数据加密服务

入门实践

文档版本 02

发布日期 2024-04-19

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 入门实践

当用户完成了创建密钥、创建密钥对、创建凭据等基本操作后，可以根据自身的业务需求使用DEW提供的一系列常用实践。

表 1-1 常用最佳实践

实践		描述
数据保护	**加解密小量数据**	当有少量数据（例如：口令、证书、电话号码等）需要加解密时，用户可以通过密钥管理服务（Key Management Service，KMS）控制台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。
	加解密大量数据	当有大量数据（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。
	使用加密SDK进行本地文件加解密	加密SDK提供了数据的加解密、文件流加解密等功能，用户只需调用加解密接口即可轻松实现海量数据加解密。当出现大型文件、图片等数据通过HTTPS请求到KMS服务进行保护时会消耗大量网络资源，加密效率低的问题时，可以使用加密SDK进行本地文件加解密。
	跨Region容灾加解密	当单Region加解密出现服务侧故障时，无法再对数据进行加解密操作，用户可以通过密钥管理服务（Key Management Service，KMS）实现跨Region容灾加解密，保证业务不中断。
	如何使用KMS对文件进行完整性保护	当有大量文件（例如：镜像、电子保单或者重要文件等）需要在传输或者存储时确保不被篡改，用户可以使用KMS对文件摘要进行签名。再次使用时可以重新计算摘要进行验签。确保文件在传输或者存储过程中没有被篡改。

实践		描述
云服务使用KMS加密	ECS服务端加密	KMS支持对ECS服务进行一键加密，弹性云服务器资源加密包括镜像加密和数据盘加密。 • 在创建弹性云服务器时，用户如果选择加密镜像，弹性云服务器的系统盘会自动开启加密功能，加密方式与镜像保持一致。 • 在创建弹性云服务器时，用户也可以对添加的数据盘进行加密。
	OBS服务端加密	当用户启用OBS服务端加密功能时： • 在上传对象时，数据会在服务端加密成密文后存储。 • 在下载加密对象时，存储的密文会先在服务端解密为明文，再提供给用户。 在OBS服务中需要上传的对象可以通过KMS提供密钥的方式进行服务端加密。
	EVS服务端加密	当用户由于业务需求需要对存储在云硬盘的数据进行加密时，EVS服务与KMS集成，通过KMS提供的密钥实现磁盘数据的加密。
	IMS服务端加密	用户创建私有镜像时，可以通过选择KMS加密的方式，使用KMS提供的密钥对镜像进行加密，确保镜像数据安全性。
	RDS数据库加密	用户在创建RDS数据库实例和扩容磁盘并启用加密功能后，磁盘数据会在服务端加密成密文后存储。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。
	DDS数据库加密	用户在创建DDS数据库实例和扩容磁盘并启用加密功能后，磁盘数据会在服务端加密成密文后存储。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。
凭据加密	如何使用凭据管理服务替换硬编码的数据库账号密码	用户在日常访问应用程序的过程中，通常会嵌入凭据直接访问程序。在需要更新凭据时，除了创建新的凭据以外，还需要花费一些时间更新应用程序以使用新的凭据。需要使用华为云凭据管理服务更便捷高效、高安全性的进行凭据管理。
	如何使用凭据管理服务解决AK&SK泄露问题	通过统一身份认证服务（Identity and Access Management，IAM ）对弹性云服务器（Elastic Cloud Server，ECS）的委托获取临时访问密钥来保护AK&SK。
	如何使用凭据管理服务自动轮转安全密码	通过函数工作流和凭据管理服务，定期生成和轮转强安全密码，以满足用户安全合规的密码生成、托管、以及定期自动轮换的要求。

实践		描述
	单用户凭据轮换策略	单用户凭据轮换是指一个凭据中更新一个用户所保存的信息，这是最基础的凭据轮换策略，适用于大多数日常使用场景。
	双用户凭据轮换策略	双用户轮换策略是指在一个凭据中更新两个用户所保存的信息。为防止在修改用户密码和更新凭据时出现访问失败的情况，需要使用双用户凭据轮换策略确保应用程序的高可用性。
	通过函数工作流轮转IAM凭证	使用函数工作流模板，通过凭据管理服务轮转IAM凭证。
API调用	使用指数退避方法对DEW服务请求错误进行重试	当用户调用API时，收到返回的错误信息，可参照使用指数退避方法对请求错误进行重试。

A 修订记录

发布日期	修订说明
2024-04-19	第二次正式发布。 新增“如何使用KMS对文件进行完整性保护”。 新增“通过函数工作流轮转IAM凭证”。 新增“如何使用凭据管理服务自动轮转安全密码”。
2023-07-14	第一次正式发布。