数据安全中心

用户指南（高安专区）

文档版本	01
发布日期	2026-09-10

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 高安专区概述

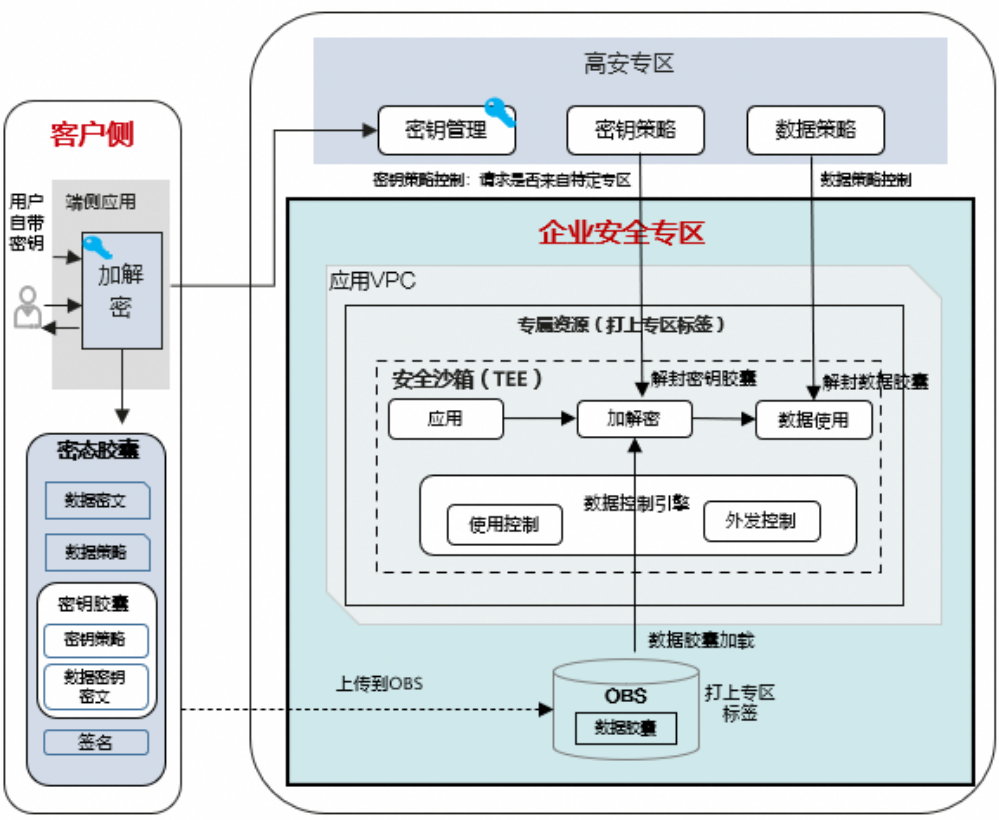
在企业数据上云的业务场景中，用户通常需要将本地数据加密后上传至华为云对象存储服务（OBS）进行持久化存储，随后通过弹性云服务器（ECS）进行数据分析、容器集群（CCE）进行数据加工标注、以及AI开发平台（ModelArts）进行模型训练等多种方式对数据进行处理。各处理节点均通过专用加解密SDK完成数据的解密、处理、结果加密回写等操作。然而，数据在多节点间流转时，传统的监控手段难以清晰展示数据从本地上传、云端存储、各节点处理、结果回写到客户端下载的完整路径，也无法实时监控数据在各环节的加密状态是否合规。这导致企业在进行安全审计和合规溯源时面临较大困难，难以向监管机构或内部管理层证明数据全链路的安全性。为解决这一痛点，华为云数据安全中心（DSC）推出企业高安专区特性，将OBS桶、ECS节点、CCE集群、ModelArts实例等资源逻辑组织为统一的企业数据空间，实现数据和资源的逻辑隔离、数据全链路流动可视化、加密状态实时监控以及操作审计与血缘溯源，帮助企业增强对云上数据安全的信任与管控能力。

约束与限制

- 当前资源类型仅支持：OBS桶、ECS实例、CCE集群、ModelArts专属资源池。
- 加解密操作必须通过DEW的加解密SDK进行。
- 依赖CTS服务收集OBS的数据操作日志，依赖DEW的加解密SDK上报加解密操作日志，依赖LTS做日志存储。
- 仅支持在**华北-北京四**、**华东-上海一**、**西南-贵阳一**使用该功能。

方案架构

- **数据强隔离：**企业独享安全专区，租户间数据、资源强隔离。
- **全流程加密：**数据端到端加密，密钥由用户自主控制。



2 购买高安专区

高安专区提供包年/包月（预付费）的计费方式，默认支持创建8个专区，包含100个专区资源管理配额，单账号下，DSC免费支持管理10TB的OBS文件数据量。同时，也为您提供了**高安专区配额扩展包**，在资源管理配额不够用时，可购买使用，1个扩展包含100个专区资源管理配额。

购买高安专区

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“高安专区”，进入“高安专区”控制台。

步骤3 单击“开通高安专区”，在“开通高安专区”页面配置相关参数，详见**表2-1**。

图 2-1 购买高安专区

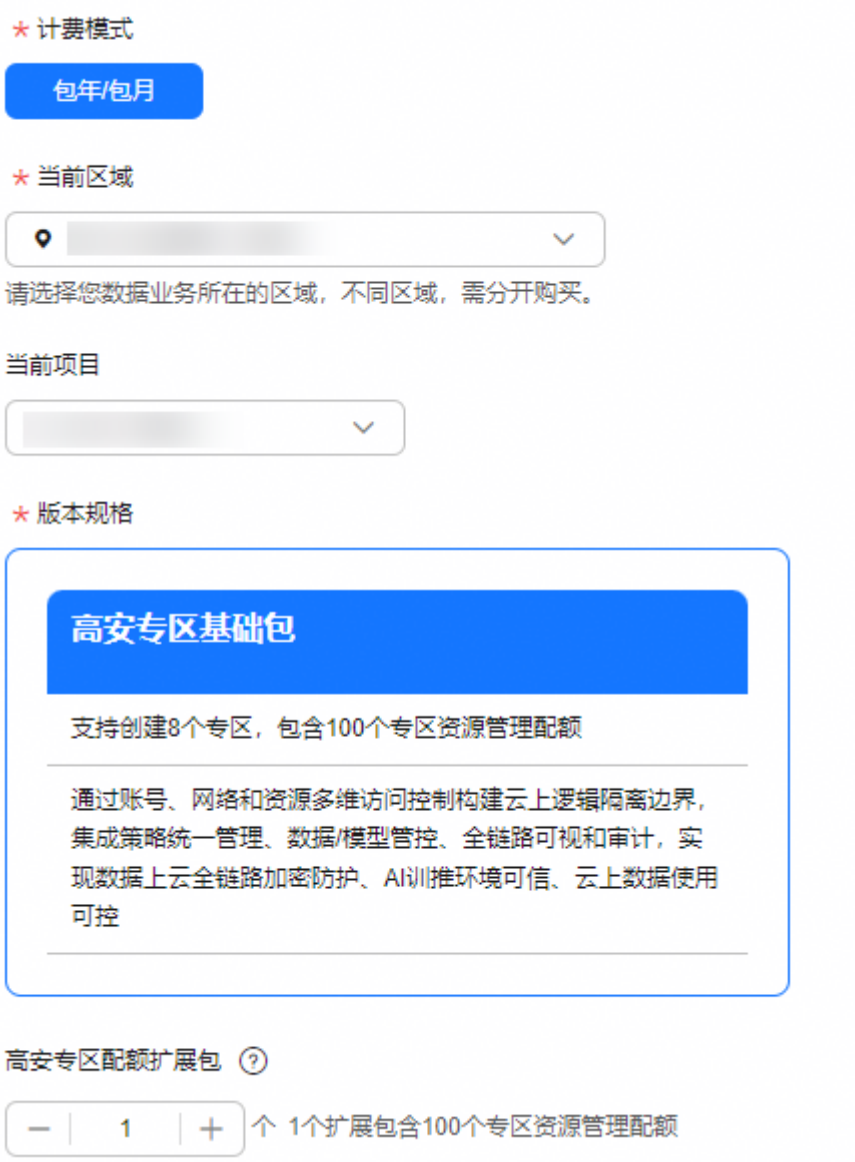


表 2-1 购买高安专区参数说明

参数名称	说明
计费模式	默认仅支持**包年/包月**。
当前区域	根据您数据业务所在的区域，选择专区区域。 当前DSC不支持跨区域使用，不同区域，需分开购买。
当前项目	选择区域对应的项目。

参数名称	说明
版本规格	仅支持**高安专区基础包**。 支持创建8个专区，包含100个专区资源管理配额。 单账号下，DSC免费支持管理10TB的OBS文件数据量。
高安专区配额扩展包	支持额外购买高安专区资源扩展包。1个扩展包含100个专区资源管理配额。

步骤4 选择“购买时长”。单击时间轴的点，选择购买时长 ，可以选择1个月～1年的时长。

勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤5 在页面的右下角，单击“立即购买”。

步骤6 确认订单无误后，阅读并勾选“我已阅读并同意《数据安全中心免责声明》”，单击“去支付”。

步骤7 进入“付款”页面，请选择付款方式进行付款。

----结束

购买高安专区配额扩展包

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“高安专区”，进入“高安专区”控制台。

步骤3 在页面右上角，单击“变更扩展包”，在“高安专区配额扩展包”栏中，增加扩展包数量。

步骤4 在页面的右下角，单击“立即购买”。

步骤5 确认订单无误后，阅读并勾选“我已阅读并同意《数据安全中心免责声明》”，单击“去支付”。

步骤6 进入“付款”页面，请选择付款方式进行付款。

----结束

退订高安专区实例或扩展包

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“高安专区”，进入“高安专区”控制台。

步骤3 在页面右上角，单击“退订”，进入“退订”页面。

步骤4 选择退订的实例和退订的原因，退订操作确认后，单击“退订”，根据界面提示完成退订操作。

----结束

相关文档

- 购买高安专区后，即可创建专区，实现租户间数据、资源强隔离，具体请参见**高安专区管理**。
- 购买高安专区后，即可使用加密与密钥管理，通过密钥策略确保密钥仅在该边界内生成、存储和使用，防止密钥明文泄露到非受信环境，形成一个可信密钥空间。其核心需求价值体现在**解决密钥管理碎片化、提升密码服务可信度、保障数据安全合规**，具体请参见**加密与密钥管理概述**。

3 查看安全专区总览

在多账号、多专区的数据安全治理场景下，用户需要整体掌握安全专区的建设规模与风险现状。但专区、账号、资源、风险信息分散在不同页面，无法一站式掌握整体概况，难以快速进入拓扑视图开展资产核查。安全专区总览集中展示创建专区数、用户数、纳管资源数、未修复风险，同时提供专区列表，支持进入资源拓扑视图查看资产与数据流关系。

前提条件

已**创建高安专区**，并已经在专区内添加了资源，详见**添加资源**章节。

查看安全专区总览

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“高安专区”，直接进入“高安专区总览”页面。

步骤3 在页面顶部，为您展示了创建专区数、用户数、纳管资源数、未修复风险。

图 3-1 高安专区总览

步骤4 在专区列表，单击专区名称，进入专区基本信息页面，可执行以下操作。

- **查看高安专区基本信息**：查看该专区的“基本信息”、“默认安全策略”和“资源拓扑视图”
- **添加IAM用户**：将IAM用户添加到创建的专区内，仅专区内的用户可以访问专区内的资源。
- **添加网络**：将VPC网络添加到创建的专区内，专区内的用户仅支持通过专区内的VPC网络访问专区内的资源。
- **添加资源**：将存储资源、计算资源、KMS密钥添加到创建的专区内，实现资源强隔离。

----结束

相关文档

- **数据流转**：DSC统一采集专区内OBS读写日志及KMS加解密SDK数据操作日志，动态捕获用户访问行为路径，能够全面支撑事件溯源与风险定位，直观展示数据流转情况，帮助运维及安全人员及时识别异常与安全风险。
- **异常检测与修复**：专区风险扫描功能支持对专区策略配置进行自动化检测，可识别策略配置偏移和危险操作，并按风险等级触发告警，同时支持手动触发扫描和自动定时扫描两种方式，帮助管理员及时发现并处理专区安全隐患，保障专区隔离管理的安全性和有效性。

4 高安专区管理

创建高安专区后，仅专区内的IAM用户和VPC网络支持访问专区内的资源，实现租户间数据、资源强隔离。同时，创建高安专区后，系统将自动创建用户组 DSC-DSZ-AllUsers并绑定默认策略，同时将账号下所有IAM用户加入该用户组。

创建专区后，可单独在专区内添加IAM用户、VPC网络以及资源。

- **添加IAM用户**：将IAM用户添加到创建的专区内，仅专区内的用户可以访问专区内的资源。
- **添加网络**：将VPC网络添加到创建的专区内，专区内的用户仅支持通过专区内的VPC网络访问专区内的资源。
- **添加资源**：将存储资源、计算资源、KMS密钥添加到创建的专区内，实现资源强隔离。

前提条件

已**购买高安专区**。

创建高安专区

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“高安专区”，进入“高安专区”控制台。

步骤3 在左侧导航栏中，选择“安全专区管理”。

步骤4 单击“创建专区”，进入“创建高安专区”配置页面，完成“基础配置”。

- “专区名称”：自定义专区名称。
- “专区描述”：可选。简述创建专区的用途等等。
- “默认策略”：DSC提供了以下策略。在策略所在行的“操作”列，单击“查看策略”，可查看策略详情。
  - DSC-Policy-DSZ-ZoneAccess-${zone-id}：IAM专区访问控制策略，非专区用户禁止访问专区标签资源。
  - DSC-Policy-DSZ-TagProtection：IAM标签保护策略，禁止IAM用户直接修改专区标签，非管理员禁止修改data-zone标签。
  - DSC-Policy-DSZ-NetworkDeny：网络出口控制策略，禁止专区资源公网访问(EIP/NAT/公网IP)，禁止VPC跨区域互联互通。

- DSC-Policy-DSZ-OBSBucket：OBS桶策略，OBS桶ACL策略，限制访问范围。
- DSC-Policy-DSZ-VPCEP：VPCEP策略，VPCEP终端服务仅允许专区用户访问。

步骤5 单击“下一步”，完成“添加IAM用户与网络配置”。

- “添加IAM用户”：在下拉框中选择IAM用户。添加IAM用户后，系统将自动给选择的IAM用户绑定标签 data-security-zone，即该IAM用户有权访问专区资源。
- “添加网络”：在下拉框中选择VPC网络。添加网络后，系统将自动给选择的VPC网络资源绑定标签 data-security-zone，并自动给VPC中的KMS VPCEP终端节点添加默认策略。

步骤6 单击“下一步”，添加资源。

在下拉框中选择“资源类型”。单击“添加资源”可添加多条资源，单击右上角的“删除”，支持删除资源。

- 当“资源类型”选择“弹性云服务器ECS”、“云容器引擎CCE”、“ModelArts专属资源池”、“对象存储 OBS”时，同时需要选择资源类型对应的资源。
- 当“资源类型”选择“本地客户端”时，需要输入客户端名称、内网IP地址段（可选）、公网IP（可选）。

步骤7 单击“确定”。

----结束

添加 IAM 用户

添加IAM用户后将自动绑定标签 data-security-zone，仅专区用户有权访问专区资源。

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“高安专区”，进入“高安专区”控制台。

步骤3 在左侧导航栏中，选择“安全专区管理”。

步骤4 单击专区名称，进入“基本信息”页面。

步骤5 选择“IAM用户管理”页签。

步骤6 单击“添加用户”，在弹框中选择IAM用户后单击“确定”。

如果不需要某用户访问专区资源，在IAM用户所在行的“操作”列，单击“移除”。

----结束

添加网络

添加网络后，系统将自动给选择的VPC网络资源绑定标签 data-security-zone，并自动给VPC中的KMS VPCEP终端节点添加默认策略。

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“高安专区”，进入“高安专区”控制台。

步骤3 在左侧导航栏中，选择“安全专区管理”。

步骤4 单击专区名称，进入“基本信息”页面。

步骤5 选择“网络管理”页签。

步骤6 单击“添加网络”，在弹框中选择VPC后单击“确定”。

如果不需要某网络下的用户访问专区资源，在VPC所在行的“操作”列，单击“移除”。

----结束

添加资源

DSC支持将OBS、“弹性云服务器ECS”、“云容器引擎CCE”、“ModelArts专属资源池”和本地客户端资源添加到高安专区进行管理，添加后，资源后将自动绑定标签data-security-zone，仅专区用户有权访问专区资源。

添加存储资源

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“高安专区”，进入“高安专区”控制台。

步骤3 在左侧导航栏中，选择“安全专区管理”。

步骤4 单击专区名称，进入“基本信息”页面。

步骤5 选择“资源管理 > 存储资源”页签。

步骤6 单击“添加资源”，“类型”默认为OBS，在下拉框中选择需要添加到专区的OBS桶资源。

如果不需要专区用户访问该资源，在OBS桶所在行的“操作”列，单击“移除”。

----结束

添加计算资源

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“高安专区”，进入“高安专区”控制台。

步骤3 在左侧导航栏中，选择“安全专区管理”。

步骤4 单击专区名称，进入“基本信息”页面。

步骤5 选择“资源管理 > 计算资源”页签。

步骤6 单击“添加资源”，在弹框中选择“资源类型”。

- 当“资源类型”选择“弹性云服务器ECS”、“云容器引擎CCE”、“ModelArts专属资源池”时，同时需要选择资源类型对应的资源。
- 当“资源类型”选择“本地客户端”时，需要输入客户端名称、内网IP地址段（可选）、公网IP（可选）。

步骤7 单击“确定”。

如果不需要专区用户访问该资源，在资源所在行的“操作”列，单击“移除”。

----结束

添加 KMS 密钥

步骤1 登录DSC服务控制台。

步骤2 在左侧导航栏中，选择“高安专区”，进入“高安专区”控制台。

步骤3 在左侧导航栏中，选择“安全专区管理”。

步骤4 单击专区名称，进入“基本信息”页面。

步骤5 选择“资源管理 > KMS密钥”页签。

步骤6 单击“添加KMS密钥”，在弹框中选择KMS密钥后单击“确定”。

如果不需要专区用户访问该KMS密钥，在KMS密钥所在行的“操作”列，单击“移除”。

----结束

查看高安专区基本信息

步骤1 登录DSC服务控制台。

步骤2 在左侧导航栏中，选择“高安专区”，进入“高安专区”控制台。

步骤3 在左侧导航栏中，选择“安全专区管理”。

步骤4 单击专区名称，进入“基本信息”页面。

步骤5 在“基本信息”页签，可查看该专区的“基本信息”、“默认安全策略”和“资源拓扑视图”。

图 4-1 专区基本信息

----结束

编辑/删除高安专区

- **编辑专区**：在待修改专区名称所在行的“操作”列，单击“编辑”，修改名称或者描述信息后，单击“确定”。
- **删除专区**：在待修改专区名称所在行的“操作”列，单击“删除”，在“删除专区”的弹框中，输入“DELETE”后单击“确定”。

须知

删除专区后不可恢复，请谨慎操作。

相关文档

加密与密钥管理，通过密钥策略确保密钥仅在该边界内生成、存储和使用，防止密钥明文泄露到非受信环境，形成一个可信密钥空间。其核心需求价值体现在**解决密钥管理碎片化、提升密码服务可信度、保障数据安全合规**，具体请参见**加密与密钥管理概述**。

5 加密与密钥管理

5.1 加密与密钥管理概述

加密与密钥管理，通过密钥策略确保密钥仅在该边界内生成、存储和使用，防止密钥明文泄露到非受信环境，形成一个可信密钥空间。

可信密钥空间是专门用于密钥全生命周期管理的安全基础设施，其核心需求价值体现在**解决密钥管理碎片化、提升密码服务可信度、保障数据安全合规**，是构建可信数据空间、零信任架构等现代安全体系的关键支撑。

通过一个可信密钥空间系统，实现：

- **安全边界控制**：确保密钥明文仅在受信环境中使用。
- **灵活的访问策略**：支持基于身份、时间、环境等多维度的访问控制。
- **多场景适配**：支持多种部署场景。
- **多环境支持**：适配裸金属、ECS、容器等多种运行环境。

基本概念

使用该功能前，请先了解以下名词的含义。

名词	解释
可信密钥空间	一个由受信任的硬件密码设备（如KMS、HSM、TEE）和授权设备/应用组件（接入点）构成的逻辑安全边界，通过密钥策略确保密钥仅在该边界内生成、存储和使用，防止密钥明文泄露到非受信环境。
接入点	经过授权认证、部署在可信密钥空间逻辑安全边界内的设备或应用组件，作为密钥服务与外部应用系统之间的受控访问接口，负责接收密钥使用请求、执行策略验证、调用底层密码能力（如TEE、CPU）执行密码运算，并确保密钥明文始终不离开可信边界。
密钥策略	针对密钥使用权限和操作约束的规则集合，聚焦于“谁、在什么条件下、可以对密钥执行什么操作”的精细化控制。

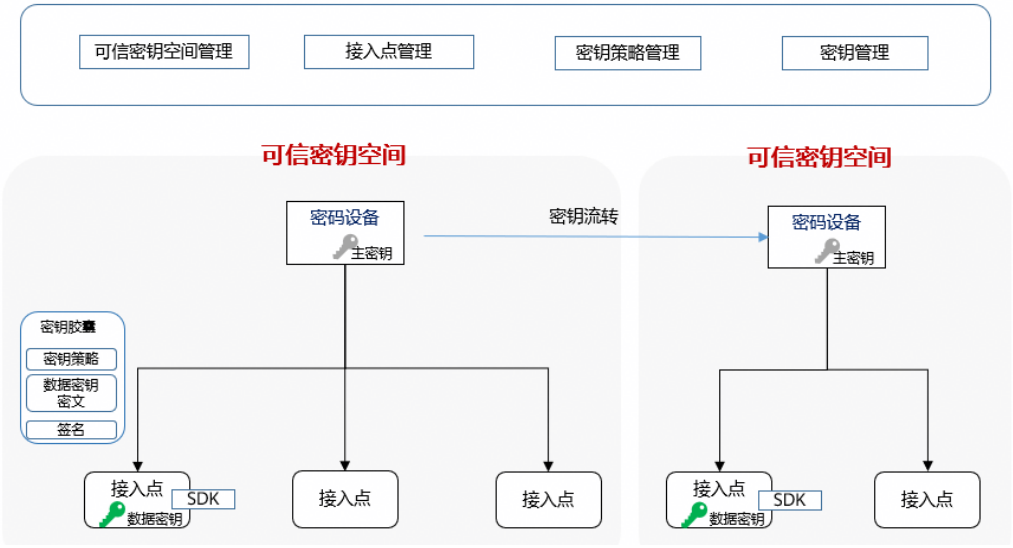
名词	解释
密钥胶囊	一种将数据加密密钥与密钥策略封装在一起的密钥数据包，它通过密码学技术将密钥与使用条件（如时间限制、身份验证要求、运行设备等）绑定，确保密钥仅在满足预设策略的条件下才能被解密和使用。
主密钥	租户创建或托管的密钥，位于硬件密码设备内，由硬件进行保护，安全边界为硬件密码设备。
数据密钥	租户创建的密钥，使用主密钥进行保护，安全边界为可信密钥空间。

方案架构

本方案通过**可信密钥空间**实现密钥全生命周期管控与跨空间密钥流转，上层提供可信密钥空间管理、接入点管理、密钥策略管理、密钥管理四大管控能力。

每个可信密钥空间内部部署密码设备，由密码设备保管本空间的**主密钥**，主密钥仅存在于密码设备内部，不对外导出。主密钥用于保护下层的数据密钥，下发至各业务接入点；业务接入点通过 SDK 完成数据密钥调用，同时生成包含密钥策略、数据密钥密文、签名信息的**密钥胶囊**。

支持多个可信密钥空间之间执行**密钥流转**，源可信密钥空间将密钥安全流转至目标可信密钥空间，由目标侧密码设备使用自身主密钥完成密钥保护，密钥在跨空间流转过程中全程受密码能力保护。各接入点受所属可信密钥空间统一管控，依托 SDK 获取受保护的数据密钥，完成业务加解密操作，实现主密钥与数据密钥分级保护、跨可信密钥空间密钥互通，保障密钥存储、分发、流转全流程安全可控。



相关文档

- **密钥管理**：在可信密钥空间创建的密钥，数据密钥明文仅在可信密钥空间内使用。
- **接入点管理**：接入点是云服务器、CCE集群或本地服务器等应用运行环境，只有符合密钥策略的接入点才能解封**密钥胶囊**。

- **密钥策略**：密钥策略定义哪些接入点或安全专区在什么条件下能够解密数据密钥密文，确保密钥不会被乱用。

5.2 密钥管理

可信密钥空间是一个由受信任的硬件密码设备和授权接入点构成的逻辑安全边界，通过密钥策略确保密钥仅在该边界内生成、存储和使用。

在可信密钥空间创建的密钥，数据密钥明文仅在可信密钥空间内使用。

前提条件

已**购买高安专区**。

约束限制

- 不同可信密钥空间默认相互隔离。
- 每个空间有唯一身份标识。

创建高安专区密钥

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“加密与密钥管理”，进入“密钥管理”页面。

步骤3 单击“创建密钥”，进入“创建密钥”页面，配置密钥参数。

表 5-1 密钥参数说明

参数名称	参数说明
密钥名称	自定义密钥名称。
算法类型	仅支持“对称”密钥算法。
密钥用途	密钥的用途，仅支持加解密。
密钥算法	仅支持选择AES_256、SM4。
企业项目	该参数针对企业用户使用。 如果您是企业用户，且已创建企业项目，则请从下拉列表中为密钥选择需要绑定的企业项目，默认项目为“default”。 未开通企业管理的用户页面则没有“企业项目”参数项，无需进行配置。 • 企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。更多关于企业项目的信息，请参见**《什么是企业项目管理？》**。 • 如需开通企业项目，请参考**如何开通企业项目/企业多账号**。

参数名称	参数说明
所属密钥库	选择密钥归属的密钥库。选择密钥库后，将通过密钥库来存储密钥，并提供安全的密钥生成功能，确保生成的密钥是随机的、安全的，并且能够被安全地存储和备份。 如果需新建密钥库，请参见**创建密钥库** 。
密钥材料来源	• 密钥管理：由KMS生成的密钥材料。 • 外部：使用客户本地的密钥材料。创建后需要导入密钥材料。
高级配置	可配置密钥的描述信息。

步骤4 单击“确定”，完成密钥创建。

用户可在密钥列表上查看已完成创建的密钥，密钥材料来源为“密钥管理”时默认状态为“启用”。

密钥材料来源为“外部”时默认状态为“等待导入”，需要**导入密钥材料**。

----结束

导入密钥材料（可选）

创建高安专区密钥中创建的密钥的“密钥材料来源”为“外部”时，需要参考本章节把本地的密钥材料导入到控制台。

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“加密与密钥管理”，进入“密钥管理”页面。

步骤3 在外部密钥所在行的“操作”列，单击“导入密钥材料”，完成“获取包装密钥和导入令牌”。

- 选择“密钥包装算法”。

表 5-2 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。
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。

- 根据情境，选择“已有密钥材料”或“下载密钥材料”。

- “已有密钥材料”：仅限使用API接口获取到包装密钥和导入令牌的场景。执行**步骤4**。
- “下载密钥材料”：引导程序已自动帮您传递导入令牌，您仅需使用下载的包装密钥，从您的密钥管理设备中导出密钥材料。中途退出引导程序，导入令牌将自动失效。执行**步骤5**。

步骤4 **步骤3**中选择“已有密钥材料”时，执行该操作。

1. **通过调用API接口下载密钥材料**。
2. **使用包装密钥加密密钥材料**。
3. **步骤3**中选择“已有密钥材料”后单击“下一步”，在“导入密钥材料”配置项，填写“密钥材料”内容。

   “密钥材料”填写**步骤4.2**中使用包装密钥加密后的密钥材料。例如：**使用包装密钥加密密钥材料**中的“EncryptedKeyMaterial.bin”文件。

   图 5-1 导入密钥材料

4. 单击“下一步”，在“密钥导入令牌”配置项，根据**表5-3**设置参数。

   图 5-2 导入密钥令牌

表 5-3 导入密钥令牌参数说明

参数	操作说明
密钥ID	创建密钥时，随机生成的密钥ID。
密钥导入令牌	填写**步骤4.1**获取的导入令牌。
密钥材料失效模式	– 永不失效：导入的密钥材料永久不失效。 – 失效时间：用户可指定导入的密钥材料的失效时间，默认失效时间为24小时。 密钥材料失效后，KMS会在24小时内自动删除密钥材料，删除后密钥将无法使用，且密钥状态变更为“等待导入”。

步骤5 **步骤3**中选择“下载密钥材料”时，执行该操作。

1. 单击“下载密钥材料”后，密钥材料将下载到本地。下载的文件为包装密钥，如**图 下载文件**所示。

图 5-3 下载文件

- wrappingKey_*密钥ID*：即包装密钥，编码为二进制格式，用于加密密钥材料的包装密钥。
- 导入令牌：引导程序自动传递导入令牌，无需下载，如果中途退出引导程序，导入令牌将自动失效。

须知

包装密钥将在24小时后失效，失效后将不能使用。如果包装密钥失效，请重新下载包装密钥。

控制台将自动传递导入令牌。因此，下载密钥材料后，请勿关闭或中途退出“导入密钥材料”对话框，否则将导致导入的令牌自动失效。

2. **使用包装密钥加密密钥材料**。
3. 单击“下一步”，在“导入密钥材料”页面，单击“添加文件”，上传**步骤5.2**中加密后密钥材料。

图 5-4 导入密钥材料

4. 单击“下一步”，进入“密钥导入令牌”页面。根据表5-4设置参数。

图 5-5 导入密钥令牌

表 5-4 导入密钥令牌参数说明

参数	操作说明
密钥ID	创建密钥时，随机生成的密钥ID。
密钥材料失效模式	- 永不失效：导入的密钥材料永久不失效。 - 失效时间：用户可指定导入的密钥材料的失效时间，默认失效时间为24小时。 密钥材料失效后，KMS会在24小时内自动删除密钥材料，删除后密钥将无法使用，且密钥状态变更为“等待导入”。

步骤6 单击“确定”，页面右上角弹出“密钥导入成功”，则说明导入密钥成功。

须知

密钥ID、导入的密钥材料和导入的令牌需要全部匹配，密钥材料才能导入成功，否则会导入失败。

用户可在密钥列表中查看到导入的密钥信息，导入密钥的默认状态为“启用”。

----结束

管理密钥

为您提供如下相关操作。

将密钥迁入企业项目

企业项目为用户提供企业组织架构以及和业务管理模型匹配的云治理平台，帮助企业以公司、部门、项目等组织架构分级管理和项目业务结构来实现企业在云上的管理，提供企业项目管理、资源管理、人员管理、财务管理、应用管理能力。

如果您开通了企业项目管理，可以通过密钥管理界面对指定的自定义密钥迁移至其他企业项目。如需开通企业项目，请参考**如何开通企业项目/企业多账号**。

步骤1 在左侧导航栏中，选择“加密与密钥管理”，进入“密钥管理”页面。

步骤2 在目标密钥所在行，选择“更多 > 分配至项目”，弹出对话框。

如果用户为非企业用户，操作列不显示“分配至项目”按钮。

步骤3 在弹出的对话框中，选择迁入项目。单击“确定”，完成操作。

----结束

启用自定义密钥

该任务指导用户通过密钥管理界面对单个或多个自定义密钥进行启用操作，使被禁用的密钥恢复到数据加解密能力。新建的自定义密钥默认为“启用”状态。

步骤1 在左侧导航栏中，选择“加密与密钥管理”，进入“密钥管理”页面。

步骤2 在密钥列表中，在需要启用的密钥所在行的“操作”列，单击“启用”。

步骤3 在弹出窗口中，单击“确定”，完成启用单个密钥操作。

如果您想批量启用密钥，可以勾选所有需要启用的密钥，然后在列表左上角，单击“启用”。

----结束

禁用自定义密钥

该任务指导用户通过密钥管理界面对指定的自定义密钥进行禁用，以紧急保护数据，自定义密钥被禁用后，用户将不能使用该密钥进行加解密任何数据。

- 默认密钥不支持禁用操作。
- 密钥被禁用后，仍然会计费。只有删除密钥，才会停止计费。

步骤1 在左侧导航栏中，选择“加密与密钥管理”，进入“密钥管理”页面。

步骤2 在密钥列表中，在需要启用的密钥所在行的“操作”列，单击“禁用”。

步骤3 在弹出窗口中，勾选“我已知晓禁用以上密钥产生的影响”，单击“确定”，完成禁用单个密钥操作。

如果您想批量禁用密钥，可以勾选所有需要禁用的密钥，然后在列表左上角，单击“禁用”。

----结束

计划删除密钥

不支持直接删除密钥，仅支持计划删除密钥，即通过设置预删除周期（推迟时间范围为7天～1096天），在到期后删除密钥。

处于“启用”、“禁用”或“等待导入”状态的自定义密钥才支持删除，默认密钥不支持删除。

除了确认密钥使用情况以外，也可以开启验证操作，确保删除密钥操作进行多次验证，降低密钥误删导致的磁盘等加密不可用情况。开启验证的操作请参见**敏感操作保护**。

须知

系统会在推迟删除周期后删除密钥，使用该密钥加密的内容及产生的数据密钥也将无法解密。删除密钥前，请确认该密钥已不再使用，否则会导致您的业务不可用。

如果您想批量计划删除密钥，可以勾选所有需要计划删除的密钥，然后在列表左上角，单击“删除”。以下为您介绍如何单个删除密钥。

步骤1 在左侧导航栏中，选择“加密与密钥管理”，进入“密钥管理”页面。

步骤2 在需要删除的密钥所在行的“操作”列，单击“删除”，进入“删除密钥”界面。

步骤3 在“删除密钥”界面，填写“推迟删除”的时间。

图 5-6 推迟删除时间

步骤4 如果未开启删除验证，在确认删除提示框中输入“DELETE”后，单击“确定”，完成删除操作。

如果开启删除验证，选择验证方式后，单击“获取验证码”，在验证码对话框中输入获取的验证码，单击“确定”，完成删除操作。

如果需要关闭操作保护，可以在账号的“安全设置 > 敏感操作”中关闭。

----结束

取消计划删除密钥

该任务指导用户在未超出删除密钥的推迟时间，通过密钥管理界面对自定义密钥进行取消删除操作，取消删除后密钥处于“禁用”状态。

如果您想批量取消删除密钥，可以勾选所有需要取消删除的密钥，然后在列表左上角，单击“取消删除”。以下为您介绍如何取消单个密钥的计划删除。

步骤1 在左侧导航栏中，选择“加密与密钥管理”，进入“密钥管理”页面。

步骤2 在需要取消删除的密钥所在行的“操作”列，单击“取消删除”。

步骤3 在弹出的窗口中，单击“确定”，完成取消删除单个密钥操作。

取消删除后密钥状态为“禁用”，如需启用密钥，请参见**启用自定义密钥**操作。

----结束

附录：

通过调用 API 接口下载密钥材料

步骤1 调用“get-parameters-for-import”接口，获取包装密钥和导入令牌。

- public_key：调用API接口返回的base64编码的包装密钥内容。
- import_token：调用API接口返回的base64编码的导入令牌内容。

以获取密钥ID为“43f1ffd7-18fb-4568-9575-602e009b7ee8”，加密算法为“RSAES_OAEP_SHA_256”的包装密钥和导入令牌为例。

- 请求样例

```
{
   "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
   "wrapping_algorithm":"RSAES_OAEP_SHA_256"
}
```

- 响应样例

```
{
   "key_id": "43f1ffd7-18fb-4568-9575-602e009b7ee8",
   "public_key":"public key base64 encoded data",
   "import_token":"import token base64 encoded data",
   "expiration_time":1501578672
}
```

步骤2 保存包装密钥，包装密钥需要按照以下步骤转换格式。使用转换格式后的包装密钥加密的密钥材料才能成功导入管理控制台。

1. 复制包装密钥“public_key”的内容，粘贴到“.txt”文件中，并保存为“PublicKey.b64”。
2. 使用OpenSSL，执行以下命令，对“PublicKey.b64”文件内容进行base64转码，生成二进制数据，并将转码后的文件保存为“PublicKey.bin”。

   openssl enc -d -base64 -A -in PublicKey.b64 -out PublicKey.bin

步骤3 保存导入令牌，复制导入令牌“import_token”的内容，粘贴到“.txt”文件中，并保存为“ImportToken.b64”。

----结束

使用包装密钥加密密钥材料

可信密钥空间，仅支持对称密钥，密钥材料为“EncryptedKeyMaterial.bin”。

- **方法一**：使用下载的包装密钥在自己的HSM中加密密钥材料，详细信息请参考您的HSM操作指南。
- **方法二**：使用OpenSSL生成密钥材料，并用下载的“包装密钥”对密钥材料进行加密。

  说明

  如果用户需要使用**openssl pkeyutl**命令，OpenSSL需要是1.0.2及以上版本。

  如果用户使用SM2公钥包装，需要支持gmssl命令。

  a. 在已安装OpenSSL工具的客户端上，执行以下命令，生成密钥材料（256位对称密钥），并将生成的密钥材料以“PlaintextKeyMaterial.bin”命名保存。

  - AES256对称密钥

    openssl rand -out *PlaintextKeyMaterial.bin* 32

  - SM4国密

    openssl rand -out *PlaintextKeyMaterial.bin* 16

  b. 使用下载的“包装密钥”加密密钥材料，并将加密后的密钥材料按“EncryptedKeyMaterial.bin”命名保存。

  如果“包装密钥”由控制台下载，以下命令中的***PublicKey.bin***参数请以下载的包装密钥名称*wrappingKey_密钥ID*进行替换。

  表 5-5 使用下载的包装密钥加密生成的密钥材料

包装密钥算法	加密生成的密钥材料
RSAES_OAEP_SHA_256	**openssl pkeyutl -in *PlaintextKeyMaterial.bin* -inkey *PublicKey.bin* -out *EncryptedKeyMaterial.bin* -keyform der -pubin -encrypt -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256**
SM2_ENCRYPT	**gmssl pkeyutl -encrypt -pkeyopt ec_scheme:sm2 -pkeyopt ec_encrypt_param:sm3 -in *PlaintextKeyMaterial.bin* -pubin -inkey *PublicKey.bin* -keyform der -out *EncryptedKeyMaterial.bin***

相关文档

- **接入点管理**：接入点是云服务器、CCE集群或本地服务器等应用运行环境，只有符合密钥策略的接入点才能解封**密钥胶囊**。
- **密钥策略**：密钥策略定义哪些接入点或安全专区在什么条件下能够解密数据密钥密文，确保密钥不会被乱用。

5.3 接入点管理

接入点是云服务器、CCE集群或本地服务器等应用运行环境，只有符合密钥策略的接入点才能解封**密钥胶囊**。

创建接入点

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“加密与密钥管理”，进入“密钥管理”页面。

步骤3 在“加密与密钥管理”的导航栏中，选择“接入点管理”，进入“接入点管理”页面。

步骤4 单击“创建接入点”，在“创建接入点”页面，配置相关参数。

图 5-7 创建接入点

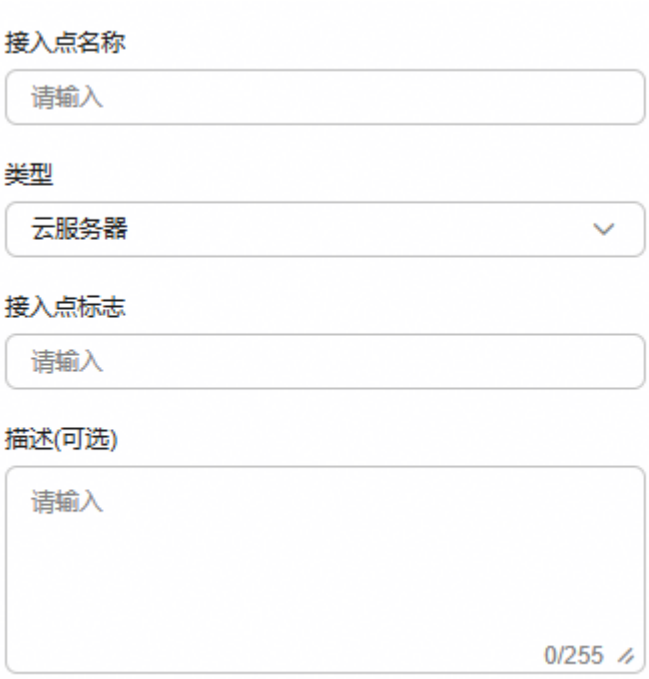


表 5-6 接入点参数说明

参数名称	参数说明
接入点名称	自定义接入点名称
类型	支持选择“云服务器”、“云容器引擎”、“通用场景”。

参数名称	参数说明
接入点标志	“类型”选择“云服务器”时，需要配置该参数。 填写云服务器的ID。

CCE集群公钥	“类型”选择“云容器引擎”时，需要配置该参数。
	参考以下方法获取CCE集群的公钥：
	1. 使用kubectl连接集群。
	2. 执行如下命令获取公钥。
	`kubectl get --raw /openid/v1/jwks`
	返回的结果即集群的公钥，回显结果示例如下：
	`# kubectl get --raw /openid/v1/jwks`
	`{"keys":[{"use":"sig","kty":"RSA","kid":"*****","alg":"RS256","n":"*****","e":"AQAB"}]}`

集群ID	“类型”选择“云容器引擎”时，需要配置该参数。 在CCE控制台，单击集群名称，在“基本信息”栏中获取集群ID。
描述（可选）	备注接入点的相关信息。

步骤5 单击“确定”，创建的接入点的“状态”为“启用”。

----结束

禁用接入点

步骤1 在左侧导航栏中，选择“加密与密钥管理”，进入“密钥管理”页面。

步骤2 在“加密与密钥管理”的导航栏中，选择“接入点管理”，进入“接入点管理”页面。

步骤3 在接入点所在行的“操作”列，单击“禁用”。

步骤4 在“禁用接入点”的弹框中，输入“DISABLE”后单击“确定”。

----结束

启用接入点

步骤1 在左侧导航栏中，选择“加密与密钥管理”，进入“密钥管理”页面。

步骤2 在“加密与密钥管理”的导航栏中，选择“接入点管理”，进入“接入点管理”页面。

步骤3 在接入点所在行的“操作”列，单击“启用”。

步骤4 在“启用接入点”的弹框中，单击“确定”。

----结束

删除接入点

步骤1 在左侧导航栏中，选择“加密与密钥管理”，进入“密钥管理”页面。

步骤2 在“加密与密钥管理”的导航栏中，选择“接入点管理”，进入“接入点管理”页面。

步骤3 在接入点所在行的“操作”列，单击“删除”。

步骤4 在“删除接入点”的弹框中，输入“DELETE”后单击“确定”。

----结束

相关文档

- **密钥管理**：在可信密钥空间创建的密钥，数据密钥明文仅在可信密钥空间内使用。
- **密钥策略**：密钥策略定义哪些接入点或安全专区在什么条件下能够解密数据密钥密文，确保密钥不会被乱用。

5.4 密钥策略

密钥策略定义哪些**接入点**或安全专区在什么条件下能够解密数据密钥密文，确保密钥不会被乱用。

创建密钥策略

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“加密与密钥管理”，进入“密钥管理”页面。

步骤3 在“加密与密钥管理”的导航栏中，选择“密钥策略”，进入“密钥策略”页面。

步骤4 单击“创建策略”，在“创建策略”页面，配置相关参数。

图 5-8 创建策略

表 5-7 创建策略参数说明

参数名称	参数说明
策略名称	自定义策略名称
配置方式	支持两种配置方式： • 可视化视图 • JSON视图

参数名称	参数说明
策略内容	“配置方式”选择“可视化视图”时，需要配置该内容。 • 选择“接入方式”：选择已创建的接入点或安全专区。 • 配置“生效时间”：单击选择开始日期和结束日期。
描述(可选)	备注信息。

步骤5 单击“确定”。

----结束

编辑或删除密钥策略

- **编辑密钥策略**：在待编辑密钥策略所在行的“操作”列，单击“编辑”，完成信息修改后，单击“确定”。
- **删除密钥策略**：在待删除密钥策略所在行的“操作”列，单击“删除”，在“删除策略”的弹框中，输入“DELETE”后单击“确定”。

相关文档

- **密钥管理**：在可信密钥空间创建的密钥，数据密钥明文仅在可信密钥空间内使用。
- **接入点管理**：接入点是云服务器、CCE集群或本地服务器等应用运行环境，只有符合密钥策略的接入点才能解封**密钥胶囊**。

6 持续运营

6.1 数据流转

专区内OBS读写日志及KMS加解密SDK数据操作日志，留存着用户操作相关行为记录。但各类日志分散存储、相互割裂，难以串联还原完整的用户访问路径，发生数据安全事件后难以快速开展溯源与问题定位，数据流转脉络无法直观呈现，异常行为与潜在风险也难以及时察觉。如何打通多源日志数据，实现全链路行为追踪，高效支撑安全事件排查处置？DSC统一采集专区内OBS读写日志及KMS加解密SDK数据操作日志，动态捕获用户访问行为路径，能够全面支撑事件溯源与风险定位，直观展示数据流转情况，帮助运维及安全人员及时识别异常与安全风险。

前提条件

已**创建高安专区**，并已经在专区内添加了OBS存储资源或KMS密钥资源，详见**添加资源**章节。

约束与限制

系统将自动采集专区内OBS读写日志及KMS加解密SDK数据操作日志，并将日志转储至云日志服务（LTS），用于数据流转分析与操作审计。启用此功能将产生 LTS 存储费用，详见**LTS 价格详情**。

查看数据操作日志与加解密操作日志

数据操作日志与加解密操作日志联合审计，能够完整还原文件从访问、加密处理全链路的数据流转过程，支撑安全溯源以及合规审计工作。

数据操作日志侧重记录**用户侧访问行为**；加解密操作日志侧重记录**系统后台加密 / 解密任务处理行为**，两类日志互补，共同完成对象存储全流程审计。

步骤1 **登录DSC服务控制台**。

步骤2 在左侧导航栏中，选择“高安专区”，进入“高安专区”控制台。

步骤3 在左侧导航栏中，选择“持续运营 > 数据流转”，进入“数据流转”页面。

步骤4 （可选）未开启日志采集功能时，请先单击“立即开启”，在弹框中单击“确定”，开启数据操作日志采集。

步骤5 在页面上方，下拉框中选择安全专区。

步骤6 选择“操作日志”页签，进入操作日志页面。

步骤7 选择“数据操作日志”，查看采集专区内OBS读写日志。

数据操作日志完整记录用户对对象存储资源的访问行为，可用于追溯文件上传、下载、删除等访问轨迹；结合**加解密状态、密钥 ID**字段，能够直观判断对象是否开启加密保护。

日志解析示例：如图6-1中日志记录显示，在对应操作时间，客户端对指定存储桶内的对象执行上传操作，对象数据大小为 8.00M，该对象加解密状态为未加密，无关联密钥 ID，本次上传操作状态为成功。

图 6-1 数据操作日志

表 6-1 数据操作日志参数说明

参数名称	参数说明
数据实体ID/名称	访问来源。产生访问操作的资源实体标识，用于定位发生操作的存储资源。
操作类型	用户对对象执行的访问动作： ● 写：对OBS桶执行**上传/写入对象**操作。 ● 读：对OBS桶执行**下载/读取对象**操作。
桶名/对象名	记录操作对应的存储桶名称以及目标文件对象名称。
数据大小	本次操作对应对象的文件存储大小。
加解密状态	标记该对象当前的加密状态，包含未加密、已加密；可快速识别对象是否完成加密处理。
密钥ID	对象加密时所使用KMS密钥的唯一标识，未加密对象该字段为空。
操作时间	用户发起数据访问操作的时间戳。
操作状态	访问动作执行结果，分为成功、失败；失败状态可用于排查访问异常问题。

步骤8 选择“加解密操作日志”，查看KMS加解密SDK数据操作日志。

加解密操作日志完整留存对象文件加密任务全流程信息，可用于追溯文件加密处理过程，核验密钥调用记录；当任务状态为失败时，可依托该日志排查密钥权限、文件权限等故障问题，满足加密操作的审计与合规溯源要求。

日志解析示例：如图6-2中日志记录显示，在指定操作时间，针对对应存储桶内的原始对象执行解密任务；记录了解密处理前后对象的名称、文件大小，本次任务调用指定密钥 ID 完成加密运算，最终任务操作状态为成功。

图 6-2 加解密操作日志

表 6-2 加解密操作日志参数说明

参数名称	参数说明
实体名称/ID	执行加解密任务对应的存储资源标识，一般为存储桶名称或任务实体ID，定位发生操作的存储资源。
操作类型	记录本次后台执行动作，分为**加密**、**解密**两种类型。
处理前对象名 / 大小	加解密处理执行前，原始对象的文件名称以及原始文件占用存储空间大小。
处理后对象名 / 大小	完成加密或者解密之后，输出生成的对象名称，以及处理完成后对象的文件大小。
密钥 ID	本次加解密任务调用KMS密钥的唯一标识；可通过该ID溯源密钥，核查密钥权限、密钥版本，密钥ID为空代表未使用密钥。
操作时间	加解密任务实际执行的时间戳。
操作状态	任务执行结果状态，包含成功、失败；状态为失败时，可结合日志进一步定位任务异常原因。

----结束

查看资源拓扑视图

资源拓扑视图是可视化展示数据安全管辖范围内各类云资源、数据资产以及它们之间关联关系的图形化页面，呈现资源之间数据流、调用依赖关系。

步骤1 登录DSC服务控制台。

步骤2 在左侧导航栏中，选择“高安专区”，进入“高安专区”控制台。

步骤3 在左侧导航栏中，选择“持续运营 > 数据流转”，进入“数据流转”页面。

步骤4 （可选）未开启日志采集功能时，请先单击“立即开启”，在弹框中单击“确定”，开启数据操作日志采集。

步骤5 在页面上方，下拉框中选择安全专区。

步骤6 选择“资源拓扑视图”页签，单击  可关闭操作日志采集。

须知

关闭后，将停止采集专区内的数据操作日志，无法查看数据流转详情和操作详情，请谨慎操作。

步骤7 选择时间段和资源，可查看该时间段内采集到的目标资源的日志拓扑视图。

----结束

相关文档

- 云日志服务（Log Tank Service，简称LTS）可以提供日志收集、分析、存储等服务。用户可以通过云日志服务快速高效地进行设备运维管理、用户业务趋势分析、安全监控审计等操作。了解更多LTS服务，详见**云日志服务LTS**。
- 对象存储服务（Object Storage Service，OBS）提供海量、安全、高可靠、低成本的数据存储能力，可供用户存储任意类型和大小的数据。适合企业备份/归档、视频点播、视频监控等多种数据存储场景。了解更多OBS服务，详见**对象存储服务**。
- 密钥管理（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。b了解更多KMS服务，详见**密钥管理概述**。

6.2 异常检测与修复

在多专区架构的企业云环境中，管理员需要对各专区的安全策略进行统一管理，以确保专区间的隔离效果符合预期。然而，随着业务规模扩大和策略数量增加，管理员难以通过人工巡检的方式实时掌握所有专区的策略配置状态，容易出现策略配置偏移或误操作危险命令等情况，可能导致专区隔离效果下降或产生安全隐患。针对上述问题，专区风险扫描功能支持对专区策略配置进行自动化检测，可识别策略配置偏移和危险操作，并按风险等级触发告警，帮助管理员及时发现并处理专区安全隐患，保障专区隔离管理的安全性和有效性。

前提条件

已**创建高安专区**，并已经在专区内添加了资源，详见**添加资源**章节。

风险等级解读

系统将识别出的资产风险按致命、高危、中等、低危四个等级呈现，风险等级解释如**表6-3**。

表 6-3 风险等级

风险等级	含义
致命（CRITICAL）	最高严重等级，存在严重泄露隐患，需要优先紧急处置。

风险等级	含义
高危（HIGH）	严重安全风险，建议尽快整改修复。
中等（MEDIUM）	一般性风险，需要规划时间处理。
低危（LOW）	轻微风险、优化建议，可选择性优化。

扫描项定义

专区默认每六个小时启动一次扫描，同时启用了以下风险扫描检查项，覆盖公网暴露、跨账号越权、资源标签漂移、IAM策略完整性等核心合规维度。每项扫描均自动执行并提供可修复建议。

公网入口与网络边界风险

表 6-4 扫描项定义

检查项ID	检查项名称	检查项描述	风险级别	修复建议
SCAN-001	专区弹性公网 IP 绑定检测	检测专区VPC内是否存在绑定了EIP的实例。当EIP状态为ACTIVE且其关联的VPC属于专区VPC集合时，判定为专区存在公网入口风险，可能被外部访问。	高危（HIGH）	解绑EIP
SCAN-004	跨专区 VPC 对等连接检测	检测是否存在跨专区的VPC对等连接。当对等连接一端位于专区内、另一端位于专区外且状态为ACTIVE时告警，提示专区网络边界被打通，存在数据横向流动风险。	中等（MEDIUM）	移除对等连接或加入专区

OBS 对象存储安全

表 6-5 扫描项定义

检查项ID	检查项名称	检查项描述	风险级别	修复建议
SCAN-010	OBS 桶策略外部账号访问检测	检测OBS桶策略是否允许外部账号访问。当策略中Principal或NotPrincipal包含非本domainId的具体账号ID，或Principal为通配符*且Allow读类Action时，判定为桶可被外部访问。	致命（CRITICAL）	移除外部访问权限
SCAN-011	OBS 对象 ACL 外部访问检测	抽样检测OBS桶内对象的ACL配置。当Grant列表包含AllUsers组且授予READ/WRITE权限，或包含非owner的CanonicalGrantee时，判定为对象可被外部访问。	致命（CRITICAL）	移除外部ACL
SCAN-012	OBS 桶公网可读检测	检测OBS桶是否可被公网读取。通过ACL维度（含AllUsers读权限）与策略维度（Principal为*且Allow读类Action）双重判定，任一命中即告警。	致命（CRITICAL）	禁用公网访问
SCAN-015	OBS 桶 Deny 策略结构完整性检测	检测OBS桶策略中DenyCrossAccountAccess语句结构是否完整。当缺失对应Sid，或其Action缺少PutBucketPolicy/PutBucketAcl时，判定为防跨账号篡改策略被裁剪，存在被外部修改风险。	高危（HIGH）	通过API-022重配桶策略

跨账号共享与委托风险

表 6-6 扫描项定义

检查项ID	检查项名称	检查项描述	风险级别	修复建议
SCAN-016	RAM 资源外部共享检测	检测RAM（资源访问管理）共享资源是否共享到外部委托人。当shared_resources列表非空时，说明专区资源已被共享给外部账号，存在数据外泄风险。	致命（CRITICAL）	移除外部委托人
SCAN-017	RAM 允许外部委托人检测	检测RAM资源共享是否开启allow_external_principals字段为true。开启后允许外部账号主动加入共享，存在资源被非预期账号访问的风险。	高危（HIGH）	禁用外部委托人
SCAN-018	IAM 委托信任外部账号检测	检测IAM委托是否信任外部账号。当trust_domain_name不以op_svc_开头且trust_domain_id不等于当前domainId时，判定为委托信任了外部账号，存在跨账号越权风险。	高危（HIGH）	移除外部账号信任

KMS 密钥授权

表 6-7 扫描项定义

检查项ID	检查项名称	检查项描述	风险级别	修复建议
SCAN-027	KMS 密钥 Grant 授权检测	检测KMS密钥是否创建了Grant授权。只要存在grantee_principal（被授权主体）非空即视为存在密钥被越权访问的风险，需审查授权范围是否合理。	高危（HIGH）	审查KMS授权

IAM 用户组与策略完整性

表 6-8 扫描项定义

检查项ID	检查项名称	检查项描述	风险级别	修复建议
SCAN-030	AllUsers 用户组成员完整性检测	检测DSC-DSZ-AllUsers用户组成员是否完整。当用户组不存在，或实际成员与专区期望的ACTIVE用户集合存在差异（缺失或多余成员）时告警，提示用户组与专区用户不同步。	高危（HIGH）	重建组/同步成员
SCAN-031	专区资源标签漂移检测	检测专区资源（非LOCAL_SERVER）的标签是否漂移。通过TMS/OBS查询资源标签，当标签key对应的value不等于zoneId或标签缺失时，判定为标签漂移，可能导致资源归属判定失效。	中等（MEDIUM）	重新应用专区标签
SCAN-032	专区 IAM 用户标签漂移检测	检测专区IAM用户的标签是否漂移。通过IAM查询用户标签，当标签key对应的value不等于zoneId或标签缺失时判定为漂移，可能导致用户归属专区判定失效。	中等（MEDIUM）	重新应用用户标签
SCAN-033	AllUsers 组 IAM 策略完整性检测	检测AllUsers用户组附加的三条专区IAM策略（ZoneAccess、TagProtection、NetworkDeny）是否完整且内容与DB记录一致。当用户组缺失、策略未附加或策略文档内容不匹配时告警，提示专区访问控制策略被篡改或丢失。	致命（CRITICAL）	补充缺失策略/通过DSC API重新附加

VPCEP 端点策略

表 6-9 扫描项定义

检查项ID	检查项名称	检查项描述	风险级别	修复建议
SCAN-009	KMS VPCEP 端点策略漂移检测	检测KMS VPC终端节点（VPCEP）的策略是否与DB中记录的预期策略一致。当端点无策略或策略JSON比对不匹配时，判定为策略漂移，可能导致终端节点的访问控制被绕过。	高危（HIGH）	通过API-022重新配置VPCEP策略

查看风险概况

步骤1 登录DSC服务控制台。

步骤2 在左侧导航栏中，选择“高安专区”，进入“高安专区”控制台。

步骤3 在左侧导航栏中，选择“持续运营 > 异常检测与修复”。

步骤4 查看**风险概况**。显示检测的专区总数、不同等级的风险资产总数。

单击  ，可关闭风险概况，建议不要关闭。

风险概况中的各严重级别统计（致命、高危、中等、低危）按检查项类型计数，表示扫描覆盖了多少种不合规检查项。

图 6-3 风险概况

步骤5 查看不同专区的风险检测结果。直观展示资产的合规得分、开放风险，以及不同等级风险的分布统计。

- 单击  ，开启后，仅查看有开放风险的资产。
- 在下拉框中选择排序方式，风险列表可按风险数排序、合规分排序、上次扫描时间排序。

关键字段解读：

- **合规分**：对该资产整体安全合规水平的综合打分，满分一般100分。100分以下代表资产存在多项安全风险，合规水平有待提升，需要处置风险项拉高分数。

说明

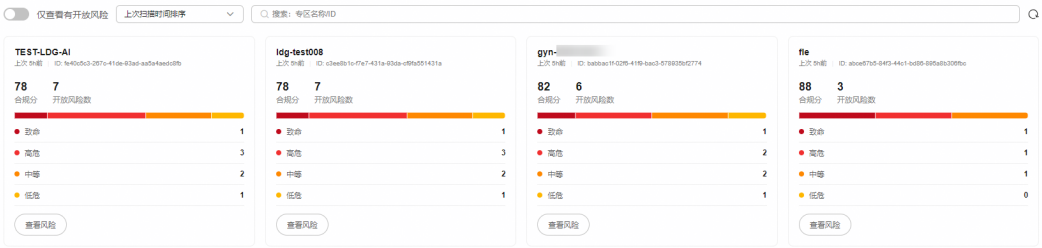
合规分满分100分，用于量化高安专区的安全合规程度。系统根据每项检查结果的严重程度进行加权计分，严重级别越高权重越大：致命（CRITICAL）权重10、高危（HIGH）权重5、中等（MEDIUM）权重2、低危（LOW）权重1。

计算公式为：合规分 = 100 × (1 - 违规项权重之和 ÷ 总权重)。其中“总权重”是所有已执行检查项的权重之和，“违规项权重之和”是未通过检查项的权重之和。通过的检查项不扣分，但其权重计入总权重（分母）。因环境异常无法执行的检查项（ERROR状态）不纳入计分。

举例说明：假设本次执行了20项检查，包含3个致命、5个高危、8个中等、4个低危，总权重为75。若其中有1个致命、1个高危、2个中等、3个低危共7项未通过，违规权重为22，则合规分 = 100 × (1 - 22/75) ≈ 71分。由此可见，严重级别的问题对分数影响更大。同样7项未通过，若全部为低危（权重7），合规分约为91分；但包含1个致命级别后，合规分降至71分。这体现了系统对高风险问题的重点关注。

- **开放风险数**：识别出的对外开放类安全风险（权限过宽、匿名访问、公开可读、未加密等对外暴露类风险）。

图 6-4 风险评估



步骤6 单击“查看风险”，查看该专区风险的具体内容，如风险级别、检查项等内容。

各检查项的定义及修复建议，请参考**扫描项定义**。

图 6-5 风险详情

步骤7 单击“操作”列的“查看”，参照修复方法整改资产风险。

----结束

相关文档

- **数据流转**：DSC统一采集专区内OBS读写日志及KMS加解密SDK数据操作日志，动态捕获用户访问行为路径，能够全面支撑事件溯源与风险定位，直观展示数据流转情况，帮助运维及安全人员及时识别异常与安全风险。