）是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力。KMS为OBS提供用户主密钥管理控制能力，应用于对象存储服务的服务端加密功能（SSE-KMS加密方式）。

与云硬盘的关系

云硬盘（Elastic Volume Service，EVS）可以为云服务器提供高可靠、高性能、规格丰富并且可弹性扩展的块存储服务，可满足不同场景的业务需求，适用于分布式文件系统、开发测试、数据仓库以及高性能计算等场景。KMS为EVS提供用户主密钥管理控制能力，应用于云硬盘的加密功能。

与镜像服务的关系

镜像服务（Image Management Service，IMS）提供镜像的生命周期管理能力。KMS为IMS提供用户主密钥管理控制能力，应用于镜像服务的私有镜像加密功能。

与弹性文件服务的关系

弹性文件服务（Scalable File Service，SFS）提供按需扩展的高性能文件存储（NAS）。KMS为SFS提供用户主密钥管理控制能力，应用于弹性文件服务的文件系统加密功能。

与云数据库的关系

云数据库（Relational Database Service，RDS）是一种基于云计算平台的即开即用、稳定可靠、弹性伸缩、便捷管理的在线云数据库服务。KMS为RDS提供用户主密钥管理控制能力，应用于云数据库的磁盘加密功能。

与弹性云服务器的关系

弹性云服务器（Elastic Cloud Server，ECS）是由CPU、内存、操作系统、云硬盘组成的基础的计算组件。弹性云服务器创建成功后，您就可以像使用自己的本地PC或物理服务器一样，在云上使用弹性云服务器。

KPS为ECS提供密钥对的管理控制能力，应用于用户登录弹性云服务器时，对用户身份认证的功能。

Dedicated HSM提供的专属加密实例可以为部署在弹性云服务器内的业务系统加密敏感数据，用户可完全控制密钥的生成、存储和访问授权，保证数据在传输、存储过程中的完整性、保密性。

与文档数据库服务的关系

文档数据库服务（Document Database Service，DDS）完全兼容MongoDB协议，提供安全、高可用、高可靠、弹性伸缩和易用的数据库服务，同时提供一键部署、弹性扩容、容灾、备份、恢复、监控和告警等功能。KMS为DDS提供用户主密钥管理控制能力，应用于文档数据库的磁盘加密功能。

与云审计服务的关系

云审计服务（Cloud Trace Service，CTS）记录数据加密服务相关的操作事件，方便用户日后的查询、审计和回溯，具体请参见《云审计服务用户指南》。

表 11-1 云审计服务支持的 KMS 操作列表

操作名称	资源类型	事件名称
创建密钥	cmk	createKey
创建数据密钥	cmk	createDataKey
创建不含明文数据密钥	cmk	createDataKeyWithoutPlaintext
启用密钥	cmk	enableKey
禁用密钥	cmk	disableKey
加密数据密钥	cmk	encryptDatakey
解密数据密钥	cmk	decryptDatakey
计划删除密钥	cmk	scheduleKeyDeletion
取消计划删除密钥	cmk	cancelKeyDeletion
创建随机数	rng	genRandom
修改密钥别名	cmk	updateKeyAlias
修改密钥描述	cmk	updateKeyDescription
密钥删除风险提示	cmk	deleteKeyRiskTips
导入密钥材料	cmk	importKeyMaterial
删除密钥材料	cmk	deleteImportedKeyMaterial
创建授权	cmk	createGrant
退役授权	cmk	retireGrant
撤销授权	cmk	revokeGrant

操作名称	资源类型	事件名称
加密数据	cmk	encryptData
解密数据	cmk	decryptData
添加标签	cmk	dealUnifiedTags
删除标签	cmk	dealUnifiedTags
批量添加标签	cmk	dealUnifiedTags
批量删除标签	cmk	dealUnifiedTags
开启密钥轮换	cmk	enableKeyRotation
修改密钥轮换周期	cmk	updateKeyRotationInterval

表 11-2 云审计服务支持的 CSMS 操作列表

操作名称	资源类型	事件名称
创建凭据	secret	createSecret
更新凭据	secret	updateSecret
删除凭据	secret	forceDeleteSecret
计划删除凭据	secret	scheduleDelSecret
取消计划删除凭据	secret	restoreSecretFromDeletedStatus
创建凭据状态	secret	createSecretStage
更新凭据状态	secret	updateSecretStage
删除凭据状态	secret	deleteSecretStage
创建凭据版本	secret	createSecretVersion
下载凭据备份	secret	backupSecret
恢复凭证备份	secret	restoreSecretFromBackupBlob
更新凭据版本	secret	putSecretVersion
凭据轮转	secret	rotateSecret
创建凭据事件	secret	createSecretEvent
更新凭据事件	secret	updateSecretEvent
删除凭据事件	secret	deleteSecretEvent
创建资源标签	secret	createResourceTag

操作名称	资源类型	事件名称
删除资源标签	secret	deleteResourceTag

表 11-3 云审计服务支持的 KPS 操作列表

操作名称	资源类型	事件名称
创建或导入SSH密钥对	keypair	createOrImportKeypair
删除SSH密钥对	keypair	deleteKeypair
导入私钥	keypair	importPrivateKey
导出私钥	keypair	exportPrivateKey
绑定SSH密钥对	keypair	bindKeypair
解绑SSH密钥对	keypair	unbindKeypair
清除私钥	keypair	clearPrivateKey

表 11-4 云审计服务支持的 DHSM 操作列表

操作名称	资源类型	事件名称
购买云加密实例	hsm	purchaseHsm
实例化云加密实例	hsm	createHsm
删除云加密实例	hsm	deleteHsm

与统一身份认证服务的关系

统一身份认证服务（Identity and Access Management, IAM）为数据加密服务提供了权限管理的功能。

需要拥有KMS Administrator权限的用户才能使用DEW服务。

需要同时拥有KMS Administrator和Server Administrator权限的用户才能使用密钥对管理功能。

如需开通该权限，请联系拥有Security Administrator权限的用户，详细内容请参考《统一身份认证服务用户指南》。

12 个人数据保护机制

为了确保您的个人数据（例如用户名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，DEW通过控制个人数据访问权限以及记录操作日志等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

DEW收集及产生的个人数据如表12-1所示：

表 12-1 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
租户ID	• 在控制台进行任何操作时Token中的租户ID • 在调用API接口时Token中的租户ID	否	是，租户ID是用户的身份标识信息

存储方式

租户ID不属于敏感数据，明文存储。

访问权限控制

用户只能查看自己业务的相关日志。

日志记录

用户个人数据的所有操作，包括修改、查询和删除等，DEW都会记录审计日志并上传至云审计服务（CTS），用户可以并且仅可以查看自己的审计日志。