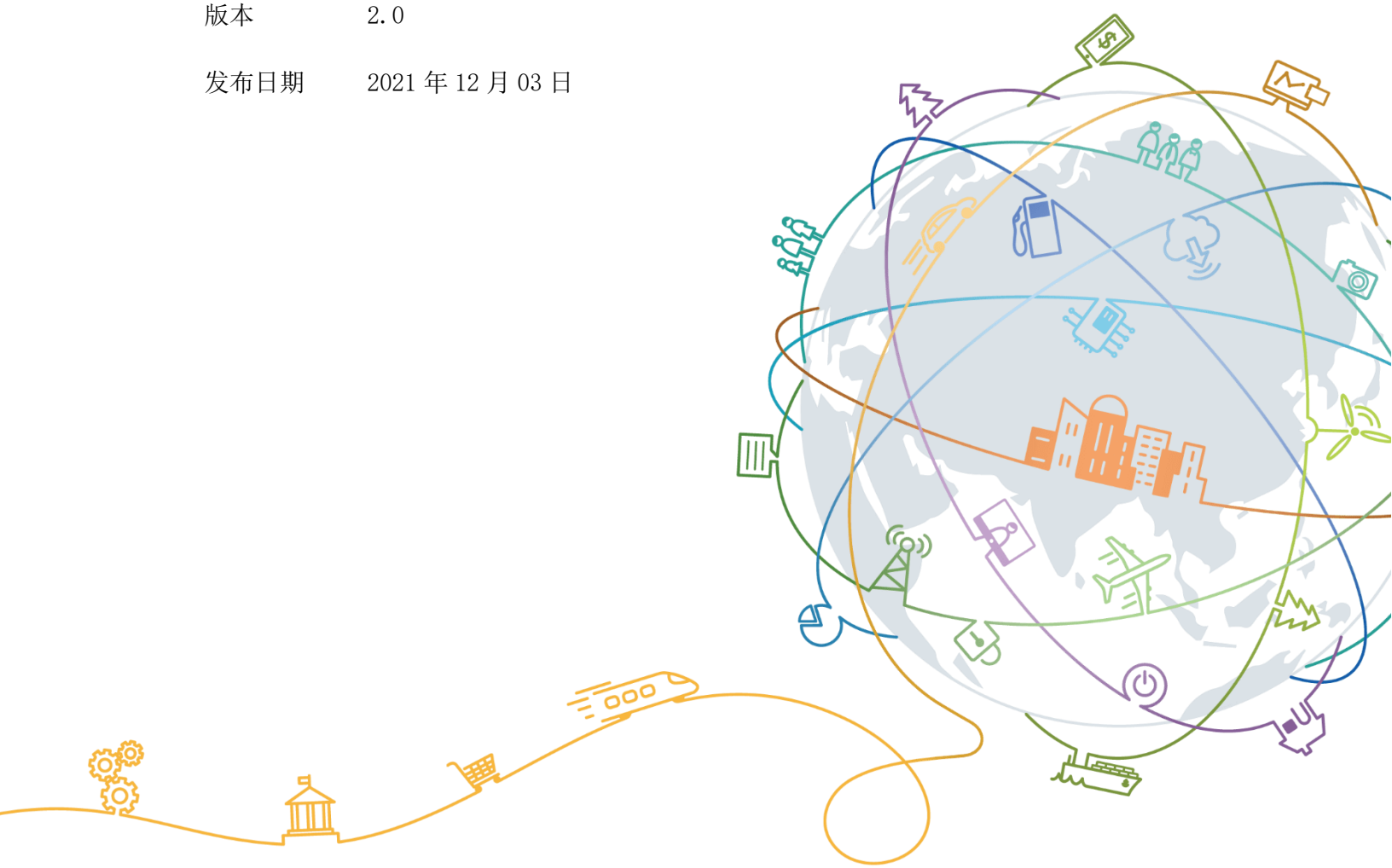
华为云安全基线配置指南

版本　　2.0

发布日期　　2021 年 12 月 03 日



华为技术有限公司

商标声明

注意

您购买的产品、服务或特性等应受华为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南，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保证。

华为技术有限公司

地址：深圳市龙岗区坂田华为总部办公楼　　邮编：518129

网址：**https://www.huawei.com**

客户服务邮箱：**support@huawei.com**

客户服务电话：4008302118

目录

1. 概述

安全基线是一个信息系统的最小安全保障，云安全基线是云环境最基本的安全保证，是开展安全防护的基础。如果云服务没有达到安全基线要求，云上业务及资产将面临巨大安全风险。为了帮助客户提高云环境的安全防护能力，华为云作为云服务供应商，为客户提供了华为云安全基线检查和配置的操作指南。

本文精选了为租户安全保驾护航均尤为重要的服务，涉及计算、网络、存储、数据库和安全等方面。本指南并不是所有可能的安全配置的详尽列表，建议客户将本基线配置指南作为一个起点，并根据实际需要在此基础上进行补充或裁剪。

1.1 目标读者

本文档适用于计划开发、部署、评估或使用华为云服务的系统管理员、应用管理员、平台部署人员、安全专家、审计员、服务台等。

1.2 等级定义

本文档安全基线的等级定义如下：

- Level 1：该类配置为实现组织安全的基本要求，旨在降低组织攻击面。
- Level 2：该类配置在 Level 1 配置的基础上进行了扩展，适用于安全至上的环境，但实施该类配置可能会对组织业务造成影响。

2. 华为云安全配置建议

华为云为客户提供态势感知（SA）服务以帮助客户执行自动基线检查。态势感知支持检测云服务关键配置项，通过执行扫描任务，检查云服务基线配置风险状态，分类呈现云服务配置检测结果，告警提示存在安全隐患的配置，并提供相应配置加固建议和帮助指导。详情可参见云服务基线检查用户指南。

若客户未购买 SA 服务，则可以使用本指南对云服务的安全基线进行检查和配置。

2.1 身份与访问管理

身份和访问管理策略是为确保云平台环境安全而采取的深入防御方法的第一步，本节将介绍配置身份和访问管理策略时可参考的建议。

2.1.1 创建非管理员权限的 IAM 用户

等级：Level 2

配置建议：

“admin”为缺省用户，具有所有云服务资源的操作权限，当所有用户全部属于 admin 用户组或共用一个企业管理员帐号是不安全的。为了更好的管控人员或应用程序对云资源的使用，可以使用统一身份认证服务（IAM）的用户管理功能，给员工或应用程序创建 IAM 用户。

检查步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航栏窗格中，选择“用户”
3. 检查右侧是否存在除企业管理员外的其他帐号
4. 在左侧导航栏窗格中，选择“用户组”
5. 检查右侧用户组是否存在除 admin 组外的其他用户组且用户数不为 0

配置步骤：

1. 管理员登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航窗格中，选择“用户”，单击右上方的“创建用户”
3. 在“创建用户”页面填写“用户信息”，如需一次创建多个用户，可以单击“添加用户”进行批量创建，每次最多可创建 10 个用户
4. 在“创建用户”页面选择“访问方式”，完成后单击“下一步”
5. 单击“创建用户”，IAM 用户创建完成，用户列表中显示新创建的 IAM 用户

详情可参见创建 IAM 用户操作指导

2.1.2 确保管理员帐号已启用 MFA

等级：Level 2

配置建议：

虚拟 Multi-Factor Authentication（MFA）是多因素认证方式的一种，如需使用，用户需要先在智能设备上安装一个 MFA 应用程序（例如："华为云"手机应用程序），才能绑定虚拟 MFA 设备。绑定 MFA 后，用户在登录时或进行敏感操作前需输入 MFA 随机产生的 6 位数字认证码。MFA 设备可以基于硬件也可以基于软件，目前华为云仅支持基于软件的虚拟 MFA。

检查步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择"统一身份认证"
2. 在左侧导航栏窗格中，选择"用户"，进入具备管理员权限用户的"安全设置"
3. 检查"虚拟 MFA 设备"是否显示"已绑定"

配置步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择"统一身份认证"
2. 在左侧导航栏窗格中选择"安全设置"，进入"安全设置>敏感操作"页面，单击"虚拟 MFA"右侧的"前往绑定"
3. 根据右侧弹出的绑定虚拟 MFA 页面，在 MFA 应用程序中添加用户
4. 添加用户后，在"华为云"手机应用程序"虚拟 MFA 页面"，查看虚拟 MFA 的动态口令页面，动态口令每 30 秒自动更新一次
5. 在"绑定虚拟 MFA"页面输入连续的两组口令，然后单击"确定"，完成绑定虚拟 MFA 设备的操作

以上配置步骤主要针对"暂未升级华为帐号"的用户，如用户"已升级华为帐号"，点击"前往绑定"后跳转至"华为帐号>安全验证"页面，根据提示绑定虚拟 MFA。

2.1.3 启用用户登录保护

等级：Level 1

配置建议：

为了进一步提高帐号安全性，有效避免钓鱼式攻击或者用户密码意外泄漏，用户可在 IAM 的安全设置中开启登录保护。开启后用户登录时除了需要口令认证还需要通过虚拟 MFA 或短信或邮件验证，以再次确认登录者身份。

检查步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航栏窗格中，选择“安全设置”
3. 在新窗口中选择“敏感操作”
4. 检查“登录保护”是否为“已设置”

配置步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航栏窗格中选择“安全设置”
3. 在新窗口中选择“敏感操作”，点击“立即设置”， 开启“登录保护”，并配置“验证方式”

2.1.4 启用用户操作保护

等级：Level 2

配置建议：

为了进一步提高帐号安全性，有效确保用户安全地使用云产品，用户可在 IAM 中开启操作保护。开启后，主帐号及子用户在控制台进行敏感操作时（例如：删除弹性云服务器、弹性 IP 解绑等），将通过虚拟 MFA 或手机短信或邮件再次确认操作者的身份。

检查步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航栏窗格中，选择“安全设置”
3. 在新窗口中选择“敏感操作”
4. 检查“操作保护”是否为“已开启”

配置步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航栏窗格中选择“安全设置”
3. 在新窗后中选择“敏感操作”，点击“立即启用”， 开启“登录保护”，并配置“验证方式”

2.1.5 启用访问密钥保护

等级：Level 2

配置建议：

为了提高帐号资源的安全性，建议开启访问密钥保护功能。“访问密钥保护”功能默认为关闭状态。开启该功能后，仅管理员才可以创建、启用/停用或删除 IAM 用户的访问密钥。

检查步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航栏窗格中选择“安全设置”
3. 在新窗口中选择“敏感操作”，检查是否已开启“访问密钥保护”

配置步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航栏窗格中选择“安全设置”
3. 在新窗后中选择“敏感操作”，启用“访问密钥保护”

2.1.6 管理员帐号禁用 AK/SK

等级：Level 2

配置建议：

由于管理员具有 IAM 用户管理权限，且具有大范围的操作权限，为了避免因 AK/SK 泄露带来的安全隐患，建议管理员帐号禁用 AK/SK 身份凭证。

检查步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在右上角账户下拉列表中选择“我的凭证”
3. 在左侧导航栏窗格中，选择“访问密钥”
4. 检查右侧访问密钥列表中是否显示为“暂无数据”

配置步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在右上角帐号下拉列表中选择“我的凭证”
3. 在左侧导航栏窗格中，选择“访问密钥”，删除“访问密钥”

2.1.7 配置 IAM 帐号强密码策略

等级：Level 1

配置建议：

IAM 用户的密码策略应设置强密码策略，建议满足以下要求：

- 包含以下字符中的 3 种：大写字母、小写字母、数字和特殊字符
- 密码长度不小于 8 位
- 新密码不能与最近的历史密码相同（重复次数设置为 3）

检查步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航栏窗格中选择“安全设置”
3. 在新窗口中选择“密码策略”，检查策略要求是否符合（或强于）强密码策略

配置步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航栏窗格中选择“安全设置”
3. 在新窗口中选择“密码策略”，依次配置“密码设置策略”、“密码有效期策略”、“密码最短使用时间策略”

2.1.8 配置登录验证策略

等级：Level 1

配置建议：

管理员可以设置登录验证策略，包括“会话超时策略”、“帐号锁定策略”、“帐号停用策略”、“最近登录提示”、“登录验证提示”。

1、会话超时策略：如果用户超过设置的时长未操作界面，会话将会失效，需要重新登录。管理员可以设置会话超时的时长，会话超时时长默认为 1 个小时，可以在 15 分钟~24 小时之间进行设置。

2、帐号锁定策略：如果在限定时间长度内达到登录失败次数后，用户会被锁定一段时间，锁定时间结束后，才能重新登录。管理员可以设置限定时间长度、限定时间内登录失败次数、帐号锁定时长。

3、帐号停用策略：如果 IAM 用户在设置的有效期内没有通过界面控制台或者 API 访问华为云，将会被停用。帐号停用策略默认关闭，管理员可以选择开启，并在 1~240 天之间进行设置。该策略仅对帐号下的 IAM 用户生效，对帐号本身不生效。IAM 用户被停用后，可以联系管理员重新启用。

4、最近登录提示：如果开启最近登录提示，用户登录成功后，将在“登录验证”页面中看到上次登录成功时间，最近登录提示可以帮助用户查看是否存在异常登录信息，如果存在不是本人的登录信息，建议立即修改密码。最近登录提示默认关闭，管理员可以选择开启。

5、登录验证提示：管理员可以在最近登录提示中进行公告，例如欢迎语，或者提示用户谨慎删除资源等。登录验证提示默认关闭，管理员可以选择开启。

检查步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航栏窗格中选择“安全设置”
3. 在新窗口中选择“登录验证策略”，检查是否配置“会话超时策略”、“帐号锁定策略”，是否开启“帐号停用策略”、“最近登录提示”，是否填写“登录验证提示”

配置步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航栏窗格中选择“安全设置”
3. 在新窗口中选择“登录验证策略”，依次配置“会话超时策略”、“帐号锁定策略”、“帐号停用策略”、“最近登录提示”、“登录验证提示”

2.1.9 配置 IAM 的网络访问控制策略

等级：Level 2

配置建议：

管理员可以设置访问控制策略，限制用户只能从特定 IP 地址区间、网段及 VPC Endpoint 访问华为云：

1、允许访问的 IP 地址区间：限制用户只能从设定范围内的 IP 地址访问华为云，可以在 0.0.0.0~255.255.255.255 之间设置。默认值为 0.0.0.0~255.255.255.255。如不设置或设置为默认值意味着用户的 IAM 用户可以从任意地方访问华为云。

2、允许访问的 IP 地址或网段：限制用户只能从设定的 IP 地址或网段访问华为云，例如：10.10.10.10/32。

3、 允许访问的 VPC Endpoint：仅在“API 访问”页签中可进行配置。限制用户只能从具有设定 ID 的 VPC Endpoint 访问华为云 API，例如：0ccad098-b8f4-495a-9b10-613e2a5exxxx

访问控制生效条件：

- 控制台访问：仅对帐号下的 IAM 用户登录控制台生效，对帐号本身不生效。
- API 访问：仅对帐号下的 IAM 用户通过 API 网关访问 API 接口生效，修改后 2 小时内生效。

检查步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航栏窗格中选择“安全设置”
3. 在新窗口中选择“访问控制”，检查“允许访问的 IP 地址区间”、“允许访问的 IP 地址或网段”列表下是否有信息

配置步骤：

1. 使用管理员帐号登录控制台，鼠标移动至右上方的帐号名，在下拉列表中选择“统一身份认证”
2. 在左侧导航栏窗格中选择“安全设置”
3. 在新窗口中选择“访问控制”，依次配置“允许访问的 IP 地址区间”、“允许访问的 IP 地址或网段”

2.1.10 启用 CBH 的多因子认证

等级：Level 1

配置建议：

为了进一步提高堡垒机帐号安全性，用户可启用云堡垒机服务（CBH）的多因子认证功能。启用后，用户通过 Web 浏览器或 SSH 客户端登录 CBH 实例时需进行多因子认证。多因子认证方式包括：手机短信、手机令牌、USBKey、动态令牌。

检查步骤：

1. 使用 CBH 管理员帐号通过 Web 浏览器登录云堡垒机系统
2. 在左侧导航栏窗格中，选择“用户>用户管理”，进入用户列表页面，选择“管理>用户配置”，检查是否启用多因子认证

配置步骤：

1. 使用 CBH 管理员帐号通过 Web 浏览器登录云堡垒机系统
2. 在左侧导航栏窗格中，选择“用户>用户管理”，进入用户列表页面，选择“管理>用户配置”，启用多因子认证，并根据提示，配置相关参数

2.1.11 创建密钥对安全登录 ECS

等级：Level 2

配置建议：

如果存在弹性云服务器（ECS）对外暴露弹性公网 IP（EIP）的情况，用户登录 ECS 时建议使用密钥方式进行身份验证。用户可以使用已有密钥对或新建一个密钥对，实现远程登录时的身份验证。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择选择“计算> 弹性云服务器 ECS”
3. 在左侧导航树中，选择“密钥对”，在“密钥对管理”页面，检查是否存在密钥信息

配置步骤：

1. 登录管理控制台
2. 在服务列表选择选择“计算> 弹性云服务器 ECS”
3. 在左侧导航树中，选择“密钥对”，在“密钥对管理”页面，单击“创建密钥对”，输入密钥名称，单击“确定”
4. 浏览器会提示下载或自动下载私钥文件。文件名是用户为密钥对指定的名称，文件扩展名为“.pem”。请将私钥文件保存在安全位置，然后在系统弹出的提示框中单击“确定”

2.2 网络安全

本节将介绍在华为云上配置网络策略时可参考的安全建议。

2.2.1 配置安全组入方向规则

等级：Level 1

配置建议：

安全组的规则默认是全部放行出方向上的数据报文，限制入方向上的数据报文。安全组入方向规则的配置应满足最小化原则。一般在非业务必需的情况下，源地址为 0.0.0.0/0，公网地址掩码小于 32 以及内网地址掩码小于 24 即被视为不满足最小化访问控制原则。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“网络>虚拟私有云 VPC”

3. 在左侧导航栏选择“访问控制>安全组”，在右侧列表单击安全组名称
4. 切换至“入方向规则”页签，检查是否存在不满足最小化访问控制的规则

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“网络>虚拟私有云 VPC”
3. 在左侧导航栏选择“访问控制>安全组”， 在右侧列表单击安全组名称
4. 切换至“入方向规则”页签，根据最小化访问控制规则填写安全组参数

详情可参见安全组创建指导与配置示例

2.2.2 禁用高危端口及远程管理端口

等级：Level 1

配置建议：

添加安全组规则时，用户必须指定通信端口或端口范围。华为建议在安全组入方向规则中不应该对外开放高危端口、远程管理端口，如业务所必需，建议根据最小化开放原则开放此类端口。源地址为0.0.0.0/0，公网地址掩码小于 32 以及内网地址掩码小于 24 即被视为不满足最小化访问控制原则。

高危端口至少包括：20、21、135、137、138、139、445、389、593、1025

远程管理端口包括：22、23、177、513、3389、4899、6000~6063、5900、5901

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“网络>虚拟私有云 VPC”
3. 在左侧导航栏选择“访问控制>安全组”
4. 选择对应的安全组，点击进入“配置规则>入方向规则”
5. 切换至“入方向规则”页签，检查是否存在不满足对外最小化开放的高危端口、远程管理端口

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“网络>虚拟私有云 VPC”
3. 在左侧导航栏选择“访问控制>安全组”
4. 选择对应的安全组，点击进入“配置规则>入方向规则”
5. 在“入方向规则”页签，根据提示，配置协议端口

2.2.3 配置 VPC 实现网络隔离

等级：Level 1

配置建议：

如果用户在当前区域下有多套业务部署，且期望不同业务之间进行网络隔离时，则可为每个业务在当前区域建立相应的 VPC。不同区域的 VPC 之间内网不互通，同区域的不同 VPC 内网不互通，同一个 VPC 下的不同可用区之间内网互通。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“网络>虚拟私有云 VPC”，进入“网络控制台”
3. 在左侧导航栏点击“虚拟私有云”，在右侧列表检查是否存在多个 VPC 的规划

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“网络>虚拟私有云 VPC”，进入“网络控制台”
3. 在左侧导航栏点击创建“虚拟私有云”，按要求创建 VPC

2.2.4 配置 VPC 子网 ACL 规则

等级：Level 1

配置建议：

网络 ACL 与安全组类似，都是安全防护策略，当用户想增加额外的安全防护层时，就可以启用网络 ACL。安全组对 ECS 进行防护，网络 ACL 对子网进行防护，两者结合起来，可以实现更精细、更复杂的安全访问控制。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“网络>虚拟私有云 VPC”
3. 在左侧导航栏选择“子网”，检查列表中各子网的“网络 ACL”是否不为空

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“网络>虚拟私有云 VPC”

3. 在左侧导航栏选择“访问控制>网络 ACL”
4. 在页面右侧区域，单击“创建网络 ACL”
5. 在“创建网络 ACL”页面，根据提示，填写网络 ACL 参数

详情可参见网络 ACL 创建指导与配置实例

2.2.5 VPC 对等链接的安全配置

等级：Level 2

配置建议：

对等连接是指两个 VPC 之间的网络连接，对于对等连接的路由应该满足最小访问权限原则。建议本端路由的目的地址最好限定在最小子网网段内，对端路由的目的地址最好限定在最小子网网段内。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“网络>虚拟私有云 VPC”，进入“网络控制台”
3. 在左侧导航栏选择“对等连接”，检查是否有相关信息

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“网络>虚拟私有云 VPC”，进入“网络控制台”
3. 在左侧导航栏选择“对等连接”，点击进入“创建对等连接”
4. 在“创建对等连接”页面，根据提示，配置参数

详情可参见 VPC 对等连接创建指导与配置示例

2.2.6 启用 ELB 监听器的访问控制

等级：Level 1

配置建议：

共享型负载均衡器用户可以通过添加白名单和黑名单的方式控制访问负载均衡监听器的 IP。通过白名单能够设置允许特定 IP 访问，而其它 IP 不许访问。通过黑名单能够设置允许特定的 IP 不能访问，而其它 IP 允许访问。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“网络>弹性负载均衡 ELB”，进入“负载均衡器”
3. 在右侧列表单击负载均衡器名称，进入监听器管理界面
4. 检查各个监听器是否配置访问控制策略

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“网络>弹性负载均衡 ELB”，进入“负载均衡器”
3. 在右侧列表单击负载均衡器名称，进入监听器管理界面
4. 在需要添加访问控制策略的监听器基本信息页面，单击访问控制右侧“修改访问控制”按钮，配置访问控制策略

详情可参见监听器访问控制策略配置指导

2.2.7 启用 Anti-DDoS 流量清洗防护功能

等级：Level 1

配置建议：

DDoS 原生基础防护（Anti-DDoS 流量清洗）服务（Anti-DDoS）为公网 IP 提供四到七层的 DDoS 攻击防护和攻击实时告警通知服务。Anti-DDoS 通过对互联网访问公网 IP 的业务流量进行实时监测，及时发现异常 DDoS 攻击流量。在不影响正常业务的前提下，可根据用户配置的防护策略，清洗掉攻击流量。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>DDoS 防护”，进入“Anti-DDoS 流量清洗”界面
3. 检查各个公网 IP 的防护状态是否为“正常（默认防护）”

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>DDoS 防护”，进入“Anti-DDoS 流量清洗”界面
3. 选择“公网 IP”页签，单击“设置默认防护策略”
4. 在弹出的设置默认防护策略窗口中，勾选“手动设置”， 单击“OK”，完成默认防护策略的设置
5. 默认防护策略设置完成后，新购买的公网 IP 均按照默认防护策略启动防护

详情可参见 DDos 原生基础防护操作指导

2.2.8 启用 DDoS 高防防护功能

等级：Level 2

配置建议：

当用户的服务器遭受大流量DDoS攻击时，DDoS高防可以保护用户业务持续可用。配置开通DDoS高防，通过高防 IP 代理源站 IP 对外提供服务，将恶意攻击流量引流到高防 IP 清洗，确保重要业务不被攻击中断。建议娱乐、金融、政府、电商、媒资、在线交易等行业启用 DDoS 高防。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>DDoS 防护”
3. 在左侧导航栏选择“DDoS 高防>概览”
4. 检查是否配置开通 DDoS 高防

配置步骤：

1. 登录管理控制台
2. 进入购买 DDoS 高防实例入口，在“购买 DDoS 高防”界面，选择规格
3. 选择“购买时长”和“购买数量”，单击“立即购买”
4. 在“订单详情”页面，如果确认订单无误，单击“去支付”
5. 在“购买 DDoS 高防”的支付界面，单击“确认付款”，完成订单支付
6. 在“订单支付成功”界面，选择“服务列表>安全>DDoS 高防服务”，系统跳转至 DDoS 高防实例列表界面

详情可参见 DDoS 高防配置指导

2.2.9 启用 Web 应用防火墙功能

等级：Level 2

配置建议：

对于有 Web 业务的用户，建议启用 Web 应用防火墙服务（WAF）。启用后，网站所有的公网流量都会先经过 WAF，恶意攻击流量会被 WAF 检测并过滤，而正常流量返回给源站 IP，从而确保源站 IP 安全、稳定、可用。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“安全> Web 应用防火墙 WAF”
3. 检查是否配置开通 Web 应用防火墙

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“安全> Web 应用防火墙 WAF”
3. 首次使用 WAF，单击“立即购买 WAF”，进入购买页面，选择云模式后，选择服务版本、扩展包，以及购买时长
4. 添加防护域名：在左侧导航树中选择“网站设置”，在域名列表的左上角，单击“添加防护网站”，进入添加防护域名页面，根据提示，分别完成“对外协议”、“源站协议”、“源站地址”、“源站端口”的配置
5. 域名接入：按界面提示，到该域名的 DNS 服务商处，将其解析指向新的 CNAME 值
6. 开启 WAF 防护：在目标域名所在行的“防护策略”栏中，单击“配置防护策略”。 在“Web 基础防护”配置框中，更改 Web 基础防护的“状态”和“模式”

2.2.10 配置 WAF 地理位置访问控制策略

等级：Level 2

配置建议：

用户可以通过 WAF 配置地理位置访问控制规则，以实现对指定国家、地区的来源 IP 的自定义访问控制。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>Web 应用防火墙 WAF”
3. 在左侧导航栏中单击选择“防护策略”，在右侧页面中选择“所有策略规则”
4. 在新页面中检查“地理位置访问控制”中是否添加了相应的规则，且状态为“已开启”

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>Web 应用防火墙 WAF”

3. 在左侧导航栏中单击选择“防护策略”，进入防护策略配置入口，在“地理位置访问控制”配置框中，用户可根据自己的需要更改“状态”，单击“自定义地理位置访问控制规则”，进入“地理位置访问控制”页面
4. 在“地理位置访问控制”页面左上角，单击“添加规则”，在弹出的对话框，添加地理位置访问控制规则

详情可参见地理访问控制规则配置指导

2.2.11 配置 WAF 回源 IP（源站服务器部署在 ECS）

等级：Level 1

配置建议：

回源 IP 是 WAF 用来代理客户端请求服务器时用的源 IP，在服务器看来，接入 WAF 后所有源 IP 都会变更为 WAF 的回源 IP，真实的客户端 IP 会被加载 HTTP 头部的字段中。当用户的源站服务器部署在华为云 ECS 或华为云 ELB 上，需要放行 WAF 所有回源 IP。

当 WAF 后未配置 ELB，应配置只允许 WAF 的回源 IP 访问 ECS。

检查步骤：

1. 登录管理控制台
2. 澄清是否存在 WAF 后配置使用 ELB 的业务场景，如果无，则不涉及；如果有，则继续
3. 在服务列表选择“安全>Web 应用防火墙 WAF”，进入到 “网站设置”，记录好“Web 应用防护墙的回源 IP 网段”
4. 在服务列表选择“计算>弹性云服务器 ECS”，在相应的 ECS 实例中，检查安全组入方向规则
5. 检查是否仅允许 WAF 回源 IP 段访问源站 ECS 的业务端口

配置步骤：

1. 登录管理控制台
2. 选择“安全与合规> Web 应用防火墙 WAF”，在左侧导航树中，选择“网站设置”，进入 “网站设置” 页面
3. 在网站列表右侧，单击“Web 应用防火墙回源 IP 网段”，查看 Web 应用防火墙所有回源 IP 段
4. 在“Web 应用防火墙回源 IP 网段”对话框，单击“复制 IP 段”，复制所有回源 IP
5. 选择“计算>弹性云服务器 ECS”，在目标 ECS 所在行的“名称/ID”列中，单击目标 ECS 实例名称，进入 ECS 实例的详情页面
6. 选择“安全组”页签，展开安全组，在目标安全组的右上角，单击“更改安全组规则”

7. 选择“入方向规则”页签，单击“添加规则”，进入“添加入方向规则”页面，成功添加安全组规则后，安全组规则将允许 WAF 回源 IP 段的所有入方向流量

详情可参见 WAF 回源 IP 配置指导

2.2.12 配置 WAF 回源 IP（源站服务器部署在 ELB）

等级：Level 1

配置建议：

回源 IP 是 WAF 用来代理客户端请求服务器时用的源 IP，在服务器看来，接入 WAF 后所有源 IP 都会变更 WAF 的回源 IP，真实的客户端 IP 会被加载 HTTP 头部的字段中。当客户的源站服务器部署在华为云 ECS 或华为云 ELB 上，需要放行 WAF 所有回源 IP。

当 WAF 后配置了 ELB，应配置只允许 WAF 的回源 IP 访问 ELB。

检查步骤：

1. 登录管理控制台
2. 澄清是否存在 WAF 后配置使用 ELB 的业务场景，如果无，则不涉及；如果有，则继续
3. 在服务列表选择“安全与合规> Web 应用防火墙 WAF”，进入到“网站设置”，记录好“Web 应用防火墙回源 IP 网段”
4. 在服务列表选择“网络>弹性负载均衡 ELB”，在相应的 ELB 实例中，进入到监听器中
5. 检查每个端口监听器中的“基本信息”的“访问控制”是否设置为“白名单”形式

配置步骤：

1. 登录管理控制台
2. 选择“安全与合规> Web 应用防火墙 WAF”，在左侧导航树中，选择“网站设置”
3. 在网站列表右侧，单击“Web 应用防火墙回源 IP 网段”，查看 Web 应用防火墙所有回源 IP 段
4. 在“Web 应用防火墙回源 IP 网段”对话框，单击“复制 IP 段”，复制所有回源 IP
5. 选择“网络>弹性负载均衡 ELB”，在目标 ELB 所在行的“监听器”列中，单击监听器名称，进入监听器的详情页面
6. 在监听器基本信息页面，单击“修改访问控制”，在弹出的对话框中，“访问策略”选择“白名单”
7. 将所有 WAF 的回源 IP 段添加到“IP 地址组”中，设置只允许 WAF 的回源 IP 段访问负载均衡监听器

详情可参见 WAF 回源 IP 配置指导

2.2.13 启用 WAF 对 Web 基础防护的拦截模式

等级：Level 1

配置建议：

Web 基础防护支持“拦截”和“仅记录”模式。“仅记录”模式仅会记录攻击行为，并不会对攻击行为进行阻断，建议开启 Web 基础防护的“拦截”模式，以在发现攻击后立即阻断并记录。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“安全> Web 应用防火墙 WAF”
3. 在左侧导航栏选择“网站设置”
4. 检查目标域名所在行的“防护策略”中的“Web 基础防护”的状态是否为“开启（拦截模式）”

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“安全> Web 应用防火墙 WAF”
3. 在左侧导航栏选择“网站设置”
4. 在目标域名所在行的“防护策略”栏中，单击“配置防护策略”，在“Web 基础防护”配置框中，选择“拦截”模式

详情可参见 WAF 防护规则配置指导

2.2.14 配置 CDN 安全访问策略

等级：Level 1

配置建议：

为了提高内容分发网络（CDN）的安全性，可以通过设置防盗链、IP 黑白名单的方式对访问者身份进行识别和过滤，限制部分用户访问。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“存储>内容分发网络 CDN”
3. 在左侧导航栏中单击选择“域名管理”

4. 在右侧页面的域名列表中，选择具体的域名，单击“设置”，进入“访问控制”页签，检查是否配置规则

配置步骤：

1. 登录管理控制台，在服务列表选择“存储>内容分发网络 CDN”，进入 CDN 控制台
2. 在左侧导航栏中，选择“域名管理”，在域名列表中，单击需要修改的域名或域名所在行的“设置”，进入域名配置页面
3. 选择“访问控制”页签
4. 在防盗链配置模块，单击“编辑”，系统弹出“配置防盗链”对话框，单击“状态”开关按钮，开启该配置项，根据页面提示，完成相关参数配置
5. 在 IP 黑白名单配置模块，单击“编辑”，系统弹出“配置 IP 黑白名单”对话框，单击“状态”开关按钮，开启该配置项，根据页面提示，完成相关参数配置

详情可参见 CDN 访问控制配置指导

2.3 数据安全

本节将介绍在华为云上配置数据安全保护措施时可参考的安全建议。

2.3.1 禁用 OBS 桶的公共访问权限

等级：Level 1

配置建议：

除业务所必需，建议 OBS 桶对于匿名用户（含未注册华为云的所有人）禁用对外公开访问的权限。

检查步骤：

1. 登录管理控制台，在服务列表选择“存储>对象存储服务 OBS”
2. 在 OBS 管理控制台左侧导航栏选择“对象存储”
3. 在桶列表单击待操作的桶，在“访问权限控制”中检查是否在“公共访问权限”栏赋予匿名用户的“桶访问权限”、“ACL 访问权限”

配置步骤：

1. 登录管理控制台，在服务列表选择“存储>对象存储服务 OBS”
2. 在 OBS 管理控制台左侧导航栏选择“对象存储”
3. 在桶列表单击待操作的桶，进入“概览”页面

4. 在左侧导航栏，单击“访问权限控制>桶 ACLs”
5. 在“桶 ACLs”中，单击“编辑”，通过勾选相应权限对拥有者、匿名用户组赋予目标桶的 ACL 权限
6. 单击“增加”，可对特定帐号添加 ACL 权限，输入特定帐号的“帐号 ID”或“帐号名”，并为其设定相应的 ACL 权限；“帐号 ID”或“帐号名”可通过“我的凭证”页面查看

用户还可针对 OBS 桶的对象配置 ACL，详情可参见 OBS 桶对象 ACL 配置指导

2.3.2 启用 OBS 桶存储加密功能

等级：Level 2

配置建议：

启用 OBS 桶的服务端加密后，用户在上传对象时，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成明文后再提供给用户，以提高数据存储的安全性。

检查步骤：

1. 登录管理控制台，在服务列表选择“存储>对象存储服务 OBS”
2. 在 OBS 管理控制台左侧导航栏选择“对象存储”
3. 在桶列表单击待操作的桶，进入“概览”页面
4. 在“基础配置”下，检查“默认加密”是否为“已配置”状态

配置步骤：

1. 登录管理控制台，在服务列表选择“存储>对象存储服务 OBS”
2. 在 OBS 管理控制台左侧导航栏选择“对象存储”
3. 在桶列表单击待操作的桶，进入“概览”页面
4. 在“基础配置”下，单击“默认加密”卡片，系统弹出“默认加密”对话框
5. 选择“开启”
6. 开启“KMS 加密”后，KMS 密钥会默认选中“obs/default”。用户也可以通过单击“创建 KMS 密钥”进入数据加密服务（DEW）页面创建自定义密钥，然后通过 KMS 密钥的下拉框选中创建的 KMS 密钥。

2.3.3 启用 EVS 加密功能

等级：Level 2

配置建议：

云硬盘 EVS 可以为弹性云服务器提供高可靠、高性能的块存储服务，启用 EVS 的加密功能后，可以对存储在云硬盘的数据进行加密。加密云硬盘使用的密钥由数据加密服务（DEW）中的密钥管理（KMS）提供，无需您自行构建和维护密钥管理基础设施。

检查步骤：

1. 登录管理控制台，在服务列表选择“存储>云硬盘 EVS”
2. 在磁盘列表单击待操作的云硬盘，进入“概览”页面
3. 在“配置信息”下，检查“加密”是否为“是”状态

配置步骤：

用户可使用 KMS 提供的默认主密钥加密硬盘，默认主密钥由 EVS 通过 KMS 自动创建的密钥，名称为“evs/default”，用户也可以自行通过 DEW 服务创建密钥，用户自行创建的密钥称为用户主密钥。安全管理员可以直接授权 EVS 访问 KMS，授权后，对于同一个租户而言，同一个区域下的普通用户都可以直接使用加密功能。

1. 在 EVS 管理控制台，单击“购买磁盘”。
2. 在“购买磁盘”界面展开“更多”，勾选“加密”，如果当前未授权 EVS 访问 KMS，则会弹出“创建委托”对话框，单击“是”，授权 EVS 访问 KMS，当授权成功后，EVS 可以获取 KMS 密钥用来加解密云硬盘。如果已授权，会弹出“加密设置”对话框，根据界面提示，配置相关信息。

详情可参见 EVS 服务端加密配置指导

2.3.4 确保 MySQL 数据库实例 root 远程登录安全控制

等级：Level 1

配置建议：

MySQL 数据库实例的 root 帐号应该做好远程登录的控制，限制仅应用端、DAS 管理网段等业务需要才可登录，防止 root 帐号被暴力破解。

检查步骤：

3. 登录管理控制台
4. 选择“数据库>云数据库 RDS”，在左侧导航栏中单击选择“实例管理”
5. 在右侧列表单机具体 RDS 实例
6. 单击”登录”，在新的页面单击”SQL 窗口”，执行命令：**use mysql** 进入到 mysql 库
7. 输入命令：**select user,host from user** 检查对于 root 帐号的 host 键值是否为“%”

配置步骤：

1. 登录管理控制台
2. 选择“数据库>云数据库 RDS”，在左侧导航栏中单击选择“实例管理”
3. 在右侧列表单机具体 RDS 实例
4. 单击”登录”，在新的页面单击”SQL 窗口”，执行命令：**use mysql** 进入到 mysql 库
5. 通过命令执行对 host 赋予远程访问权限

详情可参见数据库代理（读写分离）配置指导

2.3.5 启用 MySQL 数据库实例的 SSL 加密

等级：Level 2

配置建议：

为了确保数据在客户端和服务器端传输过程中的机密性和完整性，可启用数据库实例的 SSL 加密功能。启用该功能后会增加网络连接响应时间和 CPU 消耗，开启或关闭 SSL 加密会导致实例重启，实例重启时客户端会断开连接，请谨慎操作。

检查步骤：

1. 登录管理控制台
2. 选择“数据库>云数据库 RDS”，进入云数据库 RDS 信息页面
3. 在“实例管理”页面，选择指定的实例，单击实例名称
4. 检查是否开启 SSL 加密

配置步骤：

1. 登录管理控制台
2. 选择“数据库>云数据库 RDS”，进入云数据库 RDS 信息页面
3. 在“实例管理”页面，选择指定的实例，单击实例名称
4. 在“基本信息”页面，在“数据库信息”模块的“SSL”处，开启 SSL 加密

2.3.6 禁用 RDS/GaussDB 数据库公网连接

等级：Level 1

配置建议：

对于 RDS，如非业务所必须，不建议开通公网连接权限。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“数据库>云数据库 RDS”
3. 在左侧导航栏中单机选择“实例管理”
4. 在右侧列表单击具体 RDS 实例
5. 在具体实例的“连接管理>连接信息”中检查“公网地址”是否为空

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“数据库>云数据库 RDS”
3. 在左侧导航栏中单机选择“实例管理”
4. 在右侧列表单机具体 RDS 实例
5. 在具体实例的“连接管理>连接信息”在“连接信息”模块“弹性公网 IP”处，单击“解绑”，在弹出框中单击“是”，解绑 EIP

GaussDB 的配置步骤与 RDS 的类似。

2.3.7 配置 RDS/GaussDB 数据库公网安全访问策略

等级：Level 1

配置建议：

当数据库配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，需最小化控制访问源并开启 SSL 通道，同时更改默认的数据库端口（例如禁用 3306 端口）。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“数据库>云数据库 RDS”
3. 在左侧导航栏中单机选择“实例管理”
4. 在右侧列表单击具体 RDS 实例
5. 在具体实例的“连接管理>连接信息”中检查“数据库端口”是否修改为非 3306 端口、“SSL”是否开启
6. 在具体实例的“连接管理>安全组规则”中检查入方向规则，是否限制最小化访问、可信源访问

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“数据库>云数据库 RDS”
3. 在左侧导航栏中单机选择“实例管理”
4. 在右侧列表单击具体 RDS 实例
5. 在具体实例的“连接管理 >连接信息”中配置数据库端口，启用“SSL”
6. 在具体实例的“连接管理>安全组规则”中配置入方向规则，以限制最小化访问

GaussDB 的配置步骤与 RDS 的类似。

2.3.8 启用 CTS 事件文件的完整性校验功能

等级：Level 2

配置建议：

在安全和事故调查中，事件文件被删除或者被私下篡改会导致操作记录的真实性受到影响，无法对调查提供有效真实的依据。事件文件完整性校验功能旨在帮助用户确保事件文件的真实性。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“管理与部署>云审计服务 CTS”，进入云审计服务页面
3. 单击左侧导航树的“追踪器”，进入追踪器信息页面
4. 单击追踪器的配置按钮，在弹出的“配置追踪器”窗口中，检查“开启文件校验”是否开启

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“管理与部署>云审计服务 CTS”，进入云审计服务页面
3. 单击左侧导航树的“追踪器”，进入追踪器信息页面
4. 单击追踪器的配置按钮，在弹出的“配置追踪器”窗口中，打开“开启文件校验”开关，点击确定按钮，即可开启事件文件完整性校验功能

2.3.9 启用 DSC Access Key 泄露检测功能

等级：Level 2

配置建议：

开发者可能会将云服务账号生成的 Access Key 嵌入代码中以实现 API 快速调用，但若将包含 Aceess Key 的代码上传至公共代码托管平台 GitHub 中，可能导致企业密钥泄露的风险。建议检测公开代码库是否泄露 Aceess Key。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“安全与合规>数据安全中心 DSC”
3. 检查是否开通数据安全中心服务

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“安全与合规>数据安全中心 DSC”，进入数据安全中心总览界面
3. 在左侧导航树中选择“数据使用审计”，并选择“Access Key 泄露检测”页签，进入“Access Key 泄露检测”页面，查看并处理 Access Key 泄露事件

2.4 日志与监控

本节将介绍在华为云上配置日志与监控策略时可参考的安全建议。

2.4.1 启用 CTS

等级：Level 1

配置建议：

用户开通云审计服务（CTS）后，系统会自动创建一个追踪器，该追踪器会自动识别并关联当前租户所使用的所有云服务，并将当前租户的所有操作记录在该追踪器中。CTS 服务具备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常见应用场景。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“管理与部署>云审计服务 CTS”
3. 在左侧导航栏窗格中，进入“事件列表”，检查是否存在事件数据
4. 在左侧导航栏窗格中，进入“追踪器”，检查管理事件追踪器“system”的状态是否为正常

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“管理与部署>云审计服务 CTS”，进入云审计服务授权页面
3. 单击“同意授权并开通”，进入云审计服务页面。CTS 最多显示近 7 天的事件，为了长期保存操作记录，可以将事件文件保存至 OBS 中

2.4.2 启用 CTS 的关键操作通知功能

等级：Level 1

配置建议：

启用 CTS 的关键操作通知功能后，CTS 会对这些关键操作（例如：高危操作、越权操作）通过消息通知服务（SMN）实时向相关订阅者发送通知，该功能由 CTS 触发，SMN 完成通知发送。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“管理与部署>云审计服务 CTS”，进入云审计服务页面
3. 在左侧导航栏窗格中，进入“关键操作通知”，检查“通知名称”中是否存在已创建好的通知且状态“正常”

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“管理与部署>云审计服务 CTS”，进入云审计服务页面
3. 在左侧导航栏中选择“关键操作通知”，页面跳转到关键操作通知页面
4. 单击页面右上角的“创建关键操作通知”，页面跳转到创建关键操作通知参数填写页面
5. 填写“基本信息”参数
6. 配置关键操作和用户
7. 配置 SMN 主题

详情可参见配置关键操作通知

2.4.3 启用 LTS 日志转储

等级：Level 1

配置建议：

主机和云服务的日志数据上报至云日志服务（LTS）后，在默认存储事件过期后会被自动删除。因此，对于需要长期存储的日志数据，应在 LTS 中配置日志转储。LTS 支持将日志转储至以下云服务：

- OBS：提供日志存储功能，长期保存日志
- 数据接入服务（DIS）：提供日志长期存储能力和丰富的大数据分析能力

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“管理与部署>云日志服务 LTS”
3. 在左侧导航栏中单击选择“日志转储”
4. 在右侧列表的转储对象中，依次检查 OBS 桶、DIS 通道，查看“转储状态”是否正常

配置步骤：

1. 在云日志服务管理控制台，左侧导航栏中，单击“日志转储”
2. 在“日志转储”页面右上角，单击“配置转储”
3. 在“配置转储”页面，设置转储日志相关参数
4. 单击“确定”，完成配置。当转储任务状态为“正常”时，表示转储任务创建成功

详情可参见 LTS 日志转储配置指导

2.4.4 启用 VPC 流量日志功能

等级：Level 2

配置建议：

VPC 流日志功能可以记录虚拟私有云中的流量信息，帮助用户优化安全组和防火墙控制规则、监控网络流量、进行网络攻击分析等。当用户想要了解虚拟私有云网卡的流量详情时，用户可以通过 LTS 实时查看虚拟私有云的网卡日志数据。

检查步骤：

1. 登录管理控制台
2. 选择“服务列表>网络>虚拟私有云 VPC”
3. 在左侧导航栏，选择“VPC 流日志”，检查是否有信息

配置步骤：

1. 登录管理控制台
2. 选择“服务列表>网络>虚拟私有云 VPC”

3. 在左侧导航栏，选择“VPC 流日志”
4. 在页面右上角，单击“创建 VPC 流日志”，按照提示配置参数

2.4.5 启用 RDS 数据库审计功能

等级：Level 1

配置建议：

当用户开通 SQL 审计功能，系统会将所有的 SQL 操作记录下来存入日志文件，方便用户下载并查询。SQL 审计功能默认关闭，启用该功能可能会有一定的性能影响。

检查步骤：

1. 登录管理控制台
2. 选择“数据库>云数据库 RDS”，进入云数据库 RDS 信息页面
3. 在“实例管理”页面，选择目标实例，单击实例名称，进入实例的“基本信息”页签
4. 在左侧导航栏单击“SQL 审计”，单击“设置 SQL 审计”，检查是否开启“审计日志开关”

配置步骤：

1. 登录管理控制台
2. 选择“数据库>云数据库 RDS”，进入云数据库 RDS 信息页面
3. 在“实例管理”页面，选择目标实例，单击实例名称，进入实例的“基本信息”页签
4. 在左侧导航栏单击“SQL 审计”，单击“设置 SQL 审计”，在弹出框中设置 SQL 审计日志保留策略，单击“确定”，保存设置策略。保留天数默认为 7 天，可设置范围为 1~732 天

2.4.6 启用主机全量日志功能

等级：Level 1

配置建议：

当用户选择了主机接入方式时，LTS 可以将主机待采集日志的路径配置到日志流中，ICAgent 将按照日志采集规则采集日志，并将多条日志进行打包，以日志流为单位发往 LTS，用户可以在 LTS 控制台实时查看日志。

检查步骤：

1. 登录管理控制台
2. 选择“服务列表>云日志服务 LTS”，单击左侧导航栏“日志管理”

3. 在左侧导航栏单击“日志接入-主机接入”，检查是否配置主机接入信息、所属日志组、所属日志流

配置步骤：

1. 登录管理控制台
2. 选择“服务列表>云日志服务 LTS”，单击左侧导航栏“日志管理”
3. 单击 “创建日志组”，在弹出框内，输入日志组名称，单击“确定”，创建完成
4. 选择已创建的日志组名称，进入该日志组页面。单击“创建日志流”，在弹出框内，输入日志流名称，单击“确定”，创建完成
5. 安装 ICAgent
6. 在云日志服务管理控制台，单击“日志管理”，在日志组列表中，单击已创建的日志组名称
7. 在日志流列表中，单击已创建的日志流名称
8. 在左侧导航栏单击“日志接入-主机接入”，单击“新增路径”，配置日志采集路径，根据提示，完成相关参数配置

详情可参见云主机日志配置指导

2.4.7 启用 ELB 访问日志记录功能

等级：Level 1

配置建议：

ELB 在外部流量分发时，会记录 HTTP(S)详细的访问日志记录，如 URI 请求、客户端 IP 和端口、状态码。ELB 日志可用于审计，也可用于通过时间和日志中的关键词信息搜索日志，同时也可以通过各种 SQL 聚合函数来分析某段时间内的外部请求统计数据，以掌握真实用户的网站使用频率等。

检查步骤：

1. 登录管理控制台
2. 选择“服务列表>网络>弹性负载均衡 ELB”，在“负载均衡器”界面，单击需要检查的负载均衡器名称
3. 在该负载均衡器界面的“访问日志”页签，检查“启动日志记录”的开关是否开启，日志组、日志流是否已配置

配置步骤：

1. 登录管理控制台

2. 选择“服务列表>云日志服务 LTS”，单击左侧导航栏“日志管理”
3. 单击 “创建日志组”，在弹出框内，输入日志组名称，单击“确定”，创建完成
4. 选择已创建的日志组名称，进入该日志组页面。单击“创建日志流”，在弹出框内，输入日志流名称，单击“确定”，创建完成
5. 选择“服务列表>网络>弹性负载均衡 ELB”，在“负载均衡器”界面，单击需要配置访问日志的负载均衡器名称
6. 在该负载均衡器界面的“访问日志”页签，单击“配置访问日志”，开启日志记录，选择在 LTS 中创建的日志组和日志流

2.4.8 启用 WAF 全量日志功能

等级：Level 1

配置建议：

启用 WAF 全量日志功能后，可以将攻击日志、访问日志记录到 LTS 中。通过 LTS 记录的 WAF 日志数据，快速高效地进行实时决策分析、设备运维管理以及业务趋势分析。开启全量日志功能是将 WAF 日志记录到 LTS，不影响 WAF 性能。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>Web 应用防火墙 WAF”
3. 在左侧导航栏中单击选择“防护事件”
4. 在右侧列表选择“全量日志”
5. 检查“全量日志”开关是否开启，日志组、记录攻击日志的日志流、记录访问日志的日志流是否已配置

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>Web 应用防火墙 WAF”
3. 在左侧导航栏中单击选择“防护事件”
4. 在右侧列表选择“全量日志”，开启全量日志，并选择日志组和日志流

详情可参见启用 WAF 全量日志操作指导

2.4.9 启用 WAF 防护事件告警通知

等级：Level 1

配置建议：

通过对攻击日志进行通知设置，WAF 可将仅记录和拦截的攻击日志通过用户设置的接收通知方式（例如邮件或短信）发送给用户。

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>Web 应用防火墙 WAF”
3. 在左侧导航栏中单击选择“防护事件”
4. 在右侧列表选择“通知”，检查“通知状态”开关是否开启

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>Web 应用防火墙 WAF”
3. 在左侧导航栏中单击选择“防护事件”
4. 在右侧列表选择“通知”，配置告警通知参数

详情可参见配置 WAF 告警通知指南

2.4.10 配置 RDS 数据库性能监控与告警功能

等级：Level 1

配置建议：

设置告警规则：用户可自定义监控目标与通知策略，及时了解 RDS 服务运行状况，从而起到预警作用。

设置秒级监控：用于提高监控指标的瞬时精确值，RDS for MySQL 支持秒级监控，包括 1 秒监控和 5 秒监控。

检查步骤：

1. 登录管理控制台
2. 在服务列表中选择”管理与监管 > 云监控服务 CES”，进入”云监控”服务信息页面
3. 在左侧导航栏选择”告警 > 告警规则”，进入”告警规则”页面
4. 检查是否开启告警策略

配置步骤：

1. 登录管理控制台
2. 在服务列表中选择”管理与监管 > 云监控服务 CES”，进入”云监控”服务信息页面
3. 在左侧导航栏选择”云服务监控 > 关系型数据库”中选择监控对象
4. 选择需要添加告警规则的实例，单击操作列的”创建告警规则”。
5. 在“创建告警规则”页面，根据提示，启动和配置监控与告警规则

2.4.11 启用 DBSS 数据库安全审计功能

等级：Level 2

配置建议：

数据库应开通数据库审计功能，数据库安全服务（DBSS）的数据库安全审计提供旁路模式审计功能，通过实时记录用户访问数据库行为，形成细粒度的审计报告，对风险行为和攻击行为进行实时告警，对数据库的内部违规和不正当操作进行定位追责。

检查步骤：

1. 登录管理控制台
2. 选择“安全>数据库安全服务 DBSS”
3. 进入“数据库安全审计”，点击“实例列表”，检查数据库安全审计实例状态是否为“运行中”
4. 添加数据库：进入添加数据库入口，在弹出的对话框中，设置数据库的信息，添加成功后数据库列表中将新增一条“审计状态”为“已关闭”的数据库
5. 进入“数据库列表”，检查相应数据库安全审计实例下的数据库审计状态是否为“已开启”，Agent 运行状态是否为“正在运行”

配置步骤：

1. 登录管理控制台
2. 选择“安全>数据库安全服务 DBSS”
3. 添加数据库：进入添加数据库入口，在弹出的对话框中，设置数据库的信息，添加成功后数据库列表中将新增一条“审计状态”为“已关闭”的数据库
4. 添加 Agent： 登录数据库安全服务管理控制台，进入添加 Agent 入口，在弹出的“添加 Agent”对话框中，根据数据库类型以及数据库部署场景，为待审计的数据库添加 Agent
5. 添加安全组规则：Agent 添加完成后，需要为数据库安全审计实例所在的安全组添加入方向规则，使 Agent 与审计实例之间的网络连通

6. 下载并安装 Agent：安全组规则添加完成后，用户需要下载 Agent，并根据 Agent 的添加方式在数据库端或应用端安装 Agent
7. 开启数据库安全审计：进入“数据库列表”界面，在选择实例下拉框中，选择需要开启审计的数据库安全审计实例

详情可参见数据库安全服务配置指导

2.4.12 启用 DBSS 数据库安全审计告警通知功能

等级：Level 1

配置建议：

通过设置告警通知，当数据库发生设置的告警事件时，用户可以收到 DBSS 发送的告警通知，及时了解数据库的安全风险。否则，无论是否有危险，用户都只能登录管理控制台自行查看，无法收到告警信息。

检查步骤：

1. 登录管理控制台
2. 选择“安全>数据库安全服务 DBSS”
3. 在左侧导航栏中单击选择“数据库安全审计>设置”
4. 在右侧页面，选择具体的数据库安全审计实例，进入“告警通知”页面
5. 检查“全局设置”中的消息通知开关是否开启

配置步骤：

1. 登录管理控制台
2. 选择“安全>数据库安全服务 DBSS”
3. 在左侧导航栏中单击选择“数据库安全审计>设置”
4. 在右侧页面，选择具体的数据库安全审计实例，进入“告警通知”页面，设置告警通知

详情可参见数据库安全服务告警通知配置指导

2.4.13 启用 OBS 桶日志功能

等级：Level 1

配置建议：

出于分析或审计等目的，用户可以开启 OBS 桶日志记录功能。通过访问日志记录，桶的拥有者可以深入分析访问该桶的用户请求性质、类型或趋势。当用户开启一个桶的日志记录功能后，OBS 会自动对这个桶的访问请求记录日志，并生成日志文件写入用户指定的桶中。

检查步骤：

1. 登录管理控制台
2. 选择“存储>对象存储服务 OBS”
3. 在左侧导航栏窗格中，选择“对象存储”
4. 进入具体的桶中，在“概览”中的基础配置中，检查“日志记录”是否为“已配置”状态

配置步骤：

1. 登录管理控制台
2. 选择“存储>对象存储服务 OBS”
3. 在左侧导航栏窗格中，选择“对象存储”
4. 在桶列表单击待操作的桶，进入“概览”页面
5. 在“基础配置”下，单击“日志记录”卡片，系统弹出“日志记录”对话框
6. 选择“启用”， 根据提示配置参数

2.4.14 启用 SA 并配置威胁告警通知

等级：Level 1

配置建议：

态势感知（SA）利用大数据分析技术，可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为用户呈现出全局安全攻击态势。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>态势感知 SA”
3. 检查是否配置开启态势感知
4. 在左侧导航树中，选择“设置>通知设置>告警设置”，检查是否配置通知告警

配置步骤：

1. 登录管理控制台

2. 在服务列表选择“安全>态势感知 SA”，进入态势感知管理控制台。单击“去开通”，选择配置“最大配额数”、“网站配额”、“态势大屏”和“购买时长”，购买专业版态势感知
3. 配置告警项：在左侧导航树中，选择“设置>通知设置>告警设置>通知告警”，进入威胁告警通知配置页面
4. 配置消息通知主题：选择“应用服务>消息通知服务 SMN”，进入消息通知服务页面，在左侧导航栏，选择“主题管理>主题”，进入页面后创建主题，主题创建成功后，选择短信、邮件等终端方式订阅主题

2.4.15 启用 ELB 健康状态检查

等级：Level 1

配置建议：

启用 ELB 的健康检查功能后，ELB 可对后端服务器发送健康状态请求，通过健康检查来判断后端服务器是否可用，从而决定业务流量的分发。

检查步骤：

1. 登录管理控制台
2. 选择“服务列表>网络>弹性负载均衡 ELB”
3. 在“负载均衡器”界面，检查右侧页面的左上方是否有提示异常状态的后端服务器数量
4. 进入具体的负载均衡器，选择“监听器”，再选择“后端服务器组”，检查健康检查是否处于“已开启”
5. 检查下方的后端服务器中的“健康检查结果”是否为“正常”

配置步骤：

1. 登录管理控制台
2. 选择“服务列表>网络>弹性负载均衡 ELB”
3. 在“负载均衡器”界面，单击需要开启健康检查的负载均衡名称
4. 在“后端服务器组”页签下，选择需要开启健康检查的后端服务器组名称
5. 在基本信息页面，单击“健康检查”右侧的“配置”。 在“配置健康检查”界面，可根据需要开启健康检查

详情可参考 ELB 健康检查配置指导

2.4.16 启用 CES 的主机监控功能

等级：Level 1

配置建议：

启用云监控服务（CES）的主机监控功能，可实现对 ECS /裸金属服务器（BMS）的基础监控、操作系统监控、进程监控。全面了解云上资源的使用情况，业务的运行情况，并及时收到异常告警做出反应，保证业务顺畅运行。

检查步骤：

1. 登录管理控制台
2. 单击“管理与部署>云监控服务 CES”
3. 在左侧导航栏窗格中，进入“总览”中的“主机监控”，选择“弹性云服务器”
4. 检查右侧页面中各弹性云服务器中的插件状态是否为“运行中”
5. 检查各主机的 CPU 使用率、内存使用率、磁盘使用率是否异常（高于 80%）

配置步骤：

1. 登录管理控制台
2. 单击“管理与部署>云监控服务 CES”
3. 单击页面左侧的“主机监控”，进入“主机监控”页面
4. 选择要安装 Agent 的 ECS 或 BMS，安装 Agent 插件
5. 1 至 5 分钟后，当插件状态为“运行中”，说明 Agent 已安装成功。单击弹性云服务器右侧操作列的“查看监控指标”可查看监控数据

详情可参见 CES 主机监控配置指导

2.4.17 启用 CES 的站点监控功能

等级：Level 1

配置建议：

用户可根据业务需要进行站点监控，用于模拟真实用户对远端服务器的访问，从而探测远端服务器的可用性、连通性等问题，建议站点监控可用性应高于 95%。

检查步骤：

1. 登录管理控制台

2. 单击“管理与部署>云监控服务 CES”
3. 在左侧导航栏窗格中，进入“总览”中的“站点”
4. 检查右侧页面中是否已配置相应的站点监控（HTTP(S)、TCP、UDP、ICMP）
5. 检查各站点监控的“可用探测点百分比”是否高于 95%

配置步骤：

1. 登录管理控制台
2. 单击“管理与部署>云监控服务 CES”
3. 在“站点监控”界面，单击右上角“创建站点监控”，进入“创建站点监控”界面
4. （首次配置时）选择站点监控存储数据所属的区域
5. 在弹出的“创建站点监控”对话框中根据界面提示配置参数，配置完成后，单击“确定”，完成创建站点监控

详情可参见 CES 站点监控配置指导

2.4.18 启用 HSS

等级：Level 1

配置建议：

主机实例（例如：ECS、BMS）应安装企业主机安全防护（HSS）且开启防护，全面识别并管理主机资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>企业主机安全 HSS”
3. 在左侧导航栏中单击选择“总览”
4. 在右侧页面中检查“主机防护统计”中未防护主机数是否为 0

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>企业主机安全 HSS”
3. 进入企业主机安全页面，在界面右上角，单击“购买主机安全”
4. 购买成功后，安装 Agent，并开启主机防护

详情可参见启用主机安全防护指导

2.4.19 启动 HSS 网页防篡改功能

等级：Level 1

配置建议：

应开启 HSS 中的网络防篡改防护，以保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>企业主机安全 HSS”
3. 在左侧导航栏中单击选择“网页防篡改>防护列表”
4. 在右侧页面中检查“防护主机数”是否不为 0，且“防护目录”数是否不为 0
5. 在具体的主机中，点击“防护设置”，检查“防护目录设置”中是否不为空

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“安全>企业主机安全 HSS”
3. 在左侧导航栏中单击选择“网页防篡改>防护列表”
4. 单击“防护设置”，进入“防护设置”页面，根据提示，添加防护目录

详情可参见 HSS 网页防篡改配置指导

2.4.20 启用 VSS

等级：Level 1

配置建议：

漏洞扫描服务（VSS）启用后，可以帮助快速检测出网站存在的漏洞，并提供详细的漏洞分析报告，并针对不同类型的漏洞提供专业可靠的修复建议。

检查步骤：

1. 登录管理控制台
2. 选择“安全> 漏洞扫描服务 VSS”，检查是否配置开通 VSS
3. 在左侧导航栏选择“资产列表”
4. 检查是否有配置域名，且认证状态为“已认证”

配置步骤：

1. 登录管理控制台
2. 选择“安全> 漏洞扫描服务 VSS”，进入漏洞扫描服务管理界面，进行服务选型配置
3. 参数设置完毕后，根据提示购买“漏洞扫描服务
4. 开通漏洞扫描服务后，将网站资产以 IP 或域名的形式添加到漏洞扫描服务中并完成域名认证，方可进行漏洞扫描

详情可参见网站漏洞扫描配置指导

2.5 响应与恢复

本节将介绍在华为云上配置告警与监控响应以及数据备份策略时可参考的安全建议。

2.5.1 数据库安全审计日志备份

等级：Level 1

配置建议：

数据库审计日志应开启自动备份功能，将数据库的审计日志备份到 OBS 桶，实现高可用，以便根据需要备份或恢复数据库审计日志。

检查步骤：

1. 登录管理控制台
2. 选择“安全>数据库安全服务 DBSS”，在左侧导航栏中单击选择“数据库安全审计>设置”
3. 在右侧页面，选择具体的数据库安全审计实例，进入“备份与恢复”页面
4. 检查下方是否显示“自动备份运行中”
5. 点击“设置自动备份”，检查自动备份开关是否为“开启”，备份周期是否为“每天”
6. 检查下方的备份任务状态，是否均为“自动备份完成”

配置步骤：

1. 登录管理控制台
2. 选择“安全>数据库安全服务 DBSS”，在左侧导航栏中单击选择“数据库安全审计>设置”
3. 在右侧页面，选择具体的数据库安全审计实例，进入“备份与恢复”页面
4. 单击“设置自动备份”，在弹出的对话框中，设置自动备份参数

详情可参见数据库审计日志备份与恢复指导

2.5.2 启用实例的 CSBS 功能

等级：Level 1

配置建议：

启用云服务器备份功能，以提供对 ECS 和 BMS 的备份保护服务。云服务器备份服务（CSBS）支持基于多云硬盘一致性快照技术的备份服务，并支持利用备份数据恢复服务器数据，最大限度保障用户数据的安全性和正确性，确保业务安全。

检查步骤：

1. 登录管理控制台
2. 选择“备份>云服务器备份服务 CSBS”
3. 在左侧导航栏中单击选择“云服务器备份”
4. 在右侧列表单击具体存储库，检查“状态”是否为“可用”，检查“备份策略状态”是否为“启用”，“已绑定服务器”非 0

配置步骤：

1. 登录管理控制台
2. 选择“备份>云服务器备份服务 CSBS”
3. 在左侧导航栏中单击选择“云服务器备份”
4. 在界面右上角单击“创建云服务器备份”
5. 在服务器列表中勾选需要备份的服务器或磁盘，在下方的“备份配置”区域为已选择的服务器配置备份方式

详情可参见创建云服务器备份指导

2.5.3 启用 EVS 备份功能

等级：Level 1

配置建议：

对于部分存放重要数据的数据盘可通过云备份服务（CBR）实现 EVS 备份。

检查步骤：

1. 登录管理控制台
2. 在服务列表选择“存储>云备份 CBR”

3. 在左侧导航栏中单击选择“云硬盘备份”
4. 在右侧列表单击具体存储库，检查“状态”是否为“可用”，检查“备份策略状态”是否为“启用”，“已绑定磁盘”非 0

配置步骤：

1. 登录管理控制台
2. 在服务列表选择“存储>云备份 CBR”
3. 在左侧导航栏中单击选择“云硬盘备份”
4. 在界面右上角单击“购买云硬盘备份存储库”
5. 选择计费模式，然后在磁盘列表中勾选需要备份的磁盘
6. 输入存储库容量

详情可参见云硬盘备份配置指导

2.5.4 启用 RDS/GaussDB 数据库实例备份功能

等级：Level 1

配置建议：

RDS 支持数据库实例的备份和恢复，以保证当数据库或表被恶意或误删除后能够恢复。启用 RDS 的自动备份功能后，系统会在数据库实例的备份时段中创建数据库实例的自动备份，并根据指定的备份保留期保存数据库实例的自动备份。如果需要，用户可以将数据恢复到备份保留期中的任意时间点。

检查步骤：

1. 登录管理控制台
2. 选择“数据库>云数据库 RDS”，进入 RDS 信息页面
3. 在“实例管理”页面，选择指定的实例，单击实例名称
4. 在左侧导航栏，单击“备份恢复”，检查是否存在备份策略

配置步骤：

1. 登录管理控制台
2. 选择“数据库>云数据库 RDS”，进入 RDS 信息页面
3. 在“实例管理”页面，选择指定的实例，单击实例名称
4. 在左侧导航栏，单击“备份恢复”，单击“修改备份策略”，用户可以查看已设置的备份策略，或修改已有策略

详情可参见 RDS 备份策略配置指导 、GuassDB 备份策略配置指导

2.5.5 启用 OBS 桶跨区备份功能

等级：Level 2

配置建议：

跨区域复制能够通过创建跨区域复制规则，将一个桶（源桶）中的数据自动、异步地复制到不同区域的另外一个桶（目标桶）中（源桶和目标桶必须属于同一个帐号）。跨区域复制能够为用户提供跨区域数据容灾的能力，满足用户数据复制到异地进行备份的需求。

检查步骤：

1. 登录管理控制台
2. 选择“存储>对象存储服务 OBS”
3. 在左侧导航栏选择“对象存储”
4. 进入具体的桶中，在“跨区域复制”中，检查是否存在跨区域复制规则，且状态为“已启用”

配置步骤：

1. 登录管理控制台
2. 选择“存储>对象存储服务 OBS”
3. 在左侧导航栏选择“对象存储”
4. 在桶列表单击待操作的桶，进入“概览”页面
5. 在左侧导航栏，单击“跨区域复制”
6. 单击“创建规则”，系统将弹出“创建跨区域复制规则”对话框，根据业务规划配置跨区域复制规则

3. 结语

本文为客户检查并实施华为云云服务安全基线配置提供了指导，帮助客户提高云环境的安全防御能力。

本文仅供客户作为参考，不具备任何法律效力或构成法律建议，也不作为保证任何客户在云上环境一定安全的依据。客户应酌情评估自身使用云服务的情况，并根据实际需要在本基线配置指南的基础上进行补充或裁剪。

4. 版本历史

日期	版本	描述
2021 年 8 月 27 日	1.0	首次发布