配置审计

用户指南

文档版本	01
发布日期	2023-12-30

华为技术有限公司

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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 资源清单

1.1 查看资源

1.1.1 查看所有资源列表

操作场景

如果您需要查看当前账号下的资源，可以通过“资源清单”页面查看。

须知

资源数据同步到Config存在延迟，因此资源发生变化时不会实时更新“资源清单”中的数据。对于已开启资源记录器的用户，Config会在24小时内校正资源数据。

资源清单中的资源数据依赖于资源记录器所收集的资源数据，如果相关资源无法在资源清单页面查询到，请确认资源记录器是否开启，或该资源类型是否被资源记录器收集资源数据，如何配置资源记录器请参见**配置资源记录器**。

如您未开启资源记录器且需查看您拥有的资源信息，请前往**我的资源**页面查看。

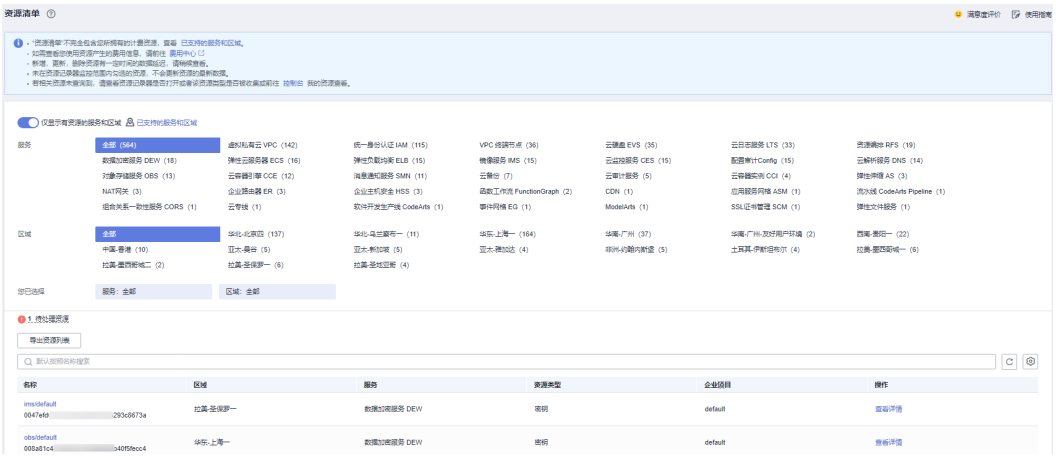
操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

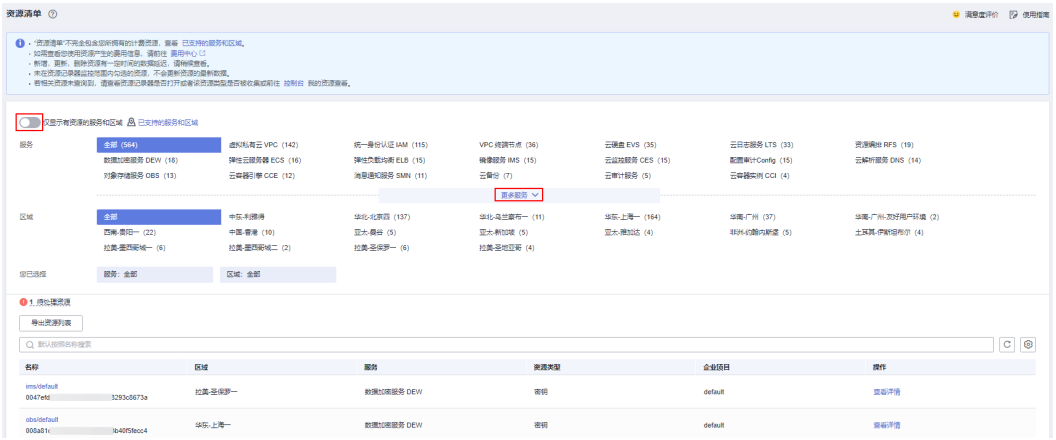
“资源清单”页面默认展示您拥有资源的服务，下方的资源列表默认展示您拥有的全部资源。

图 1-1 查看资源默认页面



步骤3 您可以通过关闭“仅显示有资源的服务和区域”开关，查看配置审计支持的所有服务。

图 1-2 查看配置审计支持的所有服务



步骤4 单击页面左上方的“已支持的服务和区域”按钮，界面将显示当前已支持的全部服务、资源类型和区域等信息。

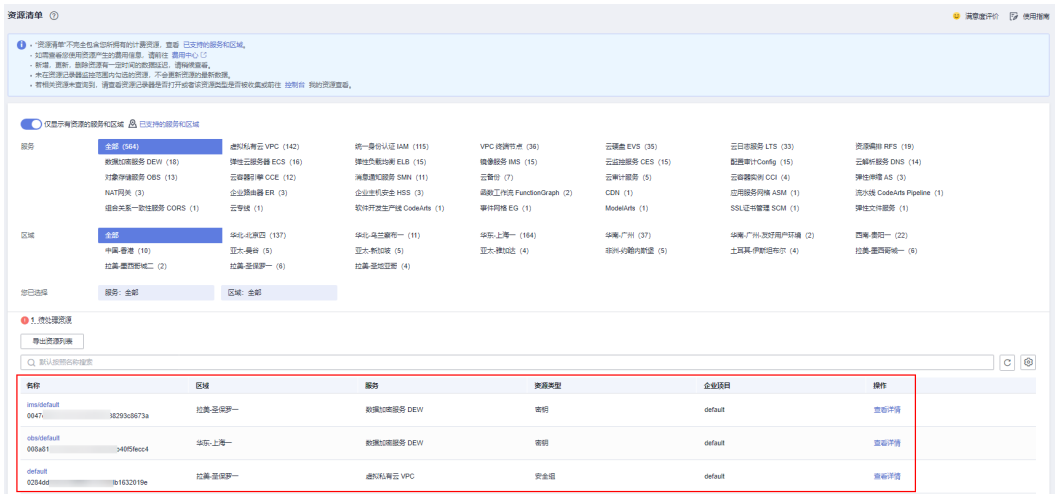
----结束

1.1.2 查看单个资源详情

操作场景

“资源清单”页面的资源列表默认展示资源的部分属性，如果您需要查看某个资源的资源详情，可按如下操作查看。

图 1-3 资源列表



操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 在“资源清单”页面的资源列表中，单击需要查看的资源名称，进入资源概览页。

可以查看资源概览、资源合规、关联资源、资源时间线。

图 1-4 查看资源概览

步骤4 单击资源概览右上角的“查看详情”，跳转到资源对应服务的控制台，查看该资源的详情。

也可以通过单击资源列表操作列的“查看详情”，查看该资源的详情。

----结束

1.1.3 筛选资源

操作场景

在“资源清单”页面，您可以通过选择服务、资源类型和区域来筛选资源，其中全局级服务无需选择区域。如需进行更精细的资源筛选，您还可以通过在页面中部的搜索框中输入搜索条件，快速定位到目标资源。

本章节为您介绍如何通过搜索框快速定位目标资源。

目前支持的筛选条件

表 1-1 支持的筛选条件

筛选条件	说明
名称	资源名称支持模糊搜索，并且忽略大小写。
资源ID	资源ID支持模糊搜索，但不忽略大小写。
标签	选择标签后，会依次弹出所有的标签键及对应的标签值列表，您再依次选择标签键及对应的标签值即可。
企业项目	通过企业项目筛选框选择企业项目，资源列表将自动筛选并展示此企业项目下的资源。

说明

根据企业项目筛选资源的功能必须要先**开通企业项目**才可以使用。

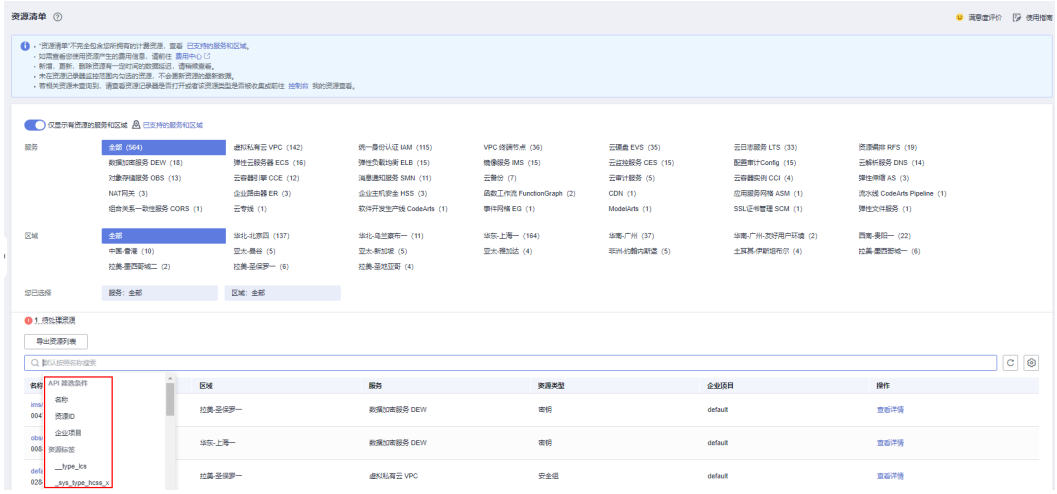
操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 在“资源清单”页面中部搜索框中，可通过名称、资源ID、标签和企业项目筛选出您需要查看的资源。

图 1-5 筛选资源



----结束

1.1.4 导出资源列表

操作场景

在“资源清单”页面筛选出需要查看的资源后，您可以导出资源列表。

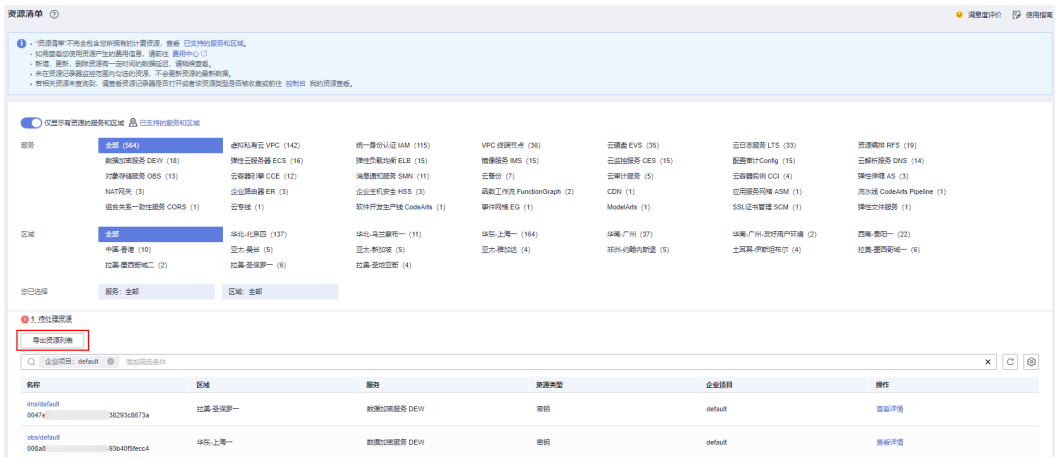
操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的☰图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 筛选出需要查看的资源后，单击列表左上方的“导出资源列表”按钮，导出列表中的资源信息。

图 1-6 导出资源列表



----结束

说明

导出的文件格式为Excel格式，文件中将包含您筛选出的全部资源的特定资源属性。

1.2 查看资源合规

操作场景

资源合规特性用于评估您的资源是否满足合规要求，当您的资源在某一合规规则的评估范围内，您可以在资源概览页查看该资源的合规性信息。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 在“资源清单”页面的资源列表中，单击需要查看的资源名称，进入资源概览页。

步骤4 选择“资源合规”页签，规则列表中展示评估当前资源的全部合规规则及其评估结果等信息。

步骤5 单击规则列表中的某一规则名称，系统跳转至该合规规则详情页。

图 1-7 查看资源合规信息

----结束

1.3 查看资源关系

操作场景

资源关系记录了您在华为云上的不同资源之间的关联情况。例如云硬盘与云服务器之间的绑定关系，云服务器与虚拟私有云之间的归属关系等。借助资源关系，您可以方便地掌握您在云平台上拥有的所有资源的组成结构和依赖关系。

我们为大部分资源都定义了与其相关的资源关系，您可以参阅**支持的资源关系**来了解目前支持的资源关系。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 在“资源清单”页面的资源列表中，单击需要查看的资源名称，进入资源概览页。

步骤4 选择“关联资源”页签，可查看关联的全部资源。

将鼠标悬停在关联资源的资源名称上方，界面将显示此资源的信息以及资源关系。

步骤5 在“关联资源”页签右上角，可以切换以列表或拓扑图的形式显示关联资源。

图 1-8 查看关联资源

----结束

说明

您可以通过单击关联资源页签中对应资源的名称，跳转至此资源的概览页查看相关信息。

1.4 查看资源历史

前提条件

只有开启并配置了资源记录器，才会记录资源的历史变更信息。关于资源记录器请参阅**资源记录器**。

操作场景

资源历史是过去某段时间内资源不同状态的集合。资源发生任何属性的变化和资源关系的变化，都会在资源时间线中生成一条记录，该记录会包含资源变更情况的详细信息，默认的保存期限为7年。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 在“资源清单”页面的资源列表中，单击需要查看的资源名称，进入资源概览页。

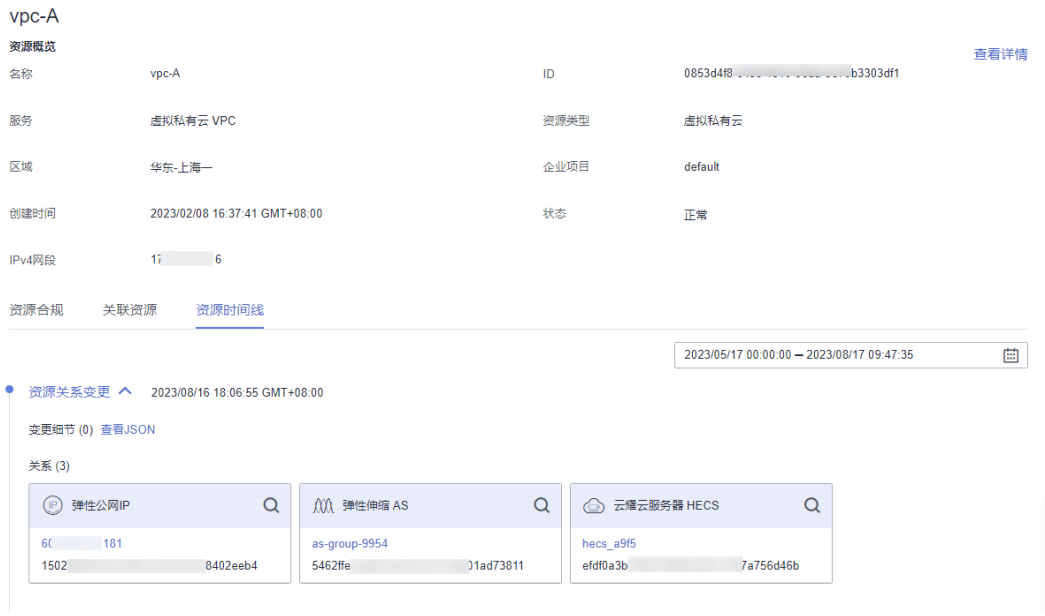
步骤4 选择“资源时间线”页签，查看资源变更的历史记录。

步骤5 在“资源时间线”页签的右上角设置筛选时间。

“资源时间线”页面默认展示过去3个月的资源变更历史记录。

您也可以通过单击“查看JSON”来查看此时资源的所有属性。

图 1-9 查看资源时间线



----结束

2 资源记录器

2.1 资源记录器概述

概述

资源记录器为您提供面向资源的配置记录监控能力，帮您轻松实现海量资源的自主监管，用来跟踪您在云平台上的资源变更情况。

资源记录器可以为您提供以下功能：

- 在资源被创建、修改或删除时发送通知给您；
- 在资源关系发生变更时发送通知；
- 对资源变更消息进行定期（6小时）存储；
- 对资源快照进行定期（24小时）存储。

资源记录器支持的资源，请参阅**支持的服务和区域**。

资源记录器支持的资源关系，请参阅**支持的资源关系**。

约束与限制

- 开启并配置资源记录器时，“**主题**”和“**资源转储**”至少需要配置一个。
- 在配置资源记录器时，配置了“主题”，但只创建了SMN主题，未添加订阅以及执行请求订阅，在资源发生变更时，将无法收到消息通知。
- 未在资源记录器监控范围内勾选的资源，不会更新资源的最新数据。
- 资源记录器收集到的资源配置信息数据默认保留7年（2557天）。

须知

Config服务的相关功能均依赖于资源记录器收集的资源数据，不开启资源记录器将会影响其他功能的正常使用，例如资源清单页面无法获取资源最新数据、合规规则无法进行准确的资源评估、资源聚合器无法聚合源账号的资源数据等，因此强烈建议您保持资源记录器的开启状态。

2.2 配置资源记录器

操作场景

您必须先开启资源记录器，然后才可以配置并使用资源记录器来跟踪云平台上的资源变更情况。

资源记录器配置完毕后，您可以随时修改资源记录器的配置或关闭资源记录器。

本章节包含如下内容：

- **开启并配置资源记录器**
- **修改资源记录器**
- **关闭资源记录器**
- **跨账号授权**
- **资源变更消息和资源快照转储至OBS加密桶**

开启并配置资源记录器

开启并配置资源记录器后，当您的资源变更（被创建、修改、删除）、资源关系变更时，您均可收到通知，同时还可对您的资源变更消息和资源快照进行定期存储。

步骤1 登录管理控制台。

步骤2 单击页面左上角的  图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源记录器”，进入“资源记录器”页面。

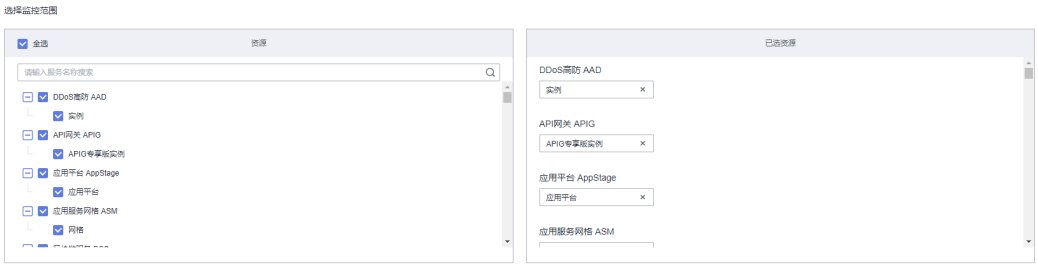
步骤4 打开资源记录器开关，在弹出的确认框中单击“是”，资源记录器开启成功。

图 2-1 开启资源记录器

步骤5 选择资源的监控范围。

默认情况下，资源记录器的监控范围会覆盖当前所有支持的资源。您可以修改资源记录器的监控范围，选择指定的资源类型进行监控。

图 2-2 选择监控范围



步骤6 配置资源转储。

选择OBS桶，用于存储资源变更消息及资源快照。

- **配置当前账号下OBS桶：**

  选择您账号下的OBS桶，用于存储资源变更消息及资源快照，如果用于转储的OBS桶指定了前缀，则还需添加桶前缀。如您的账号下无OBS桶，则需先创建OBS桶，详见**《对象存储服务用户指南》**。

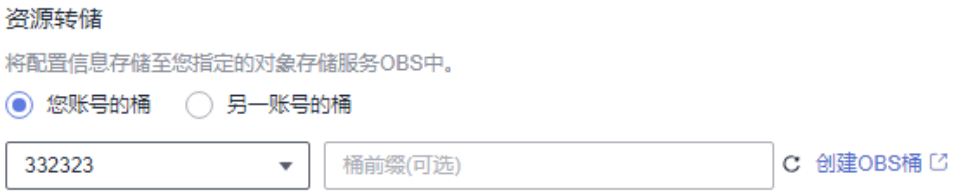
- **配置其他账号下OBS桶：**

  选择“另一账号的桶”，并输入区域ID和桶名称，如果用于转储的OBS桶指定了前缀，则还需添加桶前缀。需先使用其他账号对当前账号授予相关OBS桶的权限，具体操作请参见**跨账号授权**。

说明

开启资源记录器时，如果指定了当前账号或其他账号下的OBS桶，Config会向目标OBS桶中写入一个名为ConfigWritabilityCheckFile的空文件，此文件用来验证资源转储是否能够成功写入OBS桶。

图 2-3 配置资源转储



步骤7 配置数据保留周期。

资源记录器收集到的资源配置信息数据默认保留7年（2557天），您可以将配置信息数据设置自定义保留周期，自定义数据保留周期的可设置范围为最短30天，最长7年（2557天）。

说明

虽然Config使用SMN和OBS发送资源变更消息通知和存储资源变更消息及资源快照，但Config自身也会保存资源的历史变更信息。此处配置的数据保留时间仅针对于Config，不会对SMN和OBS存储的数据产生影响。

当您配置数据保留周期后，Config会在指定周期内保留您的资源历史数据，超出指定周期的数据将会被删除。

图 2-4 配置数据保留周期

步骤8 开启并配置消息通知（SMN）主题。

打开主题开关，选择主题所在区域和主题名，用于接收资源变更时产生的消息通知。

- **配置当前账号下消息通知主题：**

  选择“您自己的主题”，并选择主题所在区域和主题名，用于接收资源变更时产生的消息通知。如无SMN主题，则需先创建SMN主题，详见**《消息通知服务用户指南》**。

- **配置其他账号下消息通知主题：**

  选择“另一账号的主题”，并输入主题URN。需先使用其他账号对当前账号授予相关SMN主题的权限，具体操作请参见**跨账号授权**。

说明

创建SMN主题后，还需执行“添加订阅”和“请求订阅”操作，消息通知才会生效。详见**《消息通知服务用户指南》**。

图 2-5 配置 SMN 主题

步骤9 进行授权，选择“快速授权”或“自定义授权”。

- **快速授权：**将为您快速创建一个名为“rms_tracker_agency”的委托权限，该权限是可以让资源记录器正常工作的权限，包含调用消息通知服务（SMN）发送通知的权限和对象存储服务（OBS）的写入权限（例如SMN Administrator和OBS OperateAccess权限）。由于快速授权的委托中并不包含KMS的相关权限，因此资源记录器无法将资源变更消息和资源快照存储到“使用KMS方式加密的OBS桶”中。如有需要，您可以在委托中添加对应权限（KMS Administrator）或使用自定义授权，具体请参见**资源变更消息和资源快照转储至OBS加密桶**。
- **自定义授权：**您可自行在统一身份认证服务（IAM）中创建委托权限，并进行自定义授权，授权对象为云服务RMS，但必须包含可以让资源记录器正常工作的权限（调用消息通知服务（SMN）发送通知的权限和对象存储服务（OBS）的写入权限）。如果需要将资源变更消息和资源快照存储到“使用KMS方式加密的OBS桶”中，还需要添加KMS的密钥管理员权限（KMS Administrator），具体请参见**资源变更消息和资源快照转储至OBS加密桶**。创建委托详见**《统一身份认证服务用户指南》**。

  说明

  此处的授权为**委托授权**，授权消息通知服务（SMN）的发送通知权限和对象存储服务（OBS）的写入权限给Config服务，允许资源记录器将消息通知发送到您的SMN主题和将资源变更消息以及资源快照存储到您的OBS桶。

图 2-6 授权

步骤10 配置完成后，单击“保存”。

步骤11 在弹出的确认框中单击“是”，资源记录器配置成功。

----结束

修改资源记录器

资源记录器开启并配置完成后，您可以随时修改资源记录器的配置。

步骤1 进入“资源记录器”页面。

步骤2 单击页面上方的“修改资源记录器”。

图 2-7 修改资源记录器

步骤3 修改资源记录器的相关配置。

步骤4 修改完成后，单击页面下方的“保存”。

步骤5 在弹出的确认框中单击“是”，资源记录器的配置修改成功。

----结束

关闭资源记录器

如您不再需要使用资源记录器记录资源变更情况，您可以随时关闭它。

步骤1 进入“资源记录器”页面。

步骤2 关闭资源记录器开关。

步骤3 在弹出的确认框中单击“确定”，资源记录器的关闭成功。

图 2-8 关闭资源记录器

----结束

跨账号授权

- **跨账号授予SMN主题发送通知的权限**
  a. 用授权账号登录管理控制台，进入对应区域的SMN服务控制台。
  b. 参考**设置主题策略**对待授权账号授予相关SMN主题的权限。
- **跨账号授予OBS桶存储文件的权限**
  a. 用授权账号登录管理控制台，进入OBS管理控制台。
  b. 参考**自定义创建桶策略（JSON视图）**对待授权账号授予相关OBS桶的权限。将如下策略添加到桶策略中：

```
{
  "Statement": [
```

```
    {
        "Sid": "org-bucket-policy",
        "Effect": "Allow",
        "Principal": {
            "ID": [
                "domain/account ID:agency/rms_tracker_agency"  //account ID为需要被授权账号的domain_id；rms_tracker_agency为被授权的委托名称
            ]
        },
        "Action": [
            "PutObject"
        ],
        "Resource": [
            "targetBucketName/RMSLogs/*/Snapshot/*",
            "targetBucketName/RMSLogs/*/Notification/*"
        ]
    }
  ]
}
```

说明

桶策略的授权对象是创建资源记录器时使用的委托，授权资源为资源记录器转储的文件路径（如果在配置资源记录器时为转储的OBS桶指定了前缀，则资源记录器转储的文件路径也需添加相应前缀），授权操作为写入文件到OBS桶所需的PutObject操作。

资源变更消息和资源快照转储至 OBS 加密桶

- **使用SSE-OBS方式加密的OBS桶**

  如果您需要将资源变更消息和资源快照存储至使用SSE-OBS方式加密的OBS桶，无需其他操作，只需选择对应OBS桶进行存储即可。

- **使用SSE-KMS默认密钥方式加密的OBS桶**

  如果您需要将资源变更消息和资源快照存储至使用SSE-KMS默认密钥方式加密的OBS桶，则需要在对资源记录器的委托中新增KMS的管理员权限（KMS Administrator）。

- **使用SSE-KMS自定义密钥方式加密的OBS桶**

  如果您需要将资源变更消息和资源快照存储使用SSE-KMS自定义密钥方式加密的OBS桶，则需要在对资源记录器的委托中新增KMS的管理员权限（KMS Administrator）。

  另外，如果您选择将资源变更消息和资源快照存储至其他账号的使用SSE-KMS自定义密钥方式加密的OBS桶，则除了需要在对资源记录器的委托中新增KMS的管理员权限（KMS Administrator），还需要在被存储的OBS桶的密钥中设置密钥的跨账号权限。具体可参考以下步骤：

  a. 用授权账号登录管理控制台，进入数据加密服务的“密钥管理”界面。
  b. 单击目标自定义密钥的别名，进入密钥详细信息的授权页面。
  c. 参考**创建授权**对待授权账号授予其使用相关自定义密钥的权限。
     - “被授权对象”选择“账号”，并输入待授权账号的账号ID。
     - “授权操作”勾选“创建数据密钥”。

2.3 消息通知

您在开启资源记录器并成功配置消息通知（SMN）主题（创建主题 -> 添加订阅 -> 请求订阅）后，当发生资源变更时，消息通知会推送消息到您所配置的SMN主题。

关于SMN的相关操作，具体请参见**《消息通知服务用户指南》**。

目前，消息通知服务支持Config以下几种类型的消息通知：

- 资源变更（创建/修改/删除）的消息通知；
- 资源关系变更的消息通知；
- 资源变更消息存储完成的消息通知；
- 资源快照存储完成的消息通知。

如果您想了解关于资源变更消息通知的后台代码示例，请参见**消息通知模型**。

2.4 资源存储

您在开启资源记录器，并成功配置OBS桶后，资源记录器会定期（24小时）将资源快照文件存储到您配置的OBS桶中。

如果您想了解关于资源存储的后台代码示例，请参见**资源存储模型**。

2.5 资源变更消息存储

您在开启资源记录器，并成功配置消息通知（SMN）主题（创建主题 -> 添加订阅 -> 请求订阅）和对象存储桶（OBS）后，Config会定期（6小时）将您的资源变更消息存储到您配置的OBS桶中。

如果您想了解关于资源变更消息存储的后台代码示例，请参见**资源变更消息存储模型**。

3 资源合规

3.1 资源合规规则

3.1.1 添加预定义合规规则

操作场景

资源合规特性帮助您快速创建一组合规规则，用于评估您的资源是否满足合规要求。您可以选择Config提供的系统内置预设策略或自定义策略，并指定需要评估的资源范围来创建一个合规规则；合规规则创建后，有多种机制**触发规则评估**，然后查看合规规则的评估结果来了解资源的合规情况。

本章节指导您如何使用系统内置的预设策略来快速添加资源合规规则。

约束与限制

每个账号最多可以添加500个合规规则。

须知

仅被资源记录器收集的资源可参与资源评估，为保证资源合规规则的评估结果符合预期，强烈建议您保持资源记录器的开启状态，不同场景的说明如下：

- 如您从未开启过资源记录器，则资源合规规则无法评估任何资源数据。
- 如您已开启资源记录器，但仅在资源记录器监控范围内勾选部分资源，则资源合规规则仅会评估所选择的资源数据。
- 如您开启资源记录器并勾选全部资源，但后续又关闭资源记录器，则资源合规规则仅会评估资源记录器由开启到关闭期间收集到的资源数据。

关于如何开启并配置资源记录器请参见：**配置资源记录器**。

操作步骤

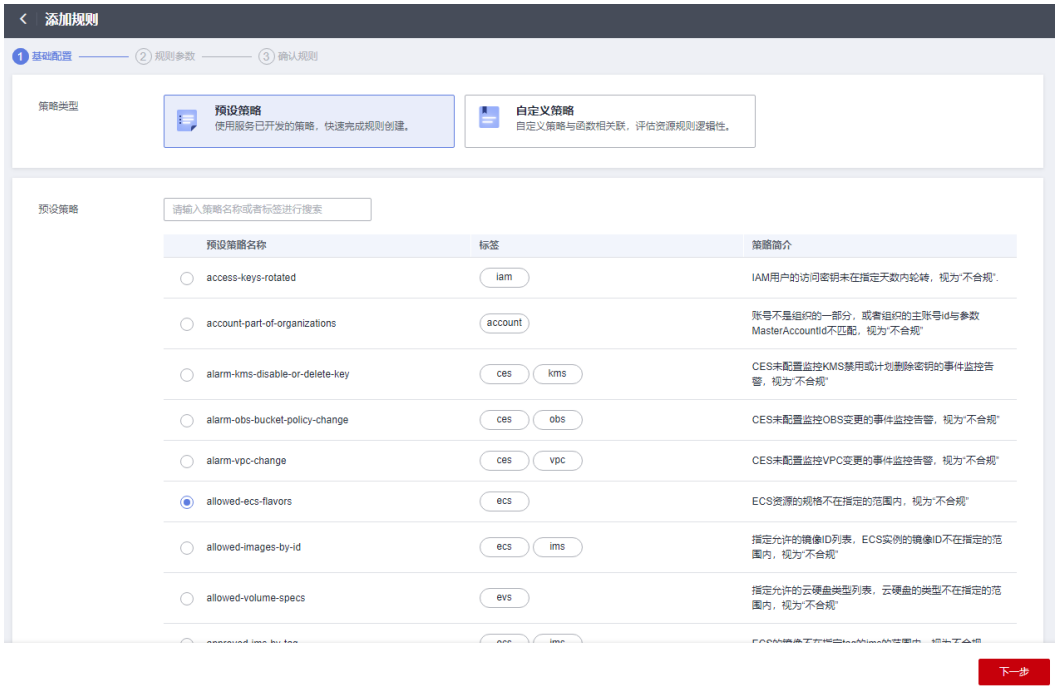
步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 在“规则”页签下单击“添加规则”，进入“基础配置”页面，基础配置完成后，单击页面右下角的“下一步”。

图 3-1 添加合规规则-基础配置



相关参数配置，详见**表1 基础配置参数说明**。

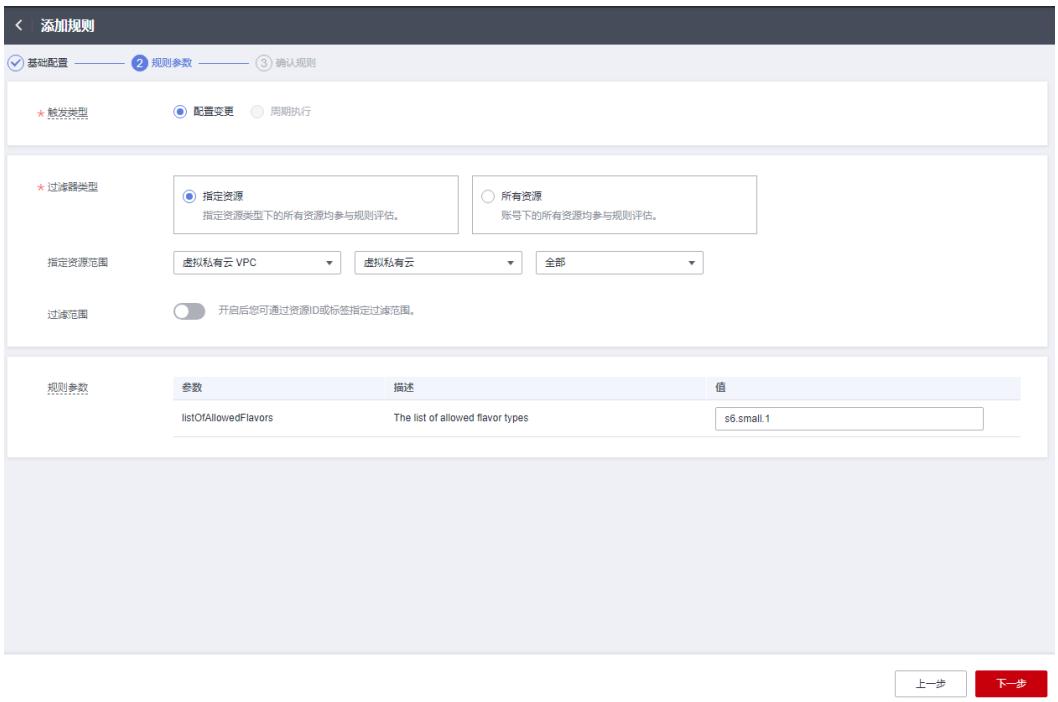
表 3-1 基础配置参数说明

参数	说明
策略类型	策略类型有： ● 预设策略 ● 自定义策略
预设策略	预设策略即服务已开发的策略。 使用服务已开发的策略，快速完成合规规则创建。 预设策略详情见**系统内置预设策略**。
自定义策略	允许用户通过自定义策略来创建合规规则。 自定义策略详情见**添加自定义合规规则**。
规则名称	规则名称默认复用所选择预设策略的名称，不能与已存在的合规规则名称重复，如有重复需自行修改。 合规规则名称仅支持数字、字母、下划线和中划线。

参数	说明
规则简介	规则简介默认复用所选择预设策略的简介，也可自行修改。 目前对合规规则简介的内容不做限制。
FunctionGraph 函数	用户自定义策略执行函数的urn。 创建FunctionGraph函数请参见**创建FunctionGraph函数**。 仅当“策略类型”选择“自定义策略”时需配置此参数。
授权	此处的授权为**委托授权**，授权函数工作流（FunctionGraph）的只读权限和调用权限给Config服务，允许自定义合规规则查询函数工作流以及将事件发送至函数工作流。 仅当“策略类型”选择“自定义策略”时需配置此参数。 **说明** • **快速授权**：将为您快速创建一个名为“rms_custom_policy_agency”的委托权限，该权限是可以让自定义合规规则正常工作的权限，包含函数工作流（FunctionGraph）的只读权限和调用权限。 • **自定义授权**：您可自行在统一身份认证服务（IAM）中创建委托权限，并进行自定义授权，但必须包含可以让自定义合规规则正常工作的权限（函数工作流（FunctionGraph）的只读权限和调用权限），创建委托详见**《统一身份认证服务用户指南》**。

步骤5 进入“规则参数”页面，规则参数配置完成后，单击“下一步”。

图 3-2 添加合规规则-规则参数



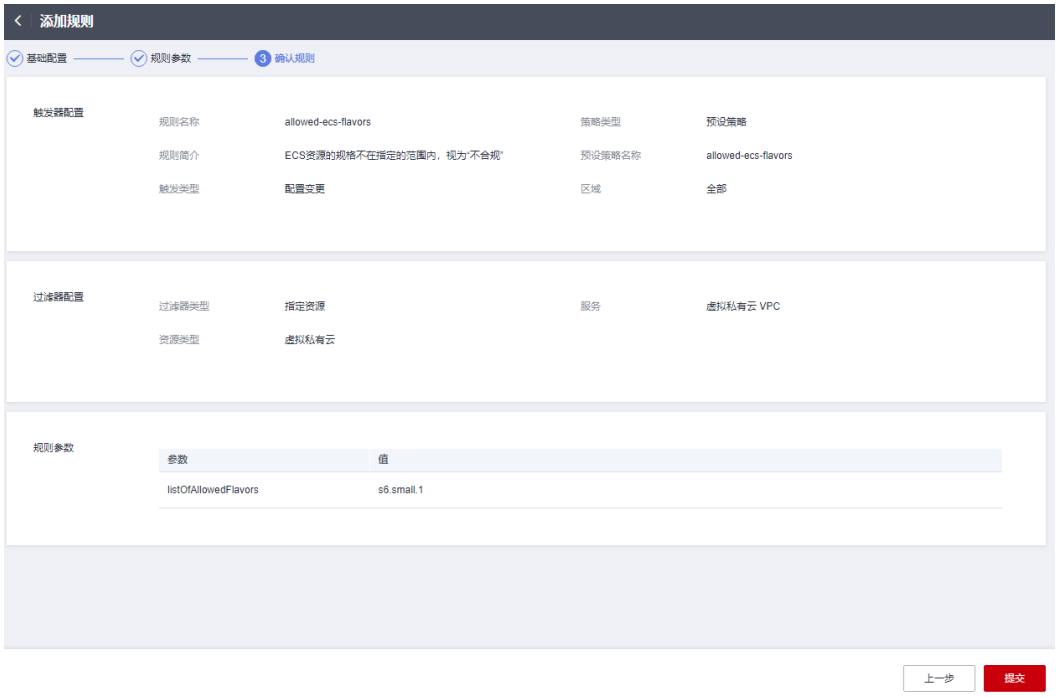
相关参数配置，详见**表2 合规规则参数说明**。

表 3-2 合规规则参数说明

参数	说明
触发类型	用于触发资源合规规则。 触发类型有： ● 配置变更：在指定的云资源发生更改时触发规则评估。 ● 周期执行：按照您设定的频率运行。
过滤器类型	用于指定资源类型参与规则评估。 过滤器类型分为： ● 指定资源：指定资源类型下的所有资源均参与规则评估。 ● 所有资源：账号下的所有资源均参与规则评估。 仅当“触发类型”为“配置变更”时需配置此参数。
指定资源范围	过滤器类型选择“指定资源”后，需选择指定资源范围。 ● 服务：选择资源所属的服务； ● 资源类型：选择对应服务下的资源类型； ● 区域：选择资源所在的区域。 仅当“触发类型”为“配置变更”时需配置此参数。
过滤范围	使用过滤范围可指定资源类型下的某个具体资源参与规则评估。 过滤范围开启后您可通过资源ID或标签指定过滤范围。 仅当“触发类型”为“配置变更”时需配置此参数。
周期频率	设置合规规则周期执行的频率。 仅当“触发类型”为“周期执行”时需配置此参数。
规则参数	此处的“规则参数”和第一步所选的“预设策略”或“自定义策略”相对应，是对第一步所选的预设策略或自定义策略进行具体参数设置。 例如：第一步预设策略选择“required-tag-check”，指定一个标签，不具有此标签的资源，视为“不合规”，则这里的规则参数就需要指定具体的标签键和值作为判断是否合规的依据。 有的“预设策略”需要添加规则参数，有的“预设策略”不需要添加规则参数（例如：volumes-encrypted-check：已挂载的云硬盘未进行加密，视为“不合规”）。 自定义策略的规则参数最多可以设置10个，由您自行配置。

步骤6 进入“确认规则”页面，确认规则信息无误后，单击“提交”按钮，完成合规规则添加。

图 3-3 添加合规规则-确认规则



说明

合规规则创建后会立即自动触发首次评估。

----结束

3.1.2 添加自定义合规规则

操作场景

当Config提供的系统内置预设策略不能满足检测资源合规性的需求时，您可以通过编写函数代码，添加自定义策略来完成复杂场景的资源审计。

自定义策略是一个用户开发并发布在函数工作流（FunctionGraph）上的函数。将合规规则和函数相关联，函数接收Config发布的事件，从事件中接收到规则参数和Config服务收集到的资源属性；函数评估该规则下资源的合规性并通过Config的OpenAPI回传Config服务合规评估结果。合规规则的事件发送因触发类型为配置变更或周期执行而异。要了解如何使用FunctionGraph函数以及如何开发它们，请参阅《FunctionGraph用户指南》。

须知

仅被资源记录器收集的资源可参与资源评估，为保证资源合规规则的评估结果符合预期，强烈建议您保持资源记录器的开启状态，不同场景的说明如下：

- 如您从未开启过资源记录器，则资源合规规则无法评估任何资源数据。
- 如您已开启资源记录器，但仅在资源记录器监控范围内勾选部分资源，则资源合规规则仅会评估所选择的资源数据。
- 如您开启资源记录器并勾选全部资源，但后续又关闭资源记录器，则资源合规规则仅会评估资源记录器由开启到关闭期间收集到的资源数据。

关于如何开启并配置资源记录器请参见：**配置资源记录器**。

本章节指导您如何通过自定义策略来添加资源合规规则，主要包含如下步骤：

1. **创建FunctionGraph函数**；
2. **添加自定义合规规则**。

创建 FunctionGraph 函数

步骤1 登录**函数工作流控制台**，在左侧的导航栏选择“函数 > 函数列表”。

步骤2 单击右上方的“创建函数”，进入“创建函数”页面。

步骤3 选择“创建空白函数”，“函数类型”选择“事件函数”，并配置IAM委托。IAM委托授权给函数工作流（FunctionGraph），且需要包含权限“rms:policyStates:update”。

步骤4 配置完成后单击“创建函数”，页面跳转至代码配置页面，继续配置代码源。

步骤5 在代码框中写入评估函数，完成后单击“部署”。

评估函数的代码示例可参考**示例函数(Python)**。

步骤6 选择“设置”，按需修改常规设置中的“执行超时时间”和“内存”，并配置“并发”。

步骤7 完成后单击“保存”。

具体请参见**创建事件函数**。

----结束

添加自定义合规规则

步骤1 登录管理控制台。

步骤2 单击页面左上角的☰图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 单击页面中部的“添加规则”，进入“基础配置”页面。

步骤5 “策略类型”选择“自定义策略”，配置相关参数并进行授权，授权方式可以选择“快速授权”或“自定义授权”，配置完成后单击“下一步”。

- **快速授权：**将为您快速创建一个名为“rms_custom_policy_agency”的委托权限，该权限是可以让自定义合规规则正常工作的权限，包含调用函数工作流（FunctionGraph）的获取函数和异步执行函数的权限。
- **自定义授权：**您可自行在统一身份认证服务（IAM）中创建委托权限，并进行自定义授权，授权对象为配置审计（Config），授权内容为：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "functiongraph:function:invokeAsync",
                "functiongraph:function:getConfig"
            ]
        }
    ]
}
```

创建委托详见**《统一身份认证服务用户指南》**。

图 3-4 添加合规规则-自定义策略

步骤6 进入“规则参数”页面，规则参数配置完成后，单击“下一步”。

步骤7 进入“确认规则”页面，确认规则信息无误后，单击“提交”按钮，完成自定义合规规则创建。

----结束

3.1.3 查看合规规则

操作场景

资源合规规则添加完成后，您可以在规则列表中查看所有已添加的合规规则，进入规则详情页可查看规则的评估结果和规则详情配置等信息。

在规则详情页的右上角，您还可以进行触发规则评估（立即评估）、修改规则（编辑规则）、停用/启用规则、删除规则操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

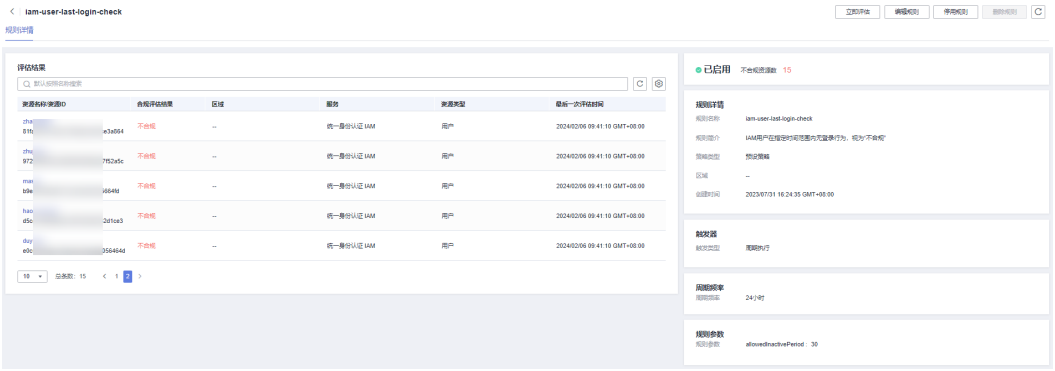
步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 在“规则”页签下的列表中，可查看所有已添加的合规规则以及其运行状态、合规评估结果等信息。

步骤5 在规则列表中单击合规规则的规则名称，进入“规则详情页”。

页面左侧为此合规规则评估结果的详细信息，页面右侧为此合规规则的配置详情。

图 3-5 规则详情



说明

合规规则的运行状态分为：

- 已启用：表示此合规规则可用。
- 已停用：表示此合规规则已停用。
- 评估中：表示正在使用此合规规则进行资源评估。
- 提交中：表示自定义合规规则正在提交评估任务给FunctionGraph函数。

当规则评估正在进行中时，规则的运行状态显示为“评估中”，当规则评估结束后，规则的运行状态变为“已启用”，此时可查看规则评估结果。

----结束

3.1.4 触发规则评估

操作场景

触发规则评估的方式包括**自动触发**和**手动触发**。

- **自动触发**

  新创建一个合规规则时，会触发此规则的评估任务。

  合规规则更新时，会触发此规则的评估任务。

  合规规则被重新启用时，会触发此规则的评估任务。

  当触发类型为“配置变更”时，合规规则范围内的资源发生变更，则会将该规则应用到此资源上，进行评估。

  当触发类型为“周期执行”时，系统将按照您设定的频率，触发此规则的评估任务。

- **手动触发**

  如果您想立即使用已有合规规则进行规则评估，可随时手动触发规则评估，具体操作请参见如下步骤。

  当调用“**run-evaluation**”接口时，会触发此合规规则的评估任务。

约束与限制

合规规则仅评估资源记录器收集的资源数据，不同场景的说明如下：

- 如您从未开启过资源记录器，则触发规则评估后，合规规则不会评估任何资源。
- 如您已开启资源记录器，但仅在资源记录器监控范围内勾选部分资源，则触发规则评估后，合规规则仅会评估您所选择的资源。
- 如您开启资源记录器并勾选全部资源，但后续又关闭资源记录器，则触发规则评估后，合规规则仅会评估资源记录器由开启到关闭期间收集到的资源数据。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的 图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 在“规则”页签下的合规规则列表中，单击合规规则操作列的“立即评估”。

步骤5 在弹出的确认框中，单击“确定”，立即触发此合规规则的规则评估。

图 3-6 手动触发规则评估

----结束

3.1.5 编辑资源合规规则

操作场景

资源合规规则添加完成后，您可以随时对其进行修改、停用、启用、删除操作。

您可以在规则列表的操作列或规则详情页中进行这些操作，本章节以规则列表的操作为例进行说明，包含如下内容：

- **停用合规规则**

- 启用合规规则
- 修改合规规则
- 删除合规规则

说明

托管合规规则不支持进行修改、停用、启用、删除操作，托管合规规则是由组织合规规则或合规规则包创建的，由组织合规规则创建的托管规则只能由创建规则的组织账号进行修改和删除操作，由合规规则包创建的托管规则可以通过更新合规规则包进行参数修改，且只能通过删除相应合规规则包来进行删除。具体请参见组织合规规则和合规规则包。

停用合规规则

步骤1 登录管理控制台。

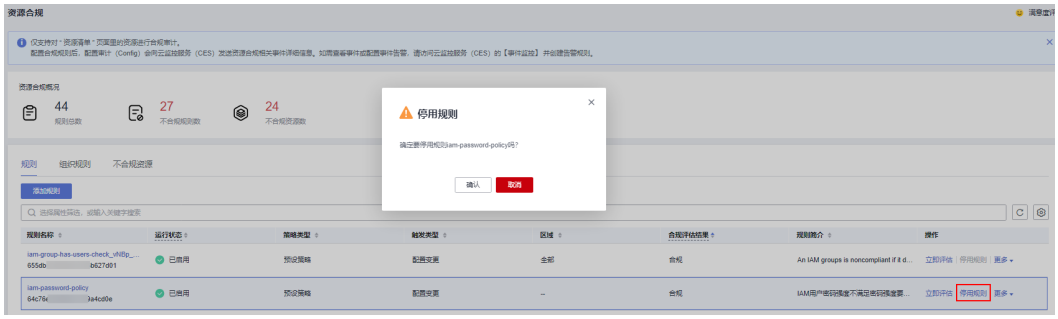
步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 在“规则”页签下的合规规则列表中，单击启用状态的合规规则操作列的“停用规则”。

步骤5 在弹出的确认框中，单击“确定”，停用此合规规则。

图 3-7 停用规则



----结束

启用合规规则

步骤1 登录管理控制台。

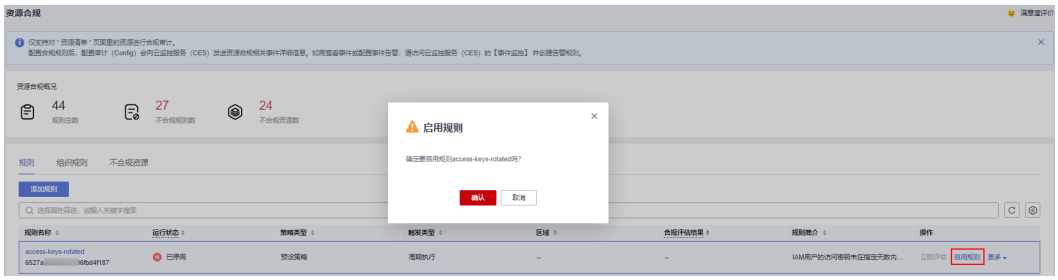
步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 在“规则”页签下的合规规则列表中，单击停用状态的合规规则操作列的“启用规则”。

步骤5 在弹出的确认框中，单击“确定”，启用此合规规则。

图 3-8 启用规则



----结束

修改合规规则

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 在“规则”页签下的合规规则列表中，单击合规规则操作列的“更多>编辑规则”。

图 3-9 编辑规则

步骤5 进入“编辑规则”页面，修改“规则名称”和“规则简介”后，单击“下一步”。

步骤6 修改“规则参数”的相关配置后，单击“下一步”。

步骤7 确认规则修改无误后，单击“提交”，此合规规则的配置修改完成。

----结束

删除合规规则

删除合规规则前需先停用该规则。

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 在“规则”页签下的合规规则列表中，单击停用状态的合规规则操作列的“更多>删除规则”。

图 3-10 删除规则

步骤5 在弹出的确认框中，单击“确定”，此合规规则删除完成。

----结束

3.1.6 自定义合规规则样例

3.1.6.1 示例函数(Python)

评估由配置变更触发的示例函数

Config服务检测到自定义合规规则范围内的资源发生更改时，会调用函数的示例如下：

```
import requests
import http.client
import time

requests.packages.urllib3.disable_warnings()


def get_policy_resource(domain_id, resource):
    return {
        "domain_id": domain_id,
        "region_id": resource.get("region_id"),
        "resource_id": resource.get("id"),
        "resource_name": resource.get("name"),
        "resource_provider": resource.get("provider"),
        "resource_type": resource.get("type")
    }


'''
合规规则评估逻辑：返回“Compliant”或“NonCompliant”。
本示例中，当资源类型为ecs.cloudservers，且该ECS的VPC_ID字段不是合规规则参数所指定的VPC_ID时，会返回不合规，否则返回合规。
'''
def evaluate_compliance(resource, parameter):
    if resource.get("provider") != "ecs" or resource.get("type") != "cloudservers":
        return "Compliant"
    vpc_id = resource.get("properties", {}).get("metadata", {}).get("vpcId")
    return "Compliant" if vpc_id == parameter.get("vpcId") else "NonCompliant"


def update_policy_state(token, domain_id, evaluation):
    endpoint = "https://rms.myhuaweicloud.com"
    url = "{}/v1/resource-manager/domains/{}/policy-states".format(endpoint, domain_id)
```

```
    return requests.put(
        url=url,
        headers={
            "X-Auth-Token": token
        },
        json=evaluation,
        verify=False,
    )


def handler(event, context):
    resource = event.get("invoking_event", {})
    parameters = event.get("rule_parameter")
    compliance_state = evaluate_compliance(resource, parameters)

    requests = {
        "policy_resource": get_policy_resource(event.get("domain_id"), resource),
        "trigger_type": event.get("trigger_type"),
        "compliance_state": compliance_state,
        "policy_assignment_id": event.get("policy_assignment_id"),
        "policy_assignment_name": event.get("policy_assignment_name"),
        "function_urn": event.get("function_urn"),
        "evaluation_time": event.get("evaluation_time"),
        "evaluation_hash": event.get("evaluation_hash")
    }

    for retry in range(3):
        response = update_policy_state(context.getToken(), event.get("domain_id"), requests)
        if response.status_code == http.client.TOO_MANY_REQUESTS:
            print("TOO_MANY_REQUESTS: retry again")
            time.sleep(1)
        else:
            if response.status_code == http.client.OK:
                print("Update policyState successfully.")
            else:
                print("Failed to update policyState.")
                print(response.json())
            break
```

评估由周期执行触发的示例函数

Config针对周期执行的自定义合规规则，会调用函数的示例如下：

```
import requests
import http.client
import time

requests.packages.urllib3.disable_warnings()


def get_policy_resource(domain_id, resource):
    return {
        "domain_id": domain_id,
        "region_id": resource.get("region_id"),
        "resource_id": resource.get("id"),
        "resource_name": resource.get("name"),
        "resource_provider": resource.get("provider"),
        "resource_type": resource.get("type")
    }


"""
合规规则评估逻辑：返回“Compliant”或“NonCompliant”。
本示例中, 当账号设置的登录会话失效时间大于30分钟, 会返回不合规, 否则返回合规。
实现方式是调用IAM服务的接口ShowDomainLoginPolicy。
"""
def evaluate_compliance(token, domain_id):
    endpoint = "https://iam.cn-north-4.myhuaweicloud.com"
    url = "{}/v3.0/OS-SECURITYPOLICY/domains/{}/login-policy".format(endpoint, domain_id)
```

```
    r = requests.get(
        url=url,
        headers={
            "X-Auth-Token": token,
            "User-Agent": "API Explorer",
            "Content-Type": "application/json;charset=UTF-8"
        },
        verify=False,
    )
    session_timeout = r.json().get("login_policy", {}).get("session_timeout", 60)
    return "NonCompliant" if session_timeout > 30 else "Compliant"


def update_policy_state(token, domain_id, evaluation):
    endpoint = "https://rms.myhuaweicloud.com"
    url = "{}/v1/resource-manager/domains/{}/policy-states".format(endpoint, domain_id)
    return requests.put(
        url=url,
        headers={
            "X-Auth-Token": token
        },
        json=evaluation,
        verify=False,
    )


def handler(event, context):
    resource = event.get("invoking_event", {})
    if resource.get("name") != "Account":
        return
    compliance_state = evaluate_compliance(context.getToken(), event.get("domain_id"))

    requests = {
        "policy_resource": get_policy_resource(event.get("domain_id"), resource),
        "trigger_type": event.get("trigger_type"),
        "compliance_state": compliance_state,
        "policy_assignment_id": event.get("policy_assignment_id"),
        "policy_assignment_name": event.get("policy_assignment_name"),
        "function_urn": event.get("function_urn"),
        "evaluation_time": event.get("evaluation_time"),
        "evaluation_hash": event.get("evaluation_hash")
    }

    for retry in range(3):
        response = update_policy_state(context.getToken(), event.get("domain_id"), requests)
        if response.status_code == http.client.TOO_MANY_REQUESTS:
            print("TOO_MANY_REQUESTS: retry again")
            time.sleep(1)
        else:
            if response.status_code == http.client.OK:
                print("Update policyState successfully.")
            else:
                print("Failed to update policyState.")
                print(response.json())
            break
```

3.1.6.2 事件

由配置变更触发的评估的示例事件

当触发自定义合规规则时，Config服务会发送一个事件来调用该自定义合规规则的函数。下面的事件演示自定义合规规则被某个ecs.cloudservers的配置变更所触发。

```
{
  "domain_id": "domain_id",
  "policy_assignment_id": "637c6b2e6b647c4d313d9719",
  "policy_assignment_name": "period-policy-period",
```



```
 "function_urn": "urn:fss:region_1:123456789:function:default:test-custom-policyassignment:latest",
 "trigger_type": "resource",
 "evaluation_time": 1669098286719,
 "evaluation_hash": "3bf8ecaeb0864feb98639080aea5c7d9",
 "rule_parameter": {
   "vpcId": {
     "value": "fake_id"
   }
 },
 "invoking_event": {
   "id": "5e0d49c8-7ce0-4c31-9d92-28b05200b838",
   "name": "default",
   "provider": "vpc",
   "type": "securityGroups",
   "tags": {},
   "created": "2022-11-07T12:58:46.000+00:00",
   "updated": "2022-11-07T12:58:46.000+00:00",
   "properties": {
     "description": "Default security group",
     "security_group_rules": [
       {
         "remote_group_id": "5e0d49c8-7ce0-4c31-9d92-28b05200b838",
         "ethertype": "IPv6",
         "security_group_id": "5e0d49c8-7ce0-4c31-9d92-28b05200b838",
         "port_range_max": 0,
         "id": "19f581bc-08a7-4037-ae59-9a6838c43709",
         "direction": "ingress",
         "port_range_min": 0
       },
       {
         "ethertype": "IPv6",
         "security_group_id": "5e0d49c8-7ce0-4c31-9d92-28b05200b838",
         "port_range_max": 0,
         "id": "75dae7b6-0b71-496f-8f11-87fb30300e18",
         "direction": "egress",
         "port_range_min": 0
       }
     ]
   },
   "ep_id": "0",
   "project_id": "vpc",
   "region_id": "region_1",
   "provisioning_state": "Succeeded"
 }
}
```


由周期执行触发的评估的示例事件

Config以您指定的频率（如每24小时）评估您的账号时，它会发布一个事件。下面的示例事件演示自定义合规规则被周期执行所触发。


```
{
 "domain_id": "domain_id",
 "policy_assignment_id": "637c6b2e6b647c4d313d9719",
 "policy_assignment_name": "period-policy-assignment",
 "function_urn": "urn:fss:region_1:123456789:function:default:test-custom-policyassignment:latest",
 "trigger_type": "period",
 "evaluation_time": 1669098286719,
 "evaluation_hash": "3bf8ecaeb0864feb98639080aea5c7d9",
 "rule_parameter": {},
 "invoking_event": {
   "id": "domain_id",
   "name": "Account",
   "provider": null,
   "type": null,
   "tags": null,
   "created": null,
   "updated": null,
   "properties": null,
```



```
    "ep_id": null,
    "project_id": null,
    "region_id": "global",
    "provisioning_state": null
  }
}
```

3.2 组织合规规则

3.2.1 添加预定义组织合规规则

操作场景

在使用资源合规时，如果您是组织管理员或Config服务的委托管理员，您可以添加组织类型的资源合规规则，直接作用于您组织内的成员账号中。

当组织资源合规规则部署成功后，会在组织内成员账号的规则列表中显示此组织合规规则。且该组织合规规则的修改和删除操作只能由创建规则的组织账号进行，组织内的其他账号只能触发规则评估和查看规则评估结果以及详情。

您可以选择Config提供的系统内置预设策略或者自定义策略来创建组织类型的资源合规规则，本章节指导您如何使用系统内置的预设策略来快速添加组织合规规则。

约束与限制

- 每个账号最多可以添加500个合规规则。
- 非组织成员账号无法在Config控制台的“资源合规”页面中看到“组织规则”页签。

须知

仅被资源记录器收集的资源可参与资源评估，为保证资源合规规则的评估结果符合预期，强烈建议您保持资源记录器的开启状态，不同场景的说明如下：

- 如您从未开启过资源记录器，则资源合规规则无法评估任何资源数据。
- 如您已开启资源记录器，但仅在资源记录器监控范围内勾选部分资源，则资源合规规则仅会评估所选择的资源数据。
- 如您开启资源记录器并勾选全部资源，但后续又关闭资源记录器，则资源合规规则仅会评估资源记录器由开启到关闭期间收集到的资源数据。

关于如何开启并配置资源记录器请参见：**配置资源记录器**。

操作步骤

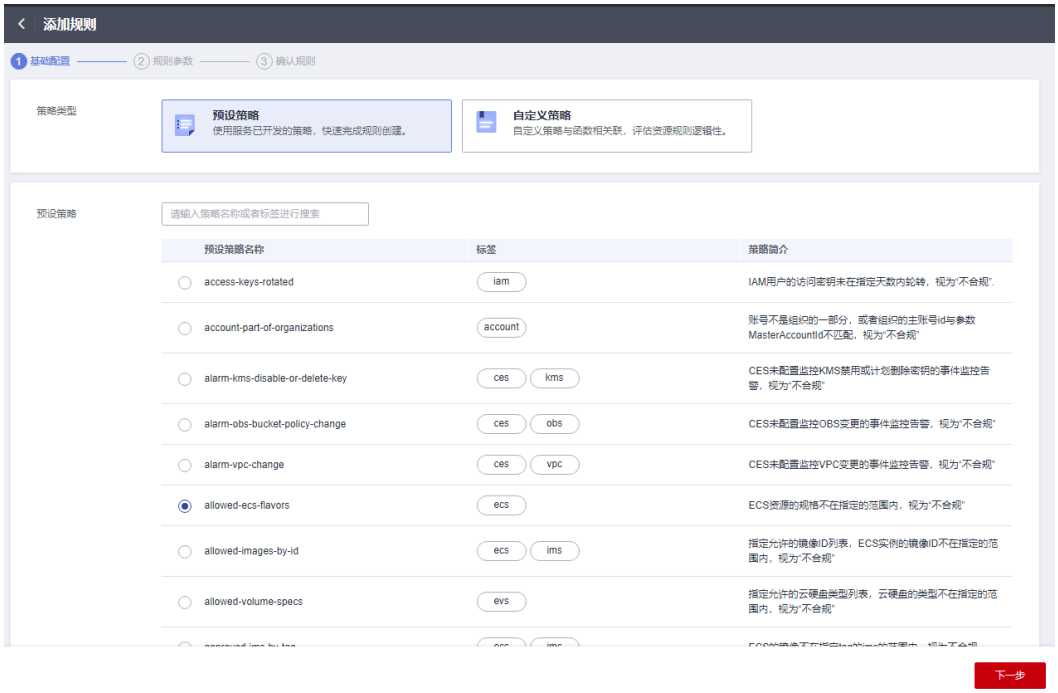
步骤1 以组织管理员账号或者Config服务的委托管理员账号登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 选择“组织规则”页签，单击“添加规则”，进入“基础配置”页面，基础配置完成后，单击“下一步”。

图 3-11 基础配置



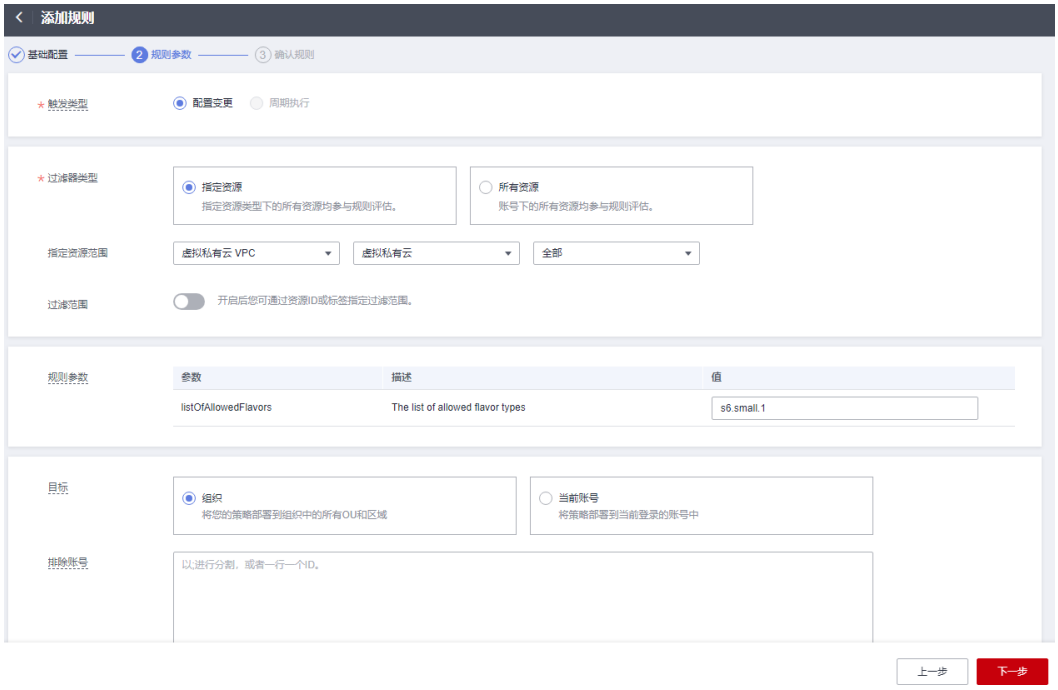
相关参数配置，详见**表3-3**。

表 3-3 基础配置参数说明

参数	说明
策略类型	策略类型有： ● 预设策略
预设策略	预设策略即服务已开发的策略。 使用服务已开发的策略，快速完成合规规则创建。 预设策略详情见**系统内置预设策略**。
规则名称	规则名称默认复用所选择预设策略的名称，不能与已存在的合规规则名称重复，如有重复需自行修改。 合规规则名称仅支持数字、字母、下划线和中划线。
规则简介	规则简介默认复用所选择预设策略的简介，也可自行修改。 目前对合规规则简介的内容不做限制。

步骤5 进入“规则参数”页面，规则参数配置完成后，单击“下一步”。

图 3-12 规则参数



相关参数配置，详见**表2 合规规则参数说明**。

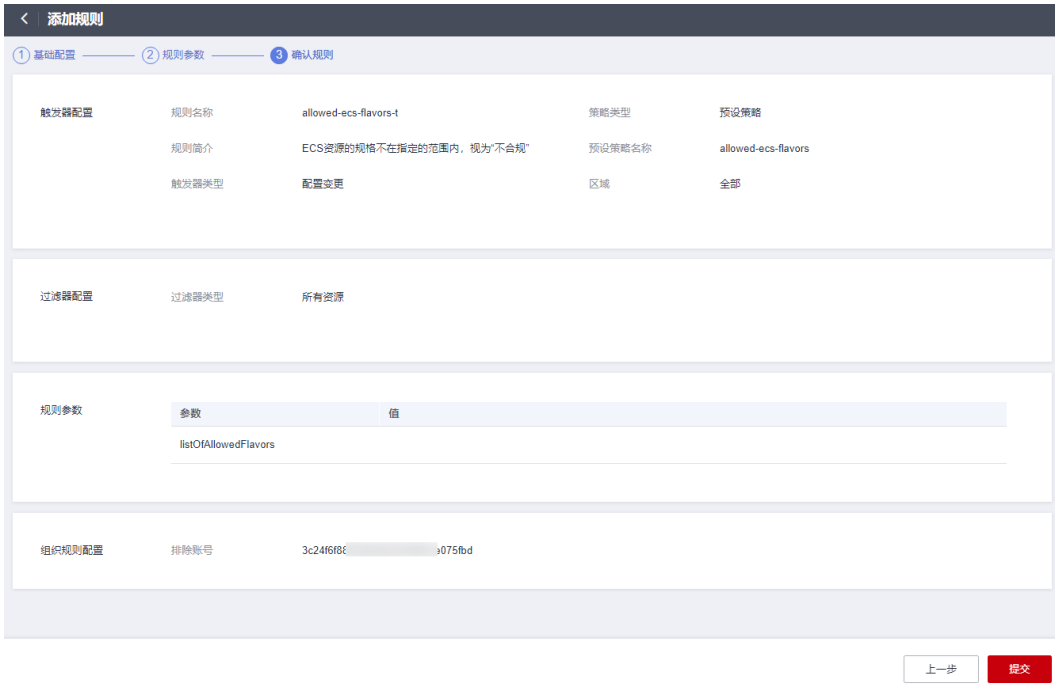
表 3-4 合规规则参数说明

参数	说明
触发类型	用于触发资源合规规则。 触发类型有： ● 配置变更：在指定的云资源发生更改时触发规则评估。 ● 周期执行：按照您设定的频率运行。
过滤器类型	用于指定资源类型参与规则评估。 过滤器类型分为： ● 指定资源：指定资源类型下的所有资源均参与规则评估。 ● 所有资源：账号下的所有资源均参与规则评估。 仅当“触发类型”选择“配置变更”时需配置此参数。
指定资源范围	过滤器类型选择“指定资源”后，需选择指定资源范围。 ● 服务：选择资源所属的服务； ● 资源类型：选择对应服务下的资源类型； ● 区域：选择资源所在的区域。 仅当“触发类型”选择“配置变更”时需配置此参数。
过滤范围	使用过滤范围可指定资源类型下的某个具体资源参与规则评估。 过滤范围开启后您可通过资源ID或标签指定过滤范围。 仅当“触发类型”选择“配置变更”时需配置此参数。

参数	说明
周期频率	设置合规规则周期执行的频率。 仅当“触发类型”选择“周期执行”时需配置此参数。
规则参数	此处的“规则参数”和第一步所选的“预设策略”相对应，是对第一步所选的预设策略进行具体参数设置。 例如：第一步预设策略选择“required-tag-check”，指定一个标签，不具有此标签的资源，视为“不合规”，则这里的规则参数就需要指定具体的标签键和值作为判断是否合规的依据。 有的“预设策略”需要添加规则参数，有的“预设策略”不需要添加规则参数（例如：volumes-encrypted-check：已挂载的云硬盘未进行加密，视为“不合规”）。
目标	目标决定了此组织合规规则配置的部署位置。 ● 组织：将策略部署到您组织内的所有成员账号中。 ● 当前账号：将策略部署到当前登录的账号中。 创建组织类型的资源合规规则时请选择“组织”。
排除账号	输入需要排除的组织内的部分账号ID，使得该组织合规规则不在排除的账号中部署。 仅当“目标”选择“组织”时可配置此参数。

步骤6 进入“确认规则”页面，确认规则信息无误后，单击“提交”按钮，完成预定义组织合规规则的创建。

图 3-13 确认规则



说明

合规规则创建后会立即自动触发首次评估。

----结束

触发规则评估

组织内的成员账号触发组织合规规则评估可参考：**触发规则评估**。

3.2.2 查看组织合规规则

操作场景

组织合规规则添加完成后，您可以参考以下步骤查看组织合规规则的列表和详情。

本章节包含**查看组织合规规则**和**查看部署至成员账号中的组织合规规则**两部分内容。

查看组织合规规则

组织合规规则添加完成后，您可以查看该组织合规规则的详情。

步骤1 使用创建组织合规规则的组织账号登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 选择“组织规则”页签，单击规则列表下的具体规则名。

图 3-14 查看组织合规规则

步骤5 进入“规则详情页”，页面左侧显示此规则作用的成员账号列表和部署状态以及排除账号列表，页面右侧显示合规规则详情。

说明

创建组织合规规则的组织账号只能看到自己添加的组织合规规则，无法看到组织内其他账号添加的组织合规规则。

----结束

查看部署至成员账号中的组织合规规则

当组织资源合规规则部署成功后，会在组织内成员账号的规则列表中显示此组织合规规则。且该组织合规规则的修改和删除操作只能由创建规则的组织账号进行，组织内的其他账号只能触发规则评估和查看规则评估结果以及详情。

步骤1 以组织成员账号登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 在“规则”页签下，单击合规规则列表中的某个具体组织合规规则名称，进入“规则详情页”。

页面左侧为合规规则评估结果，页面左侧为合规规则详情。

图 3-15 查看部署至成员账号中的组织合规规则

说明

当组织合规规则部署成功后，会在组织内成员账号的规则列表中显示此组织合规规则，系统将自动在规则名称前添加“Org-”字段。

组织内的成员账号只能触发此规则的评估和查看规则评估结果以及详情，不支持修改、停用和删除规则的操作。

----结束

3.2.3 修改组织合规规则

操作场景

组织合规规则添加完成后，您可以随时修改组织合规规则的规则名称、规则简介和规则参数。

操作步骤

步骤1 使用创建组织合规规则的组织账号登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 选择“组织规则”页签，在规则列表中单击操作列的“编辑”。

图 3-16 编辑组织合规规则

步骤5 进入“编辑规则”页面，修改“规则名称”和“规则简介”后，单击“下一步”。

步骤6 修改“规则参数”后，单击“下一步”。

步骤7 确认规则修改无误后，单击“提交”。

----结束

3.2.4 删除组织合规规则

操作场景

如果您不需要使用某个组织合规规则时，您可以删除此规则。

操作步骤

步骤1 使用创建组织合规规则的组织账号登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

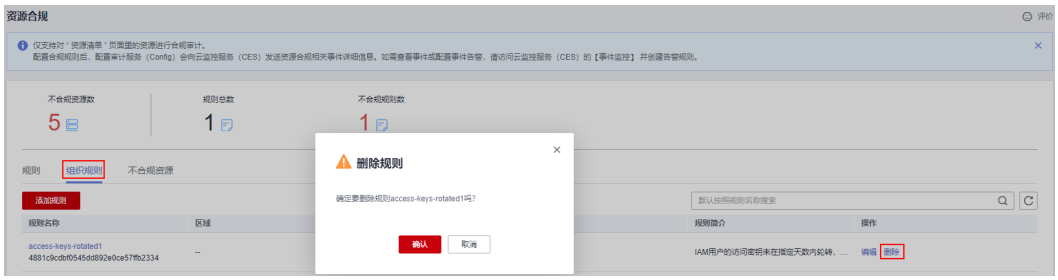
步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 选择“组织规则”页签，在规则列表中单击操作列的“删除”。

步骤5 在弹出的“删除规则”对话框中，单击。

组织合规规则删除后，此规则部署的成员账号的规则列表中也将自动删除此规则。

图 3-17 删除组织合规规则



----结束

说明

单击规则列表下的具体规则名，进入“规则详情”页面，在页面右上角单击“编辑规则”和“删除规则”按钮，也可以对此规则进行编辑和删除操作。

3.3 查看不合规资源

操作场景

当您添加并启用了多个合规规则时，您可以在“资源合规”页面中的“不合规资源”页签查看当前账号下全部不合规资源的信息。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

步骤4 选择“不合规资源”页签，列表中展示当前账号下全部的不合规资源信息。

步骤5 单击列表中某一资源的名称，界面展示该资源的概览信息。

图 3-18 查看不合规资源

----结束

3.4 合规规则概念详解

3.4.1 合规策略

合规策略是一个可以用于评估资源是否合规的逻辑表达式。将合规策略应用到资源上时，可以评估出这个资源是否符合合规策略中的要求。

合规策略本身只是一个静态的逻辑，如果想要让其生效，必须将合规策略指定到一个具体的范围（如：通过设置过滤器来指定具体的资源范围）上，即生成一个具体的合规规则。

使用JSON表达式来表示一个合规策略定义，如**表1**所示。

表 3-5 合规策略的定义-JSON 表达式格式

参数	定义	说明
id	合规策略的唯一标识符	-
name	合规策略的名称	name最大长度为64个字符。
display_name	合规策略的展示名	display_name最大长度为64个字符。
description	合规策略的描述	description最大长度为512个字符。

参数	定义	说明
parameters	合规策略的规则参数，即每个合规策略下包含的参数。 具有如下属性： • name • description • type • default_value • allowed_values • minimum • maximum • min_items • max_items • min_length • max_length • pattern	合规策略中包含的参数名称保持不变，您可以根据需要设置不同的值。 • name：规则参数的名称。 • description：规则参数的描述。 • type：规则参数值的类型，包括String，Array，Boolean，Integer，Float。 • default_value：规则参数的默认值。如果指定了默认值，用户可以不输入规则参数值，创建合规规则时将使用此默认值。 • allowed_values：规则参数值允许的值列表。如果指定了allowed_values，那么参数的值只能够从这些值中选择。 • minimum：策略参数的最小值，当参数类型为Integer或Float时生效。 • maximum： 策略参数的最大值，当参数类型为Integer或Float时生效。 • min_items：策略参数的最小项数，当参数类型为Array时生效。 • max_items： 策略参数的最大项数，当参数类型为Array时生效。 • min_length：策略参数的最小字符串长度或每项的最小字符串长度，当参数类型为String或Array时生效。 • max_length： 策略参数的最大字符串长度或每项的最大字符串长度，当参数类型为String或Array时生效。 • pattern：策略参数的字符串正则要求或每项的字符串正则要求，当参数类型为String或Array时生效。
keywords	合规策略关键词	一般为与合规策略相关的产品简称。
policy_type		• builtin：系统内置策略，这些合规策略定义由Config服务提供和维护。详见**系统内置预设策略**。 • custom: 用户自定义策略，用户创建的所有合规策略定义都具有此值。
policy_rule_type	合规策略的语法类型	DSL：一种Config服务提供的合规策略描述语言，用户可以根据此语法，将合规判断逻辑描述为一个具体的合规策略。
policy_rule	合规策略语法的逻辑表达式	关于如何使用DSL来编写合规策略的具体逻辑请参阅**DSL语法**。

参数	定义	说明
trigger_type	触发类型。 有以下类型： • resource • period	• resource：在指定的资源发生更改时运行。 • period：按照您设定的频率运行。
default_resource_types	合规策略评估的资源类型	大部分合规策略只评估部分的资源类型。创建合规规则时，建议只评估“default_resource_types”中的资源类型。

如下JSON表示了一个用于检查ECS实例的镜像ID是否在指定范围内的合规策略：

```
{
  "id": "5fa265c0aa1e6afc05a0ff07",
  "name": "allowed-images-by-id",
  "description": "指定允许的镜像ID列表，ECS实例的镜像ID不在指定的范围内，视为“不合规”",
  "parameters": {
    "listOfAllowedImages": {
      "name": "null",
      "description": "The list of allowed image IDs",
      "type": "Array"
      "allowed_values": null,
      "default_value": null,
    }
  },
  "keywords": [
    "ecs",
    "ims"
  ],
  "policy_type": "builtin",
  "policy_rule_type": "dsl",
  "trigger_type": "resource",
  "policy_rule": {
    "allOf": [
      {
        "value": "${resource().provider}",
        "comparator": "equals",
        "pattern": "ecs"
      },
      {
       "value": "${resource().type}",
       "comparator": "equals",
       "pattern": "cloudservers"
      },
      {
       "value": "${resource().properties.metadata.meteringImageId}",
        "comparator": "notIn",
       "pattern": "${parameters('listOfAllowedImages')}"
      }
    ]
  },
}
```

更多样例详见**自定义合规规则样例**。

3.4.2 合规规则

通过指定合规策略和合规策略所应用的范围（如：在某一区域的某些资源）来构成合规规则。

使用JSON表达式来表示一个合规规则定义，如表3-6所示。

表 3-6 合规规则的定义-JSON 表达式格式

参数	定义	限制	说明
id	合规规则唯一标识符	-	-
policy_assignment_type	合规规则类型	-	包含以下两种： • builtin：预设策略，此时合规规则需要设置参数policy_definition_id。 • custom：自定义策略，此时合规规则需要设置参数custom_policy。 如不设置此参数，则默认为预设策略。
name	合规规则的名称	字符串类型，最多64个字符。	规则名称默认复用所选择合规策略的名称，也可自行修改。 name最大长度为64个字符。
description	合规规则的描述	字符串类型，最多512个字符。	指的是规则简介，默认复用所选择合规策略的简介，需自行修改。 description最大长度为512个字符。
period	周期频率	-	包含以下几种： • One_Hour: 1小时。 • Three_Hours: 3小时。 • Six_Hours: 6小时。 • Twelve_Hours: 12小时。 • TwentyFour_Hours: 24小时。

参数	定义	限制	说明
policy_filter	合规规则过滤器，用于过滤范围内的哪些资源参与此规则的评估。 过滤器的属性主要有以下几个： ● region_id: 区域ID。 ● resource_provider: 指定资源服务。 ● resource_type：指定资源服务下的资源类型。 ● resource_id：资源ID。 ● tag_key：资源标签的键。 ● tag_value：资源标签的值。	policy_filter：Object类型。 ● region_id：字符串类型，最多128个字符，只能包括字母、数字、中划线（-）。 ● resource_provider：字符串类型，最多128个字符，只能包括字母、数字。 ● resource_type：字符串类型，最多128个字符，只能包括字母、数字。 ● resource_id：字符串类型，最多256个字符。 ● tag_key：字符串类型，最多128个字符。 ● tag_value：字符串类型，最多256个字符。	**说明** 资源类型（resource_provider）是判断过滤器类型（指定资源/所有资源）的依据，如果policy_filter中资源类型存在，则过滤器类型为“指定资源”；如果policy_filter中资源类型不存在，则过滤器类型为“所有资源”。 因此policy_filter中没有设置单独的过滤器类型属性。
state	合规规则的运行状态	-	包含以下几种： ● Enabled：运行中，表示此合规规则可用。 ● Disabled：已停用，表示此合规规则已停用。 ● Evaluating：评估中，表示正在使用此合规规则进行资源评估。
created	合规规则的创建时间	-	**说明** 时间具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。
updated	合规规则的更新时间	-	
policy_definition_id	合规策略ID	字符串类型，最多64个字符，只能包括字母、数字、中划线（-）。	policy_definition_id指定此规则绑定的合规策略ID。

参数	定义	限制	说明
custom_policy	自定义策略，包含如下属性： ● function_urn：函数urn。 ● auth_type：调用函数的鉴权方式。 ● auth_value：调用函数的鉴权值。	custom_policy：Object类型 。 ● function_urn：字符串类型，最多1024个字符。 ● auth_type：字符串类型，当前只支持"agency" 。 ● auth_value：object类型，与auth_type相关，当前只支持如下结构{"agency_name": value_name}，其中value_name为授权给Config服务调用函数的委托的名字。	custom_policy指定此规则绑定的自定义策略的函数urn和调用时的鉴权方式。
parameters	合规策略的规则参数的值	parameters：Object类型 ● key：字符串类型，只能包括字母、数字，当合规规则为自定义合规规则时，最多1024个字符。 ● value：Object类型，根据参数具体的类型，有具体的限制。	合规规则绑定的合规策略，会有相应的规则参数，规则参数的个数、类型以及范围取决于所选择的合规策略。

说明

为避免循环评估的行为，合规规则不支持评估配置审计服务的合规规则和合规规则包两种资源类型。

如下JSON表示了一个用于检查在区域1的弹性云服务器是否具有tag（env：production）标签的预设策略：

```
{
  "id": "5fcd8696dfb78231e6f2f899",
  "name": "required-tag-check",
  "description": "指定一个标签，不具有此标签的资源，视为“不合规”",
  "policy_filter": {
        "region_id": "regionid_1",
        "resource_provider": "ecs",
        "resource_type": "cloudservers",
        "tag_key": "env",
        "tag_value": "production"
  },
  "period": null,
  "state": "Enabled",
  "created": "2020-12-07T01:34:14.266Z",
```



```
  "updated": "2020-12-07T01:34:14.266Z",
  "policy_definition_id": "5fa9f89b6eed194ccb2c04db",
  "parameters": {
        "specifiedTagKey": {
        "value": "a"     },
        "specifiedTagValue": {
        "value": []
    }
  }
}
```

如下JSON表示了一个用于检查在区域1的弹性云服务器的自定义合规规则：

```
{
  "id": "719d8696dfb78231e6f2f719",
  "name": "test_consume_policy",
  "description": "指定一个标签，不具有此标签的资源，视为“不合规”",
  "policy_filter": {
        "region_id": "regionid_1",
        "resource_provider": "ecs",
        "resource_type": "cloudservers",
        "tag_key": null,
        "tag_value": null
  },
  "period": null,
  "state": "Enabled",
  "created": "2022-07-19T01:34:14.266Z",
  "updated": "2022-07-19T01:34:14.266Z",
  "policy_definition_id": null,
  "custom_policy": {
    "function_urn": "urn:fss:regionid_1:projectidforpolicy:function:default:test_consume_policy:latest",
    "auth_type": "agency",
    "auth_value": {"agency_name": "rms_fg_agency"}
  },
  "parameters": {
        "vpcId": {"value": "allowed-vpc-id"}
    }
  }
}
```

3.4.3 规则评估结果

当触发规则评估后，会生成相应的评估结果（PolicyState）。

使用JSON表达式来表示一个评估结果，如表3-7所示。

表 3-7 规则评估结果-JSON 表达式格式

参数	定义	说明
domain_id	账号ID	用于区分用户。规则评估结果的domain_id不会为空。
resource_id	评估结果所属资源的ID	-
resource_name	评估结果所属资源的名称	-
resource_provider	资源所属的服务	-
resource_type	资源类型	-

参数	定义	说明
trigger_type	触发类型	包含如下值： • resource • period
compliance_state	合规结果	包含如下值： • Compliant：合规 • NonCompliant：不合规
policy_assignment_id	评估结果对应合规规则的ID	-
policy_definition_id	评估结果对应合规策略的ID	-
evaluation_time	评估时间戳	-

如下JSON表示了一个不合规的评估结果：

```
{
  "domain_id": "domainidforpolicy",
  "resource_id": "special-ecs1-with-public-ip-with-tag",
  "resource_name": "ecs1-with-public-ip-with-tag",
  "resource_provider": "ecs",
  "resource_type": "cloudservers",
  "trigger_type": "resource",
  "compliance_state": "NonCompliant",
  "policy_assignment_id": "5fa9f8a2501013093a192b07",
  "policy_definition_id": "5fa9f8a2501013093a192b06",
  "evaluation_time": 1604974757084
}
```

3.5 系统内置预设策略

3.5.1 预设策略列表

当您在配置审计控制台添加合规规则时，可以直接选用系统内置的预设合规策略。

当前配置审计服务支持的预设策略如下表所示。

表 3-8 配置审计支持的预设策略

云服务	预设策略	触发方式	评估资源
公共可用预设策略	资源名称满足正则表达式	配置变更	全部资源
	资源具有所有指定的标签键	配置变更	支持标签的云服务和资源类型

云服务	预设策略	触发方式	评估资源
	资源存在任一指定的标签	配置变更	支持标签的云服务和资源类型
	资源具有指定前后缀的标签键	配置变更	支持标签的云服务和资源类型
	资源标签非空	配置变更	支持标签的云服务和资源类型
	资源具有指定的标签	配置变更	支持标签的云服务和资源类型
	资源属于指定企业项目ID	配置变更	全部资源
	资源在指定区域内	配置变更	全部资源
API网关 APIG	APIG专享版实例配置安全认证类型	配置变更	apig.instances
	APIG专享版实例配置访问日志	配置变更	apig.instances
	APIG专享版实例域名均关联SSL证书	配置变更	apig.instances
部署 CodeArts Deploy	CodeArts项目下的主机集群为可用状态	配置变更	codeartsdeploy.host-cluster
MapReduce服务 MRS	MRS资源属于指定安全组	配置变更	mrs.mrs
	MRS资源属于指定VPC	配置变更	mrs.mrs
	MRS集群开启kerberos认证	配置变更	mrs.mrs
	MRS集群使用多AZ部署	配置变更	mrs.mrs
	MRS集群未绑定公网IP	配置变更	mrs.mrs
NAT网关 NAT	NAT私网网关绑定指定VPC资源	配置变更	nat.privateNatGateways
VPC终端节点 VPCEP	创建了指定服务名的终端节点	周期触发	vpcep.endpoints
Web应用防火墙 WAF	WAF防护域名配置防护策略	配置变更	waf.instance

云服务	预设策略	触发方式	评估资源
弹性负载均衡 ELB	ELB资源不具有公网IP	配置变更	elb.loadbalancers
	ELB监听器配置指定预定义安全策略	配置变更	elb.loadbalancers
	ELB监听器配置HTTPS监听协议	配置变更	elb.loadbalancers
	ELB后端服务器权重检查	配置变更	elb.members
弹性公网IP EIP	EIP带宽限制	配置变更	vpc.publicips
	弹性公网IP未进行任何绑定	配置变更	vpc.publicips
	EIP在指定天数内绑定到资源实例	周期触发	vpc.publicips
弹性伸缩 AS	弹性伸缩组均衡扩容	配置变更	as.scalingGroups
	弹性伸缩组使用弹性负载均衡健康检查	配置变更	as.scalingGroups
	弹性伸缩组启用多AZ部署	配置变更	as.scalingGroups
弹性文件服务器 SFS	弹性文件服务通过KMS进行加密	配置变更	sfsturbo.shares
弹性云服务器 ECS	ECS资源规格在指定的范围	配置变更	ecs.cloudservers
	ECS实例的镜像ID在指定的范围	配置变更	ecs.cloudservers
	ECS的镜像在指定Tag的IMS的范围内	配置变更	ecs.cloudservers
	绑定指定标签的ECS关联在指定安全组ID列表内	配置变更	ecs.cloudservers
	ECS资源属于指定虚拟私有云ID	配置变更	ecs.cloudservers
	ECS资源配置秘钥对	配置变更	ecs.cloudservers
	ECS资源不能公网访问	配置变更	ecs.cloudservers
	检查ECS资源是否具有多个公网IP	配置变更	ecs.cloudservers

云服务	预设策略	触发方式	评估资源
	关机状态的ECS未进行任意操作的时间检查	周期触发	ecs.cloudservers
分布式缓存服务 DCS	DCS Memcached资源支持SSL	配置变更	dcs.memcached
	DCS Memcached资源属于指定虚拟私有云ID	配置变更	dcs.memcached
	DCS Memcached资源不存在公网IP	配置变更	dcs.memcached
	DCS Memcached资源需要密码访问	配置变更	dcs.memcached
	DCS Redis实例支持SSL	配置变更	dcs.redis
	DCS Redis实例高可用	配置变更	dcs.redis
	DCS Redis实例属于指定虚拟私有云ID	配置变更	dcs.redis
	DCS Redis实例不存在公网IP	配置变更	dcs.redis
	DCS Redis实例需要密码访问	配置变更	dcs.redis
函数工作流 FunctionGraph	函数工作流的函数并发数在指定范围内	配置变更	fgs.functions
	函数工作流使用指定VPC	配置变更	fgs.functions
	函数工作流的函数不允许访问公网	配置变更	fgs.functions
	检查函数工作流参数设置	配置变更	fgs.functions
内容分发网络 CDN	CDN使用HTTPS证书	配置变更	cdn.domains
	CDN回源方式使用HTTPS	配置变更	cdn.domains
	CDN安全策略检查	配置变更	cdn.domains
	CDN使用自有证书	配置变更	cdn.domains
配置审计 Config	账号开启资源记录器	周期触发	config.trackers
数据仓库服务 DWS	DWS集群启用KMS加密	配置变更	dws.clusters
	DWS集群启用日志转储	配置变更	dws.clusters

云服务	预设策略	触发方式	评估资源
	DWS集群启用自动快照	配置变更	dws.clusters
	DWS集群启用SSL加密连接	配置变更	dws.clusters
数据复制服务 DRS	数据复制服务实时灾备任务不使用公网网络	配置变更	drs.dataGuardJob
	数据复制服务实时迁移任务不使用公网网络	配置变更	drs.migrationJob
	数据复制服务实时同步任务不使用公网网络	配置变更	drs.synchronizationJob
数据加密服务 DEW	KMS密钥不处于“计划删除”状态	配置变更	kms.keys
	KMS密钥启用密钥轮换	配置变更	kms.keys
统一身份认证服务 IAM	IAM用户的AccessKey在指定时间内轮换	周期触发	iam.users
	IAM策略中不存在KMS的任一阻拦action	配置变更	iam.roles&iam.policies
	IAM用户组添加了IAM用户	配置变更	iam.groups
	IAM用户密码策略符合要求	配置变更	iam.users
	IAM策略黑名单检查	配置变更	iam.users、iam.groups、iam.agencies
	IAM策略不具备Admin权限	配置变更	iam.roles、iam.policies
	IAM自定义策略具备所有权限	配置变更	iam.roles、iam.policies
	IAM账号存在可使用的访问密钥	周期触发	iam.users
	IAM用户访问模式	配置变更	iam.users
	IAM用户创建时设置AccessKey	配置变更	iam.users
	IAM用户归属用户组	配置变更	iam.users

云服务	预设策略	触发方式	评估资源
	IAM用户在指定时间内有登录行为	周期触发	iam.users
	IAM用户开启MFA	配置变更	iam.users
	IAM用户单访问密钥	配置变更	iam.users
	Console侧密码登录的IAM用户开启MFA认证	配置变更	iam.users
	根账号开启MFA认证	周期触发	iam.users
文档数据库服务 DDS	DDS实例开启SSL	配置变更	dds.instances
	DDS实例属于指定实例类型	配置变更	dds.instances
	DDS实例未绑定公网IP	配置变更	dds.instances
	DDS实例属于指定虚拟私有云ID	配置变更	dds.instances
消息通知服务 SMN	SMN主题配置访问日志	配置变更	smn.topic
虚拟私有云 VPC	未与子网关联的网络ACL	配置变更	vpc.firewallGroups
	默认安全组关闭出、入方向流量	配置变更	vpc.securityGroups
	VPC启用流日志	配置变更	vpc.vpcs
	安全组端口检查	配置变更	vpc.securityGroups
	安全组入站流量限制指定端口	配置变更	vpc.securityGroups
	安全组入站流量限制SSH端口	配置变更	vpc.securityGroups
虚拟专用网络 VPN	VPN连接状态为“正常”	配置变更	vpnaas.vpnConnections、vpnaas.ipsec-site-connections
云监控服务 CES	CES启用告警操作	配置变更	ces.alarms
	CES配置监控KMS禁用或计划删除的事件监控告警	周期触发	ces.alarms

云服务	预设策略	触发方式	评估资源
	CES配置监控OBS桶策略变更的事件监控告警	周期触发	ces.alarms
	指定的资源类型绑定指定指标CES告警	周期触发	ces.alarms
	检查特定指标的CES告警进行特定配置	配置变更	ces.alarms
	CES配置监控VPC变更的事件监控告警	周期触发	ces.alarms
云容器引擎 CCE	CCE集群版本为处于维护的版本	配置变更	cce.clusters
	CCE集群运行的非受支持的最旧版本	配置变更	cce.clusters
	CCE集群资源不具有公网IP	配置变更	cce.clusters
云审计服务 CTS	CTS追踪器通过KMS进行加密	配置变更	cts.trackers
	CTS追踪器启用事件分析	配置变更	cts.trackers
	CTS追踪器追踪指定的OBS桶	周期触发	cts.trackers
	CTS追踪器打开事件文件校验	配置变更	cts.trackers
	创建并启用CTS追踪器	周期触发	cts.trackers
	在指定区域创建并启用CTS追踪器	周期触发	cts.trackers
云数据库 RDS	GaussDB资源属于指定虚拟私有云ID	配置变更	gaussdb.instance
	GaussDB NoSQL部署在单个可用区	配置变更	nosql.instances
	GaussDB NoSQL开启备份	配置变更	nosql.instances
	GaussDB NoSQL使用磁盘加密	配置变更	nosql.instances
	GaussDB NoSQL开启错误日志	配置变更	nosql.instances
	GaussDB NoSQL支持慢查询日志	配置变更	nosql.instances

云服务	预设策略	触发方式	评估资源
	GaussDB实例开启审计日志	配置变更	gaussdb.instance
	GaussDB实例开启自动备份	配置变更	gaussdb.instance
	GaussDB实例开启错误日志	配置变更	gaussdb.instance
	GaussDB实例开启慢日志	配置变更	gaussdb.instance
	GaussDB for MySQL实例开启审计日志	配置变更	gaussdb.instance
	GaussDB for MySQL实例开启备份	配置变更	gaussdb.instance
	GaussDB for MySQL实例开启错误日志	配置变更	gaussdb.instance
	GaussDB for MySQL实例开启慢日志	配置变更	gaussdb.instance
	RDS实例开启备份	配置变更	rds.instances
	RDS实例开启错误日志	配置变更	rds.instances
	RDS实例开启慢日志	配置变更	rds.instances
	RDS实例支持多可用区	配置变更	rds.instances
	RDS实例不具有公网IP	配置变更	rds.instances
	RDS实例开启存储加密	配置变更	rds.instances
	RDS实例属于指定虚拟私有云ID	配置变更	rds.instances
	RDS实例配备日志	配置变更	rds.instances
云搜索服务 CSS	CSS集群启用认证	配置变更	css.clusters
	CSS集群启用快照	配置变更	css.clusters
	CSS集群开启磁盘加密	配置变更	css.clusters

云服务	预设策略	触发方式	评估资源
	CSS集群启用HTTPS	配置变更	css.clusters
	CSS集群绑定指定VPC资源	配置变更	css.clusters
	CSS集群具备多AZ容灾	配置变更	css.clusters
	CSS集群具备多实例容灾	配置变更	css.clusters
	CSS集群不能公网访问	配置变更	css.clusters
	CSS集群开启安全模式	配置变更	css.clusters
	CSS集群白名单不生效	配置变更	css.clusters
	CSS集群kibana白名单不生效	配置变更	css.clusters
云硬盘 EVS	云硬盘的类型在指定的范围内	配置变更	evs.volumes
	云硬盘创建后在指定天数内绑定资源实例	周期触发	evs.volumes
	云硬盘闲置检测	配置变更	evs.volumes
	已挂载的云硬盘开启加密	配置变更	evs.volumes
云证书管理服务 CCM	检查私有CA是否过期	周期触发	pca.ca
	检查私有证书是否过期	周期触发	pca.cert
分布式消息服务Kafka版	DMS Kafka队列打开内网SSL加密访问	配置变更	dms.kafkas
	DMS Kafka队列打开公网SSL加密访问	配置变更	dms.kafkas
	DMS Kafka队列开启公网访问	配置变更	dms.kafkas
分布式消息服务RabbitMQ版	DMS RabbitMq队列打开SSL加密访问	配置变更	dms.rabbitmqs
分布式消息服务RocketMQ版	DMS Reliability队列打开SSL加密访问	配置变更	dms.reliabilitys

3.5.2 公共可用预设策略

3.5.2.1 资源名称满足正则表达式

规则详情

表 3-9 规则详情

参数	说明
规则名称	regular-matching-of-names
规则展示名	资源名称满足正则表达式
规则描述	资源名称不满足正则表达式，视为“不合规”。
标签	name
规则触发方式	配置变更
规则评估的资源类型	全部资源
规则参数	regularExpression：指定要匹配的正则表达式，“%”表示任意个字符，“_”表示任意一个字符。

3.5.2.2 资源具有所有指定的标签键

规则详情

表 3-10 规则详情

参数	说明
规则名称	required-all-tags
规则展示名	资源具有所有指定的标签键
规则描述	指定标签列表，不具有所有指定标签键的资源，视为“不合规”。
标签	tag
规则触发方式	配置变更
规则评估的资源类型	**支持标签的云服务和资源类型**
规则参数	• TagKeys：允许的标签键列表。 • TagValues：允许的标签值列表，空列表代表全部允许。

3.5.2.3 资源存在任一指定的标签

规则详情

表 3-11 规则详情

参数	说明
规则名称	required-tag-exist
规则展示名	资源存在任一指定的标签
规则描述	指定标签列表，不具有任一指定标签的资源，视为“不合规”。
标签	tag
规则触发方式	配置变更
规则评估的资源类型	**支持标签的云服务和资源类型**
规则参数	• TagKeys：允许的标签键列表。 • TagValues：允许的标签值列表，空列表代表全部允许。

3.5.2.4 资源具有指定前后缀的标签键

规则详情

表 3-12 规则详情

参数	说明
规则名称	resource-tag-key-prefix-suffix
规则展示名	资源具有指定前后缀的标签键
规则描述	指定标签键的前缀和后缀，资源不具有任意匹配前后缀的标签键，视为“不合规”。
标签	tag
规则触发方式	配置变更
规则评估的资源类型	**支持标签的云服务和资源类型**
规则参数	• tagKeyPrefix：允许的标签键前缀，空字符串表示全部允许。 • tagKeySuffix：允许的标签键后缀，空字符串表示全部允许。

3.5.2.5 资源标签非空

规则详情

表 3-13 规则详情

参数	说明
规则名称	resource-tag-not-empty
规则展示名	资源标签非空
规则描述	资源未配置标签，视为“不合规”。
标签	tag
规则触发方式	配置变更
规则评估的资源类型	**支持标签的云服务和资源类型**
规则参数	无

3.5.2.6 资源具有指定的标签

规则详情

表 3-14 规则详情

参数	说明
规则名称	required-tag-check
规则展示名	资源具有指定的标签
规则描述	指定一个标签，不具有此标签的资源，视为“不合规”。
标签	tag
规则触发方式	配置变更
规则评估的资源类型	**支持标签的云服务和资源类型**
规则参数	• specifiedTagKey：指定的标签键，字符串类型。 • specifiedTagValue：指定的标签值列表，如果列表为空，表示允许所有值，数组类型，最多包含10个元素。

3.5.2.7 资源属于指定企业项目 ID

规则详情

表 3-15 规则详情

参数	说明
规则名称	resource-in-enterprise-project
规则展示名	资源属于指定企业项目ID
规则描述	指定企业项目ID，属于该企业项目的资源，视为“不合规”。
标签	enterprise project
规则触发方式	配置变更
规则评估的资源类型	全部资源
规则参数	epId：企业项目ID，字符串类型。

3.5.2.8 资源在指定区域内

规则详情

表 3-16 规则详情

参数	说明
规则名称	resources-in-supported-region
规则展示名	资源在指定区域内
规则描述	资源不在指定区域内，视为“不合规”。
标签	region
规则触发方式	配置变更
规则评估的资源类型	全部资源
规则参数	regions：指定区域列表，数组类型。全局资源的region为“global”。

3.5.3 API 网关 APIG

3.5.3.1 APIG 专享版实例配置安全认证类型

规则详情

表 3-17 规则详情

参数	说明
规则名称	apig-instances-authorization-type-configured
规则展示名	APIG专享版实例配置安全认证类型
规则描述	APIG专享版实例中如果存在API安全认证为“无认证”，则视为“不合规”。
标签	apig
规则触发方式	配置变更
规则评估的资源类型	apig.instances
规则参数	无

3.5.3.2 APIG 专享版实例配置访问日志

规则详情

表 3-18 规则详情

参数	说明
规则名称	apig-instances-execution-logging-enabled
规则展示名	APIG专享版实例配置访问日志
规则描述	APIG专享版实例未配置访问日志，视为“不合规”。
标签	apig
规则触发方式	配置变更
规则评估的资源类型	apig.instances
规则参数	无

3.5.3.3 APIG 专享版实例域名均关联 SSL 证书

规则详情

表 3-19 规则详情

参数	说明
规则名称	apig-instances-ssl-enabled
规则展示名	APIG专享版实例域名均关联SSL证书
规则描述	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”。
标签	apig
规则触发方式	配置变更
规则评估的资源类型	apig.instances
规则参数	无

3.5.4 部署 CodeArts Deploy

3.5.4.1 CodeArts 项目下的主机集群为可用状态

规则详情

表 3-20 规则详情

参数	说明
规则名称	codeartsdeploy-host-cluster-resource-status
规则展示名	CodeArts项目下的主机集群为可用状态
规则描述	codearts项目下的主机集群如果状态不可用，则该主机集群视为“不合规”。
标签	codeartsdeploy
规则触发方式	配置变更
规则评估的资源类型	codeartsdeploy.host-cluster
规则参数	无

3.5.5 MapReduce 服务 MRS

3.5.5.1 MRS 资源属于指定安全组

规则详情

表 3-21 规则详情

参数	说明
规则名称	mrs-cluster-in-allowed-security-groups
规则展示名	MRS资源属于指定安全组
规则描述	指定安全组ID，不属于此安全组的MRS集群，视为“不合规”。
标签	mrs
规则触发方式	配置变更
规则评估的资源类型	mrs.mrs
规则参数	mrsSecurityGroupsId：指定的安全组ID列表，数组类型。

3.5.5.2 MRS 资源属于指定 VPC

规则详情

表 3-22 规则详情

参数	说明
规则名称	mrs-cluster-in-vpc
规则展示名	MRS资源属于指定VPC
规则描述	指定虚拟私有云ID，不属于此VPC的MRS集群，视为“不合规”。
标签	mrs
规则触发方式	配置变更
规则评估的资源类型	mrs.mrs
规则参数	vpcId：虚拟私有云ID，字符串类型。

3.5.5.3 MRS 集群开启 kerberos 认证

规则详情

表 3-23 规则详情

参数	说明
规则名称	mrs-cluster-kerberos-enabled
规则展示名	MRS集群开启kerberos认证
规则描述	MRS集群未开启kerberos认证，视为“不合规”。
标签	mrs
规则触发方式	配置变更
规则评估的资源类型	mrs.mrs
规则参数	无

3.5.5.4 MRS 集群使用多 AZ 部署

规则详情

表 3-24 规则详情

参数	说明
规则名称	mrs-cluster-multiAZ-deployment
规则展示名	MRS集群使用多AZ部署
规则描述	MRS集群没有多AZ部署，视为“不合规”。
标签	mrs
规则触发方式	配置变更
规则评估的资源类型	mrs.mrs
规则参数	无

3.5.5.5 MRS 集群未绑定公网 IP

规则详情

表 3-25 规则详情

参数	说明
规则名称	mrs-cluster-no-public-ip
规则展示名	MRS集群未绑定公网IP
规则描述	MRS集群绑定公网IP，视为“不合规”。
标签	mrs
规则触发方式	配置变更
规则评估的资源类型	mrs.mrs
规则参数	无

3.5.6 NAT 网关 NAT

3.5.6.1 NAT 私网网关绑定指定 VPC 资源

规则详情

表 3-26 规则详情

参数	说明
规则名称	private-nat-gateway-authorized-vpc-only
规则展示名	NAT私网网关绑定指定VPC资源
规则描述	私网NAT网关未与指定的VPC资源绑定，视为“不合规”。
标签	nat
规则触发方式	配置变更
规则评估的资源类型	nat.privateNatGateways
规则参数	authorizedVpcIds：指定的虚拟私有云ID列表，如果列表为空，表示允许所有值；数组类型，最多包含10个元素。

3.5.7 VPC 终端节点 VPCEP

3.5.7.1 创建了指定服务名的终端节点

规则详情

表 3-27 规则详情

参数	说明
规则名称	vpcep-endpoint-enabled
规则展示名	创建了指定服务名的终端节点
规则描述	检查是否已创建指定服务名的终端节点，如果未创建则视为“不合规”。
标签	vpcep
规则触发方式	周期触发
规则评估的资源类型	vpcep.endpoints
规则参数	serviceName：指定服务名的终端节点。

3.5.8 Web 应用防火墙 WAF

3.5.8.1 WAF 防护域名配置防护策略

规则详情

表 3-28 规则详情

参数	说明
规则名称	waf-instance-policy-not-empty
规则展示名	WAF防护域名配置防护策略
规则描述	WAF防护域名未配置防护策略，视为“不合规”。
标签	waf
规则触发方式	配置变更
规则评估的资源类型	waf.instance
规则参数	无

3.5.9 弹性负载均衡 ELB

3.5.9.1 ELB 资源不具有公网 IP

规则详情

表 3-29 规则详情

参数	说明
规则名称	elb-loadbalancers-no-public-ip
规则展示名	ELB资源不具有公网IP
规则描述	ELB资源具有公网IP，视为“不合规”。
标签	elb
规则触发方式	配置变更
规则评估的资源类型	elb.loadbalancers
规则参数	无

3.5.9.2 ELB 监听器配置指定预定义安全策略

规则详情

表 3-30 规则详情

参数	说明
规则名称	elb-predefined-security-policy-https-check
规则展示名	ELB监听器配置指定预定义安全策略
规则描述	独享型负载均衡器关联的HTTPS协议类型监听器未配置指定的预定义安全策略，视为“不合规”。
标签	elb
规则触发方式	配置变更
规则评估的资源类型	elb.loadbalancers
规则参数	predefinedPolicyName：指定的预定义安全策略名称，默认值为tls-1-0。 支持的枚举值：tls-1-0、tls-1-1、tls-1-2、tls-1-0-inherit、tls-1-2-strict、tls-1-0-with-1-3、tls-1-2-fs-with-1-3、tls-1-2-fs、hybrid-policy-1-0。更多信息请参见**TLS安全策略**。

3.5.9.3 ELB 监听器配置 HTTPS 监听协议

规则详情

表 3-31 规则详情

参数	说明
规则名称	elb-tls-https-listeners-only
规则展示名	ELB监听器配置HTTPS监听协议
规则描述	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”。
标签	elb
规则触发方式	配置变更
规则评估的资源类型	elb.loadbalancers
规则参数	无

3.5.9.4 ELB 后端服务器权重检查

规则详情

表 3-32 规则详情

参数	说明
规则名称	elb-members-weight-check
规则展示名	ELB后端服务器权重检查
规则描述	后端服务器的权重为0，且其所属的后端服务器组的负载均衡算法不为“SOUCE_IP”时，视为“不合规”。
标签	elb
规则触发方式	配置变更
规则评估的资源类型	elb.members
规则参数	weight：后端云服务器的权重，请求将根据后端服务器组配置的负载均衡算法和后端云服务器的权重进行负载分发。 权重值越大，分发的请求越多。 取值范围：0-100。

3.5.10 弹性公网 IP EIP

3.5.10.1 EIP 带宽限制

规则详情

表 3-33 规则详情

参数	说明
规则名称	eip-bandwidth-limit
规则展示名	EIP带宽限制
规则描述	弹性公网IP实例可用带宽小于指定参数值，视为“不合规”。
标签	eip
规则触发方式	配置变更
规则评估的资源类型	vpc.publicips
规则参数	bandwidthSize：指定的弹性公网IP带宽大小，单位为Mbit/s，字符串类型。

3.5.10.2 弹性公网 IP 未进行任何绑定

规则详情

表 3-34 规则详情

参数	说明
规则名称	eip-unbound-check
规则展示名	弹性公网IP未进行任何绑定
规则描述	弹性公网IP未进行任何绑定，视为“不合规”。
标签	vpc
规则触发方式	配置变更
规则评估的资源类型	vpc.publicips
规则参数	无

3.5.10.3 EIP 在指定天数内绑定到资源实例

规则详情

表 3-35 规则详情

参数	说明
规则名称	eip-use-in-specified-days
规则展示名	EIP在指定天数内绑定到资源实例
规则描述	EIP创建后在指定天数内未使用，视为“不合规”。
标签	eip
规则触发方式	周期触发
规则评估的资源类型	vpc.publicips
规则参数	allowDays：指定允许的天数，数值类型。

3.5.11 弹性伸缩 AS

3.5.11.1 弹性伸缩组均衡扩容

规则详情

表 3-36 规则详情

参数	说明
规则名称	as-capacity-rebalancing
规则展示名	弹性伸缩组均衡扩容
规则描述	弹性伸缩组扩缩容时，没有使用“EQUILIBRIUM_DISTRIBUTE”优先级策略，视为“不合规”。
标签	as
规则触发方式	配置变更
规则评估的资源类型	as.scalingGroups
规则参数	无

3.5.11.2 弹性伸缩组使用弹性负载均衡健康检查

规则详情

表 3-37 规则详情

参数	说明
规则名称	as-group-elb-healthcheck-required
规则展示名	弹性伸缩组使用弹性负载均衡健康检查
规则描述	与负载均衡器关联的伸缩组未使用弹性负载均衡健康检查，视为“不合规”。
标签	as
规则触发方式	配置变更
规则评估的资源类型	as.scalingGroups
规则参数	无

3.5.11.3 弹性伸缩组启用多 AZ 部署

规则详情

表 3-38 规则详情

参数	说明
规则名称	as-multiple-az
规则展示名	弹性伸缩组启用多AZ部署
规则描述	弹性伸缩组没有启用多AZ部署，视为“不合规”。
标签	as
规则触发方式	配置变更
规则评估的资源类型	as.scalingGroups
规则参数	无

3.5.12 弹性文件服务器 SFS

3.5.12.1 弹性文件服务通过 KMS 进行加密

规则详情

表 3-39 规则详情

参数	说明
规则名称	sfsturbo-encrypted-check
规则展示名	弹性文件服务通过KMS进行加密
规则描述	弹性文件服务（SFS Turbo）未通过KMS进行加密，视为“不合规”。
标签	sfsturbo
规则触发方式	配置变更
规则评估的资源类型	sfsturbo.shares
规则参数	无

3.5.13 弹性云服务器 ECS

3.5.13.1 ECS 资源规格在指定的范围

规则详情

表 3-40 规则详情

参数	说明
规则名称	allowed-ecs-flavors
规则展示名	ECS资源规格在指定的范围
规则描述	ECS资源的规格不在指定的范围内，视为“不合规”。
标签	ecs
规则触发方式	配置变更
规则评估的资源类型	ecs.cloudservers
规则参数	listOfAllowedFlavors：允许的ECS资源的规格列表，数组类型，最多包含10个元素。字段可选值查询ECS文档获取，例如：s6.small.1、s6.xlarge.2、m7.large.8、t6.small.1。

3.5.13.2 ECS 实例的镜像 ID 在指定的范围

规则详情

表 3-41 规则详情

参数	说明
规则名称	allowed-images-by-id
规则展示名	ECS实例的镜像ID在指定的范围
规则描述	指定允许的镜像ID列表，ECS实例的镜像ID不在指定的范围内，视为“不合规”。
标签	ecs、ims
规则触发方式	配置变更
规则评估的资源类型	ecs.cloudservers
规则参数	listOfAllowedImages：允许的镜像ID列表，数组类型，最多包含10个元素。

3.5.13.3 ECS 的镜像在指定 Tag 的 IMS 的范围内

规则详情

表 3-42 规则详情

参数	说明
规则名称	approved-ims-by-tag
规则展示名	ECS的镜像在指定Tag的IMS的范围内
规则描述	ECS云主机的镜像不在指定Tag的IMS镜像的范围内，视为“不合规”。
标签	ecs、ims
规则触发方式	配置变更
规则评估的资源类型	ecs.cloudservers
规则参数	• specifiedIMSTagKey：指定的IMS镜像的标签键，字符串类型。 • specifiedIMSTagValue：指定的IMS镜像的标签值列表，如果列表为空，表示允许所有值，数组类型，最多包含10个元素。

3.5.13.4 绑定指定标签的 ECS 关联在指定安全组 ID 列表内

规则详情

表 3-43 规则详情

参数	说明
规则名称	ecs-in-allowed-security-groups
规则展示名	绑定指定标签的ECS关联在指定安全组ID列表内
规则描述	指定高危安全组ID列表，未绑定指定标签的ECS资源关联其中任意安全组，视为“不合规”。
标签	ecs
规则触发方式	配置变更
规则评估的资源类型	ecs.cloudservers
规则参数	• specifiedECSTagKey：指定的ECS的标签键，字符串类型。 • specifiedECSTagValue：指定的ECS的标签值列表，如果列表为空，表示允许所有值，数组类型，最多包含10个元素。 • specifiedSecurityGroupIds：指定的高危安全组的ID列表，数组类型，最多包含10个元素。

3.5.13.5 ECS 资源属于指定虚拟私有云 ID

规则详情

表 3-44 规则详情

参数	说明
规则名称	ecs-instance-in-vpc
规则展示名	ECS资源属于指定虚拟私有云ID
规则描述	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”。
标签	ecs、vpc
规则触发方式	配置变更
规则评估的资源类型	ecs.cloudservers
规则参数	vpcId：虚拟私有云ID，字符串类型。

3.5.13.6 ECS 资源配置秘钥对

规则详情

表 3-45 规则详情

参数	说明
规则名称	ecs-instance-key-pair-login
规则展示名	ECS资源配置秘钥对
规则描述	ECS未配置密钥对，视为“不合规”。
标签	ecs
规则触发方式	配置变更
规则评估的资源类型	ecs.cloudservers
规则参数	无

3.5.13.7 ECS 资源不能公网访问

规则详情

表 3-46 规则详情

参数	说明
规则名称	ecs-instance-no-public-ip
规则展示名	ECS资源不能公网访问
规则描述	ECS资源具有公网IP，视为“不合规”。
标签	ecs
规则触发方式	配置变更
规则评估的资源类型	ecs.cloudservers
规则参数	无

3.5.13.8 检查 ECS 资源是否具有多个公网 IP

规则详情

表 3-47 规则详情

参数	说明
规则名称	ecs-multiple-public-ip-check
规则展示名	检查ECS资源是否具有多个公网IP
规则描述	ECS云主机资源具有多个公网IP，视为“不合规”。
标签	ecs
规则触发方式	配置变更
规则评估的资源类型	ecs.cloudservers
规则参数	无

3.5.13.9 关机状态的 ECS 未进行任意操作的时间检查

规则详情

表 3-48 规则详情

参数	说明
规则名称	stopped-ecs-date-diff
规则展示名	关机状态的ECS未进行任意操作的时间检查
规则描述	关机状态的ECS云主机未进行任何操作的时间超过了允许的天数，视为“不合规”。
标签	ecs
规则触发方式	周期触发
规则评估的资源类型	ecs.cloudservers
规则参数	allowDays：指定允许的天数，字符串类型。

3.5.14 分布式缓存服务 DCS

3.5.14.1 DCS Memcached 资源支持 SSL

规则详情

表 3-49 规则详情

参数	说明
规则名称	dcs-memcached-enable-ssl
规则展示名	DCS Memcached资源支持SSL
规则描述	DCS Memcached资源可以公网访问，但不支持SSL时，视为“不合规”。
标签	dcs
规则触发方式	配置变更
规则评估的资源类型	dcs.memcached
规则参数	无

3.5.14.2 DCS Memcached 资源属于指定虚拟私有云 ID

规则详情

表 3-50 规则详情

参数	说明
规则名称	dcs-memcached-in-vpc
规则展示名	DCS Memcached资源属于指定虚拟私有云ID
规则描述	指定虚拟私有云ID，不属于此VPC的DCS Memcached资源，视为“不合规”。
标签	dcs
规则触发方式	配置变更
规则评估的资源类型	dcs.memcached
规则参数	vpcId：虚拟私有云ID，字符串类型。

3.5.14.3 DCS Memcached 资源不存在公网 IP

规则详情

表 3-51 规则详情

参数	说明
规则名称	dcs-memcached-no-public-ip
规则展示名	DCS Memcached资源不存在公网IP
规则描述	DCS Memcached资源存在公网IP时，视为“不合规”。
标签	dcs
规则触发方式	配置变更
规则评估的资源类型	dcs.memcached
规则参数	无

3.5.14.4 DCS Memcached 资源需要密码访问

规则详情

表 3-52 规则详情

参数	说明
规则名称	dcs-memcached-password-access
规则展示名	DCS Memcached资源需要密码访问
规则描述	DCS Memcached资源不需要密码访问，视为“不合规”。
标签	dcs
规则触发方式	配置变更
规则评估的资源类型	dcs.memcached
规则参数	无

3.5.14.5 DCS Redis 实例支持 SSL

规则详情

表 3-53 规则详情

参数	说明
规则名称	dcs-redis-enable-ssl
规则展示名	DCS Redis实例支持SSL
规则描述	DCS Redis资源可以公网访问，但不支持SSL时，视为“不合规”。
标签	dcs
规则触发方式	配置变更
规则评估的资源类型	dcs.redis
规则参数	无

3.5.14.6 DCS Redis 实例高可用

规则详情

表 3-54 规则详情

参数	说明
规则名称	dcs-redis-high-tolerance
规则展示名	DCS Redis实例高可用
规则描述	DCS Redis资源不是高可用时，视为“不合规”。
标签	dcs
规则触发方式	配置变更
规则评估的资源类型	dcs.redis
规则参数	无

3.5.14.7 DCS Redis 实例属于指定虚拟私有云 ID

规则详情

表 3-55 规则详情

参数	说明
规则名称	dcs-redis-in-vpc
规则展示名	DCS Redis实例属于指定虚拟私有云ID
规则描述	指定虚拟私有云ID，不属于此VPC的DCS Redis资源，视为“不合规”。
标签	dcs
规则触发方式	配置变更
规则评估的资源类型	dcs.redis
规则参数	vpcId：虚拟私有云ID，字符串类型。

3.5.14.8 DCS Redis 实例不存在公网 IP

规则详情

表 3-56 规则详情

参数	说明
规则名称	dcs-redis-no-public-ip
规则展示名	DCS Redis实例不存在公网IP
规则描述	DCS Redis资源存在公网IP时，视为“不合规”。
标签	dcs
规则触发方式	配置变更
规则评估的资源类型	dcs.redis
规则参数	无

3.5.14.9 DCS Redis 实例需要密码访问

规则详情

表 3-57 规则详情

参数	说明
规则名称	dcs-redis-password-access
规则展示名	DCS Redis实例需要密码访问
规则描述	DCS Redis资源不需要密码访问，视为“不合规”。
标签	dcs
规则触发方式	配置变更
规则评估的资源类型	dcs.redis
规则参数	无

3.5.15 函数工作流 FunctionGraph

3.5.15.1 函数工作流的函数并发数在指定范围内

规则详情

表 3-58 规则详情

参数	说明
规则名称	function-graph-concurrency-check
规则展示名	函数工作流的函数并发数在指定范围内
规则描述	FunctionGraph函数的并发数不在指定的范围内，视为“不合规”。
标签	fgs
规则触发方式	配置变更
规则评估的资源类型	fgs.functions
规则参数	• concurrencyLimitLow： 最小并发数，整数类型。 • concurrencyLimitHigh：最高并发数，整数类型。

3.5.15.2 函数工作流使用指定 VPC

规则详情

表 3-59 规则详情

参数	说明
规则名称	function-graph-inside-vpc
规则展示名	函数工作流使用指定VPC
规则描述	函数工作流未使用指定VPC，视为“不合规”。
标签	fgs
规则触发方式	配置变更
规则评估的资源类型	fgs.functions
规则参数	vpcId：虚拟私有云ID，字符串类型。

3.5.15.3 函数工作流的函数不允许访问公网

规则详情

表 3-60 规则详情

参数	说明
规则名称	function-graph-public-access-prohibited
规则展示名	函数工作流的函数不允许访问公网
规则描述	函数工作流的函数允许访问公网，视为“不合规”。
标签	fgs
规则触发方式	配置变更
规则评估的资源类型	fgs.functions
规则参数	无

3.5.15.4 检查函数工作流参数设置

规则详情

表 3-61 规则详情

参数	说明
规则名称	function-graph-settings-check
规则展示名	检查函数工作流参数设置
规则描述	函数工作流的运行时、超时时间、内存限制不在指定范围内，视为“不合规”。
标签	fgs
规则触发方式	配置变更
规则评估的资源类型	fgs.functions
规则参数	• runtimeList：指定的运行时列表，数组类型。 • timout：最大执行超时事件（秒），整数类型。 • memorySize：最大内存限制（MB），整数类型。

3.5.16 内容分发网络 CDN

3.5.16.1 CDN 使用 HTTPS 证书

规则详情

表 3-62 规则详情

参数	说明
规则名称	cdn-enable-https-certificate
规则展示名	CDN使用HTTPS证书
规则描述	CDN未使用HTTPS证书，视为“不合规”。
标签	cdn
规则触发方式	配置变更
规则评估的资源类型	cdn.domains
规则参数	无

3.5.16.2 CDN 回源方式使用 HTTPS

规则详情

表 3-63 规则详情

参数	说明
规则名称	cdn-origin-protocol-no-http
规则展示名	CDN回源方式使用HTTPS
规则描述	CDN回源方式未使用HTTPS协议，视为“不合规”。
标签	cdn
规则触发方式	配置变更
规则评估的资源类型	cdn.domains
规则参数	无

3.5.16.3 CDN 安全策略检查

规则详情

表 3-64 规则详情

参数	说明
规则名称	cdn-security-policy-check
规则展示名	CDN安全策略检查
规则描述	CDN使用TLSv1.2以下的版本，视为“不合规”。
标签	cdn
规则触发方式	配置变更
规则评估的资源类型	cdn.domains
规则参数	无

3.5.16.4 CDN 使用自有证书

规则详情

表 3-65 规则详情

参数	说明
规则名称	cdn-use-my-certificate
规则展示名	CDN使用自有证书
规则描述	CDN使用了自有证书，视为“不合规”。
标签	cdn
规则触发方式	配置变更
规则评估的资源类型	cdn.domains
规则参数	无

3.5.17 配置审计 Config

3.5.17.1 账号开启资源记录器

规则详情

表 3-66 规则详情

参数	说明
规则名称	tracker-config-enabled-check
规则展示名	账号开启资源记录器
规则描述	如果账号未开启资源记录器，视为“不合规”。
标签	config
规则触发方式	周期触发
规则评估的资源类型	config.trackers
规则参数	无

3.5.18 数据仓库服务 DWS

3.5.18.1 DWS 集群启用 KMS 加密

规则详情

表 3-67 规则详情

参数	说明
规则名称	dws-enable-kms
规则展示名	DWS集群启用KMS加密
规则描述	DWS集群未启用KMS加密，视为“不合规”。
标签	dws
规则触发方式	配置变更
规则评估的资源类型	dws.clusters
规则参数	无

3.5.18.2 DWS 集群启用日志转储

规则详情

表 3-68 规则详情

参数	说明
规则名称	dws-enable-log-dump
规则展示名	DWS集群启用日志转储
规则描述	DWS集群未启用日志转储，视为“不合规”。
标签	dws
规则触发方式	配置变更
规则评估的资源类型	dws.clusters
规则参数	无

3.5.18.3 DWS 集群启用自动快照

规则详情

表 3-69 规则详情

参数	说明
规则名称	dws-enable-snapshot
规则展示名	DWS集群启用自动快照
规则描述	DWS集群未启用自动快照，视为“不合规”。
标签	dws
规则触发方式	配置变更
规则评估的资源类型	dws.clusters
规则参数	无

3.5.18.4 DWS 集群启用 SSL 加密连接

规则详情

表 3-70 规则详情

参数	说明
规则名称	dws-enable-ssl
规则展示名	DWS集群启用SSL加密连接
规则描述	DWS集群未启用SSL加密连接，视为“不合规”。
标签	dws
规则触发方式	配置变更
规则评估的资源类型	dws.clusters
规则参数	无

3.5.19 数据复制服务 DRS

3.5.19.1 数据复制服务实时灾备任务不使用公网网络

规则详情

表 3-71 规则详情

参数	说明
规则名称	drs-data-guard-job-not-public
规则展示名	数据复制服务实时灾备任务不使用公网网络
规则描述	数据复制服务实时灾备任务使用公网网络，视为“不合规”。
标签	drs
规则触发方式	配置变更
规则评估的资源类型	drs.dataGuardJob
规则参数	无

3.5.19.2 数据复制服务实时迁移任务不使用公网网络

规则详情

表 3-72 规则详情

参数	说明
规则名称	drs-migration-job-not-public
规则展示名	数据复制服务实时迁移任务不使用公网网络
规则描述	数据复制服务实时迁移任务使用公网网络，视为“不合规”。
标签	drs
规则触发方式	配置变更
规则评估的资源类型	drs.migrationJob
规则参数	无

3.5.19.3 数据复制服务实时同步任务不使用公网网络

规则详情

表 3-73 规则详情

参数	说明
规则名称	drs-synchronization-job-not-public
规则展示名	数据复制服务实时同步任务不使用公网网络
规则描述	数据复制服务实时同步任务使用公网网络，视为“不合规”。
标签	drs
规则触发方式	配置变更
规则评估的资源类型	drs.synchronizationJob
规则参数	无

3.5.20 数据加密服务 DEW

3.5.20.1 KMS 密钥不处于“计划删除”状态

规则详情

表 3-74 规则详情

参数	说明
规则名称	kms-not-scheduled-for-deletion
规则展示名	KMS密钥不处于“计划删除”状态
规则描述	KMS密钥处于“计划删除”状态，视为“不合规”。
标签	kms
规则触发方式	配置变更
规则评估的资源类型	kms.keys
规则参数	无

3.5.20.2 KMS 密钥启用密钥轮换

规则详情

表 3-75 规则详情

参数	说明
规则名称	kms-rotation-enabled
规则展示名	KMS密钥启用密钥轮换
规则描述	KMS密钥未启用密钥轮换，视为“不合规”。
标签	kms
规则触发方式	配置变更
规则评估的资源类型	kms.keys
规则参数	无

3.5.21 统一身份认证服务 IAM

3.5.21.1 IAM 用户的 AccessKey 在指定时间内轮换

规则详情

表 3-76 规则详情

参数	说明
规则名称	access-keys-rotated
规则展示名	IAM用户的AccessKey在指定时间内轮换
规则描述	IAM用户的AK/SK访问密钥未在指定天数内更换，视为“不合规”。
标签	iam
规则触发方式	周期触发
规则评估的资源类型	iam.users
规则参数	maxAccessKeyAge：AK/SK密钥最大更换天数，默认值为90。

3.5.21.2 IAM 策略中不存在 KMS 的任一阻拦 action

规则详情

表 3-77 规则详情

参数	说明
规则名称	iam-customer-policy-blocked-kms-actions
规则展示名	IAM策略中不存在KMS的任一阻拦action
规则描述	IAM策略中存在KMS的任一阻拦action，视为“不合规”。
标签	iam
规则触发方式	配置变更
规则评估的资源类型	iam.roles、iam.policies
规则参数	blockedActionsPatterns：KMS的阻拦action列表，数组类型。

3.5.21.3 IAM 用户组添加了 IAM 用户

规则详情

表 3-78 规则详情

参数	说明
规则名称	iam-group-has-users-check
规则展示名	IAM用户组添加了IAM用户
规则描述	IAM用户组未添加任意IAM用户，视为“不合规”。
标签	iam
规则触发方式	配置变更
规则评估的资源类型	iam.groups
规则参数	无

3.5.21.4 IAM 用户密码策略符合要求

规则详情

表 3-79 规则详情

参数	说明
规则名称	iam-password-policy
规则展示名	IAM用户密码策略符合要求
规则描述	IAM用户密码强度不满足密码强度要求，视为“不合规”
标签	iam
规则触发方式	配置变更
规则评估的资源类型	iam.users
规则参数	pwdStrength：密码强度要求，参数允许值为枚举值Strong/Medium/Low，默认值为Strong。

3.5.21.5 IAM 策略黑名单检查

规则详情

表 3-80 规则详情

参数	说明
规则名称	iam-policy-blacklisted-check
规则展示名	IAM策略黑名单检查
规则描述	IAM的用户、用户组或委托存在黑名单的策略，视为“不合规”。
标签	iam
规则触发方式	配置变更
规则评估的资源类型	iam.users、iam.groups、iam.agencies
规则参数	blackListPolicyUrns：策略黑名单列表，数组类型。

3.5.21.6 IAM 策略不具备 Admin 权限

规则详情

表 3-81 规则详情

参数	说明
规则名称	iam-policy-no-statements-with-admin-access
规则展示名	IAM策略不具备Admin权限
规则描述	IAM策略中存在admin权限（Action为*:*:*或*:*或*），视为“不合规”。
标签	iam
规则触发方式	配置变更
规则评估的资源类型	iam.roles、iam.policies
规则参数	无

3.5.21.7 IAM 自定义策略具备所有权限

规则详情

表 3-82 规则详情

参数	说明
规则名称	iam-role-has-all-permissions
规则展示名	IAM自定义策略具备所有权限
规则描述	IAM自定义策略具有allow的云服务的全部权限，视为“不合规”
标签	iam
规则触发方式	配置变更
规则评估的资源类型	iam.roles、iam.policies
规则参数	无

3.5.21.8 IAM 账号存在可使用的访问密钥

规则详情

表 3-83 规则详情

参数	说明
规则名称	iam-root-access-key-check
规则展示名	IAM账号存在可使用的访问密钥
规则描述	账号有可使用的AK/SK访问密钥，视为“不合规”。
标签	iam
规则触发方式	周期触发
规则评估的资源类型	iam.users
规则参数	无

3.5.21.9 IAM 用户访问模式

规则详情

表 3-84 规则详情

参数	说明
规则名称	iam-user-access-mode
规则展示名	IAM用户访问模式
规则描述	IAM用户同时开启控制台访问和API访问，视为“不合规”。
标签	iam
规则触发方式	配置变更
规则评估的资源类型	iam.users
规则参数	无

3.5.21.10 IAM 用户创建时设置 AccessKey

规则详情

表 3-85 规则详情

参数	说明
规则名称	iam-user-console-and-api-access-at-creation
规则展示名	IAM用户创建时设置AccessKey
规则描述	对于需要登录Console的IAM用户，在其创建时设置AK/SK访问密钥，视为“不合规”。
标签	iam
规则触发方式	配置变更
规则评估的资源类型	iam.users
规则参数	无

3.5.21.11 IAM 用户归属用户组

规则详情

表 3-86 规则详情

参数	说明
规则名称	iam-user-group-membership-check
规则展示名	IAM用户归属用户组
规则描述	IAM用户不属于任意一个IAM用户组，视为“不合规”。
标签	iam
规则触发方式	配置变更
规则评估的资源类型	iam.users
规则参数	groupIds：指定的用户组ID列表，如果列表为空，表示允许所有值；数组类型，最多包含10个元素。

3.5.21.12 IAM 用户在指定时间内有登录行为

规则详情

表 3-87 规则详情

参数	说明
规则名称	iam-user-last-login-check
规则展示名	IAM用户在指定时间内有登录行为
规则描述	IAM用户在指定时间范围内无登录行为，视为“不合规”。
标签	iam
规则触发方式	周期触发
规则评估的资源类型	iam.users
规则参数	allowedInactivePeriod：指定的时间范围，整数类型。

3.5.21.13 IAM 用户开启 MFA

规则详情

表 3-88 规则详情

参数	说明
规则名称	iam-user-mfa-enabled
规则展示名	IAM用户开启MFA
规则描述	IAM用户未开启MFA认证，视为“不合规”。
标签	iam
规则触发方式	配置变更
规则评估的资源类型	iam.users
规则参数	无

3.5.21.14 IAM 用户单访问密钥

规则详情

表 3-89 规则详情

参数	说明
规则名称	iam-user-single-access-key
规则展示名	IAM用户单访问密钥
规则描述	IAM用户拥有多个处于“active”状态的AK/SK访问密钥，视为“不合规”。
标签	iam
规则触发方式	配置变更
规则评估的资源类型	iam.users
规则参数	无

3.5.21.15 Console 侧密码登录的 IAM 用户开启 MFA 认证

规则详情

表 3-90 规则详情

参数	说明
规则名称	mfa-enabled-for-iam-console-access
规则展示名	Console侧密码登录的IAM用户开启MFA认证
规则描述	通过Console密码登录的IAM用户未开启MFA认证，视为“不合规”。
标签	iam
规则触发方式	配置变更
规则评估的资源类型	iam.users
规则参数	无

3.5.21.16 根账号开启 MFA 认证

规则详情

表 3-91 规则详情

参数	说明
规则名称	root-account-mfa-enabled
规则展示名	根账号开启MFA认证
规则描述	账号未开启MFA认证，视为“不合规”。
标签	iam
规则触发方式	周期触发
规则评估的资源类型	iam.users
规则参数	无

3.5.22 文档数据库服务 DDS

3.5.22.1 DDS 实例开启 SSL

规则详情

表 3-92 规则详情

参数	说明
规则名称	dds-instance-enable-ssl
规则展示名	DDS实例开启SSL
规则描述	DDS实例未开启SSL，视为“不合规”。
标签	dds
规则触发方式	配置变更
规则评估的资源类型	dds.instances
规则参数	无

3.5.22.2 DDS 实例属于指定实例类型

规则详情

表 3-93 规则详情

参数	说明
规则名称	dds-instance-hamode
规则展示名	DDS实例属于指定实例类型
规则描述	指定实例类型，不属于此类型的DDS实例资源，视为“不合规”。
标签	dds
规则触发方式	配置变更
规则评估的资源类型	dds.instances
规则参数	haMode：指定的haMode，字符串类型。

3.5.22.3 DDS 实例未绑定公网 IP

规则详情

表 3-94 规则详情

参数	说明
规则名称	dds-instance-has-eip
规则展示名	DDS实例未绑定公网IP
规则描述	DDS实例绑定了公网IP，视为“不合规”。
标签	dds
规则触发方式	配置变更
规则评估的资源类型	dds.instances
规则参数	无

3.5.22.4 DDS 实例属于指定虚拟私有云 ID

规则详情

表 3-95 规则详情

参数	说明
规则名称	dds-instance-in-vpc
规则展示名	DDS实例属于指定虚拟私有云ID
规则描述	指定虚拟私有云ID，不属于此VPC的DDS MongoDB资源，视为“不合规”。
标签	dds
规则触发方式	配置变更
规则评估的资源类型	dds.instances
规则参数	vpcId：虚拟私有云ID，字符串类型。

3.5.23 消息通知服务 SMN

3.5.23.1 SMN 主题配置访问日志

规则详情

表 3-96 规则详情

参数	说明
规则名称	smn-lts-enable
规则展示名	SMN主题配置访问日志
规则描述	SMN主题未配置访问日志，视为“不合规”。
标签	smn
规则触发方式	配置变更
规则评估的资源类型	smn.topic
规则参数	无

3.5.24 虚拟私有云 VPC

3.5.24.1 未与子网关联的网络 ACL

规则详情

表 3-97 规则详情

参数	说明
规则名称	vpc-acl-unused-check
规则展示名	未与子网关联的网络ACL
规则描述	检查是否存在未使用的网络ACL，如果网络ACL没有与子网关联，视为“不合规”。
标签	vpc
规则触发方式	配置变更
规则评估的资源类型	vpc.firewallGroups
规则参数	无

3.5.24.2 默认安全组关闭出、入方向流量

规则详情

表 3-98 规则详情

参数	说明
规则名称	vpc-default-sg-closed
规则展示名	默认安全组关闭出、入方向流量
规则描述	虚拟私有云的默认安全组允许入方向或出方向流量，视为“不合规”。
标签	vpc
规则触发方式	配置变更
规则评估的资源类型	vpc.securityGroups
规则参数	无

3.5.24.3 VPC 启用流日志

规则详情

表 3-99 规则详情

参数	说明
规则名称	vpc-flow-logs-enabled
规则展示名	VPC启用流日志
规则描述	检查是否已为所有VPC启用流日志。如未启用流日志，视为“不合规”。
标签	vpc
规则触发方式	配置变更
规则评估的资源类型	vpc.vpcs
规则参数	无

3.5.24.4 安全组端口检查

规则详情

表 3-100 规则详情

参数	说明
规则名称	vpc-sg-ports-check
规则展示名	安全组端口检查
规则描述	当安全组入方向源地址设置为0.0.0.0/0，且开放了所有的TCP/UDP端口时，视为“不合规”。
标签	vpc
规则触发方式	配置变更
规则评估的资源类型	vpc.securityGroups
规则参数	无

3.5.24.5 安全组入站流量限制指定端口

规则详情

表 3-101 规则详情

参数	说明
规则名称	vpc-sg-restricted-common-ports
规则展示名	安全组入站流量限制指定端口
规则描述	当安全组的入站流量不限制指定端口的所有IPv4地址(0.0.0.0/0)，视为“不合规”。
标签	vpc
规则触发方式	配置变更
规则评估的资源类型	vpc.securityGroups
规则参数	blockedPorts：需要限制的端口列表，数组类型，默认值为（20，21，3306，3389）。 ● 20：文件传输协议-数据端口。 ● 21：文件传输协议-控制端口。 ● 3306：mysql端口。 ● 3389：远程桌面协定端口。

3.5.24.6 安全组入站流量限制 SSH 端口

规则详情

表 3-102 规则详情

参数	说明
规则名称	vpc-sg-restricted-ssh
规则展示名	安全组入站流量限制SSH端口
规则描述	当安全组入方向源地址设置为0.0.0.0/0，且开放TCP 22端口，视为“不合规”。
标签	vpc
规则触发方式	配置变更
规则评估的资源类型	vpc.securityGroups
规则参数	无

3.5.25 虚拟专用网络 VPN

3.5.25.1 VPN 连接状态为“正常”

规则详情

表 3-103 规则详情

参数	说明
规则名称	vpn-connections-active
规则展示名	VPN连接状态为“正常”
规则描述	VPN连接状态不为“正常”，视为“不合规”。
标签	vpnaas
规则触发方式	配置变更
规则评估的资源类型	vpnaas.vpnConnections、vpnaas.ipsec-site-connections
规则参数	无

3.5.26 云监控服务 CES

3.5.26.1 CES 启用告警操作

规则详情

表 3-104 规则详情

参数	说明
规则名称	alarm-action-enabled-check
规则展示名	CES启用告警操作
规则描述	CES告警操作未启用，视为“不合规”。
标签	ces
规则触发方式	配置变更
规则评估的资源类型	ces.alarms
规则参数	无

3.5.26.2 CES 配置监控 KMS 禁用或计划删除的事件监控告警

规则详情

表 3-105 规则详情

参数	说明
规则名称	alarm-kms-disable-or-delete-key
规则展示名	CES配置监控KMS禁用或计划删除的事件监控告警
规则描述	CES未配置监控KMS禁用或计划删除密钥的事件监控告警，视为“不合规”。
标签	ces、kms
规则触发方式	周期触发
规则评估的资源类型	ces.alarms
规则参数	无

3.5.26.3 CES 配置监控 OBS 桶策略变更的事件监控告警

规则详情

表 3-106 规则详情

参数	说明
规则名称	alarm-obs-bucket-policy-change
规则展示名	CES配置监控OBS桶策略变更的事件监控告警
规则描述	CES未配置监控变更OBS桶策略的事件监控告警，视为“不合规”。
标签	ces、obs
规则触发方式	周期触发
规则评估的资源类型	ces.alarms
规则参数	无

3.5.26.4 指定的资源类型绑定指定指标 CES 告警

规则详情

表 3-107 规则详情

参数	说明
规则名称	alarm-resource-check
规则展示名	指定的资源类型绑定指定指标CES告警
规则描述	指定的资源类型没有绑定指定指标的CES告警，视为“不合规”。
标签	ces
规则触发方式	周期触发
规则评估的资源类型	ces.alarms
规则参数	• provider：云服务名称，字符串类型。 • resourceType：资源类型，字符串类型。 • metricName：监控指标名称，字符串类型。

3.5.26.5 检查特定指标的 CES 告警进行特定配置

规则详情

表 3-108 规则详情

参数	说明
规则名称	alarm-settings-check
规则展示名	检查特定指标的CES告警进行特定配置
规则描述	特定指标的CES告警没有进行特定配置，视为“不合规”。
标签	ces
规则触发方式	配置变更
规则评估的资源类型	ces.alarms

参数	说明
规则参数	• metricName：监控指标名称，字符串类型。 • threshold：告警阈值，字符串类型。 • count：触发告警的连续发生次数，字符串类型。 • period：监控数据粒度，字符串类型。 • comparisonOperator：告警阈值的比较条件，可以是>、=、<、>=、<=，字符串类型。 • filter：数据聚合方式，字符串类型。

3.5.26.6 CES 配置监控 VPC 变更的事件监控告警

规则详情

表 3-109 规则详情

参数	说明
规则名称	alarm-vpc-change
规则展示名	CES配置监控VPC变更的事件监控告警
规则描述	CES未配置监控VPC变更的事件监控告警，视为“不合规”。
标签	ces、vpc
规则触发方式	周期触发
规则评估的资源类型	ces.alarms
规则参数	无

3.5.27 云容器引擎 CCE

3.5.27.1 CCE 集群版本为处于维护的版本

规则详情

表 3-110 规则详情

参数	说明
规则名称	cce-cluster-end-of-maintenance-version
规则展示名	CCE集群版本为处于维护的版本

参数	说明
规则描述	CCE集群版本为停止维护的版本，视为“不合规”。
标签	cce
规则触发方式	配置变更
规则评估的资源类型	cce.clusters
规则参数	无

3.5.27.2 CCE 集群运行的非受支持的最旧版本

规则详情

表 3-111 规则详情

参数	说明
规则名称	cce-cluster-oldest-supported-version
规则展示名	CCE集群运行的非受支持的最旧版本
规则描述	如果CCE集群运行的是受支持的最旧版本（等于参数“最旧版本支持”），视为“不合规”。
标签	cce
规则触发方式	配置变更
规则评估的资源类型	cce.clusters
规则参数	无

3.5.27.3 CCE 集群资源不具有公网 IP

规则详情

表 3-112 规则详情

参数	说明
规则名称	cce-endpoint-public-access
规则展示名	CCE集群资源不具有公网IP
规则描述	CCE集群资源具有公网IP，视为“不合规”。
标签	cce
规则触发方式	配置变更

参数	说明
规则评估的资源类型	cce.clusters
规则参数	无

3.5.28 云审计服务 CTS

3.5.28.1 CTS 追踪器通过 KMS 进行加密

规则详情

表 3-113 规则详情

参数	说明
规则名称	cts-kms-encrypted-check
规则展示名	CTS追踪器通过KMS进行加密
规则描述	CTS追踪器未通过KMS进行加密，视为“不合规”。
标签	cts
规则触发方式	配置变更
规则评估的资源类型	cts.trackers
规则参数	无

3.5.28.2 CTS 追踪器启用事件分析

规则详情

表 3-114 规则详情

参数	说明
规则名称	cts-lts-enable
规则展示名	CTS追踪器启用事件分析
规则描述	CTS追踪器未启用事件分析，视为“不合规”。
标签	cts
规则触发方式	配置变更
规则评估的资源类型	cts.trackers

参数	说明
规则参数	无

3.5.28.3 CTS 追踪器追踪指定的 OBS 桶

规则详情

表 3-115 规则详情

参数	说明
规则名称	cts-obs-bucket-track
规则展示名	CTS追踪器追踪指定的OBS桶
规则描述	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”。
标签	cts
规则触发方式	周期触发
规则评估的资源类型	cts.trackers
规则参数	trackBucket：指定的OBS桶名称，字符串类型。

3.5.28.4 CTS 追踪器打开事件文件校验

规则详情

表 3-116 规则详情

参数	说明
规则名称	cts-support-validate-check
规则展示名	CTS追踪器打开事件文件校验
规则描述	CTS追踪器未打开事件文件校验，视为“不合规”。
标签	cts
规则触发方式	配置变更
规则评估的资源类型	cts.trackers
规则参数	无

3.5.28.5 创建并启用 CTS 追踪器

规则详情

表 3-117 规则详情

参数	说明
规则名称	cts-tracker-exists
规则展示名	创建并启用CTS追踪器
规则描述	账号未创建CTS追踪器，视为“不合规”。
标签	cts
规则触发方式	周期触发
规则评估的资源类型	cts.trackers
规则参数	无

3.5.28.6 在指定区域创建并启用 CTS 追踪器

规则详情

表 3-118 规则详情

参数	说明
规则名称	multi-region-cts-tracker-exists
规则展示名	在指定区域创建并启用CTS追踪器
规则描述	账号未在指定Region列表创建CTS追踪器，视为“不合规”。
标签	cts
规则触发方式	周期触发
规则评估的资源类型	cts.trackers
规则参数	regionList：指定的Region列表，数组类型。

3.5.29 云数据库 RDS

3.5.29.1 GaussDB 资源属于指定虚拟私有云 ID

规则详情

表 3-119 规则详情

参数	说明
规则名称	gaussdb-instance-in-vpc
规则展示名	GaussDB资源属于指定虚拟私有云ID
规则描述	指定虚拟私有云ID，不属于此虚拟私有云的gaussdb资源，视为“不合规”。
标签	gaussdb
规则触发方式	配置变更
规则评估的资源类型	gaussdb.instance
规则参数	vpcId：虚拟私有云ID，字符串类型。

3.5.29.2 GaussDB NoSQL 部署在单个可用区

规则详情

表 3-120 规则详情

参数	说明
规则名称	gaussdb-nosql-deploy-in-single-az
规则展示名	GaussDB NoSQL部署在单个可用区
规则描述	GaussDB NoSQL部署在单个可用区中，视为“不合规”。
标签	gaussdb nosql
规则触发方式	配置变更
规则评估的资源类型	nosql.instances
规则参数	无

3.5.29.3 GaussDB NoSQL 开启备份

规则详情

表 3-121 规则详情

参数	说明
规则名称	gaussdb-nosql-enable-backup
规则展示名	GaussDB NoSQL开启备份
规则描述	GaussDB NoSQL未开启备份，视为“不合规”。
标签	gaussdb nosql
规则触发方式	配置变更
规则评估的资源类型	nosql.instances
规则参数	无

3.5.29.4 GaussDB NoSQL 使用磁盘加密

规则详情

表 3-122 规则详情

参数	说明
规则名称	gaussdb-nosql-enable-disk-encryption
规则展示名	GaussDB NoSQL使用磁盘加密
规则描述	GaussDB NoSQL未使用磁盘加密，视为“不合规”。
标签	gaussdb nosql
规则触发方式	配置变更
规则评估的资源类型	nosql.instances
规则参数	无

3.5.29.5 GaussDB NoSQL 开启错误日志

规则详情

表 3-123 规则详情

参数	说明
规则名称	gaussdb-nosql-enable-error-log
规则展示名	GaussDB NoSQL开启错误日志
规则描述	GaussDB NoSQL未开启错误日志，视为“不合规”。
标签	gaussdb nosql
规则触发方式	配置变更
规则评估的资源类型	nosql.instances
规则参数	无

3.5.29.6 GaussDB NoSQL 支持慢查询日志

规则详情

表 3-124 规则详情

参数	说明
规则名称	gaussdb-nosql-support-slow-log
规则展示名	GaussDB NoSQL支持慢查询日志
规则描述	GaussDB NoSQL不支持慢查询日志，视为“不合规”。
标签	gaussdb nosql
规则触发方式	配置变更
规则评估的资源类型	nosql.instances
规则参数	无

3.5.29.7 GaussDB 实例开启审计日志

规则详情

表 3-125 规则详情

参数	说明
规则名称	gaussdb-instance-enable-auditLog
规则展示名	GaussDB实例开启审计日志
规则描述	未开启审计日志的GaussDB资源，视为“不合规”。
标签	gaussdb
规则触发方式	配置变更
规则评估的资源类型	gaussdb.instance
规则参数	无

3.5.29.8 GaussDB 实例开启自动备份

规则详情

表 3-126 规则详情

参数	说明
规则名称	gaussdb-instance-enable-backup
规则展示名	GaussDB实例开启自动备份
规则描述	未开启资源备份的GaussDB资源，视为“不合规”。
标签	gaussdb
规则触发方式	配置变更
规则评估的资源类型	gaussdb.instance
规则参数	无

3.5.29.9 GaussDB 实例开启错误日志

规则详情

表 3-127 规则详情

参数	说明
规则名称	gaussdb-instance-enable-errorLog
规则展示名	GaussDB实例开启错误日志
规则描述	未开启错误日志的GaussDB资源，视为“不合规”。
标签	gaussdb
规则触发方式	配置变更
规则评估的资源类型	gaussdb.instance
规则参数	无

3.5.29.10 GaussDB 实例开启慢日志

规则详情

表 3-128 规则详情

参数	说明
规则名称	gaussdb-instance-enable-slowLog
规则展示名	GaussDB实例开启慢日志
规则描述	未开启慢日志的GaussDB资源，视为“不合规”。
标签	gaussdb
规则触发方式	配置变更
规则评估的资源类型	gaussdb.instance
规则参数	无

3.5.29.11 GaussDB for MySQL 实例开启审计日志

规则详情

表 3-129 规则详情

参数	说明
规则名称	gaussdb-mysql-instance-enable-auditlog
规则展示名	GaussDB for MySQL实例开启审计日志
规则描述	未开启审计日志的GaussDB for MySQL资源，视为“不合规”。
标签	gaussdb
规则触发方式	配置变更
规则评估的资源类型	gaussdb.instance
规则参数	无

3.5.29.12 GaussDB for MySQL 实例开启备份

规则详情

表 3-130 规则详情

参数	说明
规则名称	gaussdb-mysql-instance-enable-backup
规则展示名	GaussDB for MySQL实例开启备份
规则描述	未开启备份的GaussDB for MySQL资源，视为“不合规”。
标签	gaussdb
规则触发方式	配置变更
规则评估的资源类型	gaussdb.instance
规则参数	无

3.5.29.13 GaussDB for MySQL 实例开启错误日志

规则详情

表 3-131 规则详情

参数	说明
规则名称	gaussdb-mysql-instance-enable-errorlog
规则展示名	GaussDB for MySQL实例开启错误日志
规则描述	未开启错误日志的GaussDB for MySQL资源，视为“不合规”。
标签	gaussdb
规则触发方式	配置变更
规则评估的资源类型	gaussdb.instance
规则参数	无

3.5.29.14 GaussDB for MySQL 实例开启慢日志

规则详情

表 3-132 规则详情

参数	说明
规则名称	gaussdb-mysql-instance-enable-slowlog
规则展示名	GaussDB for MySQL实例开启慢日志
规则描述	未开启慢日志的GaussDB for MySQL资源，视为“不合规”。
标签	gaussdb nosql
规则触发方式	配置变更
规则评估的资源类型	gaussdb.instance
规则参数	无

3.5.29.15 RDS 实例开启备份

规则详情

表 3-133 规则详情

参数	说明
规则名称	rds-instance-enable-backup
规则展示名	RDS实例开启备份
规则描述	未开启备份的RDS资源，视为“不合规”。
标签	rds
规则触发方式	配置变更
规则评估的资源类型	rds.instances
规则参数	无

3.5.29.16 RDS 实例开启错误日志

规则详情

表 3-134 规则详情

参数	说明
规则名称	rds-instance-enable-errorLog
规则展示名	RDS实例开启错误日志
规则描述	未开启错误日志的RDS资源，视为“不合规”。
标签	rds
规则触发方式	配置变更
规则评估的资源类型	rds.instances
规则参数	无

3.5.29.17 RDS 实例开启慢日志

规则详情

表 3-135 规则详情

参数	说明
规则名称	rds-instance-enable-slowLog
规则展示名	RDS实例开启慢日志
规则描述	未开启慢日志的RDS资源，视为“不合规”。
标签	rds
规则触发方式	配置变更
规则评估的资源类型	rds.instances
规则参数	无

3.5.29.18 RDS 实例支持多可用区

规则详情

表 3-136 规则详情

参数	说明
规则名称	rds-instance-multi-az-support
规则展示名	RDS实例支持多可用区
规则描述	RDS实例仅支持一个可用区，视为“不合规”。
标签	rds
规则触发方式	配置变更
规则评估的资源类型	rds.instances
规则参数	无

3.5.29.19 RDS 实例不具有公网 IP

规则详情

表 3-137 规则详情

参数	说明
规则名称	rds-instance-no-public-ip
规则展示名	RDS实例不具有公网IP
规则描述	RDS资源具有公网IP，视为“不合规”。
标签	rds
规则触发方式	配置变更
规则评估的资源类型	rds.instances
规则参数	无

3.5.29.20 RDS 实例开启存储加密

规则详情

表 3-138 规则详情

参数	说明
规则名称	rds-instances-enable-kms
规则展示名	RDS实例开启存储加密
规则描述	未开启存储加密的RDS资源，视为“不合规”。
标签	rds
规则触发方式	配置变更
规则评估的资源类型	rds.instances
规则参数	无

3.5.29.21 RDS 实例属于指定虚拟私有云 ID

规则详情

表 3-139 规则详情

参数	说明
规则名称	rds-instances-in-vpc
规则展示名	RDS实例属于指定虚拟私有云ID
规则描述	指定虚拟私有云ID，不属于此虚拟私有云的RDS资源，视为“不合规”。
标签	rds
规则触发方式	配置变更
规则评估的资源类型	rds.instances
规则参数	vpcId：虚拟私有云ID，字符串类型。

3.5.29.22 RDS 实例配备日志

规则详情

表 3-140 规则详情

参数	说明
规则名称	rds-instance-logging-enabled
规则展示名	RDS实例配备日志
规则描述	未配备任何日志的RDS资源，视为“不合规”。
标签	rds
规则触发方式	配置变更
规则评估的资源类型	rds.instances
规则参数	无

3.5.30 云搜索服务 CSS

3.5.30.1 CSS 集群启用认证

规则详情

表 3-141 规则详情

参数	说明
规则名称	css-cluster-authority-enable
规则展示名	CSS集群启用认证
规则描述	CSS集群未启用认证，视为“不合规”。
标签	css
规则触发方式	配置变更
规则评估的资源类型	css.clusters
规则参数	无

3.5.30.2 CSS 集群启用快照

规则详情

表 3-142 规则详情

参数	说明
规则名称	css-cluster-backup-available
规则展示名	CSS集群启用快照
规则描述	CSS集群未启用快照，视为“不合规”。
标签	css
规则触发方式	配置变更
规则评估的资源类型	css.clusters
规则参数	无

3.5.30.3 CSS 集群开启磁盘加密

规则详情

表 3-143 规则详情

参数	说明
规则名称	css-cluster-disk-encryption-check
规则展示名	CSS集群开启磁盘加密
规则描述	CSS集群未开启磁盘加密，视为“不合规”。
标签	css
规则触发方式	配置变更
规则评估的资源类型	css.clusters
规则参数	无

3.5.30.4 CSS 集群启用 HTTPS

规则详情

表 3-144 规则详情

参数	说明
规则名称	css-cluster-https-required
规则展示名	CSS集群启用HTTPS
规则描述	CSS集群未启用HTTPS，视为“不合规”。
标签	css
规则触发方式	配置变更
规则评估的资源类型	css.clusters
规则参数	无

3.5.30.5 CSS 集群绑定指定 VPC 资源

规则详情

表 3-145 规则详情

参数	说明
规则名称	css-cluster-in-vpc
规则展示名	CSS集群绑定指定VPC资源
规则描述	CSS集群未与指定的虚拟私有云资源绑定，视为“不合规”。
标签	css
规则触发方式	配置变更
规则评估的资源类型	css.clusters
规则参数	authorizedVpcIds：指定的虚拟私有云ID（VPC ID）列表，如果列表为空，表示允许所有值；数组类型，最多包含10个元素。

3.5.30.6 CSS 集群具备多 AZ 容灾

规则详情

表 3-146 规则详情

参数	说明
规则名称	css-cluster-multiple-az-check
规则展示名	CSS集群具备多AZ容灾
规则描述	CSS集群未多AZ容灾，视为“不合规”。
标签	css
规则触发方式	配置变更
规则评估的资源类型	css.clusters
规则参数	无

3.5.30.7 CSS 集群具备多实例容灾

规则详情

表 3-147 规则详情

参数	说明
规则名称	css-cluster-multiple-instances-check
规则展示名	CSS集群具备多实例容灾
规则描述	CSS集群未多实例容灾，视为“不合规”。
标签	css
规则触发方式	配置变更
规则评估的资源类型	css.clusters
规则参数	无

3.5.30.8 CSS 集群不能公网访问

规则详情

表 3-148 规则详情

参数	说明
规则名称	css-cluster-no-public-zone
规则展示名	CSS集群不能公网访问
规则描述	CSS集群开启公网访问，视为“不合规”。
标签	css
规则触发方式	配置变更
规则评估的资源类型	css.clusters
规则参数	无

3.5.30.9 CSS 集群开启安全模式

规则详情

表 3-149 规则详情

参数	说明
规则名称	css-cluster-security-mode-enable
规则展示名	CSS集群开启安全模式
规则描述	CSS集群资源未开启安全模式，视为“不合规”。
标签	css
规则触发方式	配置变更
规则评估的资源类型	css.clusters
规则参数	无

3.5.30.10 CSS 集群白名单不生效

规则详情

表 3-150 规则详情

参数	说明
规则名称	css-cluster-not-enable-white-list
规则展示名	CSS集群白名单不生效
规则描述	CSS集群白名单设置为对所有IP开放，视为“不合规”。
标签	css
规则触发方式	配置变更
规则评估的资源类型	css.clusters
规则参数	无

3.5.30.11 CSS 集群 kibana 白名单不生效

规则详情

表 3-151 规则详情

参数	说明
规则名称	css-cluster-kibana-not-enable-white-list
规则展示名	CSS集群kibana白名单不生效
规则描述	CSS集群kibana白名单设置为对所有IP开放，视为“不合规”。
标签	css
规则触发方式	配置变更
规则评估的资源类型	css.clusters
规则参数	无

3.5.31 云硬盘 EVS

3.5.31.1 云硬盘的类型在指定的范围内

规则详情

表 3-152 规则详情

参数	说明
规则名称	allowed-volume-specs
规则展示名	云硬盘的类型在指定的范围内
规则描述	指定允许的云硬盘类型列表，云硬盘的类型不在指定的范围内，视为“不合规”。
标签	evs
规则触发方式	配置变更
规则评估的资源类型	evs.volumes
规则参数	listOfAllowedSpecs：允许的云硬盘类型列表，数组类型，最多包含10个元素。字段可选值查询EVS文档获取，例如：SATA、SSD、SAS。

3.5.31.2 云硬盘创建后在指定天数内绑定资源实例

规则详情

表 3-153 规则详情

参数	说明
规则名称	evs-use-in-specified-days
规则展示名	云硬盘创建后在指定天数内绑定资源实例
规则描述	云硬盘创建后在指定天数内未使用，视为“不合规”。
标签	evs
规则触发方式	周期触发
规则评估的资源类型	evs.volumes
规则参数	allowDays：指定允许的天数，数值类型。

3.5.31.3 云硬盘闲置检测

规则详情

表 3-154 规则详情

参数	说明
规则名称	volume-unused-check
规则展示名	云硬盘闲置检测
规则描述	云硬盘未挂载给任何云服务器，视为“不合规”。
标签	evs
规则触发方式	配置变更
规则评估的资源类型	evs.volumes
规则参数	无

3.5.31.4 已挂载的云硬盘开启加密

规则详情

表 3-155 规则详情

参数	说明
规则名称	volumes-encrypted-check
规则展示名	已挂载的云硬盘开启加密
规则描述	已挂载的云硬盘未进行加密，视为“不合规”。
标签	evs、ecs
规则触发方式	配置变更
规则评估的资源类型	evs.volumes
规则参数	无

3.5.32 云证书管理服务 CCM

3.5.32.1 检查私有 CA 是否过期

规则详情

表 3-156 规则详情

参数	说明
规则名称	pca-certificate-authority-expiration-check
规则展示名	检查私有CA是否过期
规则描述	私有CA没有标记在指定时间内到期，视为“不合规”。
标签	pca
规则触发方式	周期触发
规则评估的资源类型	pca.ca
规则参数	daysToExpiration：指定到期的天数，整数类型。

3.5.32.2 检查私有证书是否过期

规则详情

表 3-157 规则详情

参数	说明
规则名称	pca-certificate-expiration-check
规则展示名	检查私有证书是否过期
规则描述	私有证书没有标记在指定时间内到期，视为“不合规”。
标签	pca
规则触发方式	周期触发
规则评估的资源类型	pca.cert
规则参数	daysToExpiration：指定到期的天数，整数类型。

3.5.33 分布式消息服务 Kafka 版

3.5.33.1 DMS Kafka 队列打开内网 SSL 加密访问

规则详情

表 3-158 规则详情

参数	说明
规则名称	dms-kafka-not-enable-private-ssl
规则展示名	DMS Kafka队列打开内网SSL加密访问
规则描述	DMS kafkas队列未打开内网SSL加密访问，视为“不合规”。
标签	dms
规则触发方式	配置变更
规则评估的资源类型	dms.kafkas
规则参数	无

3.5.33.2 DMS Kafka 队列打开公网 SSL 加密访问

规则详情

表 3-159 规则详情

参数	说明
规则名称	dms-kafka-not-enable-public-ssl
规则展示名	DMS Kafka队列打开公网SSL加密访问
规则描述	DMS kafkas队列未打开公网SSL加密访问，视为“不合规”。
标签	dms
规则触发方式	配置变更
规则评估的资源类型	dms.kafkas
规则参数	无

3.5.33.3 DMS Kafka 队列开启公网访问

规则详情

表 3-160 规则详情

参数	说明
规则名称	dms-kafka-public-access-enabled-check
规则展示名	DMS Kafka队列开启公网访问
规则描述	DMS kafkas队列开启公网访问，视为“不合规”。
标签	dms
规则触发方式	配置变更
规则评估的资源类型	dms.kafkas
规则参数	无

3.5.34 分布式消息服务 RabbitMQ 版

3.5.34.1 DMS RabbitMq 队列打开 SSL 加密访问

规则详情

表 3-161 规则详情

参数	说明
规则名称	dms-rabbitmq-not-enable-ssl
规则展示名	DMS RabbitMq队列打开SSL加密访问
规则描述	DMS rabbitmqs队列未打开SSL加密访问，视为“不合规”。
标签	dms
规则触发方式	配置变更
规则评估的资源类型	dms.rabbitmqs
规则参数	无

3.5.35 分布式消息服务 RocketMQ 版

3.5.35.1 DMS Reliability 队列打开 SSL 加密访问

规则详情

表 3-162 规则详情

参数	说明
规则名称	dms-rocketmq-not-enable-ssl
规则展示名	DMS Reliability队列打开SSL加密访问
规则描述	DMS reliabilitys队列未打开SSL加密访问，视为“不合规”。
标签	dms
规则触发方式	配置变更
规则评估的资源类型	dms.reliabilitys
规则参数	无

3.6 事件监控

事件监控提供事件类型数据上报、查询和告警的功能。方便您将资源的合规性事件收集到云监控服务，并在事件发生时进行告警。

事件监控默认开通，您可以在事件监控中查看系统事件的监控详情，事件监控的相关操作请参见：**查看事件监控数据**和**创建事件监控的告警通知**。

说明

当前Config对接云监控服务的事件监控能力仅支持华北-北京四区域。

Config目前支持的系统事件如下表所示：

表 3-163 事件监控支持的配置审计（Config）事件

事件来源	事件名称	事件级别	事件说明	处理建议	事件影响
SYS.RMS	配置不合规通知	重要	审计规则执行结果为不合规	修改资源不合规的配置项，使其合规。	无
SYS.RMS	配置合规通知	提示	审计规则执行结果变为合规	无	无
SYS.RMS	Config快照导出失败	重要	Config资源快照导出到OBS失败	建议排查OBS桶权限	无法记录资源历史变化
SYS.RMS	Config快照导出成功	提示	Config资源快照导出到OBS成功	无	无
SYS.RMS	Config历史记录导出失败	重要	Config资源历史记录导出到OBS失败	建议排查OBS桶权限	无法记录资源历史变化
SYS.RMS	Config历史记录导出成功	提示	Config资源历史记录导出到OBS成功	无	无
SYS.RMS	Config资源变化通知失败	重要	Config资源变化通知SMN失败	建议排查SMN主题权限	无法通过SMN通知到客户资源历史变化
SYS.RMS	Config资源变化通知成功	提示	Config资源变化通知SMN成功	无	无

事件来源	事件名称	事件级别	事件说明	处理建议	事件影响
SYS.RMS	Config资源关系变化通知失败	重要	Config资源关系变化通知SMN失败	建议排查SMN主题权限	无法通过SMN通知到客户资源历史变化
SYS.RMS	Config资源关系变化通知成功	提示	Config资源关系变化通知SMN成功	无	无

4 合规规则包

4.1 合规规则包概述

功能概述

合规规则包是配置审计服务合规规则的集合，通过使用合规规则包可以批量部署合规规则，并统一查看合规性数据。

当合规规则包部署成功后，会在资源合规规则列表创建出一条或多条合规规则，且这些合规规则无法更新、停用和删除，只能通过合规规则包进行删除。

如果您是组织管理员或Config服务的委托管理员，您还可以添加组织类型的合规规则包，直接作用于您组织内的成员账号中。

约束与限制

- 每个账号最多可以创建50个合规规则包（包括组织合规规则包），最多可以创建500个合规规则。
- 创建合规规则包（包括组织合规规则包）需要开启资源记录器，仅被资源记录器收集的资源可参与资源评估。

基本概念

示例模板：

配置审计服务提供给用户的合规规则包模板，合规规则包示例模板旨在帮助用户快速创建合规规则包，其中包含适合用户场景的合规规则和输入参数。

预定义合规规则包：

通过“示例模版”创建的合规规则包，用户只需要填入所需的规则参数即可完成合规规则包的部署流程。

自定义合规规则包：

用户根据自身需求编写合规规则包的模板文件，在模板文件中填入适合自身使用场景的预设规则或自定义规则，然后通过“上传模版”或“OBS存储桶”方式完成合规规则包的部署流程。自定义模板文件格式和文件内容格式均为JSON，不支持tf格式和zip格式的文件内容。

合规性数据：

一个合规规则包包含一个或多个合规规则，而每一条合规规则会评估一个或多个资源的合规结果，配置审计服务提供了如下的合规性数据，供您了解合规规则包的评估结果概览：

- 合规规则包的合规性评估：代表合规规则包中的所有合规规则是否评估到不合规的资源。若存在不合规资源，则合规评估结果为“不合规”；若不存在不合规资源，则合规评估结果为“合规”。
- 合规规则的合规性评估：代表合规规则包中的单个合规规则是否评估到不合规的资源。若存在不合规资源，则合规评估结果为“不合规”；若不存在不合规资源，则合规评估结果为“合规”。
- 合规规则包的合规分数：代表合规规则包中所有规则的合规资源数之和与所有规则的评估资源数之和的百分比。若该值为100，则代表合规规则包中所有的合规评估结果均为合规；若该值为0，则代表合规规则包中所有的合规评估结果均为不合规。

图 4-1 合规分数计算公式

$$\text{score} = \frac{\sum_{\text{合规规则}} \text{规则评估的合规资源数}}{\sum_{\text{合规规则}} \text{规则评估的资源总数}} \times 100\%$$

资源栈：

合规规则包下发的合规规则的创建与删除行为最终是通过资源栈来实现的。资源栈是资源编排服务的概念，详见**资源栈**。

状态：

合规规则包的部署状态。包括以下几种情况：

- 已部署：合规规则包已部署成功，合规规则均创建成功。
- 部署中：合规规则包正在部署中，合规规则正在创建中。
- 部署异常：合规规则包部署失败。
- 回滚成功：合规规则包下发的合规规则创建失败，触发合规规则的回滚行为，已创建的合规规则删除成功。
- 回滚中：合规规则包下发的合规规则创建失败，触发合规规则的回滚行为，已创建的合规规则正在删除中。
- 回滚失败：合规规则包下发的合规规则创建失败，触发合规规则的回滚行为，回滚行为失败，需在RFS服务查看失败原因。
- 删除中：合规规则包正在删除中，合规规则正在删除中。
- 删除异常：合规规则包删除失败。
- 更新成功：合规规则包修改并更新成功。
- 更新中：合规规则包修改更新中。
- 更新失败：合规规则包修改更新失败。

合规规则包的授权：

通过资源编排服务的资源栈创建和删除合规规则时，需要拥有合规规则的创建和删除的权限。因此，部署合规规则包时，需要提供一个具有相应权限的委托，供配置审计服务的合规规则包下发时使用。

- 快速授权：快速授权将为您快速创建一个名为“rms_conformance_pack_agency”的委托，该权限是可以让合规规则包创建和删除的委托，该委托的权限包含授权资源编排服务（RFS）创建、更新和删除合规规则的权限。
- 自定义授权：您可自行在统一身份认证服务（IAM）中创建委托权限，并进行自定义授权，但必须包含可以让合规规则包正常工作的权限（授权资源编排服务创建、更新和删除合规规则的权限），创建委托详见**创建委托（委托方操作）**。

4.2 合规规则包

4.2.1 创建合规规则包

操作场景

合规规则包是配置审计服务根据合规场景定制的一组合规规则的集合。您可以使用配置审计服务的示例模板，或根据自身需求配置的自定义模板来创建合规规则包。

合规规则包创建完成后，这些规则默认会执行一次评估，后续将根据规则的触发机制自动触发评估，也可以在资源合规规则列表中手动触发单个合规规则的评估。

约束与限制

- 每个账号最多可以创建50个合规规则包（包括组织合规规则包），最多可以创建500个合规规则。
- 创建或更新合规规则包需要开启资源记录器，具体请参见**配置资源记录器**。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“合规规则包”，进入“合规规则包”页面。

步骤4 单击“创建合规规则包”。

图 4-2 创建合规规则包

步骤5 在“选择模板”页面中，选择示例模板、上传本地模板文件或输入OBS模板URL后，单击“下一步”。

- 示例模板：使用配置审计服务提供的合规规则包示例模板，在下拉列表中选择一个示例模板。

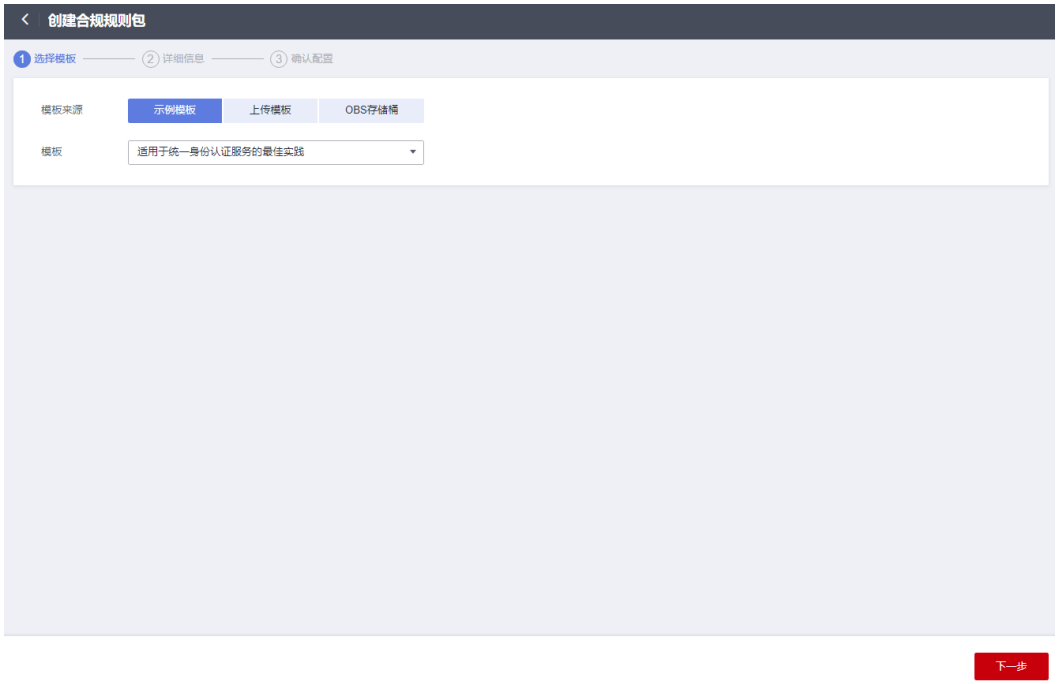
  关于每个示例模板包含的具体合规规则请参见：**合规规则包示例模板**。
- 本地模板：从本地上传模板文件，您可以根据自身的需求编写合规规则包的模板文件，然后上传并使用。

  模板文件格式和文件内容格式均为JSON，不支持tf格式和zip格式的文件内容，该文件的后缀需为.tf.json，具体请参见：**自定义合规规则包**。
- OBS存储桶：自定义合规规则包模板的OBS位置。如果您的本地模板文件大小超过50KB，请将它上传至OBS存储桶，然后输入OBS模板URL来选择并使用它。

  说明

  OBS模板URL指的是OBS桶内对象的URL。您将本地模板上传至OBS桶后，在桶内的对象列表中单击操作列的“更多 > 复制对象URL”，即可获取OBS模板URL。

图 4-3 选择模板



步骤6 进入“详细信息”页面，输入合规规则包名称，选择“快速授权”或“自定义授权”，并配置合规规则包依赖的参数，单击“下一步”。

图 4-4 详细信息

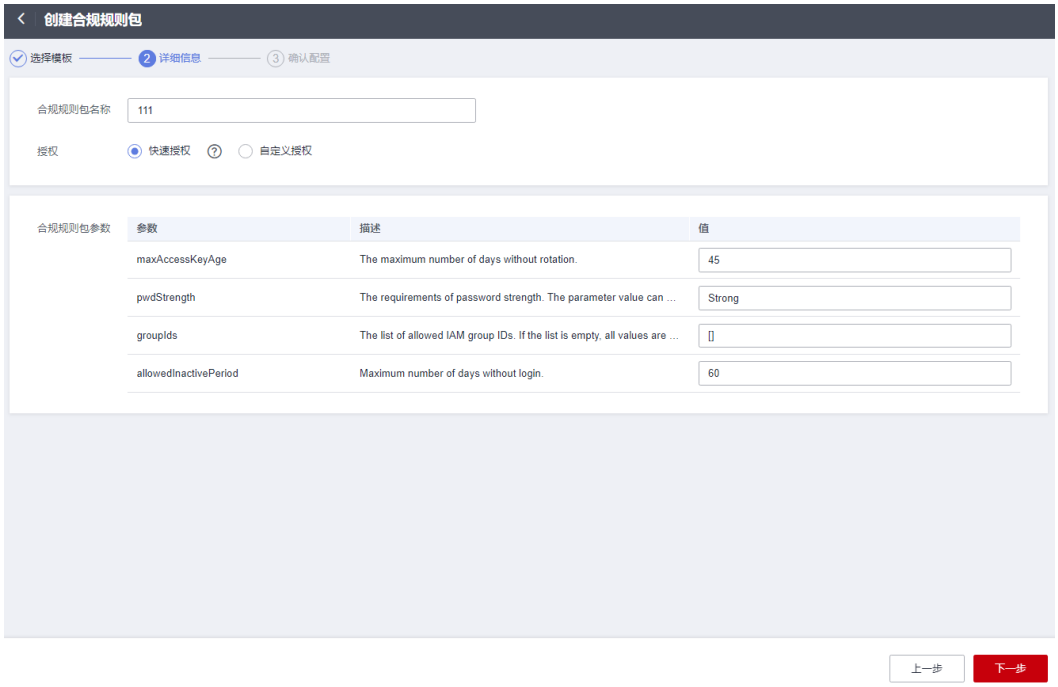
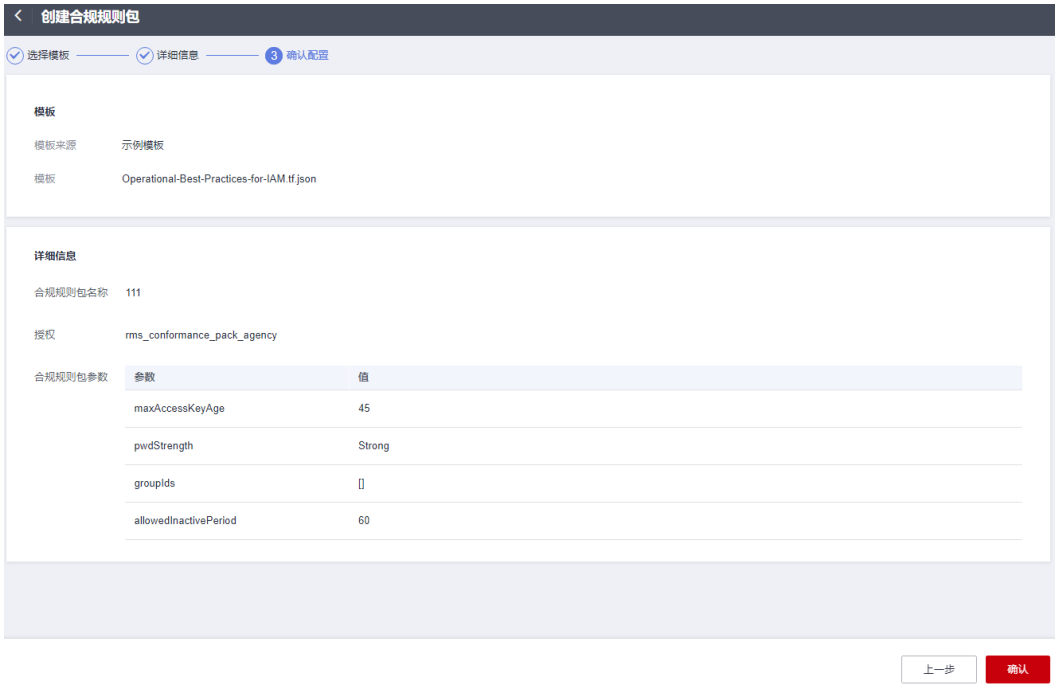


表 4-1 详细信息配置说明

参数	说明
合规规则包名称	合规规则包的名称。自定义，不可与其他合规规则包名称重复。 合规规则包名称的长度最大64字符，由英文字母、数字、下划线、中划线组成。
授权	此处的授权为**委托授权**，授予资源编排服务（RFS）创建、更新和删除合规规则的权限，允许资源编排服务的资源栈进行创建和删除合规规则包下发的合规规则。 • 快速授权：快速授权将为您快速创建一个名为“rms_conformance_pack_agency”的委托，该权限是可以让合规规则包创建和删除的委托，该委托的权限包含授权资源编排服务（RFS）创建、更新和删除合规规则的权限。 • 自定义授权：您可自行在统一身份认证服务（IAM）中创建委托权限，并进行自定义授权，但必须包含可以让合规规则包正常工作的权限（授权资源编排服务创建、更新和删除合规规则的权限），创建委托详见**创建委托（委托方操作）**。
合规规则包参数	合规规则包的参数配置与相对应的合规规则参数一致，具体请参见**系统内置预设策略**。

步骤7 进入“确认配置”页面，确认合规规则包信息无误后，单击“确定”，完成合规规则包的创建。

图 4-5 确认配置



说明

合规规则包创建或更新后会立即自动触发首次评估。

----结束

4.2.2 查看合规规则包及其合规性数据

操作场景

您可以通过列表查看所有已创建的合规规则包及其详情，并支持在列表中进行搜索过滤操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的☰图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“合规规则包”，进入“合规规则包”页面。

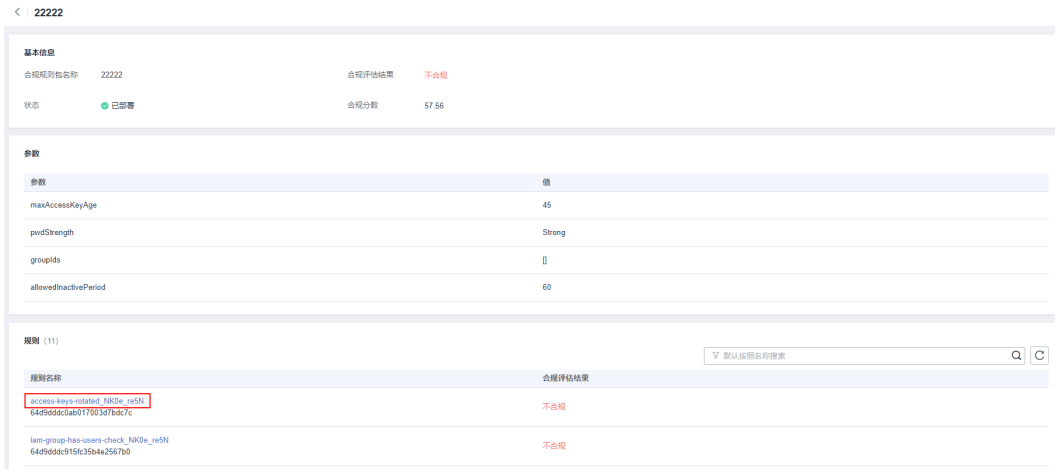
步骤4 在列表中可查看所有已创建的合规规则包，还可以查看合规规则包的合规评估结果、合规分数和状态等信息。

步骤5 在列表中单击需要查看的合规规则包名称，进入合规规则包详情页，查看该合规规则包的详细信息。

在详情页中可以查看合规规则包的基本信息和配置的参数值，以及下发的合规规则列表和每条合规规则的合规评估结果。

在“规则”列表单击某个规则的“规则名称”，界面将跳转至“资源合规”的“规则详情”页面，并自动筛选出此规则评估出的不合规资源。

图 4-6 合规规则包详情页



说明

合规规则包的部署状态有以下几种：

- 已部署：合规规则包已部署成功，合规规则均创建成功。
- 部署中：合规规则包正在部署中，合规规则正在创建中。
- 部署异常：合规规则包部署失败。
- 回滚成功：合规规则包下发的合规规则创建失败，触发合规规则的回滚行为，已创建的合规规则删除成功。
- 回滚中：合规规则包下发的合规规则创建失败，触发合规规则的回滚行为，已创建的合规规则正在删除中。
- 回滚失败：合规规则包下发的合规规则创建失败，触发合规规则的回滚行为，回滚行为失败，需在RFS服务查看失败原因。
- 删除中：合规规则包正在删除中，合规规则正在删除中。
- 删除异常：合规规则包删除失败。
- 更新成功：合规规则包修改并更新成功。
- 更新中：合规规则包修改更新中。
- 更新失败：合规规则包修改更新失败。

----结束

4.2.3 修改合规规则包

操作场景

合规规则包创建完成后，如合规规则包未部署成功，或需要修改其名称和规则参数值，您可参考以下步骤对合规规则包进行修改更新。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

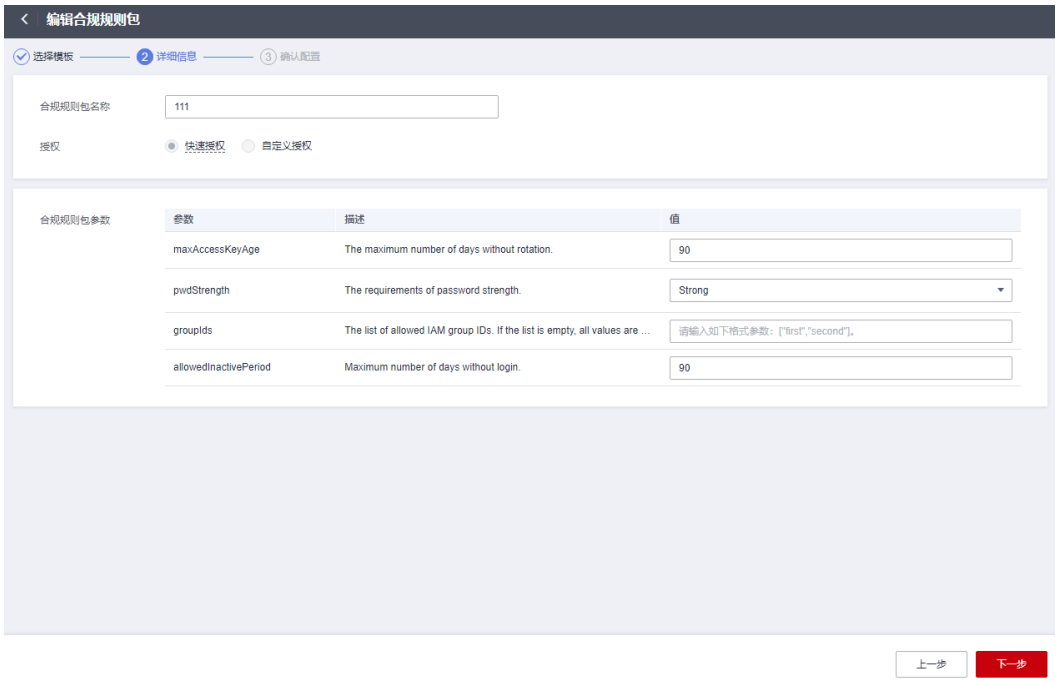
步骤3 单击页面左侧的“合规规则包”，进入“合规规则包”页面。

步骤4 在合规规则包列表中单击操作列的“编辑”，进入“编辑合规规则包”页面。

步骤5 当前不支持修改合规规则包选择的模板，单击“下一步”。

步骤6 进入“详细信息”页面，修改合规规则包名称和规则参数的值，单击“下一步”。

图 4-7 修改合规规则包



步骤7 进入“确认配置”页面，确认修改无误后，单击“确定”。

合规规则包修改完成后将会被重新部署。

----结束

4.2.4 删除合规规则包

操作场景

如果您不再需要某个合规规则包时，可按如下步骤进行删除操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

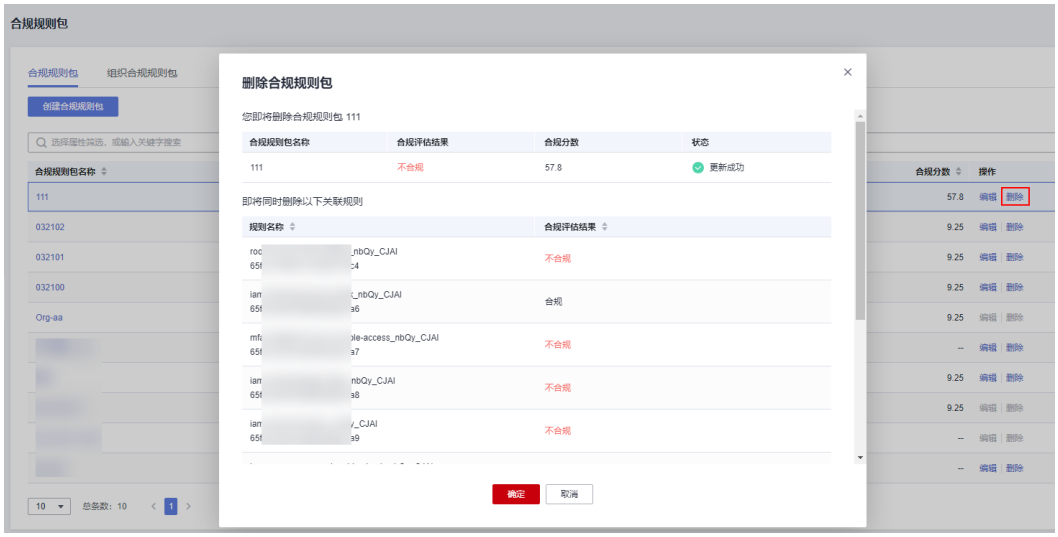
步骤3 单击页面左侧的“合规规则包”，进入“合规规则包”页面。

步骤4 在合规规则包列表中单击操作列的“删除”。

步骤5 在弹出的确认框中单击“确定”，完成合规规则包的删除。

合规规则包删除后，此合规规则包下发的合规规则在资源合规规则列表中也将自动删除。

图 4-8 删除合规规则包



----结束

4.3 组织合规规则包

4.3.1 创建组织合规规则包

操作场景

如果您是组织管理员或Config服务的委托管理员，您可以添加组织类型的合规规则包，直接作用于您组织内的成员账号中。

当组织合规规则包部署成功后，会在组织内成员账号的合规规则包列表中显示此组织合规规则包。且该组织合规规则包的删除操作只能由创建组织规则包的组织账号进行，组织内的其他账号只能触发合规规则包部署规则的评估和查看规则评估结果以及详情。

组织合规规则包创建完成后，所部属的规则默认会执行一次评估，后续将根据规则的触发机制自动触发评估，也可以在资源合规规则列表中手动触发单个合规规则的评估。

约束与限制

- 每个账号最多可以创建50个合规规则包（包括组织合规规则包），最多可以创建500个合规规则。
- 创建或更新组织合规规则包需要开启资源记录器，具体请参见**配置资源记录器**。
- 非组织成员账号无法在Config控制台的“合规规则包”页面中看到“组织合规规则包”页签。

操作步骤

步骤1 以组织管理员账号或者Config服务的委托管理员账号登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“合规规则包”，进入“合规规则包”页面。

步骤4 选择“组织合规规则包”页签，单击“创建组织合规规则包”。

图 4-9 创建组织合规规则包

步骤5 在“选择模板”页面中，选择示例模板、上传本地模板文件或输入OBS模板URL后，单击“下一步”。

- 示例模板：使用配置审计服务提供的合规规则包示例模板，在下拉列表中选择一个示例模板。

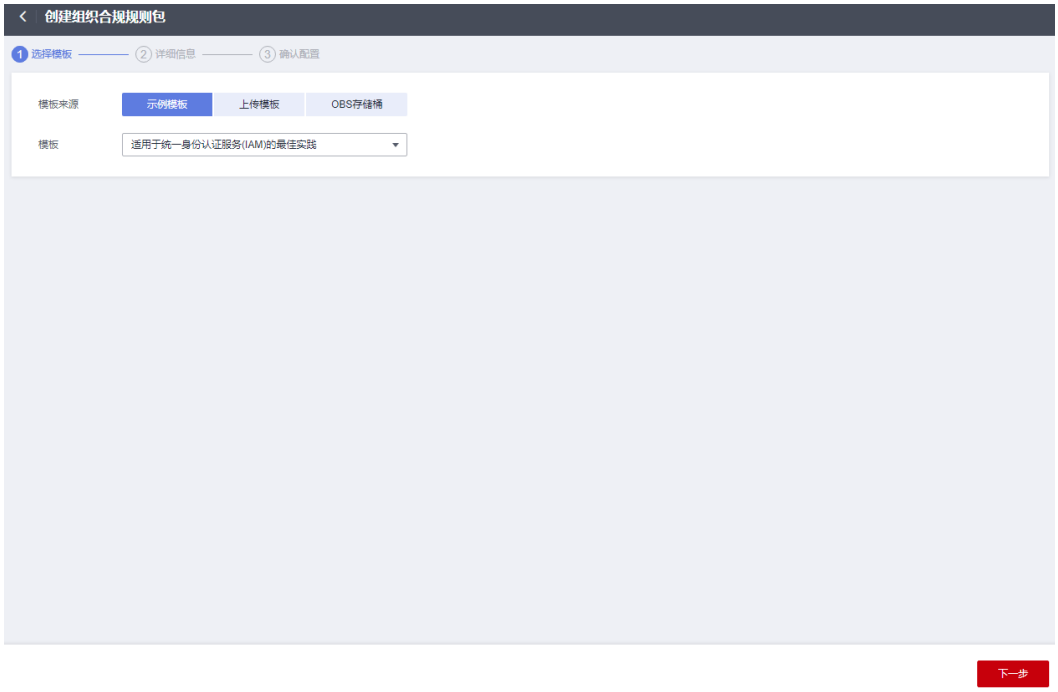
  关于每个示例模板包含的具体合规规则请参见：**合规规则包示例模板**。
- 本地模板：从本地上传模板文件，您可以根据自身的需求编写合规规则包的模板文件，然后上传并使用。

  模板文件格式和文件内容格式均为JSON，不支持tf格式和zip格式的文件内容，该文件的后缀需为.tf.json，具体请参见：**自定义合规规则包**。
- OBS存储桶：自定义合规规则包模板的OBS位置。如果您的本地模板文件大小超过50KB，请将它上传至OBS存储桶，然后输入OBS模板URL来选择并使用它。

  说明

  OBS模板URL指的是OBS桶内对象的URL。您将本地模板上传至OBS桶后，在桶内的对象列表中单击操作列的“更多 > 复制对象URL”，即可获取OBS模板URL。

图 4-10 选择模板



步骤6 进入“详细信息”页面，详细信息配置完成后，单击“下一步”。

图 4-11 详细信息

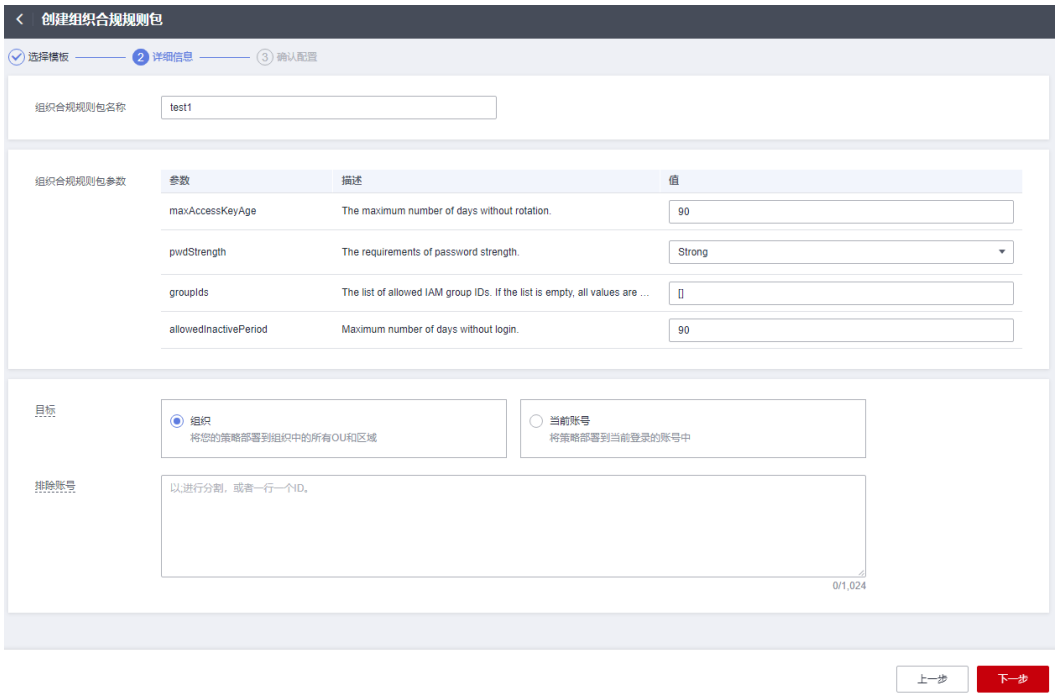
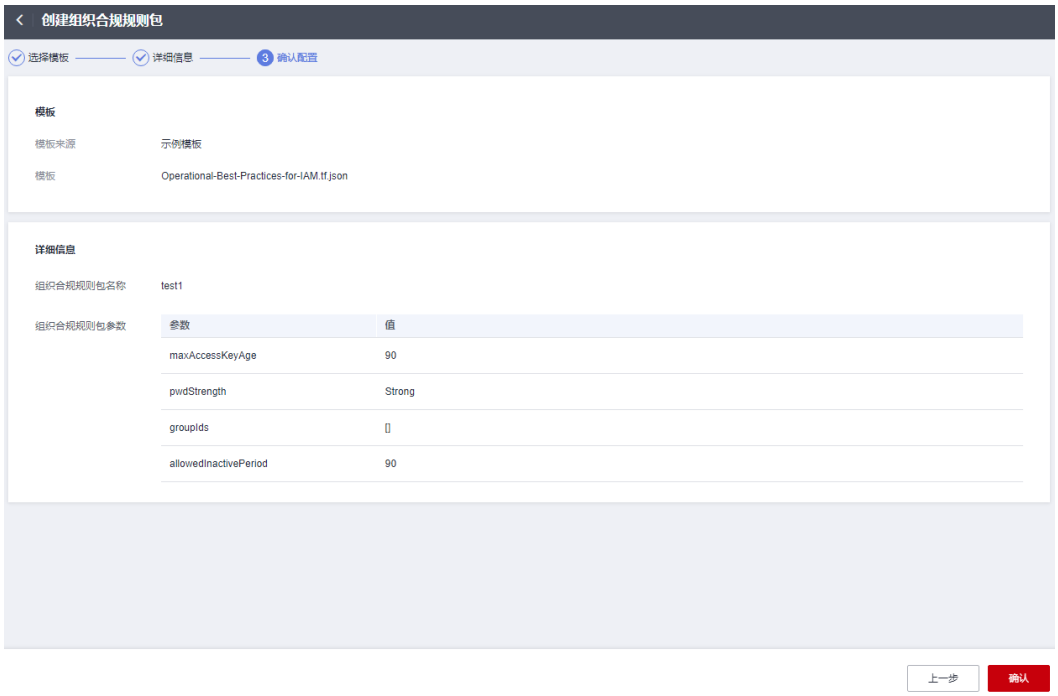


表 4-2 详细信息配置说明

参数	说明
组织合规规则包名称	组织合规规则包的名称。自定义，不可与其他组织合规规则包名称重复。 组织合规规则包名称的长度最大64字符，由英文字母、数字、下划线、中划线组成。
组织合规规则包参数	组织合规规则包的参数配置与相对应的合规规则参数一致，具体请参见**系统内置预设策略**。
目标	目标决定了此组织合规规则包配置的部署位置。 ● 组织：将策略部署到您组织内的所有成员账号中。 ● 当前账号：将策略部署到当前登录的账号中。 创建组织类型的合规规则包时请选择“组织”。
排除账号	输入需要排除的组织内的部分账号ID，使得该组织合规规则包不在排除的账号中部署。 仅当“目标”选择“组织”时可配置此参数。

步骤7 进入“确认配置”页面，确认合规规则包信息无误后，单击“确定”，完成合规规则包的创建。

图 4-12 确认配置



说明

组织合规规则包创建或更新后会立即自动触发首次评估。

----结束

4.3.2 查看组织合规规则包

操作场景

组织账号可以通过列表查看自己创建的组织合规规则包及其详情，并支持在列表中进行搜索过滤操作，但无法看到组织内其他账号添加的组织合规规则包。

当组织合规规则包部署成功后，会在组织内成员账号的合规规则包列表中显示此组织合规规则包。且该组织合规规则包的删除操作只能由创建组织规则包的组织账号进行，组织内的其他账号只能触发合规规则包部署规则的评估和查看规则评估结果以及详情。

本章节包含**查看组织合规规则包**和**查看部署至成员账号中的组织合规规则包**两部分内容。

查看组织合规规则包

步骤1 使用创建组织合规规则包的组织账号登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

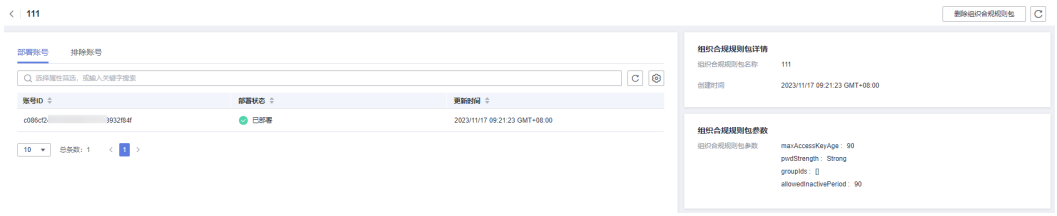
步骤3 单击页面左侧的“合规规则包”，进入“合规规则包”页面。

步骤4 选择“组织合规规则包”页签，在列表中可查看所有已创建的组织合规规则包，还可以查看各组织合规规则包的部署状态。

步骤5 在列表中单击需要查看的组织合规规则包名称，进入组织合规规则包详情页。

页面左侧为组织合规规则包部署账号和排除账号的相关信息，页面右侧为组织合规规则包的详情和参数。

图 4-13 组织合规规则包详情页



说明

组织合规规则包的部署状态有以下几种：

- 已部署：合规规则包已部署成功，合规规则均创建成功。
- 部署中：合规规则包正在部署中，合规规则正在创建中。
- 部署异常：合规规则包部署失败。
- 回滚成功：合规规则包下发的合规规则创建失败，触发合规规则的回滚行为，已创建的合规规则删除成功。
- 回滚中：合规规则包下发的合规规则创建失败，触发合规规则的回滚行为，已创建的合规规则正在删除中。
- 回滚失败：合规规则包下发的合规规则创建失败，触发合规规则的回滚行为，回滚行为失败，需在RFS服务查看失败原因。
- 删除中：合规规则包正在删除中，合规规则正在删除中。
- 删除异常：合规规则包删除失败。
- 更新成功：合规规则包修改并更新成功。
- 更新中：合规规则包修改更新中。
- 更新失败：合规规则包修改更新失败。

----结束

查看部署至成员账号中的组织合规规则包

步骤1 以组织成员账号登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“合规规则包”，进入“合规规则包”页面。

步骤4 在“合规规则包”页签下，单击合规规则包列表中的某个组织合规规则包名称，进入合规规则包详情页。

在详情页中可以查看合规规则包的基本信息和配置的参数值，以及下发的合规规则列表和每条合规规则的合规评估结果。

在“规则”列表单击某个规则的“规则名称”，界面将跳转至“资源合规”的“规则详情”页面，并自动筛选出此规则评估出的不合规资源。

图 4-14 查看部署至成员账号中的组织合规规则包

说明

当组织合规规则包部署成功后，会在组织内成员账号的合规规则包列表中显示此组织合规规则包，系统将自动在合规规则包名称前添加“Org-”字段。

组织内的成员账号只能触发组织合规规则包部署规则的评估和查看规则评估结果以及详情，不支持删除组织合规规则包的操作。

----结束

4.3.3 修改组织合规规则包

操作场景

组织合规规则包创建完成后，你可以随时需要修改其名称和规则参数值。当组织合规规则包部署目标为组织时，如在组织的部分账号中部署失败，您还可以修改组织合规规则包的排除账号，将部署失败的账号排除后重新部署。

操作步骤

步骤1 使用创建组织合规规则包的组织账号登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

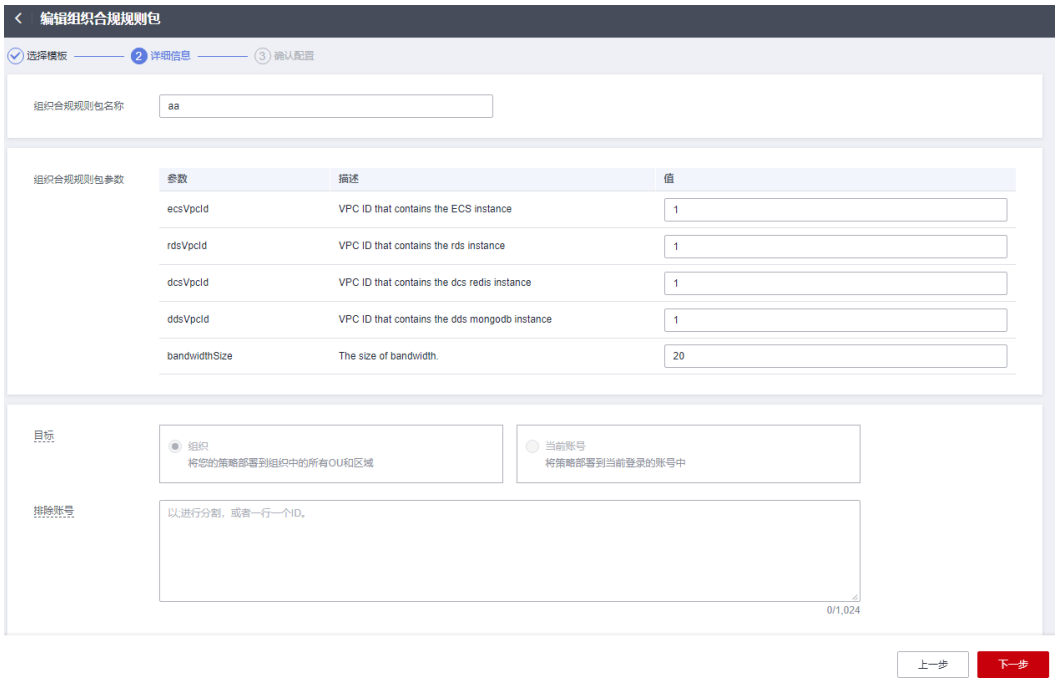
步骤3 单击页面左侧的“合规规则包”，进入“合规规则包”页面。

步骤4 选择“组织合规规则包”页签，在组织合规规则包列表中单击操作列的“编辑”。

步骤5 进入“编辑组织合规规则包”页面，当前不支持修改合规规则包选择的模板，单击“下一步”。

步骤6 进入“详细信息”页面，修改合规规则包名称和规则参数的值，单击“下一步”。

图 4-15 修改组织合规规则包



步骤7 进入“确认配置”页面，确认修改无误后，单击“确定”。

组织合规规则包修改完成后将会在部署账号中重新部署下发。

----结束

4.3.4 删除组织合规规则包

操作场景

如果您不再需要某个组织合规规则包时，可按如下步骤进行删除操作。

操作步骤

步骤1 使用创建组织合规规则包的组织账号登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

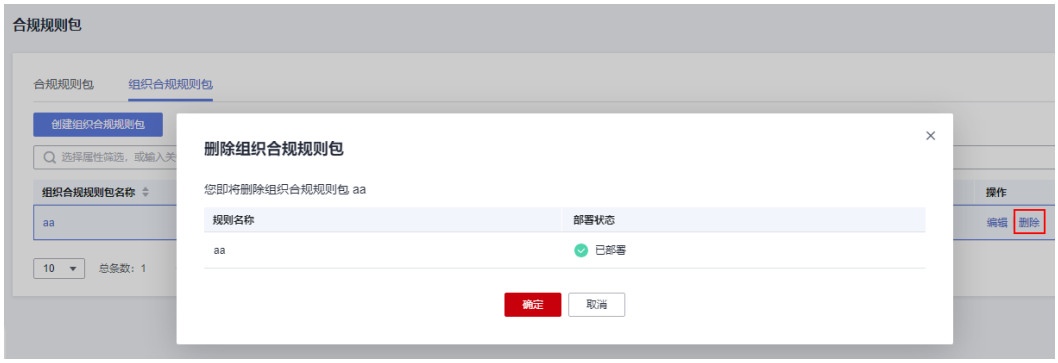
步骤3 单击页面左侧的“合规规则包”，进入“合规规则包”页面。

步骤4 选择“组织合规规则包”页签，在组织合规规则包列表中单击操作列的“删除”。

步骤5 在弹出的确认框中单击“确定”，完成组织合规规则包的删除。

组织合规规则包删除后，此组织合规规则包部署的成员账号的合规规则包列表中也将自动删除此合规规则包。

图 4-16 删除组织合规规则包



----结束

4.4 自定义合规规则包

如果您需要根据自身的需求创建自定义合规规则包，可以参考本节中的示例模板编写合规规则包模板文件，通过在创建合规规则包时选择“上传模板”或“OBS存储桶”的方式上传并使用。

概念介绍

Resource：Resource是模板中最重要的元素，通过关键字 "resource" 进行声明。当前"resource"中只支持"huaweicloud_rms_policy_assignment"一种资源，在其中指定具体的合规规则（支持预定义合规规则与自定义合规规则）的名称等配置信息。

变量：输入变量可以理解为模板的参数，通过关键字 "variable" 进行声明。通过定义输入变量，我们可以无需变更模板的源代码就能灵活修改配置。当没有变量时，不需要声明关键字 "variable" 。

Provider: Provider代表服务提供商，通过关键字 "terraform" 进行声明，详细定义请参见**Provider**。自定义合规规则包的格式为：

```
"terraform": {
  "required_providers": {
    "huaweicloud": {
      "source": "huawei.com/provider/huaweicloud",
      "version": "1.46.0"
    }
  }
}
```

其中version必须选择1.46.0或者更高的版本，支持的版本见**支持Provider版本列表**。

合规规则包示例文件： example-conformance-pack.tf.json

```
{
  "resource": {
    "huaweicloud_rms_policy_assignment": {
      "AccessKeysRotated": {
        "name": "access-keys-rotated",
        "description": "An IAM users is noncompliant if the access keys have not been rotated for more than maxAccessKeyAge number of days.",
        "policy_definition_id": "2a2938894ae786dc306a647a",
        "period": "TwentyFour_Hours",
        "parameters": {
          "maxAccessKeyAge": "${jsonencode(var.maxAccessKeyAge)}"
        }
      },
      "IamGroupHasUsersCheck": {
        "name": "iam-group-has-users-check",
        "description": "An IAM groups is noncompliant if it does not add any IAM user.",
        "policy_definition_id": "f7dd9c02266297f6e8c8445e",
        "policy_filter": {
          "resource_provider": "iam",
          "resource_type": "groups"
        },
        "parameters": {}
      },
      "IamPasswordPolicy": {
        "name": "iam-password-policy",
        "description": "An IAM users is noncompliant if password policy for IAM users matches the specified password strength.",
        "policy_definition_id": "2d8d3502539a623ba1907644",
        "policy_filter": {
          "resource_provider": "iam",
          "resource_type": "users"
        },
        "parameters": {
          "pwdStrength": "${jsonencode(var.pwdStrength)}"
        }
      },
      "IamRootAccessKeyCheck": {
        "name": "iam-root-access-key-check",
        "description": "An account is noncompliant if the the root iam user have active access key.",
        "policy_definition_id": "66cac2ddc17b6a25ad077253",
        "period": "TwentyFour_Hours",
        "parameters": {}
      },
      "IamUserConsoleAndApiAccessAtCreation": {
        "name": "iam-user-console-and-api-access-at-creation",
        "description": "An IAM user with console access is noncompliant if access keys are setup during the initial user setup.",
        "policy_definition_id": "a5f29eb45cddce8e6baa033d",
```



```
      "policy_filter": {
        "resource_provider": "iam",
        "resource_type": "users"
      },
      "parameters": {}
    },
    "IamUserGroupMembershipCheck": {
      "name": "iam-user-group-membership-check",
      "description": "An IAM user is noncompliant if it does not belong to any IAM user group.",
      "policy_definition_id": "846f5708463c1490c4eebd60",
      "policy_filter": {
        "resource_provider": "iam",
        "resource_type": "users"
      },
      "parameters": {
        "groupIds": "${jsonencode(var.groupIds)}"
      }
    },
    "IamUserLastLoginCheck": {
      "name": "iam-user-last-login-check",
      "description": "An IAM user is noncompliant if it has never signed in within the allowed number of
days.",
      "policy_definition_id": "6e4bf7ee7053b683f28d7f57",
      "period": "TwentyFour_Hours",
      "parameters": {
        "allowedInactivePeriod": "${jsonencode(var.allowedInactivePeriod)}"
      }
    },
    "IamUserMfaEnabled": {
      "name": "iam-user-mfa-enabled",
      "description": "An IAM user is noncompliant if it does not have multi-factor authentication (MFA)
enabled.",
      "policy_definition_id": "b92372b5eb51330306cec9c2",
      "policy_filter": {
        "resource_provider": "iam",
        "resource_type": "users"
      },
      "parameters": {}
    },
    "IamUserSingleAccessKey": {
      "name": "iam-user-single-access-key",
      "description": "An IAM user with console access is noncompliant if iam user have multiple active
access keys.",
      "policy_definition_id": "6deae3856c41b240b3c0bf8d",
      "policy_filter": {
        "resource_provider": "iam",
        "resource_type": "users"
      },
      "parameters": {}
    },
    "MfaEnabledForIamConsoleAccess": {
      "name": "mfa-enabled-for-iam-console-access",
      "description": "An IAM user is noncompliant if it uses a console password and does not have multi-
factor authentication (MFA) enabled.",
      "policy_definition_id": "63f8301e47b122062a68b868",
      "policy_filter": {
        "resource_provider": "iam",
        "resource_type": "users"
      },
      "parameters": {}
    },
    "RootAccountMfaEnabled": {
      "name": "root-account-mfa-enabled",
      "description": "An account is noncompliant if the the root iam user does not have multi-factor
authentication (MFA) enabled.",
      "policy_definition_id": "61d787a75cf7f5965da5d647",
      "period": "TwentyFour_Hours",
      "parameters": {}
    }
```



```
    }
  },
  "variable": {
    "maxAccessKeyAge": {
      "description": "The maximum number of days without rotation. ",
      "type": "string",
      "default": "90"
    },
    "pwdStrength": {
      "description": "The requirements of password strength. The parameter value can only be 'Strong',
'Medium', or 'Low'.",
      "type": "string",
      "default": "Strong"
    },
    "groupIds": {
      "description": "The list of allowed IAM    group IDs. If the list is empty, all values are allowed.",
      "type": "list(string)",
      "default": []
    },
    "allowedInactivePeriod": {
      "description": "Maximum number of days without login.",
      "type": "number",
      "default": 90
    }
  },
  "terraform": {
    "required_providers": {
      "huaweicloud": {
        "source": "huawei.com/provider/huaweicloud",
        "version": "1.46.0"
      }
    }
  }
}
```

合规规则包示例文件： example-conformance-pack-with-custom-policy.tf.json

```
{
    "resource": {
        "huaweicloud_rms_policy_assignment": {
            "CustomPolicyAssignment": {
                "name": "customPolicy${var.name_suffix}",
                "description": "合规包自定义合规规则，所有资源都是不合规的",
                "policy_filter": {
                    "resource_provider": "obs",
                    "resource_type": "buckets"
                },
                "parameters": {},
                "custom_policy": {
                    "function_urn": "${var.function_urn}",
                    "auth_type": "agency",
                    "auth_value": {
                        "agency_name": "\"config_custom_policy_agency\""
                    }
                }
            }
        }
    },
    "variable": {
        "name_suffix": {
            "description": "",
            "type": "string"
        },
        "function_urn": {
            "description": "",
            "type": "string"
        }
    },
    "terraform": {
```



```
    "required_providers": {
      "huaweicloud": {
        "source": "huawei.com/provider/huaweicloud",
        "version": "1.46.0"
      }
    }
  }
}
```

4.5 合规规则包示例模板

4.5.1 概述

配置审计服务提供合规规则包的示例模板，帮助用户通过示例模板快速创建合规规则包，每个合规规则包的示例模板中包含都多个合规规则，也就是配置审计服务的预设策略，每个预设策略的具体说明请参见**系统内置预设策略**。您可以通过**列举预定义合规规则包模板**接口查看所有的合规规则包示例模板。

配置审计服务控制台当前提供如下合规规则包的示例模板：

- **等保三级2.0规范检查的标准合规包**
- **适用于金融行业的合规实践**
- **华为云网络安全合规实践**
- **适用于统一身份认证服务（IAM）的最佳实践**
- **适用于云监控服务（CES）的最佳实践**
- **适用于计算服务的最佳实践**
- **适用于弹性云服务器（ECS）的最佳实践**
- **适用于弹性负载均衡（ELB）的最佳实践**
- **适用于管理与监管服务的最佳实践**
- **适用于云数据库（RDS）的最佳实践**
- **适用于弹性伸缩（AS）的最佳实践**
- **适用于云审计服务（CTS）的最佳实践**
- **适用于人工智能与机器学习场景的合规实践**
- **适用于自动驾驶场景的合规实践**
- **资源开启公网访问最佳实践**
- **适用于日志和监控的最佳实践**
- **适用于空闲资产管理的最佳实践**
- **华为云架构可靠性最佳实践**
- **适用于中国香港金融管理局的标准合规包**
- **适用于中小企业的ENISA的标准合规包**
- **适用于SWIFT CSP的标准合规包**
- **适用于德国云计算合规标准目录的标准合规包**
- **适用于PCI-DSS的标准合规包**
- **适用于医疗行业的合规实践**

4.5.2 等保三级 2.0 规范检查的标准合规包

本文为您介绍等保三级2.0规范检查的标准合规包的业务背景、应用场景，以及合规包中的默认规则。

业务背景

等保三级2.0规范是指中国政府在信息安全领域制定的一项标准，是中国信息安全等级保护制度的重要组成部分。该规范主要针对政府、金融、电信、能源等关键信息基础设施行业，旨在保障其信息系统的安全性、完整性和可用性，防范和应对各种安全威胁和风险。

关于网络安全等级保护基本要求的更多详细信息，请参见**GB/T 22239-2019**。

免责条款

本合规规则包模板为您提供通用的操作指引，帮助您快速创建符合目标场景的合规规则包。为避免疑义，本“合规”仅指资源符合规则定义本身的合规性描述，不构成任何法律意见。本合规规则包模板不确保符合特定法律法规或行业标准的要求，您需自行对您的业务、技术操作的合规性和合法性负责并承担与此相关的所有责任。

默认规则

此表中的建议项编号对应**GB/T 22239-2019**中参考文档的章节编号，供您查阅参考。

表 4-3

建议项编号	建议项说明	华为云合规规则	指导
8.1.2.1	b）应保证网络各个部分的带宽满足业务高峰期需要。	eip-bandwidth-limit	确保带宽满足业务高峰期需要。
8.1.2.1	c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。	dcs-redis-in-vpc	确保分布式缓存服务（DCS）所有流量都安全地保留在虚拟私有云（VPC）中。
8.1.2.1	c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。	dds-instance-in-vpc	确保文档数据库（DDS）所有流量都安全地保留在虚拟私有云（VPC）中。
8.1.2.1	c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。	ecs-instance-in-vpc	确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。

建议项编号	建议项说明	华为云合规规则	指导
8.1.2.1	c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。	rds-instances-in-vpc	确保关系型数据库（RDS）所有流量都安全地保留在虚拟私有云（VPC）中。
8.1.2.1	d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	dcs-redis-in-vpc	确保分布式缓存服务（DCS）所有流量都安全地保留在虚拟私有云（VPC）中。
8.1.2.1	d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	dds-instance-in-vpc	确保文档数据库（DDS）所有流量都安全地保留在虚拟私有云（VPC）中。
8.1.2.1	d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	ecs-instance-in-vpc	确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。
8.1.2.1	d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。	rds-instances-in-vpc	确保关系型数据库（RDS）所有流量都安全地保留在虚拟私有云（VPC）中。
8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。	ecs-instance-no-public-ip	由于华为云ecs实例可能包含敏感信息，确保华为云ecs实例无法公开访问来管理对华为云的访问。
8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。	elb-loadbalancers-no-public-ip	确保弹性负载均衡（ELB）无法公网访问，管理对华为云中资源的访问。

建议项编号	建议项说明	华为云合规规则	指导
8.1.3.1	b）应能够对非授权设备私自联到内部网络的行为进行限制或检查。	rds-instance-no-public-ip	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账户需要原则和访问控制。
8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。	ecs-instance-no-public-ip	由于华为云ecs实例可能包含敏感信息，确保华为云ecs实例无法公开访问来管理对华为云的访问。
8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。	elb-loadbalancers-no-public-ip	确保弹性负载均衡（ELB）无法公网访问，管理对华为云中资源的访问。
8.1.3.2	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。	rds-instance-no-public-ip	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账户需要原则和访问控制。
8.1.3.5	c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务（CTS）用于记录华为云管理控制台操作。
8.1.4.1	d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。	iam-user-mfa-enabled	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账户被盗用的事件。

建议项编号	建议项说明	华为云合规规则	指导
8.1.4.7	a）应采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	elb-tls-https-listeners-only	确保弹性负载均衡的监听器已配置HTTPS监听协议。由于可能存在敏感数据，因此启用传输中加密有助于保护该数据。
8.1.4.7	b）应采用密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	volumes-encrypted-check	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。
8.1.4.9	c）应提供重要数据处理系统的热冗余，保证系统的高可用性。	rds-instance-multi-az-support	华为云RDS中的多可用区支持为数据库实例提供了增强的可用性和持久性。当您预置多可用区数据库实例时，华为云 RDS会自动创建主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用区都在其物理上不同的独立基础设施上运行，并且经过精心设计，高度可靠。如果发生基础设施故障，华为云 RDS会自动故障转移到备用数据库，以便您可以在故障转移完成后立即恢复数据库操作。

4.5.3 适用于金融行业的合规实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-4 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
access-keys-rotated	IAM用户的AccessKey在指定时间内轮换	iam	企业用户通常都会使用访问密钥（AK/SK）的方式对云上资源的进行API访问，但是访问密钥需要做到定期的自动轮换，以降低密钥泄露等潜在的安全风险。	IAM用户的访问密钥未在指定天数内轮转，视为“不合规”.	用户可以通过使用API调用的方式轮换访问密钥。
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	根据ELB对云服务器的健康检查结果进行的检查，健康检查会将异常的实例从伸缩组中移除。这条规则确保与负载均衡器关联的伸缩组使用了弹性负载均衡健康检查。	与负载均衡器关联的伸缩组未使用弹性负载均衡健康检查，视为“不合规”	如果您将多个负载均衡器添加到伸缩组，则只有在所有负载均衡器均检测到云服务器状态为正常的情况下，才会认为该弹性云服务器正常。否则只要有一个负载均衡器检测到云服务器状态异常，伸缩组会将该弹性云服务器移出伸缩组。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
css-cluster-https-required	CSS集群启用HTTPS	css	开启HTTPS访问后，访问集群将进行通讯加密。关闭HTTPS访问后，会使用HTTP协议与集群通信，无法保证数据安全性，并且无法开启公网访问功能。	CSS集群未启用https，视为“不合规”	仅安全模式的集群支持开启HTTPS访问。启用HTTPS访问的安全集群可以单击“下载证书”获取CER安全证书，用于接入安全模式的集群。安全证书暂不支持在公网环境下使用。
css-cluster-in-vpc	CSS集群绑定指定VPC资源	css	云搜索服务CSS的集群创建在虚拟私有云（VPC）的子网内，VPC通过逻辑方式进行网络隔离，为用户的集群提供安全、隔离的网络环境。此规则确保云搜索服务（CSS）位于虚拟私有云（VPC）中。	CSS集群未与指定的vpc资源绑定，视为“不合规”	可以将不合规的CSS集群与指定vpc关联。
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	确保云审计服务（CTS）的追踪器已配置KMS加密存储用于归档的审计事件。	CTS追踪器未通过KMS进行加密，视为“不合规”	建议您配置独立OBS桶并配置KMS加密存储专门用于归档审计事件。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-lts-enable	CTS追踪器启用事件分析	cts	确保使用云日志服务（LTS）集中收集云审计服务（CTS）的数据。	CTS追踪器未启用事件分析，视为“不合规”	开通云审计日志后，系统会自动创建一个名为system的管理事件追踪器，并将当前租户的所有操作记录在该追踪器中。在追踪器中配置CTS转储到LTS，配置完成后会在LTS自动创建日志组日志流
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	由于CTS只支持查询7天的审计事件，为了您事后审计、查询、分析等要求，启用CTS追踪器请配置OBS服务桶。	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”	云审计服务管理控制台支持配置已开启的追踪器的OBS桶、LTS转储和配置已创建的追踪器关键事件操作通知。
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	在安全和事故调查中，通常由于事件文件被删除或者被私下篡改，而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您确保事件文件的真实性。	CTS追踪器未打开事件文件校验，视为“不合规”	在配置转储页面打开“文件校验”开关，即可开启事件文件完整性校验功能。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-tracker-exists	创建并启用CTS追踪器	cts	云审计服务支持创建数据类事件追踪器，用于记录数据操作日志。数据类追踪器用于记录数据事件，即针对租户对OBS桶中的数据的操作日志，例如上传、下载等。	账号未创建CTS追踪器，视为“不合规”	可进入云审计服务页面，导航栏选择“追踪器”，单击“创建追踪器”，根据提示操作。
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs，vpc	虚拟私有云（VPC）为弹性云服务器构建了一个逻辑上完全隔离的专有区域，您可以在自己的逻辑隔离区域中定义虚拟网络，为弹性云服务器构建一个逻辑上完全隔离的专有区域，确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”	您可以通过网络配置，为不合规的ECS资源选择特定的虚拟私有云。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	由于华为云ecs实例可能包含敏感信息，确保华为云ecs实例无法公开访问来管理对华为云的访问。	ECS资源具有公网IP，视为“不合规”	您可以登录弹性云服务器页面，在弹性云服务器列表中，在待调整带宽的弹性云服务器操作列下，单击“操作”列下的“更多 > 网络设置 > 解绑弹性公网IP”，将不合规的ECS资源解除弹性公网绑定。
eip-unbound-check	弹性公网IP未进行任何绑定	vpc	弹性公网IP（EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。此规则确保弹性公网IP未闲置。	弹性公网IP未进行任何绑定，视为“不合规”	用户可以通过申请弹性公网IP并将弹性公网IP绑定到特定的资源上。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	确保弹性负载均衡的监听器均已配置HTTPS监听协议。HTTPS协议适用于需要加密传输的应用。由于可能存在敏感数据，因此启用传输中加密有助于保护该数据。	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”	您可以添加一个HTTPS监听转发来自HTTPS协议的请求。独享型负载均衡前端协议为“HTTPS”时，后端协议可以选择“HTTP”或“HTTPS”。共享型负载均衡前端协议为“HTTPS”时，后端协议默认为“HTTP”，且不支持修改。如果您的独享型负载均衡实例类型为网络型（TCP/UDP），则无法创建HTTPS监听器。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
function-graph-concurrency-check	函数工作流的函数并发数在指定范围内	fgs	FunctionGraph会根据实际的请求情况自动弹性伸缩函数实例，并发变高时，会分配更多的函数实例来处理请求，并发减少时，相应的实例也会变少。此规则可确保建立函数工作流（FunctionGraph）的并发上限和下限。	FunctionGraph函数并发数不在指定的范围内，视为“不合规”	对于不合规的实例，在函数详情页可以修改函数并发数的值。
iam-group-has-users-check	IAM用户组添加了IAM用户	iam	管理员创建用户组并授权后，将用户加入用户组中，使用户具备用户组的权限，实现用户的授权。给已授权的用户组中添加或者移除用户，快速实现用户的权限变更。确保IAM组至少有一个用户，帮助您将最小权限和职责分离的原则与访问权限和授权结合起来。	IAM用户组未添加任意IAM用户，视为“不合规”	管理员在用户组列表中，单击新建的用户组，选择“用户组管理”，在“可选用户”中选择需要添加至用户组中的用户。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
iam-password-policy	IAM用户密码策略符合要求	iam	确保IAM用户密码强度满足密码强度要求。	IAM用户密码强度不满足密码强度要求，视为“不合规”	用户可以根据提示修改密码达到需要的密码强度。
iam-root-access-key-check	IAM账号存在可使用的访问密钥	iam	确保根访问密钥已删除。	账号存在可使用的访问密钥，视为“不合规”	用户可以根据规则评估结果删除账号可使用的访问密钥。
iam-user-group-membership-check	IAM用户归属用户组	iam	管理员创建用户组并授权后，将用户加入用户组中，使用户具备用户组的权限，实现用户的授权。给已授权的用户组中添加或者移除用户，快速实现用户的权限变更。	IAM用户不属于任意一个IAM用户组，视为“不合规”	可以选择一个用户组，以管理员的身份，将不合规的IAM用户添加到用户组中。
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	管理员创建IAM用户后，这个新建的IAM用户可以登录华为云。避免IAM用户资源闲置。	IAM用户在指定时间范围内无登录行为，视为“不合规”	您可以在华为云登录页面或者打开IAM用户专属链接，输入用户名和密码的方式登录IAM用户。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
iam-user-mfa-enabled	IAM用户开启MFA	iam	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账户被盗用的事件。	IAM用户未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。
kms-rotation-enabled	KMS密钥启用密钥轮换	kms	广泛重复的使用加密密钥，会对加密密钥的安全造成风险。为了确保加密密钥的安全性，建议您定期轮换密钥，更改原密钥的密钥材料。定期轮换密钥，有助于减少每个密钥加密的数据量，增强应对安全事件的能力以及加强对数据的隔离能力。	KMS密钥未启用密钥轮换，视为“不合规”	用户可以登录控制台，打开密钥轮换开关。仅对称密钥支持开启密钥轮换，开启密钥轮换需要密钥处于“启用”状态，“密钥材料来源”为“密钥管理”。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行 MFA，您可以减少账户被盗用的事件，并防止敏感数据被未经授权的用户访问。	通过Console密码登录的IAM用户未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。
mrs-cluster-in-vpc	MRS资源属于指定VPC	mrs	虚拟私有云（VPC）为mrs集群构建了一个逻辑上完全隔离的专有区域，您可以在自己的逻辑隔离区域中定义虚拟网络，为mrs集群构建一个逻辑上完全隔离的专有区域，确保mrs集群所有流量都安全地保留在虚拟私有云（VPC）中。	指定虚拟私有云ID，不属于此VPC的MRS资源，视为“不合规”	您可以通过网络配置，为不合规的MRS资源选择特定的虚拟私有云。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS 1.8.0版本之前未开启Kerberos认证的集群不支持访问权限细分。只有开启Kerberos认证才有角色管理权限，MRS 1.8.0及之后版本的所有集群均拥有角色管理权限。	MRS集群未开启kerberos认证，视为“不合规”	MRS服务暂不支持集群创建完成后手动开启和关闭Kerberos服务，如需更换Kerberos认证状态，建议重新创建MRS集群，然后进行数据迁移。
mrs-cluster-no-public-ip	MRS集群未绑定公网IP	mrs	确保MapReduce服务（MRS）无法公网访问。华为云MRS集群主节点可能包含敏感信息，并且此类账户需要访问控制。	MRS集群绑定公网IP，视为“不合规”	对于不合规的MRS资源，用户可以解除其与弹性公网IP的绑定。
private-nat-gateway-authorized-vpc-only	NAT私网网关绑定指定VPC资源	nat	确保NAT私网网关仅连接到授权的虚拟私有云（VPC）中，管理对华为云中资源的访问。	NAT私网网关未与指定的VPC资源绑定，视为“不合规”	用户可以修改NAT私网网关关联的子网。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-multi-az-support	RDS实例支持多可用区	rds	华为云RDS中的多可用区支持为数据库实例提供了增强的可用性和持久性。当您预置多可用区数据库实例时，华为云RDS会自动创建主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用区都在其物理上不同的独立基础设施上运行，并且经过精心设计，高度可靠。如果发生基础设施故障，华为云 RDS 会自动故障转移到备用数据库，以便您可以在故障转移完成后立即恢复数据库操作。	RDS实例仅支持一个可用区，视为“不合规”	华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-no-public-ip	RDS实例不具有公网IP	rds	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账户需要原则和访问控制。	RDS资源具有公网IP，视为“不合规”	对于不合规的RDS资源，用户可以解除其与弹性公网IP的绑定。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
root-account-mfa-enabled	根账号开启MFA认证	iam	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。多因素认证Multi-Factor Authentication（MFA）是一种非常简单的安全实践方法，它能够在用户名称和密码之外再额外增加一层保护。启用多因素认证后，用户进行操作时，除了需要提供用户名和密码外（第一次身份验证），还需要提供验证码（第二次身份验证），多因素身份认证结合起来将为您的账号和资源提供更高的安全保护。	根账号未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	启用此规则可根据您组织的标准检查华为云ecs实例的停止时间是否超过允许的天数，确保弹性云服务器（ECS）未闲置。	关机状态的ECS未进行任意操作的时间超过了允许的天数，视为“不合规”	包年/包月资源一次性付费，到期自动停止使用。其他计费模式下关机后仍然计费。如需停止计费，请删除实例。
volume-unused-check	云硬盘闲置检测	evs	云硬盘可以挂载至云服务器，用作提供系统盘和数据盘。此规则可以确保云硬盘（EVS）未闲置。	云硬盘未挂载给任何云服务器，视为“不合规”	对非合规的EVS资源，用户可以在云硬盘页面或在弹性云服务器页面，将其挂载到云服务器上。
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs，evs	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。	已挂载的云硬盘未进行加密，视为“不合规”	当您需要使用云硬盘加密功能时，需要授权EVS访问KMS。如果您拥有“Security Administrator”权限，则可直接授权。如果权限不足，需先联系拥有“Security Administrator”权限的用户授权EVS访问KMS，然后再重新操作。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
vpc-acl-unused-check	未与子网关联的网络ACL	vpc	网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的网络流量。此规则可确保现存网络ACL均与子网关联，实现对子网的防护。	检查是否存在未使用的网络ACL,如果网络ACL没有与子网关联，视为“不合规”	您可以将网络ACL关联至VPC子网，为子网内的资源提供安全防护。
vpc-flow-logs-enabled	VPC启用流日志	vpc	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。	检查是否为VPC启用了流日志，如果该VPC未启用流日志，视为“不合规”	您可以为不合规的VPC资源开启流日志记录，方式为：创建日志组、日志流之后，进入VPC流日志列表页面创建VPC流日志，按照提示配置参数。
vpc-sg-ports-check	安全组端口检查	vpc	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。	当安全组入方向源地址设置为0.0.0.0/0，且开放了所有的TCP/UDP端口时，视为“不合规”	用户可以修改不合规的安全组的规则。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
vpn-connections-active	VPN连接状态为“正常”	vpnaas	确保VPN连接状态正常。	VPN连接状态不为“正常”，视为“不合规”	VPN连接状态显示为“未连接”的可能原因有：VPN连接两端的连接配置不正确、华为云安全组和客户设备侧ACL配置不正确。可以检查VPN连接两端的连接配置和检查华为云安全组和客户设备侧ACL配置。
waf-instance-policy-not-empty	WAF防护域名配置防护策略	waf	确保WAF防护域名未配置防护策略	WAF防护域名未配置防护策略，视为“不合规”	您可以通过Web应用防火墙服务添加策略适用的防护域名。

4.5.4 华为云网络安全合规实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-5 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
access-keys-rotated	IAM用户的AccessKey在指定时间内轮换	iam	企业用户通常都会使用访问密钥（AK/SK）的方式对云上资源的进行API访问，但是访问密钥需要做到定期的自动轮换，以降低密钥泄露等潜在的安全风险。	IAM用户的访问密钥未在指定天数内轮转，视为“不合规”.	用户可以通过使用API调用的方式轮换访问密钥。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
alarm-kms-disable-or-delete-key	CES配置监控KMS禁用或计划删除的事件监控告警	ces，kms	事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。事件即云监控服务保存并监控的云服务资源的关键操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。CES事件监控可以支持密钥管理服务(KMS)的相关事件，包含禁用密钥和计划删除密钥等。	CES未配置监控KMS禁用或计划删除密钥的事件监控告警，视为“不合规”	用户可以在事件监控中创建告警规则，选择对应的监控对象，配置告警内容参数。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
alarm-obs-bucket-policy-change	CES配置监控OBS桶策略变更的事件监控告警	ces，obs	事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。事件即云监控服务保存并监控的云服务资源的关键操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。CES事件监控可以支持对象存储服务(OBS)的相关事件，包含设置桶的策略和删除桶policy配置等。	CES未配置监控OBS桶策略变更的事件监控告警，视为“不合规”	用户可以在事件监控中创建告警规则，选择对应的监控对象，配置告警内容参数。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
alarm-vpc-change	CES配置监控VPC变更的事件监控告警	ces，vpc	事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。事件即云监控服务保存并监控的云服务资源的关键操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。CES事件监控可以支持弹性公网IP和带宽的相关事件，包含删除VPC和修改VPC等。	CES未配置监控VPC变更的事件监控告警，视为“不合规”	用户可以在事件监控中创建告警规则，选择对应的监控对象，配置告警内容参数。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
css-cluster-https-required	CSS集群启用HTTPS	css	开启HTTPS访问后，访问集群将进行通讯加密。关闭HTTPS访问后，会使用HTTP协议与集群通信，无法保证数据安全性，并且无法开启公网访问功能。	CSS集群未启用https，视为“不合规”	仅安全模式的集群支持开启HTTPS访问。启用HTTPS访问的安全集群可以单击“下载证书”获取CER安全证书，用于接入安全模式的集群。安全证书暂不支持在公网环境下使用。
css-cluster-in-vpc	CSS集群绑定指定VPC资源	css	云搜索服务CSS的集群创建在虚拟私有云（VPC）的子网内，VPC通过逻辑方式进行网络隔离，为用户的集群提供安全、隔离的网络环境。此规则确保云搜索服务（CSS）位于虚拟私有云（VPC）中。	CSS集群未与指定的VPC资源绑定，视为“不合规”	可以将不合规的CSS集群与指定VPC关联。
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	确保云审计服务（CTS）的追踪器已配置KMS加密存储用于归档的审计事件。	CTS追踪器未通过KMS进行加密，视为“不合规”	建议您配置独立OBS桶并配置KMS加密存储专门用于归档审计事件。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-lts-enable	CTS追踪器启用事件分析	cts	确保使用云日志服务（LTS）集中收集云审计服务（CTS）的数据。	CTS追踪器未启用事件分析，视为“不合规”	开通云审计日志后，系统会自动创建一个名为system的管理事件追踪器，并将当前租户的所有操作记录在该追踪器中。在追踪器中配置CTS转储到LTS，配置完成后会在LTS自动创建日志组日志流
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	由于CTS只支持查询7天的审计事件，为了您事后审计、查询、分析等要求，启用CTS追踪器请配置OBS服务桶。	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”	云审计服务管理控制台支持配置已开启的追踪器的OBS桶、LTS转储和配置已创建的追踪器关键事件操作通知。
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	在安全和事故调查中，通常由于事件文件被删除或者被私下篡改，而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您确保事件文件的真实性。	CTS追踪器未打开事件文件校验，视为“不合规”	在配置转储页面打开“文件校验”开关，即可开启事件文件完整性校验功能。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-tracker-exists	创建并启用CTS追踪器	cts	云审计服务支持创建数据类事件追踪器，用于记录数据操作日志。数据类追踪器用于记录数据事件，即针对租户对OBS桶中的数据的操作日志，例如上传、下载等。	账号未创建CTS追踪器，视为“不合规”	可进入云审计服务页面，导航栏选择“追踪器”，单击“创建追踪器”，根据提示操作。
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs，vpc	虚拟私有云（VPC）为弹性云服务器构建了一个逻辑上完全隔离的专有区域，您可以在自己的逻辑隔离区域中定义虚拟网络，为弹性云服务器构建一个逻辑上完全隔离的专有区域，确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”	您可以通过网络配置，为不合规的ECS资源选择特定的虚拟私有云。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	由于华为云ecs实例可能包含敏感信息，确保华为云ecs实例无法公开访问来管理对华为云的访问。	ECS资源具有公网IP，视为“不合规”	您可以登录弹性云服务器页面，在弹性云服务器列表中，在待调整带宽的弹性云服务器操作列下，单击“操作”列下的“更多 > 网络设置 > 解绑弹性公网IP”，将不合规的ECS资源解除弹性公网绑定。
eip-unbound-check	弹性公网IP未进行任何绑定	vpc	弹性公网IP（EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。此规则确保弹性公网IP未闲置。	弹性公网IP未进行任何绑定，视为“不合规”	用户可以通过申请弹性公网IP并将弹性公网IP绑定到特定的资源上。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	确保弹性负载均衡的监听器均已配置HTTPS监听协议。HTTPS协议适用于需要加密传输的应用。由于可能存在敏感数据，因此启用传输中加密有助于保护该数据。	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”	您可以添加一个HTTPS监听转发来自HTTPS协议的请求。独享型负载均衡前端协议为“HTTPS”时，后端协议可以选择“HTTP”或“HTTPS”。共享型负载均衡前端协议为“HTTPS”时，后端协议默认为“HTTP”，且不支持修改。如果您的独享型负载均衡实例类型为网络型（TCP/UDP），则无法创建HTTPS监听器。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
iam-group-has-users-check	IAM用户组添加了IAM用户	iam	管理员创建用户组并授权后，将用户加入用户组中，使用户具备用户组的权限，实现用户的授权。给已授权的用户组中添加或者移除用户，快速实现用户的权限变更。确保IAM组至少有一个用户，帮助您将最小权限和职责分离的原则与访问权限和授权结合起来。	IAM用户组未添加任意IAM用户，视为“不合规”	管理员在用户组列表中，单击新建的用户组，选择“用户组管理”，在“可选用户”中选择需要添加至用户组中的用户。
iam-password-policy	IAM用户密码策略符合要求	iam	确保IAM用户密码强度满足密码强度要求。	IAM用户密码强度不满足密码强度要求，视为“不合规”	用户可以根据提示修改密码达到需要的密码强度。
iam-root-access-key-check	IAM账号存在可使用的访问密钥	iam	确保根访问密钥已删除。	账号存在可使用的访问密钥，视为“不合规”	用户可以根据规则评估结果删除账号可使用的访问密钥。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
iam-user-console-and-api-access-at-creation	IAM用户创建时设置AccessKey	iam	访问密钥即AK/SK（Access Key ID/Secret Access Key），是您通过开发工具（API、CLI、SDK）访问华为云时的身份凭证，不能登录控制台。	对于从Console侧访问的IAM用户，其创建时设置访问密钥，视为“不合规”	用户可以根据规则评估结果删除或停用访问密钥。
iam-user-group-membership-check	IAM用户归属用户组	iam	管理员创建用户组并授权后，将用户加入用户组中，使用户具备用户组的权限，实现用户的授权。给已授权的用户组中添加或者移除用户，快速实现用户的权限变更。	IAM用户不属于任意一个IAM用户组，视为“不合规”	可以选择一个用户组，以管理员的身份，将不合规的IAM用户添加到用户组中。
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	管理员创建IAM用户后，这个新建的IAM用户可以登录华为云。避免IAM用户资源闲置。	IAM用户在指定时间范围内无登录行为，视为“不合规”	您可以在华为云登录页面或者打开IAM用户专属链接，输入用户名和密码的方式登录IAM用户。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
iam-user-mfa-enabled	IAM用户开启MFA	iam	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账户被盗用的事件。	IAM用户未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。
iam-user-single-access-key	IAM用户单访问密钥	iam	账号和IAM用户的访问密钥是单独的身份凭证，即账号和IAM用户仅能使用自己的访问密钥进行API调用。	IAM用户拥有多个处于“active”状态的访问密钥，视为“不合规”	用户可以根据规则评估结果删除或停用多余的访问密钥。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行 MFA，您可以减少账户被盗用的事件，并防止敏感数据被未经授权的用户访问。	通过Console密码登录的IAM用户未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。
mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS 1.8.0版本之前未开启Kerberos认证的集群不支持访问权限细分。只有开启Kerberos认证才有角色管理权限，MRS 1.8.0及之后版本的所有集群均拥有角色管理权限。	MRS集群未开启kerberos认证，视为“不合规”	MRS服务暂不支持集群创建完成后手动开启和关闭Kerberos服务，如需更换Kerberos认证状态，建议重新创建MRS集群，然后进行数据迁移。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
mrs-cluster-no-public-ip	MRS集群未绑定公网IP	mrs	确保MapReduce服务（MRS）无法公网访问。华为云MRS集群主节点可能包含敏感信息，并且此类账户需要访问控制。	MRS集群绑定公网IP，视为“不合规”	对于不合规的MRS资源，用户可以解除其与弹性公网IP的绑定。
private-nat-gateway-authorized-vpc-only	NAT私网网关绑定指定VPC资源	nat	确保NAT私网网关仅连接到授权的虚拟私有云（VPC）中，管理对华为云中资源的访问。	NAT私网网关未与指定的VPC资源绑定，视为“不合规”	用户可以修改NAT私网网关关联的子网。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-multi-az-support	RDS实例支持多可用区	rds	华为云RDS中的多可用区支持为数据库实例提供了增强的可用性和持久性。当您预置多可用区数据库实例时，华为云RDS会自动创建主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用区都在其物理上不同的独立基础设施上运行，并且经过精心设计，高度可靠。如果发生基础设施故障，华为云 RDS 会自动故障转移到备用数据库，以便您可以在故障转移完成后立即恢复数据库操作。	RDS实例仅支持一个可用区，视为“不合规”	华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-no-public-ip	RDS实例不具有公网IP	rds	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账户需要原则和访问控制。	RDS资源具有公网IP，视为“不合规”	对于不合规的RDS资源，用户可以解除其与弹性公网IP的绑定。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
root-account-mfa-enabled	根账号开启MFA认证	iam	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。多因素认证Multi-Factor Authentication（MFA）是一种非常简单的安全实践方法，它能够在用户名称和密码之外再额外增加一层保护。启用多因素认证后，用户进行操作时，除了需要提供用户名和密码外（第一次身份验证），还需要提供验证码（第二次身份验证），多因素身份认证结合起来将为您的账号和资源提供更高的安全保护。	根账号未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	启用此规则可根据您组织的标准检查华为云ecs实例的停止时间是否超过允许的天数，确保弹性云服务器（ECS）未闲置。	关机状态的ECS未进行任意操作的时间超过了允许的天数，视为“不合规”	包年/包月资源一次性付费，到期自动停止使用。其他计费模式下关机后仍然计费。如需停止计费，请删除实例。
volume-unused-check	云硬盘闲置检测	evs	云硬盘可以挂载至云服务器，用作提供系统盘和数据盘。此规则可以确保云硬盘（EVS）未闲置。	云硬盘未挂载给任何云服务器，视为“不合规”	对非合规的EVS资源，用户可以在云硬盘页面或在弹性云服务器页面，将其挂载到云服务器上。
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs，evs	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。	已挂载的云硬盘未进行加密，视为“不合规”	当您需要使用云硬盘加密功能时，需要授权EVS访问KMS。如果您拥有“Security Administrator”权限，则可直接授权。如果权限不足，需先联系拥有“Security Administrator”权限的用户授权EVS访问KMS，然后再重新操作。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
vpc-acl-unused-check	未与子网关联的网络ACL	vpc	网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的网络流量。此规则可确保现存网络ACL均与子网关联，实现对子网的防护。	检查是否存在未使用的网络ACL,如果网络ACL没有与子网关联，视为“不合规”	您可以将网络ACL关联至VPC子网，为子网内的资源提供安全防护。
vpc-flow-logs-enabled	VPC启用流日志	vpc	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。	检查是否为VPC启用了流日志，如果该VPC未启用流日志，视为“不合规”	您可以为不合规的VPC资源开启流日志记录，方式为：创建日志组、日志流之后，进入VPC流日志列表页面创建VPC流日志，按照提示配置参数。

4.5.5 适用于统一身份认证服务（IAM）的最佳实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-6 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
access-keys-rotated	IAM用户的AccessKey在指定时间内轮换	iam	企业用户通常都会使用访问密钥（AK/SK）的方式对云上资源的进行API访问，但是访问密钥需要做到定期的自动轮换，以降低密钥泄露等潜在的安全风险。	IAM用户的访问密钥未在指定天数内轮转，视为“不合规”.	用户可以通过使用API调用的方式轮换访问密钥。
iam-group-has-users-check	IAM用户组添加了IAM用户	iam	管理员创建用户组并授权后，将用户加入用户组中，使用户具备用户组的权限，实现用户的授权。给已授权的用户组中添加或者移除用户，快速实现用户的权限变更。确保IAM组至少有一个用户，帮助您将最小权限和职责分离的原则与访问权限和授权结合起来。	IAM用户组未添加任意IAM用户，视为“不合规”	管理员在用户组列表中，单击新建的用户组，选择“用户组管理”，在“可选用户”中选择需要添加至用户组中的用户。
iam-password-policy	IAM用户密码策略符合要求	iam	确保IAM用户密码强度满足密码强度要求。	IAM用户密码强度不满足密码强度要求，视为“不合规”	用户可以根据提示修改密码达到需要的密码强度。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
iam-root-access-key-check	IAM账号存在可使用的访问密钥	iam	确保根访问密钥已删除。	账号存在可使用的访问密钥，视为“不合规”	用户可以根据规则评估结果删除账号可使用的访问密钥。
iam-user-console-and-api-access-at-creation	IAM用户创建时设置AccessKey	iam	访问密钥即AK/SK（Access Key ID/Secret Access Key），是您通过开发工具（API、CLI、SDK）访问华为云时的身份凭证，不能登录控制台。	对于从Console侧访问的IAM用户，其创建时设置访问密钥，视为“不合规”	用户可以根据规则评估结果删除或停用访问密钥。
iam-user-group-membership-check	IAM用户归属用户组	iam	管理员创建用户组并授权后，将用户加入用户组中，使用户具备用户组的权限，实现用户的授权。给已授权的用户组中添加或者移除用户，快速实现用户的权限变更。	IAM用户不属于任意一个IAM用户组，视为“不合规”	可以选择一个用户组，以管理员的身份，将不合规的IAM用户添加到用户组中。
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	管理员创建IAM用户后，这个新建的IAM用户可以登录华为云。避免IAM用户资源闲置。	IAM用户在指定时间范围内无登录行为，视为“不合规”	您可以在华为云登录页面或者打开IAM用户专属链接，输入用户名和密码的方式登录IAM用户。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
iam-user-mfa-enabled	IAM用户开启MFA	iam	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账户被盗用的事件。	IAM用户未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。
iam-user-single-access-key	IAM用户单访问密钥	iam	账号和IAM用户的访问密钥是单独的身份凭证，即账号和IAM用户仅能使用自己的访问密钥进行API调用。	IAM用户拥有多个处于“active”状态的访问密钥，视为“不合规”	用户可以根据规则评估结果删除或停用多余的访问密钥。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行 MFA，您可以减少账户被盗用的事件，并防止敏感数据被未经授权的用户访问。	通过Console密码登录的IAM用户未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
root-account-mfa-enabled	根账号开启MFA认证	iam	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。多因素认证Multi-Factor Authentication（MFA）是一种非常简单的安全实践方法，它能够在用户名称和密码之外再额外增加一层保护。启用多因素认证后，用户进行操作时，除了需要提供用户名和密码外（第一次身份验证），还需要提供验证码（第二次身份验证），多因素身份认证结合起来将为您的账号和资源提供更高的安全保护。	根账号未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。

4.5.6 适用于云监控服务（CES）的最佳实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-7 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
alarm-action-enabled-check	启用了CES告警操作	ces	确保启用了CES告警操作,用户对云服务的核心监控指标设置告警规则，当监控指标触发用户设置的告警条件时,云监控服务使用消息通知服务向用户通知告警信息。	CES告警操作未启用，视为“不合规”	您需要在消息通知服务界面创建一个主题并为这个主题添加相关的订阅者，然后在添加告警规则的时候，您需要开启消息通知服务并选择创建的主题，这样在云服务发生异常时，云监控服务可以实时的将告警信息以广播的方式通知这些订阅者。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
alarm-kms-disable-or-delete-key	CES配置监控KMS禁用或计划删除的事件监控告警	ces，kms	事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。事件即云监控服务保存并监控的云服务资源的关键操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。CES事件监控可以支持密钥管理服务(KMS)的相关事件，包含禁用密钥和计划删除密钥等。	CES未配置监控KMS禁用或计划删除密钥的事件监控告警，视为“不合规”	用户可以在事件监控中创建告警规则，选择对应的监控对象，配置告警内容参数。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
alarm-obs-bucket-policy-change	CES配置监控OBS桶策略变更的事件监控告警	ces，obs	事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。事件即云监控服务保存并监控的云服务资源的关键操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。CES事件监控可以支持对象存储服务(OBS)的相关事件，包含设置桶的策略和删除桶policy配置等。	CES未配置监控OBS桶策略变更的事件监控告警，视为“不合规”	用户可以在事件监控中创建告警规则，选择对应的监控对象，配置告警内容参数。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
alarm-vpc-change	CES配置监控VPC变更的事件监控告警	ces，vpc	事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。事件即云监控服务保存并监控的云服务资源的关键操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。CES事件监控可以支持弹性公网IP和带宽的相关事件，包含删除VPC和修改VPC等。	CES未配置监控VPC变更的事件监控告警，视为“不合规”	用户可以在事件监控中创建告警规则，选择对应的监控对象，配置告警内容参数。

4.5.7 适用于计算服务的最佳实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-8 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
as-capacity-rebalancing	弹性伸缩组均衡扩容	as	EQUILIBRIUM_DISTRIBUTE（默认）：均衡分布，虚拟机扩缩容时优先保证available_zones列表中各AZ下虚拟机数量均衡，当无法在目标AZ下完成虚拟机扩容时，按照PICK_FIRST原则选择其他可用AZ。	弹性伸缩组扩缩容时，没有使用‘EQUILIBRIUM_DISTRIBUTE’优先级策略，视为“不合规”	用户可以将伸缩组扩缩容时目标AZ选择的优先级策略设置为EQUILIBRIUM_DISTRIBUTE。
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	根据ELB对云服务器的健康检查结果进行的检查，健康检查会将异常的实例从伸缩组中移除。这条规则确保与负载均衡器关联的伸缩组使用了弹性负载均衡健康检查。	与负载均衡器关联的伸缩组未使用弹性负载均衡健康检查，视为“不合规”	如果您将多个负载均衡器添加到伸缩组，则只有在所有负载均衡器均检测到云服务器状态为正常的情况下，才会认为该弹性云服务器正常。否则只要有一个负载均衡器检测到云服务器状态异常，伸缩组会将该弹性云服务器移出伸缩组。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
as-multiple-az	弹性伸缩组启用多AZ部署	as	一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。	弹性伸缩组没有启用多AZ部署，视为“不合规”	华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
ecs-instance-key-pair-login	ECS资源配置秘钥对	ecs	密钥对包含一个公钥和一个私钥，公钥自动保存在KPS（Key Pair Service）中，私钥由用户保存在本地。若用户将公钥配置在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。	ECS未配置秘钥对，视为“不合规”	您可以使用已有密钥对或新建一个密钥对，用于远程登录身份验证。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	由于华为云ecs实例可能包含敏感信息，确保华为云ecs实例无法公开访问来管理对华为云的访问。	ECS资源具有公网IP，视为“不合规”	您可以登录弹性云服务器页面，在弹性云服务器列表中，在待调整带宽的弹性云服务器操作列下，单击“操作”列下的“更多 > 网络设置 > 解绑弹性公网IP”，将不合规的ECS资源解除弹性公网绑定。
ecs-multiple-public-ip-check	检查ECS资源是否具有多个公网IP	ecs	此规则检查您的华为云ECS实例是否具有多个公网IP。拥有多个公网IP可能会增加网络安全的复杂性。	ECS资源具有多个公网IP，视为“不合规”	当云服务器拥有多张网卡时，如果需要配置多个弹性公网IP，此时需要在云服务器内部为这些网卡配置策略路由，才可以确保多张网卡均可以和外部正常通信。
eip-bandwidth-limit	EIP带宽限制	eip	确保带宽满足业务高峰期需要。带宽大小过低，可能会影响业务流量造成丢包	弹性IP实例可用带宽小于指定参数值，视为“不合规”	您可以根据独享带宽和共享带宽两种情况修改带宽值

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
function-graph-concurrency-check	函数工作流的函数并发数在指定范围内	fgs	FunctionGraph会根据实际的请求情况自动弹性伸缩函数实例，并发变高时，会分配更多的函数实例来处理请求，并发减少时，相应的实例也会变少。此规则可确保建立函数工作流（FunctionGraph）的并发上限和下限。	FunctionGraph函数并发数不在指定的范围内，视为“不合规”	对于不合规的实例，在函数详情页可以修改函数并发数的值。
function-graph-public-access-prohibited	函数工作流的函数不允许访问公网	fgs	确保函数工作流的函数不能公开访问，管理对华为云中资源的访问。公开访问可能导致资源可用性下降。	函数工作流的函数允许访问公网，视为“不合规”	部署在VPC中的函数默认是和外网隔离开的，用户可以将函数绑定VPC，并且不添加公网NAT网关。
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	启用此规则可根据您组织的标准检查华为云ecs实例的停止时间是否超过允许的天数，确保弹性云服务器（ECS）未闲置。	关机状态的ECS未进行任意操作的时间超过了允许的天数，视为“不合规”	包年/包月资源一次性付费，到期自动停止使用。其他计费模式下关机后仍然计费。如需停止计费，请删除实例。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
volume-unused-check	云硬盘闲置检测	evs	云硬盘可以挂载至云服务器，用作提供系统盘和数据盘。此规则可以确保云硬盘（EVS）未闲置。	云硬盘未挂载给任何云服务器，视为“不合规”	对非合规的EVS资源，用户可以在云硬盘页面或在弹性云服务器页面，将其挂载到云服务器上。
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs，evs	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。	已挂载的云硬盘未进行加密，视为“不合规”	当您需要使用云硬盘加密功能时，需要授权EVS访问KMS。如果您拥有“Security Administrator”权限，则可直接授权。如果权限不足，需先联系拥有“Security Administrator”权限的用户授权EVS访问KMS，然后再重新操作。

4.5.8 适用于弹性云服务器（ECS）的最佳实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-9 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
ecs-instance-key-pair-login	ECS资源配置秘钥对	ecs	密钥对包含一个公钥和一个私钥，公钥自动保存在KPS（Key Pair Service）中，私钥由用户保存在本地。若用户将公钥配置在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。	ECS未配置秘钥对，视为“不合规”	您可以使用已有密钥对或新建一个密钥对，用于远程登录身份验证。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	由于华为云ecs实例可能包含敏感信息，确保华为云ecs实例无法公开访问来管理对华为云的访问。	ECS资源具有公网IP，视为“不合规”	您可以登录弹性云服务器页面，在弹性云服务器列表中，在待调整带宽的弹性云服务器操作列下，单击“操作”列下的“更多 > 网络设置 > 解绑弹性公网IP”，将不合规的ECS资源解除弹性公网绑定。
ecs-multiple-public-ip-check	检查ECS资源是否具有多个公网IP	ecs	此规则检查您的华为云ECS实例是否具有多个公网IP。拥有多个公网IP可能会增加网络安全的复杂性。	ECS资源具有多个公网IP，视为“不合规”	当云服务器拥有多张网卡时，如果需要配置多个弹性公网IP，此时需要在云服务器内部为这些网卡配置策略路由，才可以确保多张网卡均可以和外部正常通信。
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	启用此规则可根据您组织的标准检查华为云ecs实例的停止时间是否超过允许的天数，确保弹性云服务器（ECS）未闲置。	关机状态的ECS未进行任意操作的时间超过了允许的天数，视为“不合规”	包年/包月资源一次性付费，到期自动停止使用。其他计费模式下关机后仍然计费。如需停止计费，请删除实例。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs，evs	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。	已挂载的云硬盘未进行加密，视为“不合规”	当您需要使用云硬盘加密功能时，需要授权EVS访问KMS。如果您拥有“Security Administrator”权限，则可直接授权。如果权限不足，需先联系拥有“Security Administrator”权限的用户授权EVS访问KMS，然后再重新操作。

4.5.9 适用于弹性负载均衡（ELB）的最佳实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-10 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
elb-loadbalancers-no-public-ip	ELB资源不具有公网IP	elb	确保弹性负载均衡（ELB）无法公网访问，管理对华为云中资源的访问。	ELB资源具有公网IP，视为“不合规”	用户可以解除不合规资源的公网绑定。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
elb-predefined-security-policy-https-check	ELB监听器配置指定预定义安全策略	elb	对于银行，金融类加密传输的应用，在创建和配置HTTPS监听器时，您可以选择使用安全策略，可以提高您的业务安全性。安全策略包含TLS协议版本和配套的加密算法套件。	独享型负载均衡器关联的HTTPS协议类型监听器未配置指定的预定义安全策略，视为“不合规“	独享型负载均衡支持选择默认安全策略或创建自定义策略。您可以为HTTPS监听器选择指定的预定义安全策略。
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	确保弹性负载均衡的监听器均已配置HTTPS监听协议。HTTPS协议适用于需要加密传输的应用。由于可能存在敏感数据，因此启用传输中加密有助于保护该数据。	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”	您可以添加一个HTTPS监听转发来自HTTPS协议的请求。独享型负载均衡前端协议为“HTTPS”时，后端协议可以选择“HTTP”或“HTTPS”。共享型负载均衡前端协议为“HTTPS”时，后端协议默认为“HTTP”，且不支持修改。如果您的独享型负载均衡实例类型为网络型（TCP/UDP），则无法创建HTTPS监听器。

4.5.10 适用于管理与监管服务的最佳实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-11 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
alarm-action-enabled-check	启用了CES告警操作	ces	确保启用了CES告警操作,用户对云服务的核心监控指标设置告警规则，当监控指标触发用户设置的告警条件时,云监控服务使用消息通知服务向用户通知告警信息。	CES告警操作未启用，视为“不合规”	您需要在消息通知服务界面创建一个主题并为这个主题添加相关的订阅者，然后在添加告警规则的时候，您需要开启消息通知服务并选择创建的主题，这样在云服务发生异常时，云监控服务可以实时的将告警信息以广播的方式通知这些订阅者。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
alarm-kms-disable-or-delete-key	CES配置监控KMS禁用或计划删除的事件监控告警	ces，kms	事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。事件即云监控服务保存并监控的云服务资源的关键操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。CES事件监控可以支持密钥管理服务(KMS)的相关事件，包含禁用密钥和计划删除密钥等。	CES未配置监控KMS禁用或计划删除密钥的事件监控告警，视为“不合规”	用户可以在事件监控中创建告警规则，选择对应的监控对象，配置告警内容参数。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
alarm-obs-bucket-policy-change	CES配置监控OBS桶策略变更的事件监控告警	ces，obs	事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。事件即云监控服务保存并监控的云服务资源的关键操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。CES事件监控可以支持对象存储服务(OBS)的相关事件，包含设置桶的策略和删除桶policy配置等。	CES未配置监控OBS桶策略变更的事件监控告警，视为“不合规”	用户可以在事件监控中创建告警规则，选择对应的监控对象，配置告警内容参数。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
alarm-vpc-change	CES配置监控VPC变更的事件监控告警	ces，vpc	事件监控提供了事件类型数据上报、查询和告警的功能。方便您将业务中的各类重要事件或对云资源的操作事件收集到云监控服务，并在事件发生时进行告警。事件即云监控服务保存并监控的云服务资源的关键操作。您可以通过“事件”了解到谁在什么时间对系统哪些资源做了什么操作。CES事件监控可以支持弹性公网IP和带宽的相关事件，包含删除VPC和修改VPC等。	CES未配置监控VPC变更的事件监控告警，视为“不合规”	用户可以在事件监控中创建告警规则，选择对应的监控对象，配置告警内容参数。
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	确保云审计服务（CTS）的追踪器已配置KMS加密存储用于归档的审计事件。	CTS追踪器未通过KMS进行加密，视为“不合规”	建议您配置独立OBS桶并配置KMS加密存储专门用于归档审计事件。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-lts-enable	CTS追踪器启用事件分析	cts	确保使用云日志服务（LTS）集中收集云审计服务（CTS）的数据。	CTS追踪器未启用事件分析，视为“不合规”	开通云审计日志后，系统会自动创建一个名为system的管理事件追踪器，并将当前租户的所有操作记录在该追踪器中。在追踪器中配置CTS转储到LTS，配置完成后会在LTS自动创建日志组日志流
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	在安全和事故调查中，通常由于事件文件被删除或者被私下篡改，而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您确保事件文件的真实性。	CTS追踪器未打开事件文件校验，视为“不合规”	在配置转储页面打开“文件校验”开关，即可开启事件文件完整性校验功能。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-tracker-exists	创建并启用CTS追踪器	cts	云审计服务支持创建数据类事件追踪器，用于记录数据操作日志。数据类追踪器用于记录数据事件，即针对租户对OBS桶中的数据的操作日志，例如上传、下载等。	账号未创建CTS追踪器，视为“不合规”	可进入云审计服务页面，导航栏选择“追踪器”，单击“创建追踪器”，根据提示操作。
tracker-config-enabled-check	账号开启资源记录器	config	资源记录器为您提供面向资源的配置记录监控能力，您必须先开启资源记录器，然后才可以配置并使用资源记录器来跟踪云平台上的资源变更情况。	如果账号未开启资源记录器，视为“不合规”	用户可以进入Config页面，打开资源记录器开关，根据提示选择相关配置，单击保存。

4.5.11 适用于云数据库（RDS）的最佳实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-12 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-enable-backup	RDS实例开启备份	rds	RDS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，自动备份为全量备份。系统根据您指定的备份保留期保存数据库实例的自动备份。如果需要，您可以将数据恢复到备份保留期中的任意时间点。开启自动备份策略后，会自动触发一次全量备份，备份方式为物理备份。之后会按照策略中的备份时间段和备份周期进行全量备份。自动备份策略开启后，实例每五分钟会自动进行一次增量备份，以保证数据库可靠性。确保云数据库（rds）资源开启备份。	未开启备份的RDS资源，视为“不合规”	用户可根据需要修改备份策略。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-enable-errorLog	RDS实例开启错误日志	rds	云数据库RDS服务的日志管理功能支持查看数据库级别的日志，包括数据库主库和从库运行的错误信息，以及运行较慢的SQL查询语句，有助于您分析系统中存在的问题。错误日志记录了数据库运行的实时日志，您可以通过错误日志分析系统中存在的问题，您也可以下载错误日志进行业务分析。	未开启错误日志的RDS资源，视为“不合规”	用户可以根据需要配置错误日志。
rds-instance-enable-slowLog	RDS实例开启慢日志	rds	慢日志用来记录执行时间超过当前慢日志阈值“log_min_duration_statement”的语句，您可以通过慢日志的日志明细、统计分析情况，查找出执行效率低的语句，进行优化。您也可以下载慢日志进行业务分析。	未开启慢日志的RDS资源，视为“不合规”	用户可以根据需要配置慢日志

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-multi-az-support	RDS实例支持多可用区	rds	华为云RDS中的多可用区支持为数据库实例提供了增强的可用性和持久性。当您预置多可用区数据库实例时，华为云RDS会自动创建主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用区都在其物理上不同的独立基础设施上运行，并且经过精心设计，高度可靠。如果发生基础设施故障，华为云 RDS 会自动故障转移到备用数据库，以便您可以在故障转移完成后立即恢复数据库操作。	RDS实例仅支持一个可用区，视为“不合规”	华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-no-public-ip	RDS实例不具有公网IP	rds	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账户需要原则和访问控制。	RDS资源具有公网IP，视为“不合规”	对于不合规的RDS资源，用户可以解除其与弹性公网IP的绑定。
rds-instances-enable-kms	RDS实例开启存储加密	rds	云数据库RDS for MySQL实例已开通密钥管理服务（Key Management Service，KMS），加密使用的用户主密钥由KMS产生和管理，RDS不提供加密所需的密钥和证书。由于敏感数据可以静态存在于华为云RDS实例中，因此启用静态加密有助于保护该数据。	未开启存储加密的RDS资源，视为“不合规”	如需开通透明数据加密，您可以在管理控制台右上角，选择“工单 > 新建工单”，提交开通透明数据加密的申请。

4.5.12 适用于弹性伸缩（AS）的最佳实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-13 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
as-capacity-rebalancing	弹性伸缩组均衡扩容	as	EQUILIBRIUM_DISTRIBUTE（默认）：均衡分布，虚拟机扩缩容时优先保证available_zones列表中各AZ下虚拟机数量均衡，当无法在目标AZ下完成虚拟机扩容时，按照PICK_FIRST原则选择其他可用AZ。	弹性伸缩组扩缩容时，没有使用‘EQUILIBRIUM_DISTRIBUTE’优先级策略，视为“不合规”	用户可以将伸缩组扩缩容时目标AZ选择的优先级策略设置为EQUILIBRIUM_DISTRIBUTE。
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	根据ELB对云服务器的健康检查结果进行的检查，健康检查会将异常的实例从伸缩组中移除。这条规则确保与负载均衡器关联的伸缩组使用了弹性负载均衡健康检查。	与负载均衡器关联的伸缩组未使用弹性负载均衡健康检查，视为“不合规”	如果您将多个负载均衡器添加到伸缩组，则只有在所有负载均衡器均检测到云服务器状态为正常的情况下，才会认为该弹性云服务器正常。否则只要有一个负载均衡器检测到云服务器状态异常，伸缩组会将该弹性云服务器移出伸缩组。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
as-multiple-az	弹性伸缩组启用多AZ部署	as	一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。	弹性伸缩组没有启用多AZ部署，视为“不合规”	华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

4.5.13 适用于云审计服务（CTS）的最佳实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-14 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	确保云审计服务（CTS）的追踪器已配置KMS加密存储用于归档的审计事件。	CTS追踪器未通过KMS进行加密，视为“不合规”	建议您配置独立OBS桶并配置KMS加密存储专门用于归档审计事件。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-lts-enable	CTS追踪器启用事件分析	cts	确保使用云日志服务（LTS）集中收集云审计服务（CTS）的数据。	CTS追踪器未启用事件分析，视为“不合规”	开通云审计日志后，系统会自动创建一个名为system的管理事件追踪器，并将当前租户的所有操作记录在该追踪器中。在追踪器中配置CTS转储到LTS，配置完成后会在LTS自动创建日志组日志流
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	在安全和事故调查中，通常由于事件文件被删除或者被私下篡改，而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您确保事件文件的真实性。	CTS追踪器未打开事件文件校验，视为“不合规”	在配置转储页面打开“文件校验”开关，即可开启事件文件完整性校验功能。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-tracker-exists	创建并启用CTS追踪器	cts	云审计服务支持创建数据类事件追踪器，用于记录数据操作日志。数据类追踪器用于记录数据事件，即针对租户对OBS桶中的数据的操作日志，例如上传、下载等。	账号未创建CTS追踪器，视为“不合规”	可进入云审计服务页面，导航栏选择“追踪器”，单击“创建追踪器”，根据提示操作。

4.5.14 适用于人工智能与机器学习场景的合规实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-15 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cce-cluster-end-of-maintenance-version	CCE集群版本为处于维护的版本	cce	确保CCE集群版本为处于维护中的版本。	CCE集群版本为停止维护的版本，视为“不合规”	为了保证您的服务权益，建议尽快升级到最新的商用版本。集群升级流程包括升级前检查、备份、升级和升级后验证几个步骤，具体操作流程可见CCE服务说明文档的升级概述。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cce-cluster-oldest-supported-version	CCE集群运行的非受支持的最旧版本	cce	确保CCE集群运行的不是最旧版本	如果CCE集群运行的是受支持的最旧版本（等于参数“最旧版本支持”），视为“不合规”	系统会自动为您的华为云CCE任务部署安全更新和补丁。如果发现影响华为云CCE平台版本的安全问题，华为云会修补该平台版本。要帮助对运行华为云cluster的华为云CCE任务进行补丁管理，请更新您服务的独立任务以使用最新的平台版本。
cce-endpoint-public-access	CCE集群资源不具有公网IP	cce	确保CCE集群资源不可以被公网访问	CCE集群资源具有公网IP，视为“不合规”	用户可以解除集群与EIP的绑定。
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	由于CTS只支持查询7天的审计事件，为了您事后审计、查询、分析等要求，启用CTS追踪器请配置OBS服务桶。	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”	云审计服务管理控制台支持配置已开启的追踪器的OBS桶、LTS转储和配置已创建的追踪器关键事件操作通知。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS 1.8.0版本之前未开启Kerberos认证的集群不支持访问权限细分。只有开启Kerberos认证才有角色管理权限，MRS 1.8.0及之后版本的所有集群均拥有角色管理权限。	MRS集群未开启kerberos认证，视为“不合规”	MRS服务暂不支持集群创建完成后手动开启和关闭Kerberos服务，如需更换Kerberos认证状态，建议重新创建MRS集群，然后进行数据迁移。
mrs-cluster-no-public-ip	MRS集群未绑定公网IP	mrs	确保MapReduce服务（MRS）无法公网访问。华为云MRS集群主节点可能包含敏感信息，并且此类账户需要访问控制。	MRS集群绑定公网IP，视为“不合规”	对于不合规的MRS资源，用户可以解除其与弹性公网IP的绑定。
sfsturbo-encrypted-check	弹性文件服务通过KMS进行加密	sfsturbo	由于敏感数据可能存在并帮助保护静态数据，确保弹性文件服务(SFS Turbo)已通过KMS进行加密。	弹性文件服务(SFS Turbo)未通过KMS进行加密，视为“不合规”	可以新创建加密或者不加密的文件系统，无法更改已有文件系统的加密属性。

4.5.15 适用于自动驾驶场景的合规实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-16 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
css-cluster-disk-encryption-check	CSS集群开启磁盘加密	css	确保CSS集群开启磁盘加密。由于敏感数据可能存在，请在传输中启用加密以帮助保护该数据。	CSS集群未开启磁盘加密，视为“不合规”	建议对磁盘进行加密。
css-cluster-https-required	CSS集群启用HTTPS	css	开启HTTPS访问后，访问集群将进行通讯加密。关闭HTTPS访问后，会使用HTTP协议与集群通信，无法保证数据安全性，并且无法开启公网访问功能。	CSS集群未启用https，视为“不合规”	仅安全模式的集群支持开启HTTPS访问。启用HTTPS访问的安全集群可以单击“下载证书”获取CER安全证书，用于接入安全模式的集群。安全证书暂不支持在公网环境下使用。
css-cluster-no-public-zone	CSS集群不能公网访问	css	确保CSS集群不能公网访问。由于敏感数据可能存在，请将css集群关闭公网访问。	CSS集群开启公网访问，视为“不合规”	您可以对已经创建集群的公网访问进行修改，查看，解绑。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
css-cluster-security-mode-enable	CSS集群开启安全模式	css	集群支持选择是否开启安全模式，开启之后将对集群进行通讯加密和安全认证。	CSS集群未开启安全模式，视为“不合规”	用户可以选择开启安全模式。开启后，管理员账户名默认为admin。设置并确认管理员密码。要记住设置的密码，后续访问集群需要输入密码。
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	确保云审计服务（CTS）的追踪器已配置KMS加密存储用于归档的审计事件。	CTS追踪器未通过KMS进行加密，视为“不合规”	建议您配置独立OBS桶并配置KMS加密存储专门用于归档审计事件。
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	由于CTS只支持查询7天的审计事件，为了您事后审计、查询、分析等要求，启用CTS追踪器请配置OBS服务桶。	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”	云审计服务管理控制台支持配置已开启的追踪器的OBS桶、LTS转储和配置已创建的追踪器关键事件操作通知。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	在安全和事故调查中，通常由于事件文件被删除或者被私下篡改，而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您确保事件文件的真实性。	CTS追踪器未打开事件文件校验，视为“不合规”	在配置转储页面打开“文件校验”开关，即可开启事件文件完整性校验功能。
cts-tracker-exists	创建并启用CTS追踪器	cts	云审计服务支持创建数据类事件追踪器，用于记录数据操作日志。数据类追踪器用于记录数据事件，即针对租户对OBS桶中的数据的操作日志，例如上传、下载等。	账号未创建CTS追踪器，视为“不合规”	可进入云审计服务页面，导航栏选择“追踪器”，单击“创建追踪器”，根据提示操作。
dcs-redis-no-public-ip	DCS Redis实例不存在公网IP	dcs	确保不可以通过公网访问redis资源。	dcs redis资源存在公网IP，视为“不合规”	目前只有Redis 3.0版本密码模式的实例支持公网访问，用户可以选择关闭公网访问开关。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
dcs-redis-password-access	DCS Redis实例需要密码访问	dcs	确保dcs redis资源需要密码访问。Redis实例支持密码模式和免密模式。Redis本身支持不设置密码，客户端可以直接连接Redis缓存服务并使用，但出于安全考虑，建议尽量选用密码模式，通过密码来鉴权验证，提升安全性。	dcs redis资源不需要密码访问，视为“不合规”	若选用密码模式，您需要在创建实例时自定义密码。
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	由于华为云ecs实例可能包含敏感信息，确保华为云ecs实例无法公开访问来管理对华为云的访问。	ECS资源具有公网IP，视为“不合规”	您可以登录弹性云服务器页面，在弹性云服务器列表中，在待调整带宽的弹性云服务器操作列下，单击“操作”列下的“更多 > 网络设置 > 解绑弹性公网IP”，将不合规的ECS资源解除弹性公网绑定。
elb-loadbalancers-no-public-ip	ELB资源不具有公网IP	elb	确保弹性负载均衡（ELB）无法公网访问，管理对华为云中资源的访问。	ELB资源具有公网IP，视为“不合规”	用户可以解除不合规资源的公网绑定。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	确保弹性负载均衡的监听器均已配置HTTPS监听协议。HTTPS协议适用于需要加密传输的应用。由于可能存在敏感数据，因此启用传输中加密有助于保护该数据。	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”	您可以添加一个HTTPS监听转发来自HTTPS协议的请求。独享型负载均衡前端协议为“HTTPS”时，后端协议可以选择“HTTP”或“HTTPS”。共享型负载均衡前端协议为“HTTPS”时，后端协议默认为“HTTP”，且不支持修改。如果您的独享型负载均衡实例类型为网络型（TCP/UDP），则无法创建HTTPS监听器。
iam-password-policy	IAM用户密码策略符合要求	iam	确保IAM用户密码强度满足密码强度要求。	IAM用户密码强度不满足密码强度要求，视为“不合规”	用户可以根据提示修改密码达到需要的密码强度。
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	管理员创建IAM用户后，这个新建的IAM用户可以登录华为云。避免IAM用户资源闲置。	IAM用户在指定时间范围内无登录行为，视为“不合规”	您可以在华为云登录页面或者打开IAM用户专属链接，输入用户名和密码的方式登录IAM用户。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
iam-user-mfa-enabled	IAM用户开启MFA	iam	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账户被盗用的事件。	IAM用户未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。
rds-instance-no-public-ip	RDS实例不具有公网IP	rds	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账户需要原则和访问控制。	RDS资源具有公网IP，视为“不合规”	对于不合规的RDS资源，用户可以解除其与弹性公网IP的绑定。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
root-account-mfa-enabled	根账号开启MFA认证	iam	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。多因素认证Multi-Factor Authentication（MFA）是一种非常简单的安全实践方法，它能够在用户名称和密码之外再额外增加一层保护。启用多因素认证后，用户进行操作时，除了需要提供用户名和密码外（第一次身份验证），还需要提供验证码（第二次身份验证），多因素身份认证结合起来将为您的账号和资源提供更高的安全保护。	根账号未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs，evs	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。	已挂载的云硬盘未进行加密，视为“不合规”	当您需要使用云硬盘加密功能时，需要授权EVS访问KMS。如果您拥有“Security Administrator”权限，则可直接授权。如果权限不足，需先联系拥有“Security Administrator”权限的用户授权EVS访问KMS，然后再重新操作。
vpc-flow-logs-enabled	VPC启用流日志	vpc	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。	检查是否为VPC启用了流日志，如果该VPC未启用流日志，视为“不合规”	您可以为不合规的VPC资源开启流日志记录，方式为：创建日志组、日志流之后，进入VPC流日志列表页面创建VPC流日志，按照提示配置参数。
vpc-sg-ports-check	安全组端口检查	vpc	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。	当安全组入方向源地址设置为0.0.0.0/0，且开放了所有的TCP/UDP端口时，视为“不合规”	用户可以修改不合规的安全组的规则。

4.5.16 资源开启公网访问最佳实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-17 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
css-cluster-in-vpc	CSS集群绑定指定VPC资源	css	云搜索服务CSS的集群创建在虚拟私有云（VPC）的子网内，VPC通过逻辑方式进行网络隔离，为用户的集群提供安全、隔离的网络环境。此规则确保云搜索服务（CSS）位于虚拟私有云（VPC）中。	CSS集群未与指定的VPC资源绑定，视为“不合规”	可以将不合规的CSS集群与指定VPC关联。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
drs-data-guard-job-not-public	数据复制服务实时灾备任务不使用公网网络	drs	为了解决地区故障导致的业务不可用，数据复制服务推出灾备场景，为用户业务连续性提供数据库的同步保障。当主实例所在区域发生突发生自然灾害等状况无法连接时，可将异地灾备实例切换为主实例，在应用端修改数据库链接地址后，即可快速恢复应用的业务访问。数据复制服务提供的实时灾备功能，可实现主实例和跨区域的灾备实例之间的实时同步。此规则确保DRS实时灾备任务不能公开访问。	数据复制服务实时灾备任务使用公网网络，视为“不合规”	对于不合规的DRS资源，您可以切换非公网访问

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
drs-migration-job-not-public	数据复制服务实时迁移任务不使用公网网络	drs	实时迁移是指在数据复制服务能够同时连通源数据库和目标数据库的情况下，只需要配置迁移的源、目标数据库实例及迁移对象即可完成整个数据迁移过程，再通过多项指标和数据的对比分析，帮助确定合适的业务割接时机，实现最小化业务中断的数据库迁移。确保DRS实时迁移任务不能公开访问。	数据复制服务实时迁移任务使用公网网络，视为“不合规”	对于不合规的DRS资源，您可以切换非公网访问。
drs-synchronization-job-not-public	数据复制服务实时同步任务不使用公网网络	drs	实时同步是指在不同的系统之间，将数据通过同步技术从一个数据源拷贝到其他数据库，并保持一致，实现关键业务的数据实时流动。确保DRS实时同步任务不能公开访问。确保DRS实时同步任务不能公开访问。	数据复制服务实时同步任务使用公网网络，视为“不合规”	对于不合规的DRS资源，您可以切换非公网访问。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs，vpc	虚拟私有云（VPC）为弹性云服务器构建了一个逻辑上完全隔离的专有区域，您可以在自己的逻辑隔离区域中定义虚拟网络，为弹性云服务器构建一个逻辑上完全隔离的专有区域，确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”	您可以通过网络配置，为不合规的ECS资源选择特定的虚拟私有云。
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	由于华为云ecs实例可能包含敏感信息，确保华为云ecs实例无法公开访问来管理对华为云的访问。	ECS资源具有公网IP，视为“不合规”	您可以登录弹性云服务器页面，在弹性云服务器列表中，在待调整带宽的弹性云服务器操作列下，单击“操作”列下的“更多 > 网络设置 > 解绑弹性公网IP”，将不合规的ECS资源解除弹性公网绑定。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
function-graph-inside-vpc	函数工作流使用指定VPC	fgs	函数支持用户创建虚拟私有云（VPC）并访问自己VPC内的资源。VPC开启后，函数不再具有默认的公网访问权限，如果需要访问公网，可通过在VPC内配置公网NAT网关绑定EIP的方式实现，具体请参见配置固定公网IP。	函数工作流未使用指定VPC，视为“不合规”	用户可以通过开启“允许函数访问VPC内资源”的开关，配置相应的VPC和子网。
function-graph-public-access-prohibited	函数工作流的函数不允许访问公网	fgs	确保函数工作流的函数不能公开访问，管理对华为云中资源的访问。公开访问可能导致资源可用性下降。	函数工作流的函数允许访问公网，视为“不合规”	部署在VPC中的函数默认是和外网隔离开的，用户可以将函数绑定VPC，并且不添加公网NAT网关。
mrs-cluster-no-public-ip	MRS集群未绑定公网IP	mrs	确保MapReduce服务（MRS）无法公网访问。华为云MRS集群主节点可能包含敏感信息，并且此类账户需要访问控制。	MRS集群绑定公网IP，视为“不合规”	对于不合规的MRS资源，用户可以解除其与弹性公网IP的绑定。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-no-public-ip	RDS实例不具有公网IP	rds	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账户需要原则和访问控制。	RDS资源具有公网IP，视为“不合规”	对于不合规的RDS资源，用户可以解除其与弹性公网IP的绑定。

4.5.17 适用于日志和监控的最佳实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-18 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
alarm-action-enabled-check	启用了CES告警操作	ces	确保启用了CES告警操作,用户对云服务的核心监控指标设置告警规则，当监控指标触发用户设置的告警条件时,云监控服务使用消息通知服务向用户通知告警信息。	CES告警操作未启用，视为“不合规”	您需要在消息通知服务界面创建一个主题并为这个主题添加相关的订阅者，然后在添加告警规则的时候，您需要开启消息通知服务并选择创建的主题，这样在云服务发生异常时，云监控服务可以实时的将告警信息以广播的方式通知这些订阅者。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	确保为APIG专享版实例配置访问日志。APIG支持日志自定义分析模板，便于日志的统一收集和管理，也可通过API异常调用分析进行追查和溯源。	APIG专享版实例未配置访问日志，视为“不合规”	可以在API网关控制台选择启动日志记录
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	根据ELB对云服务器的健康检查结果进行的检查，健康检查会将异常的实例从伸缩组中移除。这条规则确保与负载均衡器关联的伸缩组使用了弹性负载均衡健康检查。	与负载均衡器关联的伸缩组未使用弹性负载均衡健康检查，视为“不合规”	如果您将多个负载均衡器添加到伸缩组，则只有在所有负载均衡器均检测到云服务器状态为正常的情况下，才会认为该弹性云服务器正常。否则只要有一个负载均衡器检测到云服务器状态异常，伸缩组会将该弹性云服务器移出伸缩组。
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	确保云审计服务（CTS）的追踪器已配置KMS加密存储用于归档的审计事件。	CTS追踪器未通过KMS进行加密，视为“不合规”	建议您配置独立OBS桶并配置KMS加密存储专门用于归档审计事件。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-lts-enable	CTS追踪器启用事件分析	cts	确保使用云日志服务（LTS）集中收集云审计服务（CTS）的数据。	CTS追踪器未启用事件分析，视为“不合规”	开通云审计日志后，系统会自动创建一个名为system的管理事件追踪器，并将当前租户的所有操作记录在该追踪器中。在追踪器中配置CTS转储到LTS，配置完成后会在LTS自动创建日志组日志流
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	由于CTS只支持查询7天的审计事件，为了您事后审计、查询、分析等要求，启用CTS追踪器请配置OBS服务桶。	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”	云审计服务管理控制台支持配置已开启的追踪器的OBS桶、LTS转储和配置已创建的追踪器关键事件操作通知。
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	在安全和事故调查中，通常由于事件文件被删除或者被私下篡改，而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您确保事件文件的真实性。	CTS追踪器未打开事件文件校验，视为“不合规”	在配置转储页面打开“文件校验”开关，即可开启事件文件完整性校验功能。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-tracker-exists	创建并启用CTS追踪器	cts	云审计服务支持创建数据类事件追踪器，用于记录数据操作日志。数据类追踪器用于记录数据事件，即针对租户对OBS桶中的数据的操作日志，例如上传、下载等。	账号未创建CTS追踪器，视为“不合规”	可进入云审计服务页面，导航栏选择“追踪器”，单击“创建追踪器”，根据提示操作。
dws-enable-log-dump	DWS集群启用日志转储	dws	GaussDB(DWS) 记录您的数据库中的连接和用户活动相关信息。这些审计日志信息有助于您监控数据库以确保安全或进行故障排除或定位历史操作记录。当前这些审计日志默认存储于数据库中，您可以将审计日志转储到OBS中使负责监控数据库中活动的用户更方便的查看这些日志信息。	DWS集群未启用日志转储，视为“不合规”	GaussDB(DWS) 集群创建成功后，您可以为集群开启审计日志转储，将审计日志转储到OBS中，方便查看。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
function-graph-concurrency-check	函数工作流的函数并发数在指定范围内	fgs	FunctionGraph会根据实际的请求情况自动弹性伸缩函数实例，并发变高时，会分配更多的函数实例来处理请求，并发减少时，相应的实例也会变少。此规则可确保建立函数工作流（FunctionGraph）的并发上限和下限。	FunctionGraph函数并发数不在指定的范围内，视为“不合规”	对于不合规的实例，在函数详情页可以修改函数并发数的值。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
multi-region-cts-tracker-exists	在指定区域创建并启用CTS追踪器	cts	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。数据追踪器会记录当前区域租户对OBS桶中的数据操作的详细信息。	账号未在指定region列表创建CTS追踪器，视为“不合规”	您可以进入指定区域云审计服务页面，导航栏选择“追踪器”，单击“创建追踪器”，根据提示操作。
rds-instance-logging-enabled	RDS实例配备日志	rds	确保rds资源配备了访问日志。配置访问日志后，RDS实例新生成的日志记录会上传到云日志服务（Log Tank Service，简称LTS）进行管理。	未配备任何日志的RDS资源，视为“不合规”	您可以为不合规的RDS资源配置访问日志。方式为：登录RDS管理控制台，选择日志配置管理，选择为一个或多个实例配置访问日志。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
vpc-flow-logs-enabled	VPC启用流日志	vpc	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。	检查是否为VPC启用了流日志，如果该VPC未启用流日志，视为“不合规”	您可以为不合规的VPC资源开启流日志记录，方式为：创建日志组、日志流之后，进入VPC流日志列表页面创建VPC流日志，按照提示配置参数。

4.5.18 适用于空闲资产管理的最佳实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-19 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cce-cluster-end-of-maintenance-version	CCE集群版本为处于维护的版本	cce	确保CCE集群版本为处于维护中的版本。	CCE集群版本为停止维护的版本，视为“不合规”	为了保证您的服务权益，建议尽快升级到最新的商用版本。集群升级流程包括升级前检查、备份、升级和升级后验证几个步骤，具体操作流程可见CCE服务说明文档的升级概述。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
eip-unbound-check	弹性公网IP未进行任何绑定	vpc	弹性公网IP（EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。此规则确保弹性公网IP未闲置。	弹性公网IP未进行任何绑定，视为“不合规”	用户可以通过申请弹性公网IP并将弹性公网IP绑定到特定的资源上。
eip-use-in-specified-days	EIP在指定天数内绑定到资源实例	eip	弹性公网IP（EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。此规则确保弹性公网IP未闲置。	EIP创建指定天数内未使用，视为“不合规”	用户可以通过申请弹性公网IP并将弹性公网IP绑定到特定的资源上。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
evs-use-in-specified-days	云硬盘创建后在指定天数内绑定资源实例	evs	云硬盘可以挂载至云服务器，用作提供系统盘和数据盘。此规则可以确保云硬盘（EVS）未闲置。	EVS创建指定天数内未使用，视为“不合规”	对非合规的EVS资源，用户可以在云硬盘页面或在弹性云服务器页面，将其挂载到云服务器上。
iam-group-has-users-check	IAM用户组添加了IAM用户	iam	管理员创建用户组并授权后，将用户加入用户组中，使用户具备用户组的权限，实现用户的授权。给已授权的用户组中添加或者移除用户，快速实现用户的权限变更。确保IAM组至少有一个用户，帮助您将最小权限和职责分离的原则与访问权限和授权结合起来。	IAM用户组未添加任意IAM用户，视为“不合规”	管理员在用户组列表中，单击新建的用户组，选择“用户组管理”，在“可选用户”中选择需要添加至用户组中的用户。
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	管理员创建IAM用户后，这个新建的IAM用户可以登录华为云。避免IAM用户资源闲置。	IAM用户在指定时间范围内无登录行为，视为“不合规”	您可以在华为云登录页面或者打开IAM用户专属链接，输入用户名和密码的方式登录IAM用户。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	启用此规则可根据您组织的标准检查华为云ecs实例的停止时间是否超过允许的天数，确保弹性云服务器（ECS）未闲置。	关机状态的ECS未进行任意操作的时间超过了允许的天数，视为“不合规”	包年/包月资源一次性付费，到期自动停止使用。其他计费模式下关机后仍然计费。如需停止计费，请删除实例。
volume-unused-check	云硬盘闲置检测	evs	云硬盘可以挂载至云服务器，用作提供系统盘和数据盘。此规则可以确保云硬盘（EVS）未闲置。	云硬盘未挂载给任何云服务器，视为“不合规”	对非合规的EVS资源，用户可以在云硬盘页面或在弹性云服务器页面，将其挂载到云服务器上。
vpc-acl-unused-check	未与子网关联的网络ACL	vpc	网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的网络流量。此规则可确保现存网络ACL均与子网关联，实现对子网的防护。	检查是否存在未使用的网络ACL,如果网络ACL没有与子网关联，视为“不合规”	您可以将网络ACL关联至VPC子网，为子网内的资源提供安全防护。

4.5.19 华为云架构可靠性最佳实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-20 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	确保为APIG专享版实例配置访问日志。APIG支持日志自定义分析模板，便于日志的统一收集和管理，也可通过API异常调用分析进行追查和溯源。	APIG专享版实例未配置访问日志，视为“不合规”	可以在API网关控制台选择启动日志记录
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	根据ELB对云服务器的健康检查结果进行的检查，健康检查会将异常的实例从伸缩组中移除。这条规则确保与负载均衡器关联的伸缩组使用了弹性负载均衡健康检查。	与负载均衡器关联的伸缩组未使用弹性负载均衡健康检查，视为“不合规”	如果您将多个负载均衡器添加到伸缩组，则只有在所有负载均衡器均检测到云服务器状态为正常的情况下，才会认为该弹性云服务器正常。否则只要有一个负载均衡器检测到云服务器状态异常，伸缩组会将该弹性云服务器移出伸缩组。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-lts-enable	CTS追踪器启用事件分析	cts	确保使用云日志服务（LTS）集中收集云审计服务（CTS）的数据。	CTS追踪器未启用事件分析，视为“不合规”	开通云审计日志后，系统会自动创建一个名为system的管理事件追踪器，并将当前租户的所有操作记录在该追踪器中。在追踪器中配置CTS转储到LTS，配置完成后会在LTS自动创建日志组日志流
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	由于CTS只支持查询7天的审计事件，为了您事后审计、查询、分析等要求，启用CTS追踪器请配置OBS服务桶。	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”	云审计服务管理控制台支持配置已开启的追踪器的OBS桶、LTS转储和配置已创建的追踪器关键事件操作通知。
cts-tracker-exists	创建并启用CTS追踪器	cts	云审计服务支持创建数据类事件追踪器，用于记录数据操作日志。数据类追踪器用于记录数据事件，即针对租户对OBS桶中的数据的操作日志，例如上传、下载等。	账号未创建CTS追踪器，视为“不合规”	可进入云审计服务页面，导航栏选择“追踪器”，单击“创建追踪器”，根据提示操作。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
dws-enable-kms	DWS集群启用KMS加密	dws	确保数据仓库服务的集群启用KMS磁盘加密。	DWS集群未启用KMS加密，视为“不合规”	您可以在创建集群时启用加密。加密是集群的一项可选且不可变的设置。要从未加密的集群更改为加密集群(或反之)，必须从现有集群导出数据，然后在已启用数据库加密的新集群中重新导入这些数据。
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs, vpc	虚拟私有云（VPC）为弹性云服务器构建了一个逻辑上完全隔离的专有区域，您可以在自己的逻辑隔离区域中定义虚拟网络，为弹性云服务器构建一个逻辑上完全隔离的专有区域，确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”	您可以通过网络配置，为不合规的ECS资源选择特定的虚拟私有云。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
function-graph-concurrency-check	函数工作流的函数并发数在指定范围内	fgs	FunctionGraph会根据实际的请求情况自动弹性伸缩函数实例，并发变高时，会分配更多的函数实例来处理请求，并发减少时，相应的实例也会变少。此规则可确保建立函数工作流（FunctionGraph）的并发上限和下限。	FunctionGraph函数并发数不在指定的范围内，视为“不合规”	对于不合规的实例，在函数详情页可以修改函数并发数的值。
gaussdb-nosql-enable-disk-encryption	GaussDB NoSQL使用磁盘加密	gaussdb nosql	确保GaussDB NoSQL启用KMS磁盘加密。当启用加密功能，用户创建数据库实例成功后，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，用于提高数据安全性，但对数据库读写性能有少量影响。	GaussDB NoSQL未使用磁盘加密，视为“不合规”	您可以根据业务需要选择是否进行磁盘加密。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
kms-not-scheduled-for-deletion	KMS密钥不处于“计划删除”状态	kms	确保数据加密服务（KMS）密钥未处于“计划删除“状态，以防止误删除密钥。	KMS密钥处于“计划删除“状态，视为“不合规”	用户可以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。
multi-region-cts-tracker-exists	在指定区域创建并启用CTS追踪器	cts	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。数据追踪器会记录当前区域租户对OBS桶中的数据操作的详细信息。	账号未在指定region列表创建CTS追踪器，视为“不合规”	您可以进入指定区域云审计服务页面，导航栏选择“追踪器”，单击“创建追踪器”，根据提示操作。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-enable-backup	RDS实例开启备份	rds	RDS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，自动备份为全量备份。系统根据您指定的备份保留期保存数据库实例的自动备份。如果需要，您可以将数据恢复到备份保留期中的任意时间点。开启自动备份策略后，会自动触发一次全量备份，备份方式为物理备份。之后会按照策略中的备份时间段和备份周期进行全量备份。自动备份策略开启后，实例每五分钟会自动进行一次增量备份，以保证数据库可靠性。确保云数据库（rds）资源开启备份。	未开启备份的RDS资源，视为“不合规”	用户可根据需要修改备份策略。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-multi-az-support	RDS实例支持多可用区	rds	华为云RDS中的多可用区支持为数据库实例提供了增强的可用性和持久性。当您预置多可用区数据库实例时，华为云RDS会自动创建主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用区都在其物理上不同的独立基础设施上运行，并且经过精心设计，高度可靠。如果发生基础设施故障，华为云 RDS 会自动故障转移到备用数据库，以便您可以在故障转移完成后立即恢复数据库操作。	RDS实例仅支持一个可用区，视为“不合规”	华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instances-enable-kms	RDS实例开启存储加密	rds	云数据库RDS for MySQL实例已开通密钥管理服务（Key Management Service，KMS），加密使用的用户主密钥由KMS产生和管理，RDS不提供加密所需的密钥和证书。由于敏感数据可以静态存在于华为云RDS实例中，因此启用静态加密有助于保护该数据。	未开启存储加密的RDS资源，视为“不合规”	如需开通透明数据加密，您可以在管理控制台右上角，选择“工单 > 新建工单”，提交开通透明数据加密的申请。
sfsturbo-encrypted-check	弹性文件服务通过KMS进行加密	sfsturbo	由于敏感数据可能存在并帮助保护静态数据，确保弹性文件服务(SFS Turbo)已通过KMS进行加密。	弹性文件服务(SFS Turbo)未通过KMS进行加密，视为“不合规”	可以新创建加密或者不加密的文件系统，无法更改已有文件系统的加密属性。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs，evs	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。	已挂载的云硬盘未进行加密，视为“不合规”	当您需要使用云硬盘加密功能时，需要授权EVS访问KMS。如果您拥有“Security Administrator”权限，则可直接授权。如果权限不足，需先联系拥有“Security Administrator”权限的用户授权EVS访问KMS，然后再重新操作。
vpc-flow-logs-enabled	VPC启用流日志	vpc	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。	检查是否为VPC启用了流日志，如果该VPC未启用流日志，视为“不合规”	您可以为不合规的VPC资源开启流日志记录，方式为：创建日志组、日志流之后，进入VPC流日志列表页面创建VPC流日志，按照提示配置参数。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
vpn-connections-active	VPN连接状态为“正常”	vpnaas	VPN连接状态不为“正常”，视为“不合规”	确保VPN连接状态正常。	VPN连接状态显示为“未连接”的可能原因有：VPN连接两端的连接配置不正确、华为云安全组和客户设备侧ACL配置不正确。可以检查VPN连接两端的连接配置和检查华为云安全组和客户设备侧ACL配置。

4.5.20 适用于中国香港金融管理局的标准合规包

本文为您介绍适用于中国香港金融管理局的标准合规包的业务背景、应用场景，以及合规包中的默认规则。

业务背景

中国香港金融管理局对云计算的监管预期，是参考2021年至2022年期间进行的一轮专题审查的结果而制定的。认证机构在采用云计算之前需注意的关键原则应包括中国香港金融管理局制定的云计算指南、SA-2（外包）、OR-2（运营恢复能力）和TM- G-1（技术风险管理总体原则）。

关于中国香港金融管理局合规标准的更多信息，请参见**HKMA.2022.08.31**、**SA-2**、**OR-2**、**TM-G-1**。

应用场景

适用于中国香港金融管理局的标准合规包应用于中国香港金融企业上云需要满足的要求。

免责条款

本合规规则包模板为您提供通用的操作指引，帮助您快速创建符合目标场景的合规规则包。为避免疑义，本“合规”仅指资源符合规则定义本身的合规性描述，不构成任何法律意见。本合规规则包模板不确保符合特定法律法规或行业标准的要求，您需自行对您的业务、技术操作的合规性和合法性负责并承担与此相关的所有责任。

默认规则

此表中的建议项编号对应**HKMA.2022.08.31**中参考文档的章节编号，供您查阅参考。

表 4-21 HKMA 云计算指南

建议项编号	建议项说明	合规规则	指导
I-2	根据采用的云部署模型，包括多租户风险，以及集中风险。	iam-group-has-users-check	确保IAM群组至少有一个用户，从而帮助您将最低权限和职责分离的原则与访问权限和授权相结合。
I-2	根据采用的云部署模型，包括多租户风险，以及集中风险。	iam-user-group-membership-check	确保用户是至少一个群组的成员，从而帮助您限制访问权限和授权。
I-2	根据采用的云部署模型，包括多租户风险，以及集中风险。	iam-root-access-key-check	确保删除根访问密钥，从而帮助您限制访问权限和授权。
II-5	应实施安全控制措施，保护存储在云端的客户信息的完整性和机密性。	kms-rotation-enabled	启用密钥轮换，确保密钥在加密周期结束后轮换。
II-5	应实施安全控制措施，保护存储在云端的客户信息的完整性和机密性。	iam-password-policy	识别登录用户的密码强度符合要求。
II-5	应实施安全控制措施，保护存储在云端的客户信息的完整性和机密性。	cts-support-validate-check	启用云审计服务追踪器的日志文件校验，验证日志文件转储后是否被修改、删除或未更改。
II-5	应实施安全控制措施，保护存储在云端的客户信息的完整性和机密性。	rds-instances-enable-kms	确保云数据库(RDS)实例启用了加密。
II-5	应实施安全控制措施，保护存储在云端的客户信息的完整性和机密性。	dcs-redis-enable-ssl	为了帮助保护传输中的敏感数据，确保为Redis启用SSL协议。

此表中的建议项编号对应**SA-2**中参考文档的章节编号，供您查阅参考。

表 4-22 SA-2 外包

建议项编号	建议项说明	合规规则	指导
2.5.1	根据采用的云部署模型，包括应确保遵守客户数据的保密要求并采取防范措施保护客户数据的完整性和机密性。	cts-kms-encrypted-check	由于日志可能存在敏感数据，请确保云审计服务的追踪器已启用加密事件文件。
2.5.1	应确保遵守客户数据的保密要求并采取防范措施保护客户数据的完整性和机密性。	rds-instances-enable-kms	确保云数据库实例已启用加密。
2.5.1	应确保遵守客户数据的保密要求并采取防范措施保护客户数据的完整性和机密性。	css-cluster-disk-encryption-check	确保云搜索服务集群开启磁盘加密。
2.8.1	应保存适当和最新的资料记录，可供金管局检查。	vpc-flow-logs-enabled	VPC流日志提供了虚拟私有云的流量信息的详细记录。
2.8.1	应保存适当和最新的资料记录，可供金管局检查。	apig-instances-execution-logging-enabled	API网关日志记录访问API的用户的详细视图以及访问API的方式，实现用户活动的可见性。
2.8.1	应保存适当和最新的资料记录，可供金管局检查。	cts-lts-enable	使用云审计服务集中收集和管理日志事件活动。
2.8.1	应保存适当和最新的资料记录，可供金管局检查。	cts-support-validate-check	启用云审计服务追踪器的日志文件校验，验证日志文件转储后是否被修改、删除或未更改。

此表中的建议项编号对应**OR-2**中参考文档的章节编号，供您查阅参考。

表 4-23 OR-2 运营恢复能力

建议项编号	建议项说明	合规规则	指导
4.2.2	应注意在不同的业务周期或受季节因素影响时，其运作能力有所不同。例如，较多首次公开发行股票时，交易系统会有较大压力。	as-group-elb-healthcheck-required	弹性负载均衡定期发送网络请求，以测试弹性伸缩组中的云服务器的运行状况。
6.1	应为管理所有可能影响维持关键运作的风险做好准备。	as-multiple-az	弹性伸缩在多可用区中部署，以帮助保持足够的容量和可用性。
6.1	应为管理所有可能影响维持关键运作的风险做好准备。	css-cluster-multiple-az-check	云搜索服务在多可用区中部署，以帮助保持足够的容量和可用性。
6.1	应为管理所有可能影响维持关键运作的风险做好准备。	elb-multiple-az-check	弹性负载均衡在多可用区中部署，以帮助保持足够的容量和可用性。
6.1	应为管理所有可能影响维持关键运作的风险做好准备。	rds-instance-multi-az-support	云数据库在多可用区中部署，以帮助保持足够的容量和可用性。
6.2	业务操作风险管理的重点是防范及减少运作损失，有助认可机构维持运作稳健性。	kms-not-scheduled-for-deletion	确保KMS密钥未处于“计划删除”状态，防止被意外或恶意删除。

此表中的建议项编号对应**TM-G-1**中参考文档的章节编号，供您查阅参考。

表 4-24 TM-G-1 科技风险管理总体原则

建议项编号	建议项说明	华为云合规规则	指导
3.1.4	应采用业内认可的加密解决方案及稳健的密钥管理手法，以保护有关的加密密钥。	kms-not-scheduled-for-deletion	帮助检查所有计划删除的密钥，以防计划删除是无意的。
3.1.4	应采用业内认可的加密解决方案及稳健的密钥管理手法，以保护有关的加密密钥。	kms-rotation-enabled	启用密钥轮换，确保密钥在加密周期结束后轮换。

建议项编号	建议项说明	华为云合规规则	指导
3.2.2	较高风险的交易或活动应采用更严格的认证方法，通常应采取多因素认证机制对用户进行身份认证。	iam-password-policy	识别登录用户的密码强度符合要求。
3.2.2	较高风险的交易或活动应采用更严格的认证方法，通常应采取多因素认证机制对用户进行身份认证。	access-keys-rotated	定期更改访问密钥是安全最佳实践，它缩短了访问密钥的活动时间。
3.2.2	较高风险的交易或活动应采用更严格的认证方法，通常应采取多因素认证机制对用户进行身份认证。	iam-user-mfa-enabled	确保为所有用户启用多因素身份验证（MFA）。
3.2.2	较高风险的交易或活动应采用更严格的认证方法，通常应采取多因素认证机制对用户进行身份认证。	root-account-mfa-enabled	确保为root用户启用多因素身份验证（MFA）。
3.3.1	监控系统资源的使用，以侦测是否有异常或未经授权进行的活动。	cts-tracker-exists	启用云审计服务，可以记录华为云管理控制台操作和API调用。
3.3.1	监控系统资源的使用，以侦测是否有异常或未经授权进行的活动。	cts-lts-enable	使用云审计服务集中收集和管理日志事件活动。
3.3.2	应在安全管理职能上进行职责分离，或采取其他补偿措施，以减少未授权行为。	iam-role-has-all-permissions	确保IAM用户权限仅限于所需的操作，避免用户的权限违反最小权限和职责分离原则。
5.2.1	应制定适当的程序，以确保持续监控应用系统的性能，并及时地、全面地汇报异常情况。	alarm-action-enabled-check	确保云监控服务创建的告警规则未停用。
6.2.1	为防止不安全的网络连接，应制定及执行有关使用网络及网络服务的程序。	ecs-instance-no-public-ip	弹性云服务器可能包含敏感信息，需要限制其从公网访问。
6.2.1	为防止不安全的网络连接，应制定及执行有关使用网络及网络服务的程序。	function-graph-public-access-prohibited	函数工作流的函数不能公网访问，公网访问可能导致数据泄漏或资源可用性下降。

4.5.21 适用于中小企业的 ENISA 的标准合规包

本文为您介绍适用于中小企业的ENISA的标准合规包的业务背景、应用场景，以及合规包中的默认规则。

业务背景

ENISA中小企业网络安全指南提供了中小型企业可用于增强其网络安全态势的运营最佳实践。该指南旨在帮助中小企业了解网络安全的重要性，以及如何实施最佳实践以保护其业务免受网络威胁。关于该指南的更多信息，请参见**cybersecurity-guide-for-smes**。

应用场景

适用于中小企业的ENISA的标准合规包应用于需要满足欧盟网络安全局规范的中小企业，帮助其满足相关的法律法规要求，但需要根据具体情况进行评估和实施。

免责条款

本合规规则包模板为您提供通用的操作指引，帮助您快速创建符合目标场景的合规规则包。为避免疑义，本“合规”仅指资源符合规则定义本身的合规性描述，不构成任何法律意见。本合规规则包模板不确保符合特定法律法规或行业标准的要求，您需自行对您的业务、技术操作的合规性和合法性负责并承担与此相关的所有责任。

默认规则

此表中的建议项编号对应**cybersecurity-guide-for-smes**中参考文档的章节编号，供您查阅参考。

表 4-25 适用于中小企业的 ENISA 的标准合规包默认规则说明

建议项编号	建议项说明	合规规则	指导
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	drs-data-guard-job-not-public	确保数据复制服务实时灾备任务不能公开访问。

建议项编号	建议项说明	合规规则	指导
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	drs-migration-job-not-public	确保数据复制服务实时迁移任务不能公开访问。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	drs-synchronization-job-not-public	确保数据复制服务实时同步任务不能公开访问。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	ecs-instance-no-public-ip	由于华为云弹性云服务器实例可能包含敏感信息，确保华为云弹性云服务器实例无法公开访问来管理对华为云的访问。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	mrs-cluster-no-public-ip	确保MapReduce服务无法公网访问。华为云MapReduce服务集群主节点可能包含敏感信息，并且此类账号需要访问控制。

建议项编号	建议项说明	合规规则	指导
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	function-graph-public-access-prohibited	确保函数工作流的函数不能公开访问，管理对华为云中资源的访问。公开访问可能导致资源可用性下降。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	rds-instance-no-public-ip	确保云数据库无法公网访问，管理对华为云中资源的访问。云数据库实例可能包含敏感信息，此类账号需要原则和访问控制。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	apig-instances-ssl-enabled	确保使用SSL证书配置华为云API网关REST API阶段，以允许后端系统对来自API网关的请求进行身份验证。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	cts-kms-encrypted-check	确保云审计服务的追踪器已配置KMS加密存储用于归档的审计事件。

建议项编号	建议项说明	合规规则	指导
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	sfsturbo-encrypted-check	由于敏感数据可能存在并帮助保护静态数据，确保弹性文件服务已通过KMS进行加密。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	volumes-encrypted-check	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	cts-support-validate-check	确保云审计服务追踪器已打开事件文件校验，已避免日志文件存储后被修改、删除。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	css-cluster-disk-encryption-check	确保云搜索服务集群开启磁盘加密。由于敏感数据可能存在，请在传输中启用加密以帮助保护该数据。

建议项编号	建议项说明	合规规则	指导
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	css-cluster-disk-encryption-check	确保云搜索服务集群开启磁盘加密。由于敏感数据可能存在，请在传输中启用加密以帮助保护该数据。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	elb-tls-https-listeners-only	确保弹性负载均衡的监听器已配置HTTPS监听协议。由于可能存在敏感数据，因此启用传输中加密有助于保护该数据。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	volumes-encrypted-check	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	iam-policy-no-statements-with-admin-access	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。

建议项编号	建议项说明	合规规则	指导
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	iam-role-has-all-permissions	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	vpc-sg-restricted-ssh	当外部任意IP可以访问安全组内云服务器的SSH（22）端口时认为不合规，确保对服务器的远程访问安全性。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	private-nat-gateway-authorized-vpc-only	确保NAT私网网关仅连接到授权的虚拟私有云中，管理对华为云中资源的访问。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	rds-instances-enable-kms	为了帮助保护静态数据，请确保为您的华为云RDS实例启用加密。由于敏感数据可以静态存在于华为云RDS实例中，因此启用静态加密有助于保护该数据。

建议项编号	建议项说明	合规规则	指导
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	dws-enable-ssl	确保数据仓库服务需要SSL加密才能连接到数据库客户端。由于敏感数据可能存在，因此在传输过程中启用加密以帮助保护该数据。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	dws-enable-kms	确保数据仓库服务的集群启用KMS磁盘加密。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	gaussdb-nosql-enable-disk-encryption	确保GaussDB NoSQL启用KMS磁盘加密。
1_DEVELOP GOOD CYBERSECURITY CULTURE: REMEMBER DATA PROTECTION	根据欧盟一般数据保护条例1，任何处理或存储属于欧盟/欧洲经济区居民的个人数据的中小企业都需要确保有适当的安全控制来保护这些数据。这包括确保代表中小企业工作的任何第三方都有适当的安全措施。	vpc-sg-ports-check	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。

建议项编号	建议项说明	合规规则	指导
5_SECURE ACCESS TO SYSTEMS	鼓励每个人使用密码短语，至少三个随机的常用词组合成一个短语，提供了一个非常好的记忆性和安全性的组合。	iam-password-policy	确保IAM用户密码强度满足密码强度要求。
5_SECURE ACCESS TO SYSTEMS	鼓励每个人使用密码短语，至少三个随机的常用词组合成一个短语，提供了一个非常好的记忆性和安全性的组合。	iam-user-mfa-enabled	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账号被盗用的事件。
5_SECURE ACCESS TO SYSTEMS	鼓励每个人使用密码短语，至少三个随机的常用词组合成一个短语，提供了一个非常好的记忆性和安全性的组合。	mfa-enabled-for-iam-console-access	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行MFA，您可以减少账号被盗用的事件，并防止敏感数据被未经授权的用户访问。
5_SECURE ACCESS TO SYSTEMS	鼓励每个人使用密码短语，至少三个随机的常用词组合成一个短语，提供了一个非常好的记忆性和安全性的组合。	root-account-mfa-enabled	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA为登录凭据添加了额外的保护。
6_SECURE DEVICES: KEEP SOFTWARE PATCHED AND UP TO DATE	理想情况下，使用集中式平台管理修补。强烈建议中小企业：定期更新其所有软件，尽可能打开自动更新，确定需要手动更新的软件和硬件，考虑移动和物联网设备。	cce-cluster-end-of-maintenance-version	确保CCE集群版本为处于维护中的版本。

建议项编号	建议项说明	合规规则	指导
6_SECURE DEVICES: KEEP SOFTWARE PATCHED AND UP TO DATE	理想情况下，使用集中式平台管理修补。强烈建议中小企业：定期更新其所有软件，尽可能打开自动更新，确定需要手动更新的软件和硬件，考虑移动和物联网设备。	cce-cluster-oldest-supported-version	系统会自动为您的华为云CCE任务部署安全更新和补丁。如果发现影响华为云CCE平台版本的安全问题，华为云会修补该平台版本。要帮助对运行华为云cluster的华为云CCE任务进行补丁管理，请更新您服务的独立任务以使用最新的平台版本。
6_SECURE DEVICES: ENCRYPTION	通过加密数据来保护数据。中小企业应确保存储在笔记本电脑、智能手机和桌子等移动设备上的数据是加密的。对于通过公共网络（如酒店或机场WiFi网络）传输的数据，确保通过使用虚拟专用网（VPN）或使用SSL/TLS协议通过安全连接访问网站来加密数据。确保他们自己的网站使用适当的加密技术来保护客户端数据在互联网上传输时。	cts-kms-encrypted-check	确保云审计服务的追踪器已配置KMS加密存储用于归档的审计事件。

建议项编号	建议项说明	合规规则	指导
6_SECURE DEVICES: ENCRYPTION	通过加密数据来保护数据。中小企业应确保存储在笔记本电脑、智能手机和桌子等移动设备上的数据是加密的。对于通过公共网络（如酒店或机场WiFi网络）传输的数据，确保通过使用虚拟专用网（VPN）或使用SSL/TLS协议通过安全连接访问网站来加密数据。确保他们自己的网站使用适当的加密技术来保护客户端数据在互联网上传输时。	cts-support-validate-check	确保云审计服务追踪器已打开事件文件校验，已避免日志文件存储后被修改、删除。
6_SECURE DEVICES: ENCRYPTION	通过加密数据来保护数据。中小企业应确保存储在笔记本电脑、智能手机和桌子等移动设备上的数据是加密的。对于通过公共网络（如酒店或机场WiFi网络）传输的数据，确保通过使用虚拟专用网（VPN）或使用SSL/TLS协议通过安全连接访问网站来加密数据。确保他们自己的网站使用适当的加密技术来保护客户端数据在互联网上传输时。	sfsturbo-encrypted-check	由于敏感数据可能存在并帮助保护静态数据，确保弹性文件服务已通过KMS进行加密。

建议项编号	建议项说明	合规规则	指导
6_SECURE DEVICES: ENCRYPTION	通过加密数据来保护数据。中小企业应确保存储在笔记本电脑、智能手机和桌子等移动设备上的数据是加密的。对于通过公共网络（如酒店或机场WiFi网络）传输的数据，确保通过使用虚拟专用网（VPN）或使用SSL/TLS协议通过安全连接访问网站来加密数据。确保他们自己的网站使用适当的加密技术来保护客户端数据在互联网上传输时。	css-cluster-disk-encryption-check	确保CSS集群开启磁盘加密。由于敏感数据可能存在，请在传输中启用加密以帮助保护该数据。
6_SECURE DEVICES: ENCRYPTION	通过加密数据来保护数据。中小企业应确保存储在笔记本电脑、智能手机和桌子等移动设备上的数据是加密的。对于通过公共网络（如酒店或机场WiFi网络）传输的数据，确保通过使用虚拟专用网（VPN）或使用SSL/TLS协议通过安全连接访问网站来加密数据。确保他们自己的网站使用适当的加密技术来保护客户端数据在互联网上传输时。	css-cluster-disk-encryption-check	确保CSS集群开启磁盘加密。由于敏感数据可能存在，请在传输中启用加密以帮助保护该数据。

建议项编号	建议项说明	合规规则	指导
6_SECURE DEVICES: ENCRYPTION	通过加密数据来保护数据。中小企业应确保存储在笔记本电脑、智能手机和桌子等移动设备上的数据是加密的。对于通过公共网络（如酒店或机场WiFi网络）传输的数据，确保通过使用虚拟专用网（VPN）或使用SSL/TLS协议通过安全连接访问网站来加密数据。确保他们自己的网站使用适当的加密技术来保护客户端数据在互联网上传输时。	css-cluster-https-required	开启HTTPS访问后，访问集群将进行通讯加密。关闭HTTPS访问后，会使用HTTP协议与集群通信，无法保证数据安全性，并且无法开启公网访问功能。
6_SECURE DEVICES: ENCRYPTION	通过加密数据来保护数据。中小企业应确保存储在笔记本电脑、智能手机和桌子等移动设备上的数据是加密的。对于通过公共网络（如酒店或机场WiFi网络）传输的数据，确保通过使用虚拟专用网（VPN）或使用SSL/TLS协议通过安全连接访问网站来加密数据。确保他们自己的网站使用适当的加密技术来保护客户端数据在互联网上传输时。	volumes-encrypted-check	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。

建议项编号	建议项说明	合规规则	指导
6_SECURE DEVICES: ENCRYPTION	通过加密数据来保护数据。中小企业应确保存储在笔记本电脑、智能手机和桌子等移动设备上的数据是加密的。对于通过公共网络（如酒店或机场WiFi网络）传输的数据，确保通过使用虚拟专用网（VPN）或使用SSL/TLS协议通过安全连接访问网站来加密数据。确保他们自己的网站使用适当的加密技术来保护客户端数据在互联网上传输时。	rds-instances-enable-kms	为了帮助保护静态数据，请确保为您的华为云RDS实例启用加密。由于敏感数据可以静态存在于华为云RDS实例中，因此启用静态加密有助于保护该数据。
6_SECURE DEVICES: ENCRYPTION	通过加密数据来保护数据。中小企业应确保存储在笔记本电脑、智能手机和桌子等移动设备上的数据是加密的。对于通过公共网络（如酒店或机场WiFi网络）传输的数据，确保通过使用虚拟专用网（VPN）或使用SSL/TLS协议通过安全连接访问网站来加密数据。确保他们自己的网站使用适当的加密技术来保护客户端数据在互联网上传输时。	dws-enable-kms	确保数据仓库服务的集群启用KMS磁盘加密。

建议项编号	建议项说明	合规规则	指导
6_SECURE DEVICES: ENCRYPTION	通过加密数据来保护数据。中小企业应确保存储在笔记本电脑、智能手机和桌子等移动设备上的数据是加密的。对于通过公共网络（如酒店或机场WiFi网络）传输的数据，确保通过使用虚拟专用网（VPN）或使用SSL/TLS协议通过安全连接访问网站来加密数据。确保他们自己的网站使用适当的加密技术来保护客户端数据在互联网上传输时。	gaussdb-nosql-enable-disk-encryption	确保GaussDB NoSQL启用KMS磁盘加密。
6_SECURE DEVICES: ENCRYPTION	通过加密数据来保护数据。中小企业应确保存储在笔记本电脑、智能手机和桌子等移动设备上的数据是加密的。对于通过公共网络（如酒店或机场WiFi网络）传输的数据，确保通过使用虚拟专用网（VPN）或使用SSL/TLS协议通过安全连接访问网站来加密数据。确保他们自己的网站使用适当的加密技术来保护客户端数据在互联网上传输时。	elb-tls-https-listeners-only	确保弹性负载均衡的监听器已配置HTTPS监听协议。由于可能存在敏感数据，因此启用传输中加密有助于保护该数据。

建议项编号	建议项说明	合规规则	指导
6_SECURE DEVICES: ENCRYPTION	通过加密数据来保护数据。中小企业应确保存储在笔记本电脑、智能手机和桌子等移动设备上的数据是加密的。对于通过公共网络（如酒店或机场WiFi网络）传输的数据，确保通过使用虚拟专用网（VPN）或使用SSL/TLS协议通过安全连接访问网站来加密数据。确保他们自己的网站使用适当的加密技术来保护客户端数据在互联网上传输时。	apig-instances-ssl-enabled	确保使用SSL证书配置华为云API网关REST API阶段，以允许后端系统对来自API网关的请求进行身份验证。
6_SECURE DEVICES: ENCRYPTION	通过加密数据来保护数据。中小企业应确保存储在笔记本电脑、智能手机和桌子等移动设备上的数据是加密的。对于通过公共网络（如酒店或机场WiFi网络）传输的数据，确保通过使用虚拟专用网（VPN）或使用SSL/TLS协议通过安全连接访问网站来加密数据。确保他们自己的网站使用适当的加密技术来保护客户端数据在互联网上传输时。	dws-enable-ssl	确保数据仓库服务需要SSL加密才能连接到数据库客户端。由于敏感数据可能存在，因此在传输过程中启用加密以帮助保护该数据。
7_SECURE YOUR NETWORK: EMPLOY FIREWALLS	防火墙管理进出网络的流量，是保护中小企业系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护中小企业的网络免受互联网的侵害。	vpc-sg-restricted-ssh	当外部任意IP可以访问安全组内云服务器的SSH（22）端口时认为不合规，确保对服务器的远程访问安全性。

建议项编号	建议项说明	合规规则	指导
7_SECURE YOUR NETWORK: EMPLOY FIREWALLS	防火墙管理进出网络的流量，是保护中小企业系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护中小企业的网络免受互联网的侵害。	vpc-sg-restricted-common-ports	在华为云VPC安全组上限制通用端口的IP地址，确保对安全组内资源实例的访问。
7_SECURE YOUR NETWORK: EMPLOY FIREWALLS	防火墙管理进出网络的流量，是保护中小企业系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护中小企业的网络免受互联网的侵害。	vpc-default-sg-closed	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。
7_SECURE YOUR NETWORK: EMPLOY FIREWALLS	防火墙管理进出网络的流量，是保护中小企业系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护中小企业的网络免受互联网的侵害。	vpc-sg-ports-check	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	中小企业应定期审查任何远程访问工具，以确保它们的安全，特别是： 1、确保所有远程访问软件都已修补和更新。2、限制来自可疑地理位置或某些IP地址的远程访问。3、限制员工仅远程访问他们工作所需的系统和计算机。4、强制使用强密码进行远程访问，并在可能的情况下启用多因素身份验证。 5、确保启用监控和警报，以警告可疑攻击或异常可疑活动。	iam-password-policy	确保IAM用户密码强度满足密码强度要求。

建议项编号	建议项说明	合规规则	指导
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	中小企业应定期审查任何远程访问工具，以确保它们的安全，特别是： 1、确保所有远程访问软件都已修补和更新。2、限制来自可疑地理位置或某些IP地址的远程访问。3、限制员工仅远程访问他们工作所需的系统和计算机。4、强制使用强密码进行远程访问，并在可能的情况下启用多因素身份验证。 5、确保启用监控和警报，以警告可疑攻击或异常可疑活动。	iam-user-mfa-enabled	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账号被盗用的事件。
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	中小企业应定期审查任何远程访问工具，以确保它们的安全，特别是： 1、确保所有远程访问软件都已修补和更新。2、限制来自可疑地理位置或某些IP地址的远程访问。3、限制员工仅远程访问他们工作所需的系统和计算机。4、强制使用强密码进行远程访问，并在可能的情况下启用多因素身份验证。 5、确保启用监控和警报，以警告可疑攻击或异常可疑活动。	mfa-enabled-for-iam-console-access	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行MFA，您可以减少账号被盗用的事件，并防止敏感数据被未经授权的用户访问。

建议项编号	建议项说明	合规规则	指导
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	中小企业应定期审查任何远程访问工具，以确保它们的安全，特别是： 1、确保所有远程访问软件都已修补和更新。2、限制来自可疑地理位置或某些IP地址的远程访问。3、限制员工仅远程访问他们工作所需的系统和计算机。4、强制使用强密码进行远程访问，并在可能的情况下启用多因素身份验证。 5、确保启用监控和警报，以警告可疑攻击或异常可疑活动。	root-account-mfa-enabled	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA为登录凭据添加了额外的保护。
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	中小企业应定期审查任何远程访问工具，以确保它们的安全，特别是： 1、确保所有远程访问软件都已修补和更新。2、限制来自可疑地理位置或某些IP地址的远程访问。3、限制员工仅远程访问他们工作所需的系统和计算机。4、强制使用强密码进行远程访问，并在可能的情况下启用多因素身份验证。 5、确保启用监控和警报，以警告可疑攻击或异常可疑活动。	apig-instances-execution-logging-enabled	确保为APIG专享版实例配置访问日志。APIG支持日志自定义分析模板，便于日志的统一收集和管理，也可通过API异常调用分析进行追查和溯源。

建议项编号	建议项说明	合规规则	指导
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	中小企业应定期审查任何远程访问工具，以确保它们的安全，特别是： 1、确保所有远程访问软件都已修补和更新。2、限制来自可疑地理位置或某些IP地址的远程访问。3、限制员工仅远程访问他们工作所需的系统和计算机。4、强制使用强密码进行远程访问，并在可能的情况下启用多因素身份验证。 5、确保启用监控和警报，以警告可疑攻击或异常可疑活动。	cts-lts-enable	确保使用云日志服务集中收集云审计服务的数据。
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	中小企业应定期审查任何远程访问工具，以确保它们的安全，特别是： 1、确保所有远程访问软件都已修补和更新。2、限制来自可疑地理位置或某些IP地址的远程访问。3、限制员工仅远程访问他们工作所需的系统和计算机。4、强制使用强密码进行远程访问，并在可能的情况下启用多因素身份验证。 5、确保启用监控和警报，以警告可疑攻击或异常可疑活动。	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务用于记录华为云管理控制台操作。

建议项编号	建议项说明	合规规则	指导
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	中小企业应定期审查任何远程访问工具，以确保它们的安全，特别是： 1、确保所有远程访问软件都已修补和更新。2、限制来自可疑地理位置或某些IP地址的远程访问。3、限制员工仅远程访问他们工作所需的系统和计算机。4、强制使用强密码进行远程访问，并在可能的情况下启用多因素身份验证。 5、确保启用监控和警报，以警告可疑攻击或异常可疑活动。	multi-region-cts-tracker-exists	云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。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。
7_SECURE YOUR NETWORK: REVIEW REMOTE ACCESS SOLUTIONS	中小企业应定期审查任何远程访问工具，以确保它们的安全，特别是： 1、确保所有远程访问软件都已修补和更新。2、限制来自可疑地理位置或某些IP地址的远程访问。3、限制员工仅远程访问他们工作所需的系统和计算机。4、强制使用强密码进行远程访问，并在可能的情况下启用多因素身份验证。 5、确保启用监控和警报，以警告可疑攻击或异常可疑活动。	vpc-flow-logs-enabled	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。

建议项编号	建议项说明	合规规则	指导
9_SECURE BACKUPS	要恢复密钥形成，应维护备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应适用以下备份规则：1、备份是定期和自动化的，2、备份与中小企业的生产环境分开保存，3、备份是加密的，特别是如果备份要在不同地点之间移动，4、测试定期从备份中恢复数据的能力。理想情况下，应定期测试从头到尾的完整恢复。	rds-instance-enable-backup	确保云数据库资源开启备份。
9_SECURE BACKUPS	要恢复密钥形成，应维护备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应适用以下备份规则：1、备份是定期和自动化的，2、备份与中小企业的生产环境分开保存，3、备份是加密的，特别是如果备份要在不同地点之间移动，4、测试定期从备份中恢复数据的能力。理想情况下，应定期测试从头到尾的完整恢复。	dws-enable-snapshot	自动快照采用差异增量备份，当创建集群时，自动快照默认处于启用状态。当集群启用了自动快照时，DWS将按照设定的时间和周期以及快照类型自动创建快照，默认为每8小时一次。用户也可以对集群设置自动快照策略，并根据自身需求，对集群设置一个或多个自动快照策略。

建议项编号	建议项说明	合规规则	指导
9_SECURE BACKUPS	要恢复密钥形成，应维护备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应适用以下备份规则：1、备份是定期和自动化的，2、备份与中小企业的生产环境分开保存，3、备份是加密的，特别是如果备份要在不同地点之间移动，4、测试定期从备份中恢复数据的能力。理想情况下，应定期测试从头到尾的完整恢复。	gaussdb-nosql-enable-backup	确保GaussDB NoSQL开启备份。

4.5.22 适用于 SWIFT CSP 的标准合规包

本文为您介绍适用于SWIFT CSP的标准合规包的业务背景以及合规包中的默认规则。

业务背景

SWIFT CSP是SWIFT公司推出的一种云安全解决方案，旨在为金融机构提供更加安全、可靠的SWIFT交易网络服务。有关SWIFT CSP的更多信息，请参见SWFIT官网**https://www.swift.com/**。

免责条款

本合规规则包模板为您提供通用的操作指引，帮助您快速创建符合目标场景的合规规则包。为避免疑义，本“合规”仅指资源符合规则定义本身的合规性描述，不构成任何法律意见。本合规规则包模板不确保符合特定法律法规或行业标准的要求，您需自行对您的业务、技术操作的合规性和合法性负责并承担与此相关的所有责任。

默认规则

此表中的建议项编号对应**https://www.swift.com/**中参考文档的章节编号，供您查阅参考。

表 4-26 适用于 SWIFT CSP 的标准合规包默认规则说明

建议项编号	合规规则	指导
1.1	ecs-instance-no-public-ip	由于华为云ECS实例可能包含敏感信息，确保华为云ECS实例无法公开访问来管理对华为云的访问。
1.1	ecs-instance-in-vpc	确保弹性云服务器所有流量都安全地保留在虚拟私有云中。
1.1	vpc-default-sg-closed	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。
1.1	vpc-acl-unused-check	网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的网络流量。此规则可确保现存网络ACL均与子网关联，实现对子网的防护。
1.1	vpc-sg-ports-check	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。
1.2	iam-customer-policy-blocked-kms-actions	帮助您将最小权限和职责分离的原则与访问权限和授权结合起来，限制策略在数据加密服务上包含阻止的操作。拥有超过完成任务所需的特权可能违反最小特权和职责分离的原则。
1.2	iam-group-has-users-check	确保IAM组至少有一个用户，帮助您将最小权限和职责分离的原则与访问权限和授权结合起来。
1.2	vpc-sg-restricted-ssh	当外部任意IP可以访问安全组内云服务器的SSH（22）端口时认为不合规，确保对服务器的远程访问安全性。
1.2	smn-lts-enable	确保为指定SMN主题绑定一个云日志，用于记录主题消息发送状态等信息。
1.4	private-nat-gateway-authorized-vpc-only	确保NAT私网网关仅连接到授权的虚拟私有云中，管理对华为云中资源的访问。
1.4	vpc-sg-restricted-common-ports	在华为云VPC安全组上限制通用端口的ip地址，确保对安全组内资源实例的访问。
1.4	function-graph-public-access-prohibited	确保函数工作流的函数不能公开访问，管理对华为云中资源的访问。公开访问可能导致资源可用性下降。
2.3	ecs-multiple-public-ip-check	此规则检查您的华为云ECS实例是否具有多个公网IP。拥有多个公网IP可能会增加网络安全的复杂性。
2.3	volume-unused-check	确保云硬盘未闲置。

建议项编号	合规规则	指导
2.3	kms-not-scheduled-for-deletion	确保数据加密服务密钥未处于“计划删除”状态，以防止误删除密钥。
2.5A	sfsturbo-encrypted-check	由于敏感数据可能存在并帮助保护静态数据，确保弹性文件服务已通过KMS进行加密。
2.5A	volumes-encrypted-check	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。
4.1	iam-password-policy	确保IAM用户密码强度满足密码强度要求。
4.1	access-keys-rotated	确保根据组织策略轮换IAM访问密钥，这缩短了访问密钥处于活动状态的时间，并在密钥被泄露时减少业务影响。
4.2	iam-user-mfa-enabled	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账号被盗用的事件。
4.2	mfa-enabled-for-iam-console-access	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行MFA，您可以减少账号被盗用的事件，并防止敏感数据被未经授权的用户访问。
4.2	root-account-mfa-enabled	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA为登录凭据添加了额外的保护。
5.1	iam-role-has-all-permissions	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。
5.1	iam-root-access-key-check	确保根访问密钥已删除。
5.1	iam-user-group-membership-check	确保用户至少是一个组的成员，帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最小权限和职责分离的原则。
6.4	cts-lts-enable	确保使用云日志服务集中收集云审计服务的数据。
6.4	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务用于记录华为云管理控制台操作。

建议项编号	合规规则	指导
6.4	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。
6.4	cts-kms-encrypted-check	确保云审计服务的追踪器已配置KMS加密存储用于归档的审计事件。
6.4	cts-support-validate-check	确保云审计服务追踪器已打开事件文件校验，已避免日志文件存储后被修改、删除。
6.4	stopped-ecs-date-diff	启用此规则可根据您组织的标准检查华为云ecs实例的停止时间是否超过允许的天数，确保弹性云服务器未闲置。
6.4	vpc-flow-logs-enabled	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。

4.5.23 适用于德国云计算合规标准目录的标准合规包

本文为您介绍适用于德国云计算合规标准目录的标准合规包的业务背景、应用场景，以及合规包中的默认规则。

业务背景

德国云计算合规实践目录是一份关于如何在德国进行云计算的指南。它包括了关于数据保护、数据主权、透明度、责任、以及云服务提供商选择等方面的最佳做法。关于该指南的更多信息，请参见**C5_2020**。

应用场景

适用于德国云计算合规标准目录的标准合规包应用于需要满足德国云计算合规标准目录的企业，帮助其满足相关的法律法规要求，但需要根据具体情况进行评估和实施。

免责条款

本合规规则包模板为您提供通用的操作指引，帮助您快速创建符合目标场景的合规规则包。为避免疑义，本“合规”仅指资源符合规则定义本身的合规性描述，不构成任何法律意见。本合规规则包模板不确保符合特定法律法规或行业标准的要求，您需自行对您的业务、技术操作的合规性和合法性负责并承担与此相关的所有责任。

默认规则

此表中的建议项编号对应**C5_2020**中参考文档的章节编号，供您查阅参考。

表 4-27 适用于德国云计算合规标准目录的标准合规包默认规则说明

建议项编号	合规规则	指导
COS-03	drs-data-guard-job-not-public	确保DRS实时灾备任务不能公开访问。
COS-03	drs-migration-job-not-public	确保DRS实时迁移任务不能公开访问。
COS-03	drs-synchronization-job-not-public	确保DRS实时同步任务不能公开访问。
COS-03	ecs-instance-no-public-ip	由于华为云ECS实例可能包含敏感信息，确保华为云ECS实例无法公开访问来管理对华为云的访问。
COS-03	ecs-instance-in-vpc	确保弹性云服务器所有流量都安全地保留在虚拟私有云中。
COS-03	css-cluster-in-vpc	确保云搜索服务位于虚拟私有云中。
COS-03	css-cluster-in-vpc	确保云搜索服务位于虚拟私有云中。
COS-03	mrs-cluster-no-public-ip	确保MapReduce服务（MRS）无法公网访问。华为云MRS集群主节点可能包含敏感信息，并且此类账号需要访问控制。
COS-03	function-graph-public-access-prohibited	确保函数工作流的函数不能公开访问，管理对华为云中资源的访问。公开访问可能导致资源可用性下降。
COS-03	rds-instance-no-public-ip	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账号需要原则和访问控制。
COS-03	vpc-sg-restricted-common-ports	在华为云VPC安全组上限制通用端口的IP地址，确保对安全组内资源实例的访问。
COS-03	vpc-sg-restricted-ssh	当外部任意IP可以访问安全组内云服务器的SSH（22）端口时认为不合规，确保对服务器的远程访问安全性。
COS-03	vpc-default-sg-closed	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。
COS-03	vpc-sg-ports-check	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。

建议项编号	合规规则	指导
COS-05	iam-user-mfa-enabled	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账号被盗用的事件。
COS-05	mfa-enabled-for-iam-console-access	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行MFA，您可以减少账号被盗用的事件，并防止敏感数据被未经授权的用户访问。
COS-05	root-account-mfa-enabled	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA为登录凭据添加了额外的保护。
COS-05	ecs-instance-no-public-ip	由于华为云ecs实例可能包含敏感信息，确保华为云ecs实例无法公开访问来管理对华为云的访问。
COS-05	mrs-cluster-no-public-ip	确保MapReduce服务（MRS）无法公网访问。华为云MRS集群主节点可能包含敏感信息，并且此类账号需要访问控制。
COS-05	rds-instance-no-public-ip	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账号需要原则和访问控制。
COS-05	vpc-sg-restricted-common-ports	在华为云VPC安全组上限制通用端口的IP地址，确保对安全组内资源实例的访问。
COS-05	vpc-sg-restricted-ssh	当外部任意IP可以访问安全组内云服务器的SSH（22）端口时认为不合规，确保对服务器的远程访问安全性。
COS-05	vpc-default-sg-closed	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。
COS-05	vpc-sg-ports-check	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。
CRY-02	apig-instances-ssl-enabled	确保使用SSL证书配置华为云API网关REST API阶段，以允许后端系统对来自API网关的请求进行身份验证。
CRY-02	elb-predefined-security-policy-https-check	确保独享型负载均衡器使用了指定的安全策略。在创建和配置HTTPS监听器时，您可以选择使用安全策略，可以提高您的业务安全性。

建议项编号	合规规则	指导
CRY-02	css-cluster-https-required	开启HTTPS访问后，访问集群将进行通讯加密。关闭HTTPS访问后，会使用HTTP协议与集群通信，无法保证数据安全性，并且无法开启公网访问功能。
CRY-02	css-cluster-disk-encryption-check	确保CSS集群开启磁盘加密。由于敏感数据可能存在，请在传输中启用加密以帮助保护该数据。
CRY-02	elb-tls-https-listeners-only	确保弹性负载均衡的监听器已配置HTTPS监听协议。由于可能存在敏感数据，因此启用传输中加密有助于保护该数据。
CRY-02	dws-enable-ssl	确保数据仓库服务需要SSL加密才能连接到数据库客户端。由于敏感数据可能存在，因此在传输过程中启用加密以帮助保护该数据。
CRY-02	css-cluster-disk-encryption-check	确保CSS集群开启磁盘加密。由于敏感数据可能存在，请在传输中启用加密以帮助保护该数据。
CRY-03	cts-kms-encrypted-check	确保云审计服务的追踪器已配置KMS加密存储用于归档的审计事件。
CRY-03	sfsturbo-encrypted-check	由于敏感数据可能存在并帮助保护静态数据，确保弹性文件服务已通过KMS进行加密。
CRY-03	volumes-encrypted-check	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。
CRY-03	rds-instances-enable-kms	为了帮助保护静态数据，请确保为您的华为云RDS实例启用加密。由于敏感数据可以静态存在于华为云RDS实例中，因此启用静态加密有助于保护该数据。
CRY-04	kms-rotation-enabled	确保数据加密服务密钥启用密钥轮换。
DEV-07	cts-lts-enable	确保使用云日志服务集中收集云审计服务的数据。
DEV-07	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务（CTS）用于记录华为云管理控制台操作。
DEV-07	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。
DEV-07	cts-obs-bucket-track	确保存在至少一个CTS追踪器追踪指定的OBS桶。

建议项编号	合规规则	指导
DEV-07	multi-region-cts-tracker-exists	云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。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。
IDM-01	access-keys-rotated	确保根据组织策略轮换IAM访问密钥，这缩短了访问密钥处于活动状态的时间，并在密钥被泄露时减少业务影响。
IDM-01	mrs-cluster-kerberos-enabled	通过为华为云MRS集群启用Kerberos，可以按照最小权限和职责分离的原则来管理和合并访问权限和授权。
IDM-01	iam-password-policy	确保IAM用户密码强度满足密码强度要求。
IDM-01	iam-root-access-key-check	确保根访问密钥已删除。
IDM-01	iam-user-group-membership-check	确保用户至少是一个组的成员，帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最小权限和职责分离的原则。
IDM-01	iam-user-mfa-enabled	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账号被盗用的事件。
IDM-01	mfa-enabled-for-iam-console-access	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行MFA，您可以减少账号被盗用的事件，并防止敏感数据被未经授权的用户访问。
IDM-01	root-account-mfa-enabled	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA为登录凭据添加了额外的保护。
IDM-01	iam-group-has-users-check	确保IAM组至少有一个用户，帮助您将最小权限和职责分离的原则与访问权限和授权结合起来。
IDM-01	iam-role-has-all-permissions	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。
IDM-08	iam-password-policy	确保IAM用户密码强度满足密码强度要求。

建议项编号	合规规则	指导
CRY-01	iam-password-policy	确保IAM用户密码强度满足密码强度要求。
IDM-09	iam-user-mfa-enabled	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账号被盗用的事件。
IDM-09	mfa-enabled-for-iam-console-access	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行MFA，您可以减少账号被盗用的事件，并防止敏感数据被未经授权的用户访问。
IDM-09	root-account-mfa-enabled	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA为登录凭据添加了额外的保护。
OPS-01	rds-instance-multi-az-support	华为云RDS中的多可用区支持为数据库实例提供了增强的可用性和持久性。当您预置多可用区数据库实例时，华为云RDS会自动创建主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用区都在其物理上不同的独立基础设施上运行，并且经过精心设计，高度可靠。如果发生基础设施故障，华为云RDS会自动故障转移到备用数据库，以便您可以在故障转移完成后立即恢复数据库操作。
OPS-02	as-group-elb-healthcheck-required	弹性负载均衡是将访问流量根据转发策略分发到后端多台云服务器的流量分发控制服务。这条规则确保与负载均衡器关联的伸缩组使用弹性负载均衡健康检查。
OPS-02	rds-instance-multi-az-support	华为云RDS中的多可用区支持为数据库实例提供了增强的可用性和持久性。当您预置多可用区数据库实例时，华为云RDS会自动创建主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用区都在其物理上不同的独立基础设施上运行，并且经过精心设计，高度可靠。如果发生基础设施故障，华为云RDS会自动故障转移到备用数据库，以便您可以在故障转移完成后立即恢复数据库操作。
OPS-07	rds-instance-enable-backup	确保云数据库资源开启备份。

建议项编号	合规规则	指导
OPS-07	dws-enable-snapshot	自动快照采用差异增量备份，当创建集群时，自动快照默认处于启用状态。当集群启用了自动快照时，DWS将按照设定的时间和周期以及快照类型自动创建快照，默认为每8小时一次。用户也可以对集群设置自动快照策略，并根据自身需求，对集群设置一个或多个自动快照策略。
OPS-07	gaussdb-nosql-enable-backup	确保GaussDB NoSQL开启备份。
OPS-14	cts-support-validate-check	确保云审计服务追踪器已打开事件文件校验，已避免日志文件存储后被修改、删除。
OPS-14	cts-kms-encrypted-check	确保云审计服务的追踪器已配置KMS加密存储用于归档的审计事件。
OPS-15	apig-instances-execution-logging-enabled	确保为APIG专享版实例配置访问日志。APIG支持日志自定义分析模板，便于日志的统一收集和管理，也可通过API异常调用分析进行追查和溯源。
OPS-15	cts-lts-enable	确保使用云日志服务集中收集云审计服务的数据。
OPS-15	dws-enable-log-dump	要获取有关华为云DWS集群上用户活动的信息，请确保启用日志转储。
OPS-15	vpc-flow-logs-enabled	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。
OPS-15	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务用于记录华为云管理控制台操作。
OPS-15	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。
OPS-15	cts-obs-bucket-track	确保存在至少一个CTS追踪器追踪指定的OBS桶。
OPS-15	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。

建议项编号	合规规则	指导
PSS-05	iam-user-mfa-enabled	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账号被盗用的事件。
PSS-05	mfa-enabled-for-iam-console-access	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行MFA，您可以减少账号被盗用的事件，并防止敏感数据被未经授权的用户访问。
PSS-05	root-account-mfa-enabled	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA为登录凭据添加了额外的保护。
PSS-07	iam-password-policy	确保IAM用户密码强度满足密码强度要求。

4.5.24 适用于 PCI-DSS 的标准合规包

本文为您介绍适用于PCI-DSS的标准合规包的业务背景、应用场景，以及合规包中的默认规则。

业务背景

支付卡行业数据安全标准（PCI DSS）的制定旨在鼓励和增强支付卡账号的数据安全，并促进全球范围内广泛采用一致的数据安全措施。PCI DSS提供技术和运营基线，旨在保护账号数据的要求。虽然专门设计用于关注具有支付卡账号数据的环境，但PCI DSS还可用于防范威胁并保护支付生态系统中的其他元素。有关PCI DSS的更多信息，请参见**PCI DSS: v3.2.1**。

应用场景

适用于PCI-DSS的标准合规包应用于需要满足支付卡行业数据安全标准的企业，帮助其满足相关的法律法规要求，但需要根据具体情况进行评估和实施。

免责条款

本合规规则包模板为您提供通用的操作指引，帮助您快速创建符合目标场景的合规规则包。为避免疑义，本“合规”仅指资源符合规则定义本身的合规性描述，不构成任何法律意见。本合规规则包模板不确保符合特定法律法规或行业标准的要求，您需自行对您的业务、技术操作的合规性和合法性负责并承担与此相关的所有责任。

默认规则

此表中的建议项编号对应**PCI DSS: v3.2.1**中参考文档的章节编号，供您查阅参考。

表 4-28 适用于适用于 PCI-DSS 的标准合规包默认规则说明

建议项编号	建议项说明	合规规则	指导说明
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	css-cluster-in-vpc	确保云搜索服务（CSS）位于虚拟私有云（VPC）中。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	css-cluster-in-vpc	确保云搜索服务（CSS）位于虚拟私有云（VPC）中。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	drs-data-guard-job-not-public	确保DRS实时灾备任务不能公开访问。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	drs-migration-job-not-public	确保DRS实时迁移任务不能公开访问。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	drs-synchronization-job-not-public	确保DRS实时同步任务不能公开访问。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	ecs-instance-in-vpc	确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	ecs-instance-no-public-ip	由于华为云ECS实例可能包含敏感信息，确保华为云ECS实例无法公开访问来管理对华为云的访问。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	function-graph-inside-vpc	确保函数工作流（FunctionGraph）的所有流量都安全地位于虚拟私有云（VPC）中。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	function-graph-public-access-prohibited	确保函数工作流的函数不能公开访问，管理对华为云中资源的访问。公开访问可能导致资源可用性下降。

建议项编号	建议项说明	合规规则	指导说明
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	mrs-cluster-no-public-ip	确保MapReduce服务（MRS）无法公网访问。华为云MRS集群主节点可能包含敏感信息，并且此类账号需要访问控制。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	rds-instance-no-public-ip	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账号需要原则和访问控制。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	vpc-default-sg-closed	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	vpc-sg-ports-check	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	vpc-sg-restricted-common-ports	在华为云VPC安全组上限制通用端口的IP地址，确保对安全组内资源实例的访问。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间直接进行公共访问。	vpc-sg-restricted-ssh	当外部任意IP可以访问安全组内云服务器的SSH（22）端口时认为不合规，确保对服务器的远程访问安全性。

建议项编号	建议项说明	合规规则	指导说明
2.1	在网络上安装系统之前，请务必更改供应商提供的默认值，并删除或禁用不必要的默认账号。这适用于所有默认密码，包括但不限于操作系统、提供安全服务的软件、应用程序和系统账号、销售点（POS）终端、支付应用程序、简单网络管理协议（SNMP）社区字符串等使用的密码。	root-account-mfa-enabled	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA为登录凭据添加了额外的保护。
2.1	在网络上安装系统之前，请务必更改供应商提供的默认值，并删除或禁用不必要的默认账号。这适用于所有默认密码，包括但不限于操作系统、提供安全服务的软件、应用程序和系统账号、销售点（POS）终端、支付应用程序、简单网络管理协议（SNMP）社区字符串等使用的密码。	vpc-default-sg-closed	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	access-keys-rotated	确保根据组织策略轮换IAM访问密钥，这缩短了访问密钥处于活动状态的时间，并在密钥被泄露时减少业务影响。

建议项编号	建议项说明	合规规则	指导说明
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	access-keys-rotated	确保根据组织策略轮换IAM访问密钥，这缩短了访问密钥处于活动状态的时间，并在密钥被泄露时减少业务影响。
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	cts-kms-encrypted-check	确保云审计服务（CTS）的追踪器已配置KMS加密存储用于归档的审计事件。
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	cts-lts-enable	确保使用云日志服务（LTS）集中收集云审计服务（CTS）的数据。

建议项编号	建议项说明	合规规则	指导说明
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	cts-obs-bucket-track	确保存在至少一个CTS追踪器追踪指定的OBS桶。
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	cts-support-validate-check	确保云审计服务（CTS）追踪器已打开事件文件校验，已避免日志文件存储后被修改、删除。
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	ecs-in-allowed-security-groups	安全组为具有相同安全保护需求并相互信任的云服务器提供访问策略。当云服务器加入该安全组后，即受到安全组内用户定义的访问规则的保护。确保特定ECS实例关联高危安全组，保证安全组的性能。

建议项编号	建议项说明	合规规则	指导说明
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	ecs-multiple-public-ip-check	此规则检查您的华为云ECS实例是否具有多个公网IP。拥有多个公网IP可能会增加网络安全的复杂性。
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	iam-policy-no-statements-with-admin-access	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	iam-root-access-key-check	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。

建议项编号	建议项说明	合规规则	指导说明
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	iam-user-group-membership-check	确保用户至少是一个组的成员，帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最小权限和职责分离的原则。
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	kms-rotation-enabled	确保数据加密服务（KMS）密钥启用密钥轮换。
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	mfa-enabled-for-iam-console-access	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行MFA，您可以减少账号被盗用的事件，并防止敏感数据被未经授权的用户访问。

建议项编号	建议项说明	合规规则	指导说明
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	root-account-mfa-enabled	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA为登录凭据添加了额外的保护。
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	volumes-encrypted-check	由于敏感数据可能存在并帮助保护静态数据，因此请确保为华为云ElasticVolumeService（华为云EVS）卷启用加密。

建议项编号	建议项说明	合规规则	指导说明
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	vpc-default-sg-closed	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	vpc-flow-logs-enabled	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	vpc-sg-restricted-common-ports	在华为云VPC安全组上限制通用端口的IP地址，确保对安全组内资源实例的访问。

建议项编号	建议项说明	合规规则	指导说明
2.2	为所有系统组件制定配置标准。确保这些标准解决所有已知的安全漏洞，并与行业公认的系统强化标准保持一致。行业公认的系统强化标准的来源可能包括但不限于：互联网安全中心（CIS）国际标准化组织（ISO）SysAdmin审计网络安全（SANS）研究所美国国家标准技术研究院（NIST）。	vpc-sg-restricted-ssh	当外部任意IP可以访问安全组内云服务器的SSH（23）端口时认为不合规，确保对服务器的远程访问安全性。
2.3	使用强加密技术对所有非控制台管理访问进行加密。	apig-instances-ssl-enabled	确保使用SSL证书配置华为云API Gateway REST API阶段，以允许后端系统对来自API Gateway的请求进行身份验证。
2.3	使用强加密技术对所有非控制台管理访问进行加密。	css-cluster-https-required	开启HTTPS访问后，访问集群将进行通讯加密。关闭HTTPS访问后，会使用HTTP协议与集群通信，无法保证数据安全性，并且无法开启公网访问功能。
2.3	使用强加密技术对所有非控制台管理访问进行加密。	dws-enable-ssl	确保数据仓库服务需要SSL加密才能连接到数据库客户端。由于敏感数据可能存在，因此在传输过程中启用加密以帮助保护该数据。
2.3	使用强加密技术对所有非控制台管理访问进行加密。	elb-tls-https-listeners-only	确保弹性负载均衡的监听器已配置HTTPS监听协议。由于可能存在敏感数据，因此启用传输中加密有助于保护该数据。

建议项编号	建议项说明	合规规则	指导说明
2.4	维护PCIDSS范围内的系统组件清单。	ecs-in-allowed-security-groups	安全组为具有相同安全保护需求并相互信任的云服务器提供访问策略。当云服务器加入该安全组后，即受到安全组内用户定义的访问规则的保护。确保特定ECS实例关联高危安全组，保证安全组的性能。
2.4	维护PCIDSS范围内的系统组件清单。	eip-unbound-check	确保弹性公网IP未闲置。
2.4	维护PCIDSS范围内的系统组件清单。	eip-use-in-specified-days	确保弹性公网IP未闲置。
2.4	维护PCIDSS范围内的系统组件清单。	vpc-acl-unused-check	网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的网络流量。此规则可确保现存网络ACL均与子网关联，实现对子网的防护。
3.4	使用以下任一方法使PAN在存储的任何位置（包括便携式数字媒体、备份媒体和日志中）都不可读：基于强加密的单向哈希，（哈希必须是整个PAN的哈希）截断（哈希不能用于替换PAN的截断段）索引令牌和垫子（垫子必须安全存放）具有相关密钥管理流程和程序的强加密技术。注意：如果恶意个人可以访问PAN的截断版本和散列版本，则重建原始PAN数据是一项相对微不足道的工作。如果实体环境中存在同一PAN的哈希和截断版本，则必须实施其他控制措施，以确保哈希和截断版本无法关联以重建原始PAN。	cts-kms-encrypted-check	确保云审计服务（CTS）的追踪器已配置KMS加密存储用于归档的审计事件。

建议项编号	建议项说明	合规规则	指导说明
3.4	使用以下任一方法使PAN在存储的任何位置（包括便携式数字媒体、备份媒体和日志中）都不可读：基于强加密的单向哈希，（哈希必须是整个PAN的哈希）截断（哈希不能用于替换PAN的截断段）索引令牌和垫子（垫子必须安全存放）具有相关密钥管理流程和程序的强加密技术。注意：如果恶意个人可以访问PAN的截断版本和散列版本，则重建原始PAN数据是一项相对微不足道的工作。如果实体环境中存在同一PAN的哈希和截断版本，则必须实施其他控制措施，以确保哈希和截断版本无法关联以重建原始PAN。	rds-instances-enable-kms	为了帮助保护静态数据，请确保为您的华为云RDS实例启用加密。由于敏感数据可以静态存在于华为云RDS实例中，因此启用静态加密有助于保护该数据。
3.4	使用以下任一方法使PAN在存储的任何位置（包括便携式数字媒体、备份媒体和日志中）都不可读：基于强加密的单向哈希，（哈希必须是整个PAN的哈希）截断（哈希不能用于替换PAN的截断段）索引令牌和垫子（垫子必须安全存放）具有相关密钥管理流程和程序的强加密技术。注意：如果恶意个人可以访问PAN的截断版本和散列版本，则重建原始PAN数据是一项相对微不足道的工作。如果实体环境中存在同一PAN的哈希和截断版本，则必须实施其他控制措施，以确保哈希和截断版本无法关联以重建原始PAN。	sfsturbo-encrypted-check	由于敏感数据可能存在并帮助保护静态数据，确保弹性文件服务（SFSTurbo）已通过KMS进行加密。

建议项编号	建议项说明	合规规则	指导说明
3.4	使用以下任一方法使PAN在存储的任何位置（包括便携式数字媒体、备份媒体和日志中）都不可读：基于强加密的单向哈希，（哈希必须是整个PAN的哈希）截断（哈希不能用于替换PAN的截断段）索引令牌和垫子（垫子必须安全存放）具有相关密钥管理流程和程序的强加密技术。注意：如果恶意个人可以访问PAN的截断版本和散列版本，则重建原始PAN数据是一项相对微不足道的工作。如果实体环境中存在同一PAN的哈希和截断版本，则必须实施其他控制措施，以确保哈希和截断版本无法关联以重建原始PAN。	volumes-encrypted-check	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。
4.1	使用强大的加密和安全协议来保护通过开放公共网络传输的敏感持卡人数据，包括：仅接受受信任的密钥和证书。使用的协议仅支持安全版本或配置。加密强度适用于所使用的加密方法。开放的公共网络示例包括但不限于：互联网无线技术，包括802.11和蓝牙蜂窝技术，例如全球移动通信系统（GSM）、码分多址（CDMA）通用分组无线业务（GPRS）卫星通信	apig-instances-ssl-enabled	确保使用SSL证书配置华为云API Gateway REST API阶段，以允许后端系统对来自API Gateway的请求进行身份验证。

建议项编号	建议项说明	合规规则	指导说明
4.1	使用强大的加密和安全协议来保护通过开放公共网络传输的敏感持卡人数据，包括：仅接受受信任的密钥和证书。使用的协议仅支持安全版本或配置。加密强度适用于所使用的加密方法。开放的公共网络示例包括但不限于：互联网无线技术，包括802.11和蓝牙蜂窝技术，例如全球移动通信系统（GSM）、码分多址（CDMA）通用分组无线业务（GPRS）卫星通信	css-cluster-disk-encryption-check	确保CSS集群开启磁盘加密。由于敏感数据可能存在，请在传输中启用加密以帮助保护该数据。
4.1	使用强大的加密和安全协议来保护通过开放公共网络传输的敏感持卡人数据，包括：仅接受受信任的密钥和证书。使用的协议仅支持安全版本或配置。加密强度适用于所使用的加密方法。开放的公共网络示例包括但不限于：互联网无线技术，包括802.11和蓝牙蜂窝技术，例如全球移动通信系统（GSM）、码分多址（CDMA）通用分组无线业务（GPRS）卫星通信	css-cluster-disk-encryption-check	确保CSS集群开启磁盘加密。由于敏感数据可能存在，请在传输中启用加密以帮助保护该数据。

建议项编号	建议项说明	合规规则	指导说明
4.1	使用强大的加密和安全协议来保护通过开放公共网络传输的敏感持卡人数据，包括：仅接受受信任的密钥和证书。使用的协议仅支持安全版本或配置。加密强度适用于所使用的加密方法。开放的公共网络示例包括但不限于：互联网无线技术，包括802.11和蓝牙蜂窝技术，例如全球移动通信系统（GSM）、码分多址（CDMA）通用分组无线业务（GPRS）卫星通信	css-cluster-https-required	开启HTTPS访问后，访问集群将进行通讯加密。关闭HTTPS访问后，会使用HTTP协议与集群通信，无法保证数据安全性，并且无法开启公网访问功能。
4.1	使用强大的加密和安全协议来保护通过开放公共网络传输的敏感持卡人数据，包括：仅接受受信任的密钥和证书。使用的协议仅支持安全版本或配置。加密强度适用于所使用的加密方法。开放的公共网络示例包括但不限于：互联网无线技术，包括802.11和蓝牙蜂窝技术，例如全球移动通信系统（GSM）、码分多址（CDMA）通用分组无线业务（GPRS）卫星通信	dws-enable-ssl	确保数据仓库服务需要SSL加密才能连接到数据库客户端。由于敏感数据可能存在，因此在传输过程中启用加密以帮助保护该数据。

建议项编号	建议项说明	合规规则	指导说明
4.1	使用强大的加密和安全协议来保护通过开放公共网络传输的敏感持卡人数据，包括：仅接受受信任的密钥和证书。使用的协议仅支持安全版本或配置。加密强度适用于所使用的加密方法。开放的公共网络示例包括但不限于：互联网无线技术，包括802.11和蓝牙蜂窝技术，例如全球移动通信系统（GSM）、码分多址（CDMA）通用分组无线业务（GPRS）卫星通信	elb-tls-https-listeners-only	确保弹性负载均衡的监听器已配置HTTPS监听协议。由于可能存在敏感数据，因此启用传输中加密有助于保护该数据。
4.1	使用强大的加密和安全协议来保护通过开放公共网络传输的敏感持卡人数据，包括：仅接受受信任的密钥和证书。使用的协议仅支持安全版本或配置。加密强度适用于所使用的加密方法。开放的公共网络示例包括但不限于：互联网无线技术，包括802.11和蓝牙蜂窝技术，例如全球移动通信系统（GSM）、码分多址（CDMA）通用分组无线业务（GPRS）卫星通信	pca-certificate-authority-expiration-check	华为云云证书管理服务提供有PCA服务，可以帮助您通过简单的可视化操作，以低投入的方式创建企业内部CA并使用它签发证书。确保用户明确该私有CA的过期时间。此规则需要daysToExpiration（默认值14）。实际值应反映组织的策略。

建议项编号	建议项说明	合规规则	指导说明
4.1	使用强大的加密和安全协议来保护通过开放公共网络传输的敏感持卡人数据，包括：仅接受受信任的密钥和证书。使用的协议仅支持安全版本或配置。加密强度适用于所使用的加密方法。开放的公共网络示例包括但不限于：互联网无线技术，包括802.11和蓝牙蜂窝技术，例如全球移动通信系统（GSM）、码分多址（CDMA）通用分组无线业务（GPRS）卫星通信	pca-certificate-expiration-check	PCA是一个私有CA和私有证书管理平台。它让用户可以通过简单的可视化操作，建立用户自己完整的CA层次体系并使用它签发证书。确保用户明确该私有证书的过期时间。此规则需要daysToExpiration（默认值14）。实际值应反映组织的策略。
6.2	通过安装供应商提供的适用安全补丁，确保所有系统组件和软件免受已知漏洞的影响。在发布后一个月内安装关键安全补丁。注意：应根据要求6.1中定义的风险排序过程来识别关键安全补丁。	cce-cluster-end-of-maintenance-version	确保CCE集群版本为处于维护中的版本。
6.2	通过安装供应商提供的适用安全补丁，确保所有系统组件和软件免受已知漏洞的影响。在发布后一个月内安装关键安全补丁。注意：应根据要求6.1中定义的风险排序过程来识别关键安全补丁。	cce-cluster-oldest-supported-version	系统会自动为您的华为云CCE任务部署安全更新和补丁。如果发现影响华为云CCE平台版本的安全问题，华为云会修补该平台版本。要帮助对运行华为云cluster的华为云CCE任务进行补丁管理，请更新您服务的独立任务以使用最新的平台版本。
10.1	实施审计跟踪，将对系统组件的所有访问链接到每个用户。	apig-instances-execution-logging-enabled	确保为APIG专享版实例配置访问日志。APIG支持日志自定义分析模板，便于日志的统一收集和管理，也可通过API异常调用分析进行追查和溯源。

建议项编号	建议项说明	合规规则	指导说明
10.1	实施审计跟踪，将对系统组件的所有访问链接到每个用户。	cts-obs-bucket-track	确保存在至少一个CTS追踪器追踪指定的OBS桶。
10.1	实施审计跟踪，将对系统组件的所有访问链接到每个用户。	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务（CTS）用于记录华为云管理控制台操作。
10.1	实施审计跟踪，将对系统组件的所有访问链接到每个用户。	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。
10.1	实施审计跟踪，将对系统组件的所有访问链接到每个用户。	vpc-flow-logs-enabled	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。
10.5	保护审计跟踪，使其无法更改。	cts-kms-encrypted-check	确保云审计服务（CTS）的追踪器已配置KMS加密存储用于归档的审计事件。
11.5	部署更改检测机制（例如，文件完整性监控工具），以提醒人员注意对关键系统文件、配置文件或内容文件的未经授权的修改（包括更改、添加和删除）;并将软件配置为至少每周执行一次关键文件比较。	cts-support-validate-check	确保云审计服务（CTS）追踪器已打开事件文件校验，已避免日志文件存储后被修改、删除。

建议项编号	建议项说明	合规规则	指导说明
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	css-cluster-in-vpc	确保云搜索服务（CSS）位于虚拟私有云（VPC）中。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	css-cluster-in-vpc	确保云搜索服务（CSS）位于虚拟私有云（VPC）中。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	drs-data-guard-job-not-public	确保DRS实时灾备任务不能公开访问。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	drs-migration-job-not-public	确保DRS实时迁移任务不能公开访问。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	drs-synchronization-job-not-public	确保DRS实时同步任务不能公开访问。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	ecs-instance-in-vpc	确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	ecs-instance-no-public-ip	由于华为云ECS实例可能包含敏感信息，确保华为云ECS实例无法公开访问来管理对华为云的访问。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	function-graph-inside-vpc	确保函数工作流（FunctionGraph）的所有流量都安全地位于虚拟私有云（VPC）中。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	function-graph-public-access-prohibited	确保函数工作流的函数不能公开访问，管理对华为云中资源的访问。公开访问可能导致资源可用性下降。

建议项编号	建议项说明	合规规则	指导说明
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	mrs-cluster-no-public-ip	确保MapReduce服务（MRS）无法公网访问。华为云MRS集群主节点可能包含敏感信息，并且此类账号需要访问控制。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	rds-instance-no-public-ip	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账号需要原则和访问控制。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	vpc-default-sg-closed	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	vpc-sg-ports-check	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	vpc-sg-restricted-common-ports	在华为云VPC安全组上限制通用端口的IP地址，确保对安全组内资源实例的访问。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	vpc-sg-restricted-ssh	当外部任意IP可以访问安全组内云服务器的SSH（24）端口时认为不合规，确保对服务器的远程访问安全性。
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	css-cluster-in-vpc	确保云搜索服务（CSS）位于虚拟私有云（VPC）中。
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	css-cluster-in-vpc	确保云搜索服务（CSS）位于虚拟私有云（VPC）中。

建议项编号	建议项说明	合规规则	指导说明
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	drs-data-guard-job-not-public	确保DRS实时灾备任务不能公开访问。
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	drs-migration-job-not-public	确保DRS实时迁移任务不能公开访问。
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	drs-synchronization-job-not-public	确保DRS实时同步任务不能公开访问。
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	ecs-instance-in-vpc	确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	ecs-instance-no-public-ip	由于华为云ECS实例可能包含敏感信息，确保华为云ECS实例无法公开访问来管理对华为云的访问。
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	function-graph-inside-vpc	确保函数工作流（FunctionGraph）的所有流量都安全地位于虚拟私有云（VPC）中。
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	function-graph-public-access-prohibited	确保函数工作流的函数不能公开访问，管理对华为云中资源的访问。公开访问可能导致资源可用性下降。
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	mrs-cluster-no-public-ip	确保MapReduce服务（MRS）无法公网访问。华为云MRS集群主节点可能包含敏感信息，并且此类账号需要访问控制。

建议项编号	建议项说明	合规规则	指导说明
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	rds-instance-no-public-ip	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账号需要原则和访问控制。
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	vpc-default-sg-closed	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	vpc-sg-ports-check	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	vpc-sg-restricted-common-ports	在华为云VPC安全组上限制通用端口的IP地址，确保对安全组内资源实例的访问。
1.3.1	实施DMZ以将入站流量限制为仅提供授权的可公开访问的服务、协议和端口的系统组件。	vpc-sg-restricted-ssh	当外部任意IP可以访问安全组内云服务器的SSH（25）端口时认为不合规，确保对服务器的远程访问安全性。
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	css-cluster-in-vpc	确保云搜索服务（CSS）位于虚拟私有云（VPC）中。
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	css-cluster-in-vpc	确保云搜索服务（CSS）位于虚拟私有云（VPC）中。
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	drs-data-guard-job-not-public	确保DRS实时灾备任务不能公开访问。
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	drs-migration-job-not-public	确保DRS实时迁移任务不能公开访问。
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	drs-synchronization-job-not-public	确保DRS实时同步任务不能公开访问。

建议项编号	建议项说明	合规规则	指导说明
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	ecs-instance-in-vpc	确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	ecs-instance-no-public-ip	由于华为云ECS实例可能包含敏感信息，确保华为云ECS实例无法公开访问来管理对华为云的访问。
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	function-graph-inside-vpc	确保函数工作流（FunctionGraph）的所有流量都安全地位于虚拟私有云（VPC）中。
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	function-graph-public-access-prohibited	确保函数工作流的函数不能公开访问，管理对华为云中资源的访问。公开访问可能导致资源可用性下降。
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	mrs-cluster-no-public-ip	确保MapReduce服务（MRS）无法公网访问。华为云MRS集群主节点可能包含敏感信息，并且此类账号需要访问控制。
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	rds-instance-no-public-ip	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账号需要原则和访问控制。
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	vpc-default-sg-closed	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	vpc-sg-ports-check	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。

建议项编号	建议项说明	合规规则	指导说明
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	vpc-sg-restricted-common-ports	在华为云VPC安全组上限制通用端口的IP地址，确保对安全组内资源实例的访问。
1.3.2	将入站Internet流量限制为DMZ内的IP地址。	vpc-sg-restricted-ssh	当外部任意IP可以访问安全组内云服务器的SSH（26）端口时认为不合规，确保对服务器的远程访问安全性。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	css-cluster-in-vpc	确保云搜索服务（CSS）位于虚拟私有云（VPC）中。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	css-cluster-in-vpc	确保云搜索服务（CSS）位于虚拟私有云（VPC）中。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	drs-data-guard-job-not-public	确保DRS实时灾备任务不能公开访问。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	drs-migration-job-not-public	确保DRS实时迁移任务不能公开访问。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	drs-synchronization-job-not-public	确保DRS实时同步任务不能公开访问。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	ecs-instance-in-vpc	确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	ecs-instance-no-public-ip	由于华为云ECS实例可能包含敏感信息，确保华为云ECS实例无法公开访问来管理对华为云的访问。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	function-graph-inside-vpc	确保函数工作流（FunctionGraph）的所有流量都安全地位于虚拟私有云（VPC）中。

建议项编号	建议项说明	合规规则	指导说明
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	function-graph-public-access-prohibited	确保函数工作流的函数不能公开访问，管理对华为云中资源的访问。公开访问可能导致资源可用性下降。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	mrs-cluster-no-public-ip	确保MapReduce服务（MRS）无法公网访问。华为云MRS集群主节点可能包含敏感信息，并且此类账号需要访问控制。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	rds-instance-no-public-ip	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账号需要原则和访问控制。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	vpc-default-sg-closed	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	vpc-sg-ports-check	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	vpc-sg-restricted-common-ports	在华为云VPC安全组上限制通用端口的IP地址，确保对安全组内资源实例的访问。
1.3.4	不允许未经授权的出站流量从持卡人数据环境到Internet。	vpc-sg-restricted-ssh	当外部任意IP可以访问安全组内云服务器的SSH（27）端口时认为不合规，确保对服务器的远程访问安全性。
1.3.6	将存储持卡人数据（如数据库）的系统组件放置在内部网络区域中，与DMZ和其他不受信任的网络隔离。	css-cluster-in-vpc	确保云搜索服务（CSS）位于虚拟私有云（VPC）中。

建议项编号	建议项说明	合规规则	指导说明
1.3.6	将存储持卡人数据（如数据库）的系统组件放置在内部网络区域中，与DMZ和其他不受信任的网络隔离。	css-cluster-in-vpc	确保云搜索服务（CSS）位于虚拟私有云（VPC）中。
1.3.6	将存储持卡人数据（如数据库）的系统组件放置在内部网络区域中，与DMZ和其他不受信任的网络隔离。	drs-data-guard-job-not-public	确保DRS实时灾备任务不能公开访问。
1.3.6	将存储持卡人数据（如数据库）的系统组件放置在内部网络区域中，与DMZ和其他不受信任的网络隔离。	drs-migration-job-not-public	确保DRS实时迁移任务不能公开访问。
1.3.6	将存储持卡人数据（如数据库）的系统组件放置在内部网络区域中，与DMZ和其他不受信任的网络隔离。	drs-synchronization-job-not-public	确保DRS实时同步任务不能公开访问。
1.3.6	将存储持卡人数据（如数据库）的系统组件放置在内部网络区域中，与DMZ和其他不受信任的网络隔离。	ecs-instance-in-vpc	确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。
1.3.6	将存储持卡人数据（如数据库）的系统组件放置在内部网络区域中，与DMZ和其他不受信任的网络隔离。	ecs-instance-no-public-ip	由于华为云ECS实例可能包含敏感信息，确保华为云ECS实例无法公开访问来管理对华为云的访问。
1.3.6	将存储持卡人数据（如数据库）的系统组件放置在内部网络区域中，与DMZ和其他不受信任的网络隔离。	rds-instance-no-public-ip	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账号需要原则和访问控制。
1.3.6	将存储持卡人数据（如数据库）的系统组件放置在内部网络区域中，与DMZ和其他不受信任的网络隔离。	vpc-default-sg-closed	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。

建议项编号	建议项说明	合规规则	指导说明
1.3.6	将存储持卡人数据（如数据库）的系统组件放置在内部网络区域中，与DMZ和其他不受信任的网络隔离。	vpc-sg-ports-check	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。
1.3.6	将存储持卡人数据（如数据库）的系统组件放置在内部网络区域中，与DMZ和其他不受信任的网络隔离。	vpc-sg-restricted-common-ports	在华为云VPC安全组上限制通用端口的IP地址，确保对安全组内资源实例的访问。
1.3.6	将存储持卡人数据（如数据库）的系统组件放置在内部网络区域中，与DMZ和其他不受信任的网络隔离。	vpc-sg-restricted-ssh	当外部任意IP可以访问安全组内云服务器的SSH（28）端口时认为不合规，确保对服务器的远程访问安全性。
10.2.1	对所有系统组件实施自动审计跟踪，以重建以下事件：所有个人用户访问持卡人数据	apig-instances-execution-logging-enabled	确保为APIG专享版实例配置访问日志。APIG支持日志自定义分析模板，便于日志的统一收集和管理，也可通过API异常调用分析进行追查和溯源。
10.2.1	对所有系统组件实施自动审计跟踪，以重建以下事件：所有个人用户访问持卡人数据	cts-obs-bucket-track	确保存在至少一个CTS追踪器追踪指定的OBS桶。
10.2.1	对所有系统组件实施自动审计跟踪，以重建以下事件：所有个人用户访问持卡人数据	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务（CTS）用于记录华为云管理控制台操作。
10.2.1	对所有系统组件实施自动审计跟踪，以重建以下事件：所有个人用户访问持卡人数据	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。

建议项编号	建议项说明	合规规则	指导说明
10.2.2	对所有系统组件实施自动审计跟踪，以重建以下事件：任何具有root或管理权限的个人执行的所有操作	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务（CTS）用于记录华为云管理控制台操作。
10.2.2	对所有系统组件实施自动审计跟踪，以重建以下事件：任何具有root或管理权限的个人执行的所有操作	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。
10.2.3	为所有系统组件实施自动审计跟踪，以重建以下事件：访问所有审计跟踪	cts-obs-bucket-track	确保存在至少一个CTS追踪器追踪指定的OBS桶。
10.2.3	为所有系统组件实施自动审计跟踪，以重建以下事件：访问所有审计跟踪	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务（CTS）用于记录华为云管理控制台操作。
10.2.3	为所有系统组件实施自动审计跟踪，以重建以下事件：访问所有审计跟踪	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。

建议项编号	建议项说明	合规规则	指导说明
10.2.4	对所有系统组件实施自动审计跟踪，以重建以下事件：无效的逻辑访问尝试	apig-instances-execution-logging-enabled	确保为APIG专享版实例配置访问日志。APIG支持日志自定义分析模板，便于日志的统一收集和管理，也可通过API异常调用分析进行追查和溯源。
10.2.4	对所有系统组件实施自动审计跟踪，以重建以下事件：无效的逻辑访问尝试	cts-obs-bucket-track	确保存在至少一个CTS追踪器追踪指定的OBS桶。
10.2.4	对所有系统组件实施自动审计跟踪，以重建以下事件：无效的逻辑访问尝试	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务（CTS）用于记录华为云管理控制台操作。
10.2.4	对所有系统组件实施自动审计跟踪，以重建以下事件：无效的逻辑访问尝试	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。
10.2.5	对所有系统组件实施自动审计跟踪，以重建以下事件：识别和身份验证机制的使用和更改（包括但不限于创建新账号和提升权限），以及对具有根权限或管理权限的账号的所有更改、添加或删除	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务（CTS）用于记录华为云管理控制台操作。

建议项编号	建议项说明	合规规则	指导说明
10.2.5	对所有系统组件实施自动审计跟踪，以重建以下事件：识别和身份验证机制的使用和更改（包括但不限于创建新账号和提升权限），以及对具有根权限或管理权限的账号的所有更改、添加或删除	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。
10.2.6	对所有系统组件实施自动审计跟踪，以重建以下事件：初始化、停止或暂停审核日志	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务（CTS）用于记录华为云管理控制台操作。
10.2.6	对所有系统组件实施自动审计跟踪，以重建以下事件：初始化、停止或暂停审核日志	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。
10.2.7	对所有系统组件实施自动审计跟踪，以重建以下事件：创建和删除系统级对象	apig-instances-execution-logging-enabled	确保为APIG专享版实例配置访问日志。APIG支持日志自定义分析模板，便于日志的统一收集和管理，也可通过API异常调用分析进行追查和溯源。
10.2.7	对所有系统组件实施自动审计跟踪，以重建以下事件：创建和删除系统级对象	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务（CTS）用于记录华为云管理控制台操作。

建议项编号	建议项说明	合规规则	指导说明
10.2.7	对所有系统组件实施自动审计跟踪，以重建以下事件：创建和删除系统级对象	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。
10.3.1	对于每个事件，至少记录所有系统组件的以下审计跟踪条目：用户识别	apig-instances-execution-logging-enabled	确保为APIG专享版实例配置访问日志。APIG支持日志自定义分析模板，便于日志的统一收集和管理，也可通过API异常调用分析进行追查和溯源。
10.3.1	对于每个事件，至少记录所有系统组件的以下审计跟踪条目：用户识别	cts-obs-bucket-track	确保存在至少一个CTS追踪器追踪指定的OBS桶。
10.3.1	对于每个事件，至少记录所有系统组件的以下审计跟踪条目：用户识别	cts-tracker-exists	确保账号已经创建了CTS追踪器，云审计服务（CTS）用于记录华为云管理控制台操作。
10.3.1	对于每个事件，至少记录所有系统组件的以下审计跟踪条目：用户识别	multi-region-cts-tracker-exists	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。

建议项编号	建议项说明	合规规则	指导说明
10.3.1	对于每个事件，至少记录所有系统组件的以下审计跟踪条目：用户识别	vpc-flow-logs-enabled	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。
10.5.2	保护审计跟踪文件免遭未经授权的修改。	cts-kms-encrypted-check	确保云审计服务（CTS）的追踪器已配置KMS加密存储用于归档的审计事件。
10.5.3	及时将审计跟踪文件备份到难以更改的集中式日志服务器或介质。	cts-lts-enable	确保使用云日志服务（LTS）集中收集云审计服务（CTS）的数据。
10.5.5	对日志使用文件完整性监视或更改检测软件，以确保在不生成警报的情况下无法更改现有日志数据（尽管添加新数据不应引起警报）。	cts-support-validate-check	确保云审计服务（CTS）追踪器已打开事件文件校验，已避免日志文件存储后被修改、删除。
2.2.2	仅启用系统功能所需的必要服务、协议、守护程序等。	drs-data-guard-job-not-public	确保DRS实时灾备任务不能公开访问。
2.2.2	仅启用系统功能所需的必要服务、协议、守护程序等。	drs-migration-job-not-public	确保DRS实时迁移任务不能公开访问。
2.2.2	仅启用系统功能所需的必要服务、协议、守护程序等。	drs-synchronization-job-not-public	确保DRS实时同步任务不能公开访问。
2.2.2	仅启用系统功能所需的必要服务、协议、守护程序等。	ecs-instance-in-vpc	确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。
2.2.2	仅启用系统功能所需的必要服务、协议、守护程序等。	ecs-instance-no-public-ip	由于华为云ECS实例可能包含敏感信息，确保华为云ECS实例无法公开访问来管理对华为云的访问。

建议项编号	建议项说明	合规规则	指导说明
2.2.2	仅启用系统功能所需的必要服务、协议、守护程序等。	function-graph-inside-vpc	确保函数工作流（FunctionGraph）的所有流量都安全地位于虚拟私有云（VPC）中。
2.2.2	仅启用系统功能所需的必要服务、协议、守护程序等。	function-graph-public-access-prohibited	确保函数工作流的函数不能公开访问，管理对华为云中资源的访问。公开访问可能导致资源可用性下降。
2.2.2	仅启用系统功能所需的必要服务、协议、守护程序等。	mrs-cluster-no-public-ip	确保MapReduce服务（MRS）无法公网访问。华为云MRS集群主节点可能包含敏感信息，并且此类账号需要访问控制。
2.2.2	仅启用系统功能所需的必要服务、协议、守护程序等。	rds-instance-no-public-ip	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账号需要原则和访问控制。
2.2.2	仅启用系统功能所需的必要服务、协议、守护程序等。	vpc-default-sg-closed	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。
2.2.2	仅启用系统功能所需的必要服务、协议、守护程序等。	vpc-sg-ports-check	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。
2.2.2	仅启用系统功能所需的必要服务、协议、守护程序等。	vpc-sg-restricted-common-ports	在华为云VPC安全组上限制通用端口的IP地址，确保对安全组内资源实例的访问。
2.2.2	仅启用系统功能所需的必要服务、协议、守护程序等。	vpc-sg-restricted-ssh	当外部任意IP可以访问安全组内云服务器的SSH（29）端口时认为不合规，确保对服务器的远程访问安全性。

建议项编号	建议项说明	合规规则	指导说明
3.5.2	将对加密密钥的访问限制为所需的最少保管人数量。	iam-customer-policy-blocked-kms-actions	帮助您将最小权限和职责分离的原则与访问权限和授权结合起来，限制策略在数据加密服务上包含阻止的操作。拥有超过完成任务所需的特权可能违反最小特权和职责分离的原则。
3.6.4	已达到其加密期结束的密钥的加密密钥更改（例如，在定义的时间段过去后和/或给定密钥生成一定数量的密文之后），由关联的应用程序供应商或密钥所有者定义，并基于行业最佳实践和准则（例如，NIST特别出版物800-57）。	kms-rotation-enabled	确保数据加密服务（KMS）密钥启用密钥轮换。
3.6.5	当密钥的完整性被削弱（例如，知道明文密钥组件的员工离职）或怀疑密钥被泄露时，必要时停用或替换密钥（例如，存档、销毁和/或吊销）。注意：如果需要保留已停用或替换的加密密钥，则必须安全地存档这些密钥（例如，使用密钥加密密钥）。存档的加密密钥只能用于解密/验证目的。	kms-not-scheduled-for-deletion	确保数据加密服务（KMS）密钥未处于“计划删除“状态，以防止误删除密钥。
3.6.7	防止未经授权替换加密密钥。	kms-not-scheduled-for-deletion	确保数据加密服务（KMS）密钥未处于“计划删除“状态，以防止误删除密钥。
7.1.1	定义每个角色的访问需求，包括：每个角色需要访问其工作职能的系统组件和数据资源访问资源所需的权限级别（例如，用户、管理员等）。	iam-customer-policy-blocked-kms-actions	帮助您将最小权限和职责分离的原则与访问权限和授权结合起来，限制策略在数据加密服务上包含阻止的操作。拥有超过完成任务所需的特权可能违反最小特权和职责分离的原则。

建议项编号	建议项说明	合规规则	指导说明
7.1.1	定义每个角色的访问需求，包括：每个角色需要访问其工作职能的系统组件和数据资源访问资源所需的权限级别（例如，用户、管理员等）。	iam-group-has-users-check	确保IAM组至少有一个用户，帮助您将最小权限和职责分离的原则与访问权限和授权结合起来。
7.1.1	定义每个角色的访问需求，包括：每个角色需要访问其工作职能的系统组件和数据资源访问资源所需的权限级别（例如，用户、管理员等）。	iam-policy-no-statements-with-admin-access	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。
7.1.1	定义每个角色的访问需求，包括：每个角色需要访问其工作职能的系统组件和数据资源访问资源所需的权限级别（例如，用户、管理员等）。	iam-role-has-all-permissions	确保IAM操作仅限于所需的操作。允许用户拥有比完成任务所需的更多权限可能会违反最小权限和职责分离原则。
7.1.1	定义每个角色的访问需求，包括：每个角色需要访问其工作职能的系统组件和数据资源访问资源所需的权限级别（例如，用户、管理员等）。	iam-root-access-key-check	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。
7.1.1	定义每个角色的访问需求，包括：每个角色需要访问其工作职能的系统组件和数据资源访问资源所需的权限级别（例如，用户、管理员等）。	iam-user-group-membership-check	确保用户至少是一个组的成员，帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最小权限和职责分离的原则。
7.1.1	定义每个角色的访问需求，包括：每个角色需要访问其工作职能的系统组件和数据资源访问资源所需的权限级别（例如，用户、管理员等）。	mrs-cluster-kerberos-enabled	通过为华为云MRS集群启用Kerberos，可以按照最小权限和职责分离的原则来管理和合并访问权限和授权。

建议项编号	建议项说明	合规规则	指导说明
7.1.2	将对特权用户ID的访问限制为执行工作职责所需的最低权限。	iam-customer-policy-blocked-kms-actions	帮助您将最小权限和职责分离的原则与访问权限和授权结合起来，限制策略在数据加密服务上包含阻止的操作。拥有超过完成任务所需的特权可能违反最小特权和职责分离的原则。
7.1.2	将对特权用户ID的访问限制为执行工作职责所需的最低权限。	iam-group-has-users-check	确保IAM组至少有一个用户，帮助您将最小权限和职责分离的原则与访问权限和授权结合起来。
7.1.2	将对特权用户ID的访问限制为执行工作职责所需的最低权限。	iam-policy-no-statements-with-admin-access	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。
7.1.2	将对特权用户ID的访问限制为执行工作职责所需的最低权限。	iam-role-has-all-permissions	确保IAM操作仅限于所需的操作。允许用户拥有比完成任务所需的更多权限可能会违反最小权限和职责分离原则。
7.1.2	将对特权用户ID的访问限制为执行工作职责所需的最低权限。	iam-root-access-key-check	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。
7.1.2	将对特权用户ID的访问限制为执行工作职责所需的最低权限。	iam-user-group-membership-check	确保用户至少是一个组的成员，帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最小权限和职责分离的原则。
7.2.1	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：覆盖所有系统组件	iam-customer-policy-blocked-kms-actions	帮助您将最小权限和职责分离的原则与访问权限和授权结合起来，限制策略在数据加密服务上包含阻止的操作。拥有超过完成任务所需的特权可能违反最小特权和职责分离的原则。

建议项编号	建议项说明	合规规则	指导说明
7.2.1	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：覆盖所有系统组件	iam-group-has-users-check	确保IAM组至少有一个用户，帮助您将最小权限和职责分离的原则与访问权限和授权结合起来。
7.2.1	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：覆盖所有系统组件	iam-policy-no-statements-with-admin-access	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。
7.2.1	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：覆盖所有系统组件	iam-role-has-all-permissions	确保IAM操作仅限于所需的操作。允许用户拥有比完成任务所需的更多权限可能会违反最小权限和职责分离原则。
7.2.1	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：覆盖所有系统组件	iam-root-access-key-check	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。
7.2.1	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：覆盖所有系统组件	iam-user-group-membership-check	确保用户至少是一个组的成员，帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最小权限和职责分离的原则。
7.2.1	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：覆盖所有系统组件	mrs-cluster-kerberos-enabled	通过为华为云MRS集群启用Kerberos，可以按照最小权限和职责分离的原则来管理和合并访问权限和授权。

建议项编号	建议项说明	合规规则	指导说明
7.2.2	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：根据工作分类和职能向个人分配权限。	iam-customer-policy-blocked-kms-actions	帮助您将最小权限和职责分离的原则与访问权限和授权结合起来，限制策略在数据加密服务上包含阻止的操作。拥有超过完成任务所需的特权可能违反最小特权和职责分离的原则。
7.2.2	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：根据工作分类和职能向个人分配权限。	iam-group-has-users-check	确保IAM组至少有一个用户，帮助您将最小权限和职责分离的原则与访问权限和授权结合起来。
7.2.2	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：根据工作分类和职能向个人分配权限。	iam-policy-no-statements-with-admin-access	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。
7.2.2	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：根据工作分类和职能向个人分配权限。	iam-role-has-all-permissions	确保IAM操作仅限于所需的操作。允许用户拥有比完成任务所需的更多权限可能会违反最小权限和职责分离原则。
7.2.2	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：根据工作分类和职能向个人分配权限。	iam-root-access-key-check	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。

建议项编号	建议项说明	合规规则	指导说明
7.2.2	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：根据工作分类和职能向个人分配权限。	iam-user-group-membership-check	确保用户至少是一个组的成员，帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最小权限和职责分离的原则。
7.2.2	为系统组件建立访问控制系统，该系统根据用户的需要限制访问，除非特别允许，否则设置为“全部拒绝”。此门禁系统必须包括以下内容：根据工作分类和职能向个人分配权限。	mrs-cluster-kerberos-enabled	通过为华为云MRS集群启用Kerberos，可以按照最小权限和职责分离的原则来管理和合并访问权限和授权。
8.1.1	在允许所有用户访问系统组件或持卡人数据之前，为所有用户分配一个唯一的ID。	iam-root-access-key-check	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。
8.1.4	在90天内删除/禁用非活动用户账号。	access-keys-rotated	确保根据组织策略轮换IAM访问密钥，这缩短了访问密钥处于活动状态的时间，并在密钥被泄露时减少业务影响。
8.2.1	使用强加密技术，使所有身份验证凭据（如密码/短语）在所有系统组件的传输和存储过程中不可读。	apig-instances-ssl-enabled	确保使用SSL证书配置华为云API Gateway REST API阶段，以允许后端系统对来自API Gateway的请求进行身份验证。
8.2.1	使用强加密技术，使所有身份验证凭据（如密码/短语）在所有系统组件的传输和存储过程中不可读。	elb-tls-https-listeners-only	确保弹性负载均衡的监听器已配置HTTPS监听协议。由于可能存在敏感数据，因此启用传输中加密有助于保护该数据。

建议项编号	建议项说明	合规规则	指导说明
8.2.1	使用强加密技术，使所有身份验证凭据（如密码/短语）在所有系统组件的传输和存储过程中不可读。	rds-instances-enable-kms	为了帮助保护静态数据，请确保为您的华为云RDS实例启用加密。由于敏感数据可以静态存在于华为云RDS实例中，因此启用静态加密有助于保护该数据。
8.2.1	使用强加密技术，使所有身份验证凭据（如密码/短语）在所有系统组件的传输和存储过程中不可读。	sfsturbo-encrypted-check	由于敏感数据可能存在并帮助保护静态数据，确保弹性文件服务（SFSTurbo）已通过KMS进行加密。
8.2.1	使用强加密技术，使所有身份验证凭据（如密码/短语）在所有系统组件的传输和存储过程中不可读。	volumes-encrypted-check	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。
8.2.3	密码/密码必须满足以下条件：要求最小长度至少为7个字符。包含数字和字母字符。或者，密码/密码短语的复杂性和强度必须至少与上述指定的参数相当。	iam-password-policy	确保IAM用户密码强度满足密码强度要求。
8.2.4	至少每90天更改一次用户密码/密码。	access-keys-rotated	确保根据组织策略轮换IAM访问密钥，这缩短了访问密钥处于活动状态的时间，并在密钥被泄露时减少业务影响。
8.2.4	至少每90天更改一次用户密码/密码。	access-keys-rotated	确保根据组织策略轮换IAM访问密钥，这缩短了访问密钥处于活动状态的时间，并在密钥被泄露时减少业务影响。
8.2.4	至少每90天更改一次用户密码/密码。	iam-password-policy	确保IAM用户密码强度满足密码强度要求。
8.2.5	不要允许个人提交与他或她使用的最后四个密码/密码中的任何一个相同的新密码/密码。	iam-password-policy	确保IAM用户密码强度满足密码强度要求。

建议项编号	建议项说明	合规规则	指导说明
8.3.1	将所有非控制台访问的多重身份验证合并到CDE中，供具有管理访问权限的人员使用。	iam-user-mfa-enabled	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账号被盗用的事件。
8.3.1	将所有非控制台访问的多重身份验证合并到CDE中，供具有管理访问权限的人员使用。	mfa-enabled-for-iam-console-access	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行MFA，您可以减少账号被盗用的事件，并防止敏感数据被未经授权的用户访问。
8.3.1	将所有非控制台访问的多重身份验证合并到CDE中，供具有管理访问权限的人员使用。	root-account-mfa-enabled	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA为登录凭据添加了额外的保护。
8.3.2	对来自实体网络外部的所有远程网络访问（包括用户和管理员，包括用于支持或维护的第三方访问）进行多重身份验证。	iam-user-mfa-enabled	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账号被盗用的事件。
8.3.2	对来自实体网络外部的所有远程网络访问（包括用户和管理员，包括用于支持或维护的第三方访问）进行多重身份验证。	mfa-enabled-for-iam-console-access	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行MFA，您可以减少账号被盗用的事件，并防止敏感数据被未经授权的用户访问。

建议项编号	建议项说明	合规规则	指导说明
8.3.2	对来自实体网络外部的所有远程网络访问（包括用户和管理员，包括用于支持或维护的第三方访问）进行多重身份验证。	root-account-mfa-enabled	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA为登录凭据添加了额外的保护。

4.5.25 适用于医疗行业的合规实践

该示例模板中对应的合规规则的说明和修复项指导如下表所示：

表 4-29 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	确保为APIG专享版实例配置访问日志。APIG支持日志自定义分析模板，便于日志的统一收集和管理，也可通过API异常调用分析进行追查和溯源。	APIG专享版实例未配置访问日志，视为“不合规”	可以在API网关控制台选择启动日志记录

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
apig-instances-ssl-enabled	APIG专享版实例域名均关联SSL证书	apig	如果API分组中的API支持HTTPS请求协议，则在绑定独立域名后，还需为独立域名添加SSL证书。SSL证书是进行数据传输加密和身份证明的证书，支持单向认证和双向认证两种认证方式。	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”。	用户可以为不合规的APIG专享版实例下的域名绑定SSL证书。
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	根据ELB对云服务器的健康检查结果进行的检查，健康检查会将异常的实例从伸缩组中移除。这条规则确保与负载均衡器关联的伸缩组使用了弹性负载均衡健康检查。	与负载均衡器关联的伸缩组未使用弹性负载均衡健康检查，视为“不合规”	如果您将多个负载均衡器添加到伸缩组，则只有在所有负载均衡器均检测到云服务器状态为正常的情况下，才会认为该弹性云服务器正常。否则只要有一个负载均衡器检测到云服务器状态异常，伸缩组会将该弹性云服务器移出伸缩组。
css-cluster-disk-encryption-check	CSS集群开启磁盘加密	css	确保CSS集群开启磁盘加密。由于敏感数据可能存在，请在传输中启用加密以帮助保护该数据。	CSS集群未开启磁盘加密，视为“不合规”	建议对磁盘进行加密。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
css-cluster-https-required	CSS集群启用HTTPS	css	开启HTTPS访问后，访问集群将进行通讯加密。关闭HTTPS访问后，会使用HTTP协议与集群通信，无法保证数据安全性，并且无法开启公网访问功能。	CSS集群未启用https，视为“不合规”	仅安全模式的集群支持开启HTTPS访问。启用HTTPS访问的安全集群可以单击“下载证书”获取CER安全证书，用于接入安全模式的集群。安全证书暂不支持在公网环境下使用。
css-cluster-in-vpc	CSS集群绑定指定VPC资源	css	云搜索服务CSS的集群创建在虚拟私有云（VPC）的子网内，VPC通过逻辑方式进行网络隔离，为用户的集群提供安全、隔离的网络环境。此规则确保云搜索服务（CSS）位于虚拟私有云（VPC）中。	CSS集群未与指定的vpc资源绑定，视为“不合规”	可以将不合规的CSS集群与指定vpc关联。
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	确保云审计服务（CTS）的追踪器已配置KMS加密存储用于归档的审计事件。	CTS追踪器未通过KMS进行加密，视为“不合规”	建议您配置独立OBS桶并配置KMS加密存储专门用于归档审计事件。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-lts-enable	CTS追踪器启用事件分析	cts	确保使用云日志服务（LTS）集中收集云审计服务（CTS）的数据。	CTS追踪器未启用事件分析，视为“不合规”	开通云审计日志后，系统会自动创建一个名为system的管理事件追踪器，并将当前租户的所有操作记录在该追踪器中。在追踪器中配置CTS转储到LTS，配置完成后会在LTS自动创建日志组日志流
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	由于CTS只支持查询7天的审计事件，为了您事后审计、查询、分析等要求，启用CTS追踪器请配置OBS服务桶。	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”	云审计服务管理控制台支持配置已开启的追踪器的OBS桶、LTS转储和配置已创建的追踪器关键事件操作通知。
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	在安全和事故调查中，通常由于事件文件被删除或者被私下篡改，而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您确保事件文件的真实性。	CTS追踪器未打开事件文件校验，视为“不合规”	在配置转储页面打开“文件校验”开关，即可开启事件文件完整性校验功能。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
cts-tracker-exists	创建并启用CTS追踪器	cts	云审计服务支持创建数据类事件追踪器，用于记录数据操作日志。数据类追踪器用于记录数据事件，即针对租户对OBS桶中的数据的操作日志，例如上传、下载等。	账号未创建CTS追踪器，视为“不合规”	可进入云审计服务页面，导航栏选择“追踪器”，单击“创建追踪器”，根据提示操作。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
drs-data-guard-job-not-public	数据复制服务实时灾备任务不使用公网网络	drs	为了解决地区故障导致的业务不可用，数据复制服务推出灾备场景，为用户业务连续性提供数据库的同步保障。当主实例所在区域发生突发生自然灾害等状况无法连接时，可将异地灾备实例切换为主实例，在应用端修改数据库链接地址后，即可快速恢复应用的业务访问。数据复制服务提供的实时灾备功能，可实现主实例和跨区域的灾备实例之间的实时同步。此规则确保DRS实时灾备任务不能公开访问。	数据复制服务实时灾备任务使用公网网络，视为“不合规”	对于不合规的DRS资源，您可以切换非公网访问

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
drs-migration-job-not-public	数据复制服务实时迁移任务不使用公网网络	drs	实时迁移是指在数据复制服务能够同时连通源数据库和目标数据库的情况下，只需要配置迁移的源、目标数据库实例及迁移对象即可完成整个数据迁移过程，再通过多项指标和数据的对比分析，帮助确定合适的业务割接时机，实现最小化业务中断的数据库迁移。确保DRS实时迁移任务不能公开访问。	数据复制服务实时迁移任务使用公网网络，视为“不合规”	对于不合规的DRS资源，您可以切换非公网访问。
drs-synchronization-job-not-public	数据复制服务实时同步任务不使用公网网络	drs	实时同步是指在不同的系统之间，将数据通过同步技术从一个数据源拷贝到其他数据库，并保持一致，实现关键业务的数据实时流动。确保DRS实时同步任务不能公开访问。确保DRS实时同步任务不能公开访问。	数据复制服务实时同步任务使用公网网络，视为“不合规”	对于不合规的DRS资源，您可以切换非公网访问。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
dws-enable-log-dump	DWS集群启用日志转储	dws	GaussDB(DWS) 记录您的数据库中的连接和用户活动相关信息。这些审计日志信息有助于您监控数据库以确保安全或进行故障排除或定位历史操作记录。当前这些审计日志默认存储于数据库中，您可以将审计日志转储到OBS中使负责监控数据库中活动的用户更方便的查看这些日志信息。	DWS集群未启用日志转储，视为“不合规”	GaussDB(DWS) 集群创建成功后，您可以为集群开启审计日志转储，将审计日志转储到OBS中，方便查看。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
dws-enable-snapshot	DWS集群启用自动快照	dws	自动快照采用差异增量备份,当创建集群时，自动快照默认处于启用状态。当集群启用了自动快照时，GaussDB(DWS) 将按照设定的时间和周期以及快照类型自动创建快照，默认为每8小时一次。用户也可以对集群设置自动快照策略，并根据自身需求，对集群设置一个或多个自动快照策略。	DWS集群未启用自动快照，视为“不合规”	用户可以进入集群的详情页面，单击“快照”，在“策略列表”中打开自动快照的开关。
dws-enable-ssl	DWS集群启用SSL加密连接	dws	SSL连接方式的安全性高于普通模式，集群默认开启SSL功能允许来自客户端的SSL连接或非SSL连接，从安全性考虑，建议用户在客户端使用SSL连接方式。并且GaussDB(DWS)服务器端的证书、私钥以及根证书已经默认配置完成。	DWS集群未启用SSL加密连接，视为“不合规”	用户可以在集群的安全设置中打开SSL连接的开关。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs，vpc	虚拟私有云（VPC）为弹性云服务器构建了一个逻辑上完全隔离的专有区域，您可以在自己的逻辑隔离区域中定义虚拟网络，为弹性云服务器构建一个逻辑上完全隔离的专有区域，确保弹性云服务器（ECS）所有流量都安全地保留在虚拟私有云（VPC）中。	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”	您可以通过网络配置，为不合规的ECS资源选择特定的虚拟私有云。
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	由于华为云ecs实例可能包含敏感信息，确保华为云ecs实例无法公开访问来管理对华为云的访问。	ECS资源具有公网IP，视为“不合规”	您可以登录弹性云服务器页面，在弹性云服务器列表中，在待调整带宽的弹性云服务器操作列下，单击“操作”列下的“更多 > 网络设置 > 解绑弹性公网IP”，将不合规的ecs资源解除弹性公网绑定。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
eip-unbound-check	弹性公网IP未进行任何绑定	vpc	弹性公网IP（EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。此规则确保弹性公网IP未闲置。	弹性公网IP未进行任何绑定，视为“不合规”	用户可以通过申请弹性公网IP并将弹性公网IP绑定到特定的资源上。
eip-use-in-specified-days	EIP在指定天数内绑定到资源实例	eip	弹性公网IP（EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。此规则确保弹性公网IP未闲置。	EIP创建指定天数内未使用，视为“不合规”	用户可以通过申请弹性公网IP并将弹性公网IP绑定到特定的资源上。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
elb-predefined-security-policy-https-check	ELB监听器配置指定预定义安全策略	elb	对于银行，金融类加密传输的应用，在创建和配置HTTPS监听器时，您可以选择使用安全策略，可以提高您的业务安全性。安全策略包含TLS协议版本和配套的加密算法套件。	独享型负载均衡器关联的HTTPS协议类型监听器未配置指定的预定义安全策略，视为“不合规“	独享型负载均衡支持选择默认安全策略或创建自定义策略。您可以为HTTPS监听器选择指定的预定义安全策略。
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	确保弹性负载均衡的监听器均已配置HTTPS监听协议。HTTPS协议适用于需要加密传输的应用。由于可能存在敏感数据，因此启用传输中加密有助于保护该数据。	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”	您可以添加一个HTTPS监听转发来自HTTPS协议的请求。独享型负载均衡前端协议为“HTTPS”时，后端协议可以选择“HTTP”或“HTTPS”。共享型负载均衡前端协议为“HTTPS”时，后端协议默认为“HTTP”，且不支持修改。如果您的独享型负载均衡实例类型为网络型（TCP/UDP），则无法创建HTTPS监听器。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
function-graph-public-access-prohibited	函数工作流的函数不允许访问公网	fgs	确保函数工作流的函数不能公开访问，管理对华为云中资源的访问。公开访问可能导致资源可用性下降。	函数工作流的函数允许访问公网，视为“不合规”	部署在VPC中的函数默认是和外网隔离开的，用户可以将函数绑定VPC，并且不添加公网NAT网关。
gaussdb-nosql-enable-backup	GaussDB NoSQL开启备份	gaussdb nosql	确保GaussDB NoSQL开启备份。GeminiDB Mongo实例支持自动备份和手动备份两种方案。GeminiDB Mongo支持数据库实例的备份，以保证数据可靠性。实例删除后，手动备份数据保留。自动备份的数据和实例一起释放，备份的数据不支持下载导出。	GaussDB NoSQL未开启备份，视为“不合规”	您可以在管理控制台设置自动备份策略，系统将会按照自动备份策略中设置的备份时间段和备份周期进行自动备份，并且会按照设置的备份保留天数对备份文件进行存放。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
gaussdb-nosql-enable-disk-encryption	GaussDB NoSQL使用磁盘加密	gaussdb nosql	确保GaussDB NoSQL启用KMS磁盘加密。当启用加密功能，用户创建数据库实例成功后，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，用于提高数据安全性，但对数据库读写性能有少量影响。	GaussDB NoSQL未使用磁盘加密，视为“不合规”	您可以根据业务需要选择是否进行磁盘加密。
iam-customer-policy-blocked-kms-actions	IAM策略中不存在KMS的任一阻拦action	iam	帮助您将最小权限和职责分离的原则与访问权限和授权结合起来，限制策略在数据加密服务上包含阻止的操作。拥有超过完成任务所需的特权可能违反最小特权和职责分离的原则。	IAM策略存在允许的任一KMS阻拦的action，视为“不合规”	用户可以根据合规评估结果修改策略配置。
iam-password-policy	IAM用户密码策略符合要求	iam	确保IAM用户密码强度满足密码强度要求。	IAM用户密码强度不满足密码强度要求，视为“不合规”	用户可以根据提示修改密码达到需要的密码强度。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
iam-policy-no-statements-with-admin-access	IAM策略不具备Admin权限	iam	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。	IAM策略admin权限(*:*:*或*:*或*)，视为“不合规”	管理员可以在IAM页面修改不合规的IAM用户的权限。
iam-role-has-all-permissions	IAM自定义策略具备所有权限	iam	确保IAM用户操作仅限于所需的操作。允许用户拥有超过完成任务所需的权限可能违反最小权限和职责分离原则。	IAM自定义策略具有allow的*:*权限，视为“不合规”	管理员可以在IAM页面修改不合规的IAM用户的权限。
iam-root-access-key-check	IAM账号存在可使用的访问密钥	iam	确保根访问密钥已删除。	账号存在可使用的访问密钥，视为“不合规”	用户可以根据规则评估结果删除账号可使用的访问密钥。
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	管理员创建IAM用户后，这个新建的IAM用户可以登录华为云。避免IAM用户资源闲置。	IAM用户在指定时间范围内无登录行为，视为“不合规”	您可以在华为云登录页面或者打开IAM用户专属链接，输入用户名和密码的方式登录IAM用户。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
iam-user-mfa-enabled	IAM用户开启MFA	iam	确保为所有IAM用户通过MFA方式进行多因素认证。MFA在用户名和密码的基础上增加了一层额外的保护，通过要求对用户进行MFA来减少账户被盗用的事件。	IAM用户未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。
kms-not-scheduled-for-deletion	KMS密钥不处于“计划删除”状态	kms	确保数据加密服务（KMS）密钥未处于“计划删除“状态，以防止误删除密钥。	KMS密钥处于“计划删除“状态，视为“不合规”	用户可以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。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	确保为所有能通过控制台登录的IAM用户启用多因素认证（MFA），管理对华为云中资源的访问。MFA在用户名和密码的基础上增加了一层额外的保护。通过要求对用户进行 MFA，您可以减少账户被盗用的事件，并防止敏感数据被未经授权的用户访问。	通过Console密码登录的IAM用户未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。
mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS 1.8.0版本之前未开启Kerberos认证的集群不支持访问权限细分。只有开启Kerberos认证才有角色管理权限，MRS 1.8.0及之后版本的所有集群均拥有角色管理权限。	MRS集群未开启kerberos认证，视为“不合规”	MRS服务暂不支持集群创建完成后手动开启和关闭Kerberos服务，如需更换Kerberos认证状态，建议重新创建MRS集群，然后进行数据迁移。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
mrs-cluster-no-public-ip	MRS集群未绑定公网IP	mrs	确保MapReduce服务（MRS）无法公网访问。华为云MRS集群主节点可能包含敏感信息，并且此类账户需要访问控制。	MRS集群绑定公网IP，视为“不合规”	对于不合规的MRS资源，用户可以解除其与弹性公网IP的绑定。
multi-region-cts-tracker-exists	在指定区域创建并启用CTS追踪器	cts	云审计服务CTS提供对各种云资源操作记录的收集、存储和查询功能。首次开通云审计服务时，系统会自动为您创建一个名为system的管理追踪器。公有云的数据中心分布在全球不同区域，通过在指定区域开通云审计服务，可以将应用程序的设计更贴近特定客户的需求，或满足特定地区的法律或其他要求。数据追踪器会记录当前区域租户对OBS桶中的数据操作的详细信息。	账号未在指定region列表创建CTS追踪器，视为“不合规”	您可以进入指定区域云审计服务页面，导航栏选择“追踪器”，单击“创建追踪器”，根据提示操作。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
pca-certificate-authority-expiration-check	检查私有CA是否过期	pca	华为云云证书管理服务提供有PCA服务，可以帮助您通过简单的可视化操作，以低投入的方式创建企业内部CA并使用它签发证书。确保用户明确该私有CA的过期时间。此规则需要daysToExpiration（默认值14）。实际值应反映组织的策略。	私有CA没有标记在指定时间内到期，视为“不合规”	用户可以进入私有CA管理界面，根据需要设置CA的有效期。
pca-certificate-expiration-check	检查私有证书是否过期	pca	PCA是一个私有CA和私有证书管理平台。它让用户可以通过简单的可视化操作，建立用户自己完整的CA层次体系并使用它签发证书。确保用户明确该私有证书的过期时间。此规则需要daysToExpiration（默认值14）。实际值应反映组织的策略。	私有证书没有标记在指定时间内到期，视为“不合规”	通过云证书管理控制台创建并激活私有CA后，您就可以通过私有CA申请私有证书，在选择签发CA的过程中，您可以自定义私有证书有效期，该有效期不得超过当前已激活私有CA的有效期。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
private-nat-gateway-authorized-vpc-only	NAT私网网关绑定指定VPC资源	nat	确保NAT私网网关仅连接到授权的虚拟私有云（VPC）中，管理对华为云中资源的访问。	NAT私网网关未与指定的VPC资源绑定，视为“不合规”	用户可以修改NAT私网网关关联的子网。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-enable-backup	RDS实例开启备份	rds	RDS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，自动备份为全量备份。系统根据您指定的备份保留期保存数据库实例的自动备份。如果需要，您可以将数据恢复到备份保留期中的任意时间点。开启自动备份策略后，会自动触发一次全量备份，备份方式为物理备份。之后会按照策略中的备份时间段和备份周期进行全量备份。自动备份策略开启后，实例每五分钟会自动进行一次增量备份，以保证数据库可靠性。确保云数据库（rds）资源开启备份。	未开启备份的RDS资源，视为“不合规”	用户可根据需要修改备份策略。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-multi-az-support	RDS实例支持多可用区	rds	华为云RDS中的多可用区支持为数据库实例提供了增强的可用性和持久性。当您预置多可用区数据库实例时，华为云RDS会自动创建主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用区都在其物理上不同的独立基础设施上运行，并且经过精心设计，高度可靠。如果发生基础设施故障，华为云 RDS 会自动故障转移到备用数据库，以便您可以在故障转移完成后立即恢复数据库操作。	RDS实例仅支持一个可用区，视为“不合规”	华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
rds-instance-no-public-ip	RDS实例不具有公网IP	rds	确保云数据库（RDS）无法公网访问，管理对华为云中资源的访问。华为云RDS数据库实例可能包含敏感信息，此类账户需要原则和访问控制。	RDS资源具有公网IP，视为“不合规”	对于不合规的RDS资源，用户可以解除其与弹性公网IP的绑定。
rds-instances-enable-kms	RDS实例开启存储加密	rds	云数据库RDS for MySQL实例已开通密钥管理服务（Key Management Service，KMS），加密使用的用户主密钥由KMS产生和管理，RDS不提供加密所需的密钥和证书。由于敏感数据可以静态存在于华为云RDS实例中，因此启用静态加密有助于保护该数据。	未开启存储加密的RDS资源，视为“不合规”	如需开通透明数据加密，您可以在管理控制台右上角，选择“工单 > 新建工单”，提交开通透明数据加密的申请。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
root-account-mfa-enabled	根账号开启MFA认证	iam	确保为root用户启用多因素认证（MFA），管理对华为云中资源的访问。多因素认证Multi-Factor Authentication（MFA）是一种非常简单的安全实践方法，它能够在用户名称和密码之外再额外增加一层保护。启用多因素认证后，用户进行操作时，除了需要提供用户名和密码外（第一次身份验证），还需要提供验证码（第二次身份验证），多因素身份认证结合起来将为您的账号和资源提供更高的安全保护。	根账号未开启MFA认证，视为“不合规”	您需要在智能设备上安装一个虚拟MFA应用程序后（例如：华为云App、Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。
sfsturbo-encrypted-check	弹性文件服务通过KMS进行加密	sfsturbo	由于敏感数据可能存在并帮助保护静态数据，确保弹性文件服务(SFS Turbo)已通过KMS进行加密。	弹性文件服务(SFS Turbo)未通过KMS进行加密，视为“不合规”	可以新创建加密或者不加密的文件系统，无法更改已有文件系统的加密属性。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	启用此规则可根据您组织的标准检查华为云ecs实例的停止时间是否超过允许的天数，确保弹性云服务器（ECS）未闲置。	关机状态的ECS未进行任意操作的时间超过了允许的天数，视为“不合规”	包年/包月资源一次性付费，到期自动停止使用。其他计费模式下关机后仍然计费。如需停止计费，请删除实例。
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs，evs	由于敏感数据可能存在，为了帮助保护静态数据，确保已挂载的云硬盘已进行加密。	已挂载的云硬盘未进行加密，视为“不合规”	当您需要使用云硬盘加密功能时，需要授权EVS访问KMS。如果您拥有“Security Administrator”权限，则可直接授权。如果权限不足，需先联系拥有“Security Administrator”权限的用户授权EVS访问KMS，然后再重新操作。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
vpc-acl-unused-check	未与子网关联的网络ACL	vpc	网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的网络流量。此规则可确保现存网络ACL均与子网关联，实现对子网的防护。	检查是否存在未使用的网络ACL,如果网络ACL没有与子网关联，视为“不合规”	您可以将网络ACL关联至VPC子网，为子网内的资源提供安全防护。
vpc-default-sg-closed	默认安全组关闭出、入方向流量	vpc	确保虚拟私有云安全组能有效帮助管理网络访问，限制默认安全组上的所有流量有助于限制对华为云资源的远程访问。	虚拟私有云的默认安全组允许入方向或出方向流量，视为“不合规”	用户可以在不合规的安全组详情页面，修改出方向和入方向规则。
vpc-flow-logs-enabled	VPC启用流日志	vpc	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。	检查是否为VPC启用了流日志，如果该VPC未启用流日志，视为“不合规”	您可以为不合规的VPC资源开启流日志记录，方式为：创建日志组、日志流之后，进入VPC流日志列表页面创建VPC流日志，按照提示配置参数。

合规规则	规则中文名称	涉及云服务	说明指导	规则描述	修复项指导
vpc-sg-ports-check	安全组端口检查	vpc	确保虚拟私有云安全组上的端口受到限制，管理对华为云中资源的访问。	当安全组入方向源地址设置为0.0.0.0/0，且开放了所有的TCP/UDP端口时，视为“不合规”	用户可以修改不合规的安全组的规则。
vpc-sg-restricted-common-ports	安全组入站流量限制指定端口	vpc	在华为云vpc安全组上限制通用端口的ip地址，确保对安全组内资源实例的访问。	当安全组的入站流量不限制指定端口的所有ipv4地址(0.0.0.0/0)，视为“不合规”	用户可以修改安全组的规则中端口和地址的值。
vpc-sg-restricted-ssh	安全组入站流量限制SSH端口	vpc	当外部任意IP可以访问安全组内云服务器的SSH(22)端口时认为不合规，确保对服务器的远程访问安全性。	当安全组入方向源地址设置为0.0.0.0/0，且开放TCP 22端口，视为“不合规”	用户可以在不合规的安全组详情页面，修改出方向和入方向规则。
vpn-connections-active	VPN连接状态为“正常”	vpnaas	确保VPN连接状态正常。	VPN连接状态不为“正常”，视为“不合规”	VPN连接状态显示为“未连接”的可能原因有：VPN连接两端的连接配置不正确、华为云安全组和客户设备侧ACL配置不正确。可以检查VPN连接两端的连接配置和检查华为云安全组和客户设备侧ACL配置。

5 高级查询

5.1 高级查询概述

配置审计服务提供高级查询能力，通过使用ResourceQL自定义查询用户当前的单个或多个区域的资源配置状态。

高级查询支持用户自定义查询和浏览云服务资源，用户可以通过ResourceQL在查询编辑器中编辑和查询。

ResourceQL是结构化的查询语言(SQL) SELECT语法的一部分，它可以对当前资源数据执行基于属性的查询和聚合。查询的复杂程度不同，既可以是简单的标签或资源标识符匹配，也可以是更复杂的查询，例如查看指定具体OS版本的云服务器。

您可以使用高级查询来实现：

- 库存管理。例如检索特定规格的云服务器实例的列表。
- 安全合规检查。例如检索已启用或禁用特定配置属性（公网IP，加密磁盘）的资源的列表。
- 成本优化。例如检索未挂载到任何云服务器实例的云磁盘的列表，避免产生不必要的费用。

说明

高级查询仅支持用户自定义查询、浏览、导出云服务资源，如果要对资源进行修改、删除等管理类的操作，请前往资源所属的服务页面进行操作。

5.2 高级查询使用限制

为避免单用户长时间查询占用资源，影响其他用户，对高级查询功能做以下限制：

- 单次查询语句的执行时长不能超过15秒，否则会返回超时错误。
- 单次查询语句查询大量数据，会返回查询数据量过大的报错，需要用户主动简化查询语句。
- 单次查询结果只返回前4000条。
- 单个查询语句中最多只能做两次表的关联查询。
- 每个账号最多可以创建200个高级查询。

须知

高级查询功能依赖于资源记录器所收集的资源数据，强烈建议您保持资源记录器的开启状态，不同场景的说明如下：

- 如您从未开启过资源记录器，则高级查询语句无法查询到任何资源数据。
- 如您已开启资源记录器，但仅在资源记录器监控范围内勾选部分资源，则高级查询语句仅能查询到所选择的资源数据。
- 如您开启资源记录器并勾选全部资源，但后续又关闭资源记录器，则高级查询语句仅能查询到资源记录器由开启到关闭期间收集到的资源数据。

关于如何开启并配置资源记录器请参见：**配置资源记录器**。

5.3 新建查询

操作场景

您可以使用Config预设的查询语句，或根据资源配置属性自定义查询语句，查询具体的云资源配置。

本章节包含如下内容：

- **新建查询**
- **另存查询**
- **高级查询配置样例**

新建查询

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“高级查询”，进入“高级查询”页面。

步骤4 选择“自定义查询”页签，单击页面右上角的“新建查询”。

步骤5 根据界面提示，在查询编辑器中输入查询语句。

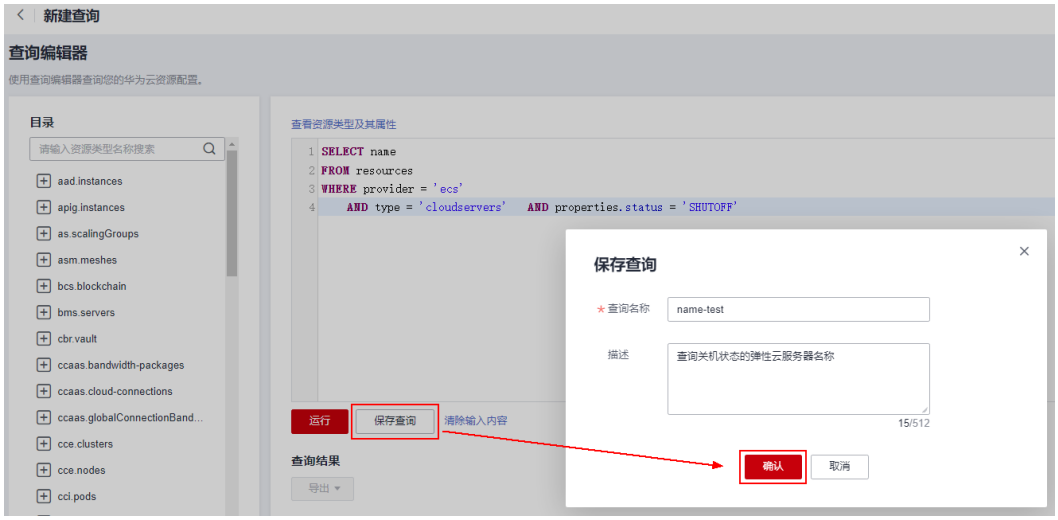
页面左侧为高级查询使用的Schema信息，也就是查询语句中properties参数需要填写的内容，为各个云服务资源类型的详细属性。查询语句的配置样例请参见**高级查询配置样例**。

步骤6 单击“保存查询”，输入查询名称和描述。

查询名称仅支持输入数字、英文字母、下划线和中划线。

步骤7 单击“确定”，保存成功。

图 5-1 保存查询



说明

如果您的自定义查询达到限额，将无法单击“保存查询”，同时页面右上方提示“您创建的查询已达到上限，请删除暂不需要使用的查询。”。

当自定义查询达到限额，您可以运行查询条件，并导出查询结果。

步骤8 单击“运行”，查看查询结果。目前只支持展示和导出前4000条查询结果。

步骤9 单击“导出”，选择要导出的文件格式（CSV格式或JSON格式）。

----结束

另存查询

您可以修改预设查询或已有自定义查询的名称、描述和查询语句，“另存为”后产生新的查询，以“预设查询”为例，您可按如下步骤操作。

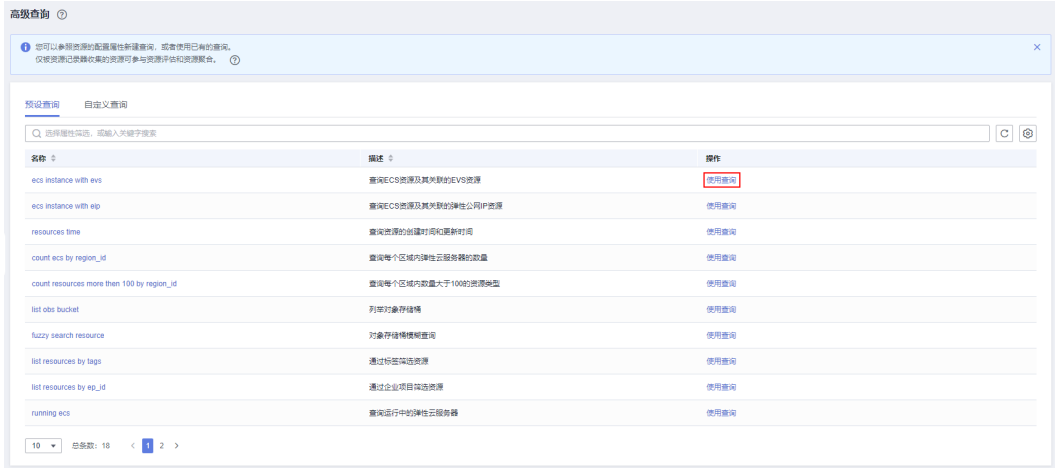
步骤1 进入“高级查询”页面，选择“预设查询”页签。

“高级查询”页面默认展示预设查询列表。

步骤2 单击目标查询操作列的“使用查询”，进入“使用查询”页面。

也可以单击查询名称，进入查询概览页，再单击查询概览页右下方的“使用查询”，进入“使用查询”页面。

图 5-2 使用预设查询



步骤3 根据界面提示，在查询编辑器中修改查询语句。

详细请参见**高级查询配置样例**。

步骤4 单击“另存为”，配置查询名称和描述。

步骤5 在弹框中，单击“确定”。

说明

通过“另存为”操作产生的新查询，将更新在自定义查询列表中。

----结束

高级查询配置样例

ResourceQL使用结构化查询语言(SQL) SELECT语法的子集来对当前云资源配置数据进行查询和关联查询。用户无需调用特定API来实现，也无需通过多个API下载全量数据并手动分析。ResourceQL仅支持从表resources中查询数据。

表 5-1 resources 参数含义

资源参数	参数类型	含义
id	String	资源ID
name	String	资源名称
provider	String	云服务名称
type	String	资源类型
region_id	String	区域ID
project_id	String	项目ID
ep_id	String	企业项目ID
checksum	String	资源详情校验码
created	Date	资源创建时间

资源参数	参数类型	含义
updated	Date	资源更新时间
provisioning_state	String	资源操作状态
tag	Array(Map<String,String>)	资源Tag
properties	Map<String,Object>	资源详细属性

用例参考如下：

- 示例1：查询关机状态的弹性云服务器名称

```
SELECT name
FROM resources
WHERE provider = 'ecs'
    AND type = 'cloudservers'
    AND properties.status = 'SHUTOFF'
```

- 示例2：查询特定规格的云硬盘

```
SELECT *
FROM resources
WHERE provider = 'evs'
    AND type = 'volumes'
    AND properties.size = 100
```

- 示例3：对象存储桶模糊查询

```
SELECT *
FROM resources
WHERE provider = 'obs'
    AND 'type' = 'buckets'
    AND name LIKE '%figure%'
```

- 示例4：查询ECS资源及其关联的EVS资源

```
SELECT ECS_EVS.id AS ecs_id, EVS.id AS evs_id
FROM (
    SELECT id, evs_id
    FROM (
    SELECT id, transform(properties.ExtVolumesAttached, x -> x.id) AS evs_list
    FROM resources
    WHERE provider = 'ecs'
        AND type = 'cloudservers'
    ) ECS
      CROSS JOIN UNNEST(evs_list) AS t (evs_id)
) ECS_EVS, (
    SELECT id
    FROM resources
    WHERE provider = 'evs'
        AND type = 'volumes'
    ) EVS
WHERE ECS_EVS.evs_id = EVS.id
```

- 示例5：查询ECS资源名称及其关联的弹性公网IP地址

```
SELECT ECS.id AS ECS_id, publicIpAddress AS ip_address
FROM (
    SELECT id, transform(properties.addresses, x -> x.addr) AS ip_list
    FROM resources
    WHERE provider = 'ecs'
        AND type = 'cloudservers'
) ECS, (
        SELECT name, properties.publicIpAddress
        FROM resources
        WHERE provider = 'vpc'
            AND type = 'publicips'
```

```
        AND properties.type = 'EIP'
        AND properties.status = 'ACTIVE'
  ) EIP
WHERE CONTAINS (ECS.ip_list, EIP.name)
```

- 示例6：查询每个区域内数量大于100的资源类型

```
WITH counts AS (
  SELECT region_id, provider, type, count(*) AS number
  FROM resources
  GROUP BY region_id, provider, type
)
SELECT *
FROM counts
WHERE number > 100
```

查询语句的详细介绍，请参见**ResourceQL语法**。

5.4 查看查询

操作场景

如果您需要查看某个查询的名称、描述和查询语句，可按如下操作查看查询。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“高级查询”，进入“高级查询”页面。

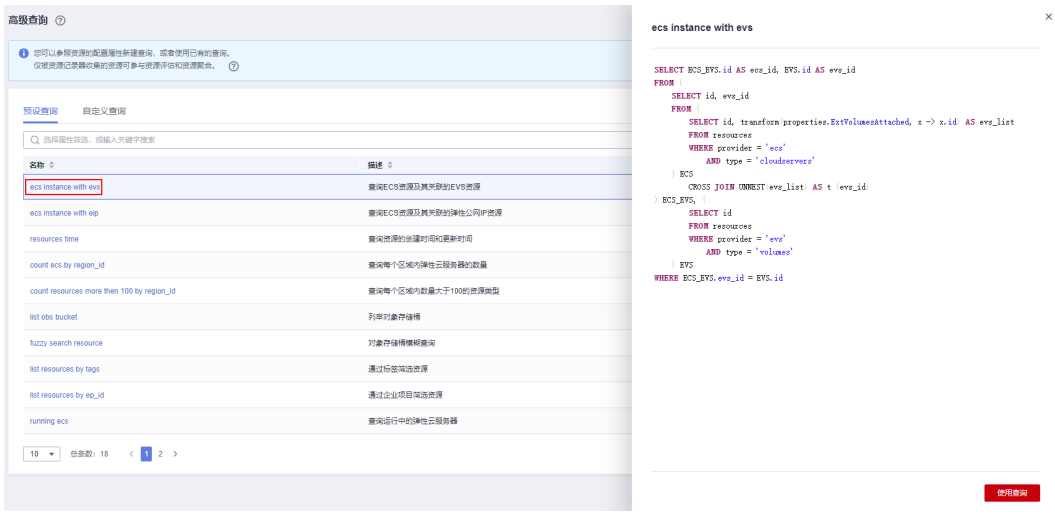
“高级查询”页面默认展示预设查询列表，您可以选择“自定义查询”页签，查看自定义查询列表。

在查询列表中可以查看查询的名称和描述等信息。

步骤4 单击需要查看的查询名称，进入查询概览页。

可以查看查询的具体SQL语句。

图 5-3 查看查询详情



----结束

5.5 修改查询

操作场景

如果您需要修改某个自定义查询的查询语句，可按如下操作修改查询。

说明

预设查询仅支持修改查询语句后，另存为新的自定义查询，不支持修改查询语句后的保存操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的☰图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

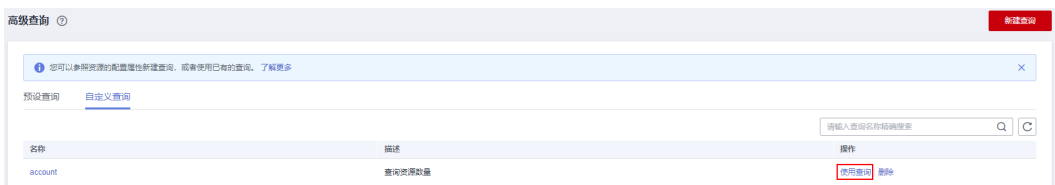
步骤3 单击页面左侧的“高级查询”，进入“高级查询”页面。

步骤4 选择“自定义查询”页签。

步骤5 在待修改查询所在行，单击操作列的“使用查询”，进入“使用查询”页面。

也可以单击查询名称，进入查询概览页，再单击查询概览页右下方的“使用查询”，进入“使用查询”页面。

图 5-4 修改自定义查询



步骤6 根据界面提示，在查询编辑器中修改查询语句。

详细请参见**高级查询配置样例**。

步骤7 查询语句修改完成后，单击“保存”。

步骤8 在弹出的确认框中可修改查询名称和描述，修改完成后，单击“确定”。

查询名称仅支持输入数字、英文字母、下划线和中划线。

----结束

5.6 删除查询

操作场景

如果您不需要使用某个自定义的查询，可按如下操作删除查询。

预设查询不支持删除操作。

操作步骤

步骤1 登录管理控制台。

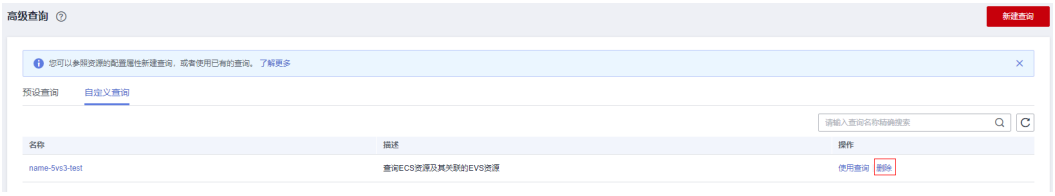
步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“高级查询”，进入“高级查询”页面。

步骤4 单击页面中的“自定义查询”，进入“自定义查询”页面。

步骤5 在待删除查询所在行，单击操作列的“删除”。

图 5-5 删除自定义查询



步骤6 在弹框中，单击“确定”。

----结束

6 资源聚合器

6.1 资源聚合器概述

功能概述

配置审计服务提供多账号资源数据聚合能力，通过使用资源聚合器聚合其他华为云账号或者组织成员账号的资源配置和合规性数据到单个账号中，方便统一查询。

资源聚合器提供只读视图，仅用于查看聚合的源账号的资源信息和合规性数据。资源聚合器不提供对源账号资源数据的修改访问权限。例如，无法通过资源聚合器部署规则，也无法通过资源聚合器从源账号提取快照文件。

说明

资源聚合器仅支持用户查询和浏览源账号中的云服务资源信息，如果要对资源进行修改、删除等管理类的操作，请前往资源所属的服务页面进行操作。

配置流程

使用资源聚合器从源账号收集资源数据，需要执行以下操作：

1. 创建资源聚合器用于从多个账号聚合资源配置和合规性数据，具体请参见**创建资源聚合器**。
2. 源账号开启资源记录器用于收集资源数据，具体请参见**配置资源记录器**。
3. 源账号授予聚合器账号收集资源配置和合规性数据的权限，具体请参见**授权资源聚合器账号**。
4. 在资源聚合器视图中查看源账号的资源配置和合规性数据，具体请参见**查看聚合的合规规则**和**查看聚合的资源**。

基本概念

源账号

源账号是配置审计服务需要聚合资源配置和合规性数据的账号。源账号可以是华为云账号或组织。

资源聚合器

资源聚合器是配置审计服务中的一种新的功能，可以从多个源账号收集资源配置和合规性数据。

聚合器账号

聚合账号是创建资源聚合器的账号。

授权

授权是指源账号向聚合器账号授予收集资源配置和合规性数据的权限。源类型为华为云账号的资源聚合器，必须获得源账号的授权才能聚合数据；源类型为组织的资源聚合器，则无需授权即可聚合整个组织中所有成员账号的数据。

6.2 资源聚合器使用限制

资源聚合器的使用限制如下：

- 单个账号最多能创建30个账号类型的资源聚合器。
- 单个资源聚合器最多能聚合30个源账号的数据。
- 单个账号类型资源聚合器每7天添加、更新和删除的最大源账号数量为1000个。
- 单个账号最多能创建1个组织类型的资源聚合器。
- 单个账号每天最多只能创建1次组织类型资源聚合器，当天创建的组织类型资源聚合器被删除后无法再次创建。
- 资源聚合器聚合的源账号必须开启资源记录器，资源聚合器才会动态收集源账号的资源配置，源账号的资源发生变更后会同步更新数据至资源聚合器。

须知

资源聚合器聚合的源账号只有开启资源记录器后，源账号的资源信息和合规性数据才会聚合到资源聚合器，不同场景的说明如下：

- 如源账号从未开启过资源记录器，则资源聚合器无法聚合此源账号的资源信息和合规性数据。
- 如源账号已开启资源记录器，但仅在资源记录器监控范围内勾选部分资源，则资源聚合器会聚合源账号所选择的资源信息以及全部合规性数据。
- 如源账号开启资源记录器并勾选全部资源，但后续又关闭资源记录器，则资源聚合器会删除收集到的资源信息和合规性数据。

关于如何开启并配置资源记录器请参见：**配置资源记录器**。

6.3 创建资源聚合器

操作场景

您可以创建账号类型或组织类型的资源聚合器。

账号类型的资源聚合器必须获得源账号的授权才能聚合数据，具体请参见**授权资源聚合器账号**。

说明

创建组织类型的资源聚合器依赖于组织服务的相关授权项，您需要具有如下权限：

- organizations:organizations:get
- organizations:accounts:list
- organizations:delegatedAdministrators:list
- organizations:trustedServices:enable
- organizations:trustedServices:list

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“资源聚合器”，在下拉列表中选择“聚合器”，进入“聚合器”页面。

步骤4 单击页面右上角的“创建聚合器”。

步骤5 在创建聚合器页面，先勾选“允许数据复制”确认框，然后配置聚合器名称和源账号信息。

如果源类型选择“添加账号”，则输入华为云账号ID，多个账号之间以逗号分隔；如果源类型选择“添加组织”，资源聚合器将直接聚合此组织下所有成员账号的数据，无需输入账号ID。

图 6-1 创建聚合器

说明

- 账号类型的资源聚合器仅支持聚合华为云账号下的资源，因此源账号ID需输入华为云账号ID（domain_id）。如何获取账号ID请参见**获取账号ID**。
- 创建组织类型资源聚合器的账号需开通组织服务，且必须为组织的管理账号或Config服务的委托管理员账号，具体请参见**添加、查看和取消委托管理员**。如果创建组织类型资源聚合器的账号为组织管理账号，Config服务会调用enableTrustedService接口启用Config与Organizations之间的集成；如果创建组织类型资源聚合器的账号为Config服务的委托管理员账号，Config服务会调用ListDelegatedAdministrators接口用于验证调用者是否为有效的委托管理员。

步骤6 单击“确定”，完成资源聚合器创建。

----结束

6.4 查看资源聚合器

操作场景

您可以通过资源聚合器列表查看所有已创建的资源聚合器及其详情，并支持在列表中进行搜索操作。

说明

查看组织资源聚合器聚合的资源信息和合规性数据依赖于组织服务的相关授权项，您需要具有如下权限：

- organizations:organizations:get
- organizations:delegatedAdministrators:list
- organizations:trustedServices:list

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的  图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“资源聚合器”，在下拉列表中选择“聚合器”，进入“聚合器”页面。

步骤4 在列表中可查看所有已创建的资源聚合器。

您可以通过页面右上方的过滤器搜索出需要查看的资源聚合器，支持根据完整的聚合器名称精确搜索。

步骤5 在列表中单击需要查看的聚合器名称，进入资源聚合器详情页，查看该资源聚合器的详细信息。

在详情页的“资源计数”列表中单击某个“资源类型”，界面将跳转至“资源”页面并自动筛选出此聚合器中某一资源类型包含的全部资源。

在详情页的“按资源计数排序的账号”列表单击某个“账号ID”，界面将跳转至“资源”页面并自动筛选出此聚合器中某一账号包含的全部资源。

在详情页的“不合规规则”列表单击某个“规则名称”，界面将显示此合规规则的详细信息。

图 6-2 资源聚合器详情页

----结束

6.5 修改资源聚合器

操作场景

资源聚合器创建完成后，您可以根据需要随时修改账号类型资源聚合器的名称和源账号，组织类型的资源聚合器仅支持修改聚合器名称。

如下步骤以修改账号类型的聚合器为例进行说明。

说明

修改组织类型的资源聚合器依赖于组织服务的相关授权项，您需要具有如下权限：

- organizations:organizations:get
- organizations:accounts:list
- organizations:delegatedAdministrators:list
- organizations:trustedServices:enable
- organizations:trustedServices:list

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“资源聚合器”，在下拉列表中选择“聚合器”，进入“聚合器”页面。

步骤4 在资源聚合器列表中选择需要修改的聚合器，单击“操作”列的“编辑”按钮。

在资源聚合器详情页中的右上角单击“编辑”按钮，也可以跳转至“编辑聚合器”页面进行修改操作。

图 6-3 修改资源聚合器

步骤5 进入“编辑聚合器”页面，修改聚合器名称和源账号。

步骤6 修改完成后，单击“确定”。

----结束

6.6 删除资源聚合器

操作场景

如果您不再需要某个资源聚合器时，可按如下步骤进行删除操作。

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的 图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“资源聚合器”，在下拉列表中选择“聚合器”，进入“聚合器”页面。

步骤4 在资源聚合器列表中选择需要删除的聚合器，单击“操作”列的“删除”按钮。

在资源聚合器详情页中的右上角单击“删除”按钮，也可以进行删除操作。

步骤5 在弹出的确认框中单击“确定”，完成资源聚合器的删除。

图 6-4 删除资源聚合器

----结束

6.7 查看聚合的合规规则

操作场景

您可以在规则列表中查看资源聚合器聚合的全部合规性数据。该列表可帮助您筛选不同资源聚合器聚合的合规性数据，且支持通过规则名称、合规评估结果和账号ID进一步筛选，还可以查看每个合规规则的详情。

说明

查看组织资源聚合器聚合的合规性数据依赖于组织服务的相关授权项，您需要具有如下权限：

- organizations:organizations:get
- organizations:delegatedAdministrators:list
- organizations:trustedServices:list

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

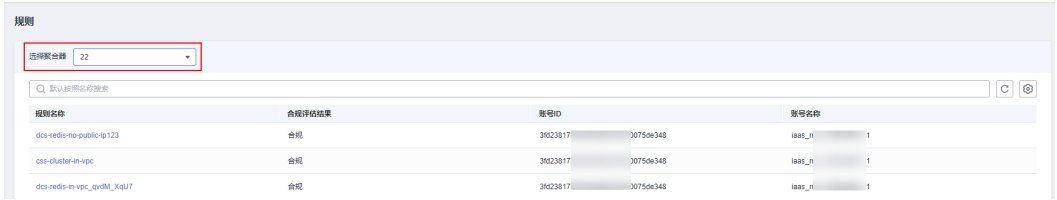
步骤3 单击页面左侧的“资源聚合器”，在下拉列表中选择“规则”，进入“规则”页面。

步骤4 在页面左上角选择需要查看的资源聚合器，列表中将展示此聚合器聚合的全部合规性数据。

在列表中单击需要查看的规则名称，即可查看此合规规则的详细信息。

在页面上方的搜索框中可使用规则名称、合规评估结果和账号ID，进一步对聚合的合规性数据进行筛选。

图 6-5 查看聚合的合规规则



----结束

6.8 查看聚合的资源

操作场景

您可以在资源列表中查看资源聚合器聚合的全部资源。该列表可帮助您筛选不同资源聚合器聚合的资源，且支持通过资源名称、账号ID和资源类型进一步筛选，还可以查看每个资源的详情。

说明

查看组织资源聚合器聚合的资源信息依赖于组织服务的相关授权项，您需要具有如下权限：

- organizations:organizations:get
- organizations:delegatedAdministrators:list
- organizations:trustedServices:list

操作步骤

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

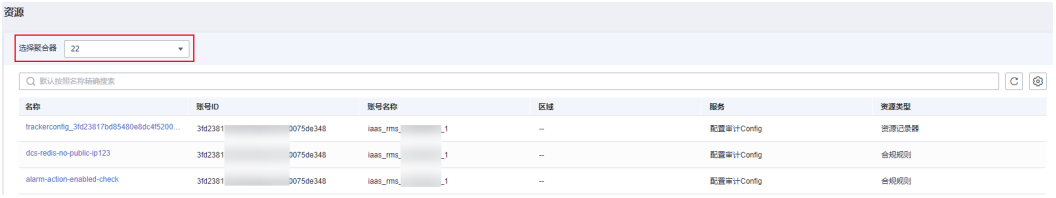
步骤3 单击页面左侧的“资源聚合器”，在下拉列表中选择“资源”，进入“资源”页面。

步骤4 在页面左上角选择需要查看的资源聚合器，列表中将展示此聚合器聚合的全部资源。

在页面上方的搜索框中可使用资源名称、账号ID和资源类型，进一步对聚合的资源进行筛选。

在资源列表中单击需要查看的资源名称，即可查看此资源的详细信息。

图 6-6 查看聚合的资源



----结束

6.9 授权资源聚合器账号

操作场景

当聚合器账号发起聚合请求时，需要源账号向聚合器账号授予收集资源配置和合规性数据的权限，资源聚合器才可以收集源账号的资源数据。授权和创建聚合器并无先后关系，先创建资源聚合器或先授权均可。

组织类型的聚合器无需授权，即可收集整个组织中所有成员账号的资源数据。

本章节将为您介绍如下内容：

- 添加授权
- 接受授权
- 删除授权

添加授权

您可以通过“添加授权”功能向聚合器账号授权，授权完成后，资源聚合器聚合您账号中的资源数据时，无需再次向您发送授权请求，即可聚合您账号中的资源数据。

步骤1 登录管理控制台。

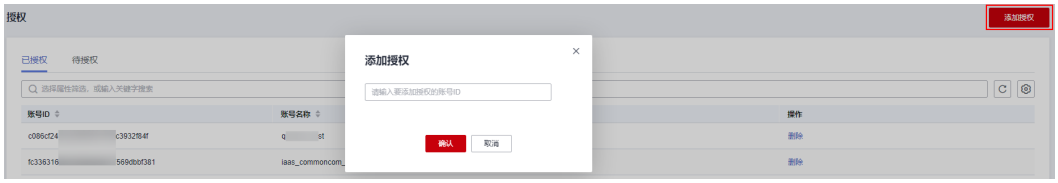
步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“资源聚合器”，在下拉列表中选择“授权”，进入“授权”页面。

步骤4 单击页面右上角的“添加授权”。

步骤5 在弹出的“添加授权”页面中，输入要添加授权的聚合器账号ID。

图 6-7 添加授权



步骤6 单击“确定”，完成授权。

授权完成后，“已授权”列表中将显示此授权记录。

----结束

接受授权

当资源聚合器需要聚合您账号中的资源数据时，您会在“待授权”页签收到聚合器账号发送的授权请求，确认授权后，资源聚合器才可以聚合您账号中的资源数据。

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“资源聚合器”，在下拉列表中选择“授权”，进入“授权”页面。

步骤4 选择“待授权”页签，在列表中选择待处理的授权请求，单击操作列的“授权”。

步骤5 在弹出的确认框中单击“确定”，完成授权。

接受授权请求后，此授权记录将在“已授权”列表中显示。

图 6-8 接受授权

----结束

删除授权

如需取消对某个资源聚合器账号的授权，您可以删除授权。

步骤1 登录管理控制台。

步骤2 单击页面左上角的 图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

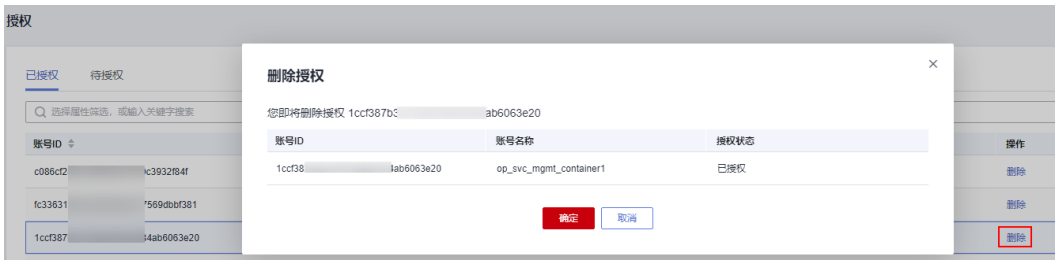
步骤3 单击页面左侧的“资源聚合器”，在下拉列表中选择“授权”，进入“授权”页面。

步骤4 选择“已授权”页签，在列表中选择待删除的授权请求，单击操作列的“删除”。

步骤5 在弹出的确认框中单击“确定”，此授权记录将移至“待授权”列表，授权状态变为“待授权”。

此时聚合器账号已无权聚合您账号中的资源数据，如需再次授权，您可以在“待授权”页签中单击此授权记录操作列的“授权”并确认，聚合器账号将再次获得您的授权。

图 6-9 删除授权



步骤6 如需彻底删除此授权记录，需在“待授权”列表中的操作列单击“删除”并确认，此授权记录彻底删除。

说明

在“待授权”列表中删除授权请求后，如需再次授权，请重新向聚合器账号授权，具体请参见**添加授权**。

----结束

6.10 高级查询

概述

资源聚合器提供高级查询能力，通过使用ResourceQL自定义查询单个或多个聚合源账号的资源配置状态。

高级查询支持用户自定义查询和浏览华为云云服务资源，用户可以通过ResourceQL在查询编辑器中编辑和查询。

您可以使用Config预设的查询语句，或根据资源配置属性自定义查询语句，查询具体的云资源配置。

ResourceQL是结构化的查询语言(SQL) SELECT语法的一部分，它可以对当前资源数据执行基于属性的查询和聚合。查询的复杂程度不同，既可以是简单的标签或资源标识符匹配，也可以是更复杂的查询，例如查看指定具体OS版本的云服务器。

说明

高级查询仅支持用户自定义查询、浏览、导出云服务资源，如果要对资源进行修改、删除等管理类的操作，请前往资源所属的服务页面进行操作。

使用限制

为避免单用户长时间查询占用资源，影响其他用户，对高级查询功能做以下限制：

- 单次查询语句的执行时长不能超过15秒，否则会返回超时错误。
- 单次查询语句查询大量数据，会返回查询数据量过大的报错，需要用户主动简化查询语句。
- 单次查询结果只返回前4000条。
- 单个查询语句中最多只能做两次表的关联查询。
- 每个账号最多可以创建200个高级查询。

须知

高级查询功能依赖于资源记录器所收集的资源数据，强烈建议您保持资源记录器的开启状态，不同场景的说明如下：

- 如您从未开启过资源记录器，则高级查询语句无法查询到任何资源数据。
- 如您已开启资源记录器，但仅在资源记录器监控范围内勾选部分资源，则高级查询语句仅能查询到所选择的资源数据。
- 如您开启资源记录器并勾选全部资源，但后续又关闭资源记录器，则高级查询语句仅能查询到资源记录器由开启到关闭期间收集到的资源数据。

关于如何开启并配置资源记录器请参见：**配置资源记录器**。

新建查询

步骤1 登录管理控制台。

步骤2 单击页面左上角的图标，在弹出的服务列表中，选择“管理与监管”下的“配置审计 Config”，进入“资源清单”页面。

步骤3 单击页面左侧的“资源聚合器”，在下拉列表中选择“高级查询”，进入“高级查询”页面。

步骤4 选择“自定义查询”页签，单击页面右上角的“新建查询”。

步骤5 在右侧的“查询范围”页面中选择需要查询资源配置的聚合器，然后在下方输入框中输入查询语句。

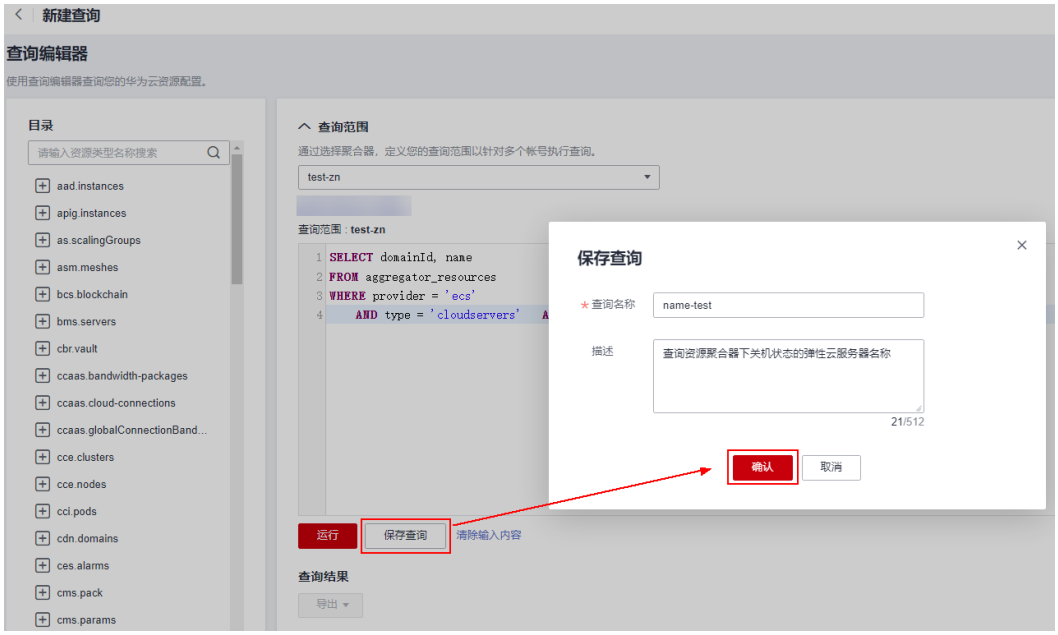
页面左侧为高级查询使用的Schema信息，也就是查询语句中properties参数需要填写的内容，为各个云服务资源类型的详细属性。查询语句的配置样例请参见**高级查询配置样例**。

步骤6 单击“保存查询”，输入查询名称和描述。

查询名称仅支持输入数字、英文字母、下划线和中划线。

步骤7 单击“确定”，保存成功。

图 6-10 保存查询



说明

如果您的自定义查询达到限额，将无法单击“保存查询”，同时页面提示“自定义查询个数已达到上限，请删除暂不需要使用的查询。”。

当自定义查询达到限额，您可以运行查询条件，并导出查询结果。

步骤8 单击“运行”，查看查询结果。目前只支持展示和导出前4000条查询结果。

步骤9 单击“导出”，选择要导出的文件格式（CSV格式或JSON格式）。

----结束

其他操作

- 您可以修改预设查询或已有自定义查询的名称、描述和查询语句，“另存为”后产生新的查询，具体请参考**其他操作**。
- 如果您需要查看某个查询的名称、描述和查询语句，请参考**查看查询**。
- 如果您需要修改某个自定义查询的查询语句，请参考**修改查询**。
- 如果您不需要使用某个自定义的查询，删除操作请参考**删除查询**。预设查询不支持删除操作。

说明

使用资源聚合器高级查询的相关功能，必须先指定需要查询的资源聚合器，从而定义您的查询范围，对指定聚合器聚合的多个源账号下的资源进行高级查询。

高级查询配置样例

ResourceQL使用结构化查询语言(SQL) SELECT语法的子集来对当前云资源配置数据进行查询和关联查询。用户无需调用特定API来实现，也无需通过多个API下载全量数据并手动分析。ResourceQL仅支持从表aggregator_resources中查询数据。

表 6-1 aggregator_resources 参数含义

资源参数	参数类型	含义
domain_id	String	账号ID
id	String	资源ID
name	String	资源名称
provider	String	云服务名称
type	String	资源类型
region_id	String	区域ID
project_id	String	项目ID
ep_id	String	企业项目ID
checksum	String	资源详情校验码
created	Date	资源创建时间
updated	Date	资源更新时间
provisioning_state	String	资源操作状态
tag	Array(Map<String,String>)	资源Tag
properties	Map<String,Object>	资源详细属性

用例参考如下：

- 示例1：查询资源聚合器下关机状态的弹性云服务器名称

```
SELECT domainId, name
FROM aggregator_resources
WHERE provider = 'ecs'
    AND type = 'cloudservers'
    AND properties.status = 'SHUTOFF'
```

- 示例2：查询资源聚合器下特定规格的云硬盘

```
SELECT *
FROM aggregator_resources
WHERE provider = 'evs'
    AND type = 'volumes'
    AND properties.size = 100
```

- 示例3：资源聚合器下对象存储桶模糊查询

```
SELECT *
FROM aggregator_resources
WHERE provider = 'obs'
    AND 'type' = 'buckets'
    AND name LIKE '%figure%'
```

- 示例4：查询每个聚合源账号下数量大于100的资源类型

```
WITH counts AS (
     SELECT region_id, provider, type, count(*) AS number
     FROM aggregator_resources
     GROUP BY domain_id, provider, type
 )
 SELECT *
```



```
FROM counts
WHERE number > 100
```

查询语句的详细介绍，请参见**ResourceQL语法**。

7 云审计-记录配置审计

7.1 支持云审计的关键操作

操作场景

平台提供了云审计服务。通过云审计服务，您可以记录与配置审计服务相关的操作事件，便于后续的查询、审计和回溯。

前提条件

已开通云审计服务。

支持审计的关键操作列表

表 7-1 云审计服务支持的 Config 操作列表

操作名称	资源类型	事件名称
创建用户的合规规则	policy	createPolicyAssignments
删除用户的合规规则	policy	deletePolicyAssignment
更新用户的合规规则	policy	updatePolicyAssignment
触发用户的合规规则进行评估	policy	runEvaluation
停用用户的合规规则	policy	disablePolicyAssignment
启用用户的合规规则	policy	enablePolicyAssignment
创建或修改用户的Tracker配置	trackerConfig	createOrUpdateTrackerConfig
删除用户的Tracker配置	trackerConfig	deleteTrackerConfig
创建用户的高级查询	storedQuery	createStoredQuery

操作名称	资源类型	事件名称
更新用户的高级查询	storedQuery	updateStoredQuery
删除用户的高级查询	storedQuery	deleteStoredQuery
更新合规评估结果	policyState	updatePolicyState
创建或更新组织合规规则	organizationPolicyAssignments	createOrganizationPolicyAssignment
删除组织合规规则	organizationPolicyAssignments	deleteOrganizationPolicyAssignment
创建授权	authorization	createAggregationAuthorization
删除授权	authorization	deleteAggregationAuthorization
创建资源聚合器	aggregator	createConfigurationAggregator
删除资源聚合器	aggregator	deleteConfigurationAggregator
更新资源聚合器	aggregator	updateConfigurationAggregator
删除待授权请求	aggregationRequests	deletePendingAggregationRequest
创建合规规则包	conformancePacks	createConformancePack
删除合规规则包	conformancePacks	deleteConformancePack

7.2 查询审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录：

- **在新版事件列表查看审计事件**
- **在旧版事件列表查看审计事件**

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。

- 用户通过云审计控制台只能查询最近7天的操作记录。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务(OBS)，才可在OBS桶里面查看历史文件。否则，您将无法追溯7天以前的操作记录。
- 云上操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。

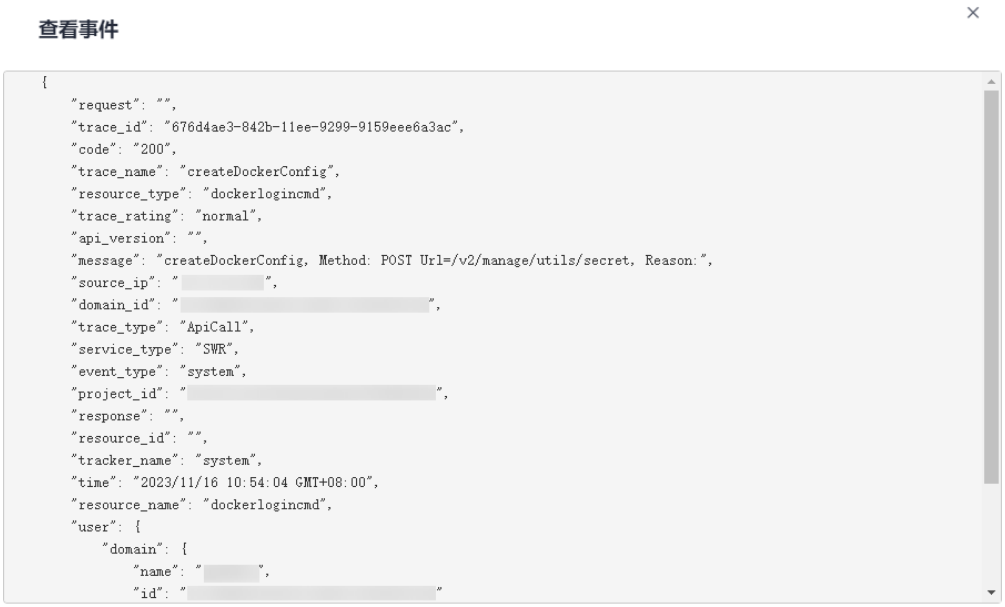
在新版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ☰ ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
   - 事件名称：输入事件的名称。
   - 事件ID：输入事件ID。
   - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
   - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
   - 云服务：在下拉框中选择对应的云服务名称。
   - 资源类型：在下拉框中选择对应的资源类型。
   - 操作用户：在下拉框中选择一个或多个具体的操作用户。
   - 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
     - normal：表示操作成功。
     - warning：表示操作失败。
     - incident：表示比操作失败更严重的情况，例如引起其他故障等。
   - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近1周内任意时间段的操作事件。
5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
   - 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
   - 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击 ↻ 按钮，可以获取到事件操作记录的最新信息。
   - 单击 ⚙ 按钮，可以自定义事件列表的展示信息。启用表格内容折行开关  ，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。
6. 关于事件结构的关键字段详解，请参见**事件结构**和**事件样例**。
7. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

在旧版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
   - 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
     - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
     - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
     - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
   - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
   - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
   - 时间范围：可选择查询最近7天内任意时间段的操作事件。
   - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
6. 选择完查询条件后，单击“查询”。
7. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
   - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击 按钮，可以获取到事件操作记录的最新信息。
8. 在需要查看的事件左侧，单击 展开该记录的详细信息。

9. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。



10. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的**事件结构**和**事件样例**。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

8 附录

8.1 支持的服务和区域

Config支持的服务和区域详见**支持的服务和区域**。

8.2 支持的资源关系

表 8-1 支持的资源关系

服务	资源类型	关系类型	相关云服务	相关资源类型
弹性云服务器 ECS	云服务器	被包含（isContainedIn）	虚拟私有云 VPC	虚拟私有云
			MapReduce服务 MRS	弹性大数据服务
		绑定（isAttachedTo）	虚拟私有云 VPC	弹性公网IP
			云硬盘 EVS	磁盘
		关联（isAssociatedWith）	虚拟私有云 VPC	安全组
			镜像服务 IMS	镜像
裸金属服务器 BMS	云服务器	被包含（isContainedIn）	虚拟私有云 VPC	虚拟私有云
		绑定（isAttachedTo）	云硬盘 EVS	磁盘
		关联（isAssociatedWith）	虚拟私有云 VPC	安全组
			镜像服务 IMS	镜像

服务	资源类型	关系类型	相关云服务	相关资源类型
云耀云服务器 HECS	云耀云服务器	被包含（isContainedIn）	虚拟私有云 VPC	虚拟私有云
		包含（contains）	虚拟私有云 VPC	弹性公网IP
		绑定（isAttachedTo）	云硬盘 EVS	磁盘
		关联（isAssociatedWith）	虚拟私有云 VPC	安全组
			镜像服务 IMS	镜像
弹性伸缩 AS	弹性伸缩组	被包含（isContainedIn）	虚拟私有云 VPC	虚拟私有云
		关联（isAssociatedWith）	虚拟私有云 VPC	安全组
分布式缓存服务 DCS	Memcached实例	被包含（isContainedIn）	虚拟私有云 VPC	虚拟私有云
		关联（isAssociatedWith）	虚拟私有云 VPC	安全组
	节点	被包含（isContainedIn）	分布式缓存服务 DCS	Redis实例
	Redis实例	被包含（isContainedIn）	虚拟私有云 VPC	虚拟私有云
		包含（contains）	分布式缓存服务 DCS	节点
		关联（isAssociatedWith）	虚拟私有云 VPC	安全组
弹性负载均衡 ELB	负载均衡器	包含（contains）	弹性负载均衡 ELB	监听器
		绑定（isAttachedTo）	虚拟私有云 VPC	弹性公网IP
			弹性负载均衡 ELB	后端服务器组
			弹性负载均衡 ELB	主备后端服务器组
	监听器	被包含（isContainedIn）	弹性负载均衡 ELB	负载均衡器

服务	资源类型	关系类型	相关云服务	相关资源类型
		绑定（isAttachedTo）	弹性负载均衡 ELB	后端服务器组
			弹性负载均衡 ELB	主备后端服务器组
	后端服务器组	包含（contains）	弹性负载均衡 ELB	后端服务器
		绑定（isAttachedTo）	弹性负载均衡 ELB	负载均衡器
			弹性负载均衡 ELB	监听器
	主备后端服务器组	包含（contains）	弹性负载均衡 ELB	后端服务器
		绑定（isAttachedTo）	弹性负载均衡 ELB	负载均衡器
			弹性负载均衡 ELB	监听器
	后端服务器	被包含（isContainedIn）	弹性负载均衡 ELB	后端服务器组
			弹性负载均衡 ELB	主备后端服务器组
虚拟私有云 VPC	虚拟私有云	包含（contains）	弹性云服务器 ECS	云服务器
			裸金属服务器 BMS	云服务器
			云耀云服务器 HECS	云耀云服务器
			弹性伸缩 AS	弹性伸缩组
			分布式缓存服务 DCS	Memcached实例
			分布式缓存服务 DCS	Redis实例
			MapReduce服务 MRS	弹性大数据服务
	安全组	关联（isAssociatedWith）	弹性云服务器 ECS	云服务器
			裸金属服务器 BMS	云服务器

服务	资源类型	关系类型	相关云服务	相关资源类型
			云耀云服务器 HECS	云耀云服务器
			弹性伸缩 AS	弹性伸缩组
			分布式缓存服务 DCS	Memcached实例
			MapReduce服务 MRS	弹性大数据服务
			分布式缓存服务 DCS	Redis实例
	带宽	包含（contains）	虚拟私有云 VPC	弹性公网IP
	弹性公网IP	被包含（isContainedIn）	虚拟私有云 VPC	带宽
		绑定（isAttachedTo）	弹性云服务器 ECS	云服务器
			弹性负载均衡 ELB	负载均衡器
			MapReduce服务 MRS	弹性大数据服务
			NAT网关	公网NAT网关
云硬盘 EVS	磁盘	绑定（isAttachedTo）	弹性云服务器 ECS	云服务器
			裸金属服务器 BMS	云服务器
			云耀云服务器 HECS	云耀云服务器
镜像服务 IMS	镜像	关联（isAssociatedWith）	弹性云服务器 ECS	云服务器
			裸金属服务器 BMS	云服务器
			云耀云服务器 HECS	云耀云服务器
NAT网关	公网NAT网关	绑定（isAttachedTo）	虚拟私有云 VPC	弹性公网IP

服务	资源类型	关系类型	相关云服务	相关资源类型
云数据库 GaussDB NoSQL	实例	包含（contains）	云数据库 GaussDB NoSQL	节点
	节点	被包含（isContainedIn）	云数据库 GaussDB NoSQL	实例
云数据库 GaussDB	实例	包含（contains）	云数据库 GaussDB	节点
	节点	被包含（isContainedIn）	云数据库 GaussDB	实例
MapReduce服务 MRS	弹性大数据服务	被包含（isContainedIn）	虚拟私有云 VPC	虚拟私有云
		绑定（isAttachedTo）	虚拟私有云 VPC	弹性公网IP
		关联（isAssociatedWith）	虚拟私有云 VPC	安全组
		包含（contains）	弹性云服务器 ECS	云服务器
云容器引擎 CCE	集群	包含（contains）	云容器引擎 CCE	节点
	节点	被包含（isContainedIn）	云容器引擎 CCE	集群
企业路由器 ER	连接	被包含（isContainedIn）	企业路由器 ER	实例
	实例	包含（contains）	企业路由器 ER	连接
统一身份认证 IAM	用户组	包含（contains）	统一身份认证 IAM	用户
	用户	被包含（isContainedIn）	统一身份认证 IAM	用户组
云数据库 RDS	实例	包含（contains）	云数据库 RDS	节点
	节点	被包含（isContainedIn）	云数据库 RDS	实例
配置审计 Config	合规规则包	包含（contains）	配置审计 Config	合规规则
	合规规则	被包含（isContainedIn）	配置审计 Config	合规规则包

8.3 支持标签的云服务和资源类型

当前华为云大部分云服务资源均支持添加标签，但部分云服务资源（如OBS桶）的标签信息暂未上传至Config服务，因此无法在Config服务中使用标签相关的能力，例如无法在“资源清单”页面通过标签搜索到相应资源，或无法使用涉及标签场景的资源合规规则等。

当前已对接Config且支持标签的云服务和资源类型如下表所示：

表 8-2 支持标签的云服务和资源类型

服务	资源类型
VPC终端节点 VPCEP	• 终端节点（vpcep.endpoints） • 终端节点服务（vpcep.endpointServices）
数据复制服务 DRS	• 实时同步任务（drs.synchronizationJob） • 实时迁移任务（drs.migrationJob） • 实时灾备任务（drs.dataGuardJob） • 数据订阅任务（drs.subscriptionJob） • 备份迁移任务（drs.backupMigrationJob）
裸金属服务器 BMS	实例（bms.servers）
弹性云服务器 ECS	云服务器（ecs.cloudservers）
云耀云服务器 HECS	实例（hecs.hcloudservers）
虚拟私有云 VPC	• 虚拟私有云（vpc.vpcs） • 弹性公网IP（vpc.publicips）
云硬盘 EVS	磁盘（evs.volumes）
弹性伸缩 AS	弹性伸缩组（as.scalingGroups）
镜像服务 IMS	镜像（ims.images）
分布式缓存服务 DCS	• Redis实例（dcs.redis） • 节点（dcs.node）
云解析服务 DNS	• 公网Zone（dns.publiczones） • 内网Zone（dns.privatezones）
虚拟专用网络 VPN	• VPN连接（vpnaas.vpnConnections） • VPN网关（vpnaas.vpnGateways）
弹性文件服务 SFS	SFS Turbo（sfsturbo.shares）
弹性负载均衡 ELB	• 负载均衡器（elb.loadbalancers） • 监听器（elb.listeners）

服务	资源类型
消息通知服务 SMN	主题（smn.topic）
分布式消息服务 DMS	• Kafka实例（dms.kafkas） • Kafka节点（dms.kafka_nodes） • RabbitMQ实例（dms.rabbitmqs） • Rabbitmq节点（dms.rabbitmq_nodes） • RocketMQ实例（dms.reliabilitys）
云数据库 RDS	• 实例（rds.instances） • 节点（rds.nodes）
MapReduce服务 MRS	弹性大数据服务（mrs.mrs）
数据仓库服务 DWS	集群（dws.clusters）
文档数据库服务 DDS	• 实例（dds.instances） • 节点（dds.nodes）
云搜索服务 CSS	集群（css.clusters）
NAT网关 NAT	• 公网NAT网关（nat.natGateways） • 私网NAT网关（nat.privateNatGateways）
云备份 CBR	存储库（cbr.vault）
数据加密服务 DEW	密钥（kms.keys）
云容器引擎 CCE	集群（cce.clusters）
云数据库 GaussDB	• 实例（gaussdb.instance） • 节点（gaussdb.nodes）
数据库安全服务 DBSS	实例（dbss.cloudservers）
内容分发网络 CDN	域名（cdn.domains）
云专线 DC	• 虚拟网关（dcaas.vgw） • 链路聚合组（dcaas.lag） • 虚拟接口（dcaas.vif） • 物理连接（dcaas.directConnect）
数据库和应用迁移 UGO	• 对象评估任务（ugo.evaluationJob） • 对象迁移任务（ugo.migrationJob）
DDoS高防服务 AAD	实例（aad.instances）
云连接 CC	• 云连接（ccaas.cloud-connections） • 带宽包（ccaas.bandwidth-packages）
云原生DDoS防护 CNAD	实例（cnad.instances）

服务	资源类型
企业路由器 ER	• 实例（er.instances） • 连接（er.attachments）
云日志服务 LTS	日志流（lts.topics）
设备接入 IoTDA	• 设备接入基础版（iotda.iotda） • 设备接入企业版（iotda.iotda_instance） • 设备接入标准版（iotda.iotda_standardinstance）
全球加速 GA	加速器实例（ga.accelerators）
开天集成工作台 MSSI	流（mssi.flow）
云堡垒机 CBH	云堡垒机实例（cbh.instance）
云防火墙 CFW	云防火墙实例（cfw.cfw_instance）
云监控服务 CES	告警规则（ces.alarms）
API网关 APIG	APIG专享版实例（apig.instances）
函数工作流 FunctionGraph	函数（fgs.functions）
分布式数据库中间件 DDM	• 实例（ddm.instances） • 节点（ddm.nodes）
湖仓构建 LakeFormation	实例（lakeformation.instance）
区块链服务 BCS	华为云链（bcs.huaweicloudchain）
产品数字化协同平台云服务 CraftArtsIPDCenter	产品数字化协同服务（ipdcenter.envs）
工业数字模型驱动引擎 iDME	• 数字化制造基础服务（idme.mbm） • 数据建模引擎运行服务（idme.runtime）
云凭据管理服务 CSMS	凭据（csms.secrets）
工业仿真工具链云服务 CraftArtsSIM	• 工业仿真云平台（craftartssim.simSpace） • 仿真求解计算（craftartssim.cpuUnit） • 仿真前后处理计算（craftartssim.guiUnit）
私有证书管理 PCA	• 私有CA（pca.ca） • 私有证书（pca.cert）
专属分布式存储服务 DSS	存储池（dss.dsspools）
专属主机 DeH	专属主机（deh.dedicatedhosts）
访问分析 AccessAnalyzer	访问分析器（accessanalyzer.analyzer）

8.4 消息通知模型

目前，消息通知服务支持Config以下几种类型的消息通知：

- 资源变更（创建/修改/删除）的消息通知；
- 资源关系变更的消息通知；
- 资源变更消息存储完成的消息通知；
- 资源快照存储完成的消息通知。

资源变更的消息通知模型

表 8-3 资源变更的消息通知模型

参数	参数类型	描述
notification_type	String	消息通知类型。
notification_creation_time	String	消息发送时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。
domain_id	String	账号ID。
detail	Object	消息详情。

表 8-4 detail 参数

参数	参数类型	描述
resource_id	String	资源ID。
resource_type	String	资源类型。
event_type	Enum	事件类型（CREATE|UPDATE|DELETE）。
capture_time	String	事件捕获时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。
resource	Object	资源详情。

表 8-5 resource

参数	参数类型	描述
id	String	资源ID。
name	String	资源名称。
provider	String	云服务名称。
type	String	云资源类型。
region_id	String	资源所在区域ID。
project_id	String	IAM项目ID。
project_name	String	IAM项目名称。
ep_id	String	企业项目ID。
ep_name	String	企业项目名称。
checksum	String	校验和。
created	String	云资源初始创建时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。
updated	String	云资源最后更新时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。
provisioning_state	String	资源操作状态。
tags	Map	租户为云资源做的标记。
properties	Map	云资源的属性详情。

资源变更消息通知示例

```
{
  "detail": {
    "resource": {
      "id": "3e62c0e6-e779-469e-b0f2-35743f6229d1",
      "name": "ecs-51c8",
      "provider": "evs",
      "type": "volumes",
      "checksum": "b3bcc019cecbb701e324e0dcf2f283236685885236b49f5ba5ea2f5f788170a1",
      "created": "2020-08-12T07:14:41.638Z",
      "updated": "2020-08-12T07:14:44.423Z",
      "tags": {},
      "properties": {
        "shareable": false,
        "volumeType": "SATA",
        "metadata": {},
        "attachments": [],
        "replicationStatus": "disabled",
        "availabilityZone": "regionid1a",
```



```
        "bootable": "true",
        "userId": "059b5c937d80d3e41ff3c00a3c883d16",
        "volTenantAttrTenantId": "059b5e0a2500d5552fa1c00adada8c06",
        "size": "40",
        "encrypted": false,
        "volumeImageMetadata": {
          "virtualEnvType": "FusionCompute",
          "isregistered": "true",
          "imageSourceType": "uds",
          "minDisk": "40",
          "platform": "CentOS",
          "size": 0,
          "osVersion": "CentOS 7.5 64bit",
          "minRam": "0",
          "name": "CentOS 7.5 64bit",
          "checksum": "d41d8cd98f00b204e9800998ecf8427e",
          "osBit": "64",
          "osType": "Linux",
          "containerFormat": "bare",
          "supportXen": "true",
          "id": "e0adce3a-a4d2-4207-9018-69ce64b4426a",
          "supportKvm": "true",
          "diskFormat": "zvhd2",
          "imageType": "gold"
        },
        "links": [
          {
            "rel": "self",
            "href": "https://evs.regionid1.xxxxxx.com/v2/059b5e0a2500d5552fa1c00adada8c06/os-vendor-volumes/3e62c0e6-e779-469e-b0f2-35743f6229d1"
          },
          {
            "rel": "bookmark",
            "href": "https://evs."regionid1.xxxxxx.com/059b5e0a2500d5552fa1c00adada8c06/os-vendor-volumes/3e62c0e6-e779-469e-b0f2-35743f6229d1"
          }
        ],
        "volHostAttrHost": ""regionid1a-pod01."regionid1#0",
        "multiattach": false,
        "status": "available"
      },
      "region_id": ""regionid1",
      "project_id": "059b5e0a2500d5552fa1c00adada8c06",
      "project_name": ""regionid1",
      "ep_id": "0",
      "ep_name": "default",
      "provisioning_state": "Succeeded"
    },
    "resource_id": "3e62c0e6-e779-469e-b0f2-35743f6229d1",
    "resource_type": "evs.volumes",
    "event_type": "CREATE",
    "capture_time": "2020-08-12T07:15:15.116Z"
  },
  "notification_type": "ResourceChanged",
  "notification_creation_time": "2020-08-12T07:14:47.192Z",
  "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```


资源关系变更的消息通知模型

表 8-6 资源关系变更的消息通知模型

参数	参数类型	描述
notification_type	String	消息通知类型。

参数	参数类型	描述
notification_creation_time	String	消息发送时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。
domain_id	String	账号ID。
detail	Object	消息详情。

表 8-7 detail

参数	参数类型	描述
resource_id	String	资源ID。
resource_type	String	资源类型。
event_type	Enum	事件类型（CHANGE）。
capture_time	String	事件捕获时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。

资源关系变更消息通知示例

```
{
  "detail": {
    "resource_id": "f65b06d1-d63b-438a-93cc-bdd55b304f0a",
    "resource_type": "ecs.cloudservers",
    "event_type": "CHANGE",
    "capture_time": "2020-08-12T07:15:14.257Z"
  },
  "notification_type": "ResourceRelationChanged",
  "notification_creation_time": "2020-08-12T07:14:56.296Z",
  "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```

资源快照存储完成的消息通知模型

表 8-8 资源快照存储完成的消息通知模型

参数	参数类型	描述
notification_type	String	消息通知类型。
notification_creation_time	String	消息发送时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。

参数	参数类型	描述
domain_id	String	租户ID。
detail	Object	消息详情。

表 8-9 detail

参数	参数类型	描述
snapshot_id	String	资源快照ID。
region_id	String	资源快照所在区域ID。
bucket_name	String	资源快照所在OBS桶名。
object_keys	Array of String	资源快照路径列表。

资源快照存储完成的消息通知示例

```
{
  "detail": {
    "snapshot_id": "474f85e6-72cd-442b-af4e-517120a5c669",
    "region_id": ""regionid1",
    "bucket_name": "test",
    "object_keys": [
      "RMSLogs/059b5c937100d3e40ff0c00a7675a0a0/Snapshot/
2020/8/11/059b5c937100d3e40ff0c00a7675a0a0_Snapshot_"regionid1_ResourceSnapshot_2020-08-10T170901_474f85e6-72cd-442b-af4e-517120a5c669_part-1.json.gz"
    ]
  },
  "notification_type": "SnapshotArchiveCompleted",
  "notification_creation_time": "2020-08-10T17:09:27.314Z",
  "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```

资源变更消息存储完成的消息通知模型

表 8-10 资源变更消息存储完成的消息通知模型

参数	参数类型	描述
notification_type	String	消息通知类型。
notification_creation_time	String	消息发送时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。
domain_id	String	账号ID。
detail	Object	消息详情。

表 8-11 detail 参数

参数	参数类型	描述
region_id	String	资源快照所在区域ID。
bucket_name	String	资源快照所在OBS桶名。
object_key	String	资源快照路径。

资源变更消息存储完成的消息通知示例

```
{
    "detail": {
        "region_id": ""regionid1",
        "bucket_name": "test",
        "object_key": "RMSLogs/059b5c937100d3e40ff0c00a7675a0a0/Notification/2020/12/10/
NotificationChunk/
059b5c937100d3e40ff0c00a7675a0a0_Notification_"regionid2_NotificationChunk_VPC_VPCS_2020-12-10T02
4612Z_2020-12-10T050621Z.json.gz"
    },
    "notification_type": "NotificationArchiveCompleted",
    "notification_creation_time": "2020-12-10T05:09:28.002Z",
    "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
}
```

8.5 资源存储模型

表 8-12 资源存储模型

参数	参数类型	描述
snapshot_id	String	资源快照ID。
items	Array of Object	资源快照项列表。
snapshot_time	String	资源快照存储时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。

表 8-13 资源快照项

参数	参数类型	描述
resource	Object	资源。
relations	Array of Object	资源关系项列表。

表 8-14 resource 参数

参数	参数类型	描述
id	String	资源ID。
name	String	资源名称。
provider	String	云服务名称。
type	String	云资源类型。
region_id	String	资源所在区域ID。
project_id	String	IAM项目ID。
project_name	String	IAM项目名称。
ep_id	String	企业项目ID。
ep_name	String	企业项目名称。
checksum	String	校验和。
created	String	云资源初始创建时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。
updated	String	云资源最后更新时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。
provisioning_state	String	资源操作状态。 枚举值： ● Succeeded：资源操作成功。 ● Failed：资源操作异常。 ● Canceled：资源操作取消。 ● Processing：资源操作正在进行中。
tags	Map	租户为云资源做的标记。
properties	Map	云资源的属性详情。

表 8-15 资源关系项

参数	参数类型	描述
from_resource_id	String	源资源ID。
to_resource_id	String	目的资源ID。

参数	参数类型	描述
from_resource_type	String	源资源类型。
to_resource_type	String	目的资源类型。
relation_type	String	资源关系的类型。

资源存储示例

```
{
  "items": [
    {
      "resource": {
        "id": "c25ee8b3-c907-4cd4-9869-6c4b07c61a0b",
        "name": "rse-cdk-07-cdk-3sbz",
        "provider": "vpc",
        "type": "securityGroups",
        "region_id": ""regionid1",
        "project_id": "fc6d40abe7e54492b7c7aa5a29d6cbab",
        "project_name": "demo_project",
        "ep_id": "0",
        "ep_name": "default",
        "checksum": "4098715092c762b3eafe25be8eeda33a10b547033f9d59b6e18f5a960a1f805d",
        "updated": "2020-05-25T10:27:17.000Z",
        "created": "2020-05-25T10:27:17.000Z",
        "provisioning_state": "Succeeded",
        "tags": {},
        "properties": {}
      },
      "relations": [
        {
          "from_resource_id": "c25ee8b3-c907-4cd4-9869-6c4b07c61a0b",
          "to_resource_id": "0088a276-162b-4f07-aa40-f6ed8b801ca1",
          "from_resource_type": "vpc.securityGroups",
          "to_resource_type": "ecs.cloudservers",
          "relation_type": "isAssociatedWith"
        }
      ]
    }
  ],
  "snapshot_id": "6e40483d-5499-4440-a369-284e528f3d85",
  "snapshot_time": "2020-06-30T06:56:00.018Z"
}
```

8.6 资源变更消息存储模型

表 8-16 资源变更消息存储模型

参数	参数类型	描述
notification_items	Array of Object	资源变更消息通知列表。

资源变更的消息通知模型

表 8-17 资源变更的消息通知模型

参数	参数类型	描述
notification_type	String	消息通知类型。
notification_creation_time	String	消息发送时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。
domain_id	String	账号ID。
detail	Object	消息详情。

表 8-18 detail 参数

参数	参数类型	描述
resource_id	String	资源ID。
resource_type	String	资源类型。
event_type	Enum	事件类型（CREATE|UPDATE|DELETE）。
capture_time	String	事件捕获时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。
resource	Object	资源详情。

表 8-19 resource

参数	参数类型	描述
id	String	资源ID。
name	String	资源名称。
provider	String	云服务名称。
type	String	云资源类型。
region_id	String	资源所在区域ID。
project_id	String	IAM项目ID。
project_name	String	IAM项目名称。

参数	参数类型	描述
ep_id	String	企业项目ID。
ep_name	String	企业项目名称。
checksum	String	校验和。
created	String	云资源初始创建时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。
updated	String	云资源最后更新时间。 具有固定格式：遵循ISO8601格式，UTC时区（例如：2018-11-14T08:59:14Z）。
provisioning_state	String	资源操作状态。
tags	Map	租户为云资源做的标记。
properties	Map	云资源的属性详情。

资源变更消息存储示例

```
{
   "notification_items": [
      {
         "detail": {
            "resource": {
               "id": "ea05ef41-8bd6-4a9c-af39-244e1ec448eb",
               "name": "as-group-test",
               "provider": "as",
               "type": "scalingGroups",
               "checksum": "",
               "region_id": ""regionid1",
               "project_id": "068d54ceca00d5302f70c00aaf6a471c",
               "project_name": "test",
               "ep_id": "0",
               "ep_name": "default"
            },
            "resource_id": "ea05ef41-8bd6-4a9c-af39-244e1ec448eb",
            "resource_type": "as.scalingGroups",
            "event_type": "DELETE",
            "capture_time": "2020-12-08T09:30:27.158Z"
         },
         "notification_type": "ResourceChanged",
         "notification_creation_time": "2020-12-08T09:30:27.272Z",
         "domain_id": "059b5c937100d3e40ff0c00a7675a0a0"
      }
   ]
}
```

8.7 DSL 语法

DSL由一个如下的逻辑运算符组成，最终的返回结果为一个布尔值。


```
{
  <logical operator>: <condition> | [<condition>, ..., <condition>]
}
```

8.7.1 逻辑运算符（logical operator）

逻辑运算符共支持以下三种类型：

- "not": <condition>
- "allOf": [<condition>, ..., <condition>]
- "anyOf": [<condition>, ..., <condition>]

not操作符表示对后面的条件结果取反；

allOf操作符仅在后面所有的条件都为真时返回真，否则返回假；

anyOf操作符在后面条件任意一个为真时即返回真，否则返回假。

allOf和anyOf操作符都实现了短路求值（Short-circuit evaluation），它们会对后续列表中的条件按顺序依次求值。

对于allOf操作符，如果某个条件返回结果为假，则其会直接返回结果假，不再计算后续的条件；

对于anyOf操作符，如果某个条件返回结果为真，则其会直接返回结果真，不再计算后续的条件。

8.7.2 条件（condition）

条件可以是一条单独的判断语句，也可以是一个嵌套的逻辑运算符。

判断语句的格式如下，其返回的是一个布尔值。它的作用是判断一个指定的值是否满足特定的要求。

```
{
  "value": "...",
  "comparator": "...",
  "pattern": "..."
}
```

说明

- value：此处为常量或者表达式，具体值的类型根据选择的比较符而定。例如：true、1、"hello"或"${resource().properties.metadata}"。
- comparator：比较符。
- pattern：此处为常量或者表达式。

支持的比较符（comparator）有以下几种：

- "equals"：比较value和pattern是否相等，类型可以是字符串，整数或者布尔；
- "notEquals"：结果与equals相反；
- "equalsIgnoreCase"：以忽略大小写的形式比较value和pattern是否相等，类型必须是字符串；
- "like"：对value和pattern进行字符串模糊匹配，你可以在pattern中添加"*"或者"?"，其中"*"可以匹配0个或多个任意字符，"?"匹配一个任意字符，类型必须是字符串；
- "notLike"：结果与like相反；

- "likeIgnoreCase"：以忽略大小写的形式对value和pattern进行字符串模糊匹配，类型必须是字符串；
- "contains"：判断pattern是否是value的子串，类型必须是字符串；
- "notContains"：结果与contains相反；
- "in"：判断value是否在pattern中，pattern必须是数组类型，value可以是字符串或者整数类型；
- "notIn"：结果与in相反；
- "containsKey"：判断value是否包含键值pattern，value必须是object类型，pattern必须是字符串类型；
- "notContainsKey"：结果与containsKey相反；
- "less"：判断value是否小于pattern，类型可以是字符串或者整数；
- "lessOrEquals"：判断value是否不大于pattern，类型可以是字符串或者整数；
- "greater"：判断value是否大于pattern，类型可以是字符串或者整数；
- "greaterOrEquals"：判断value是否不小于pattern，类型可以是字符串或者整数。

条件内部嵌套逻辑运算符的例子：

```
{
  "not": {
    "anyOf": [
      {
        "value": "${resource().properties.metadata}",
        "comparator": "notContainsKey",
        "pattern": "systemEncrypted"
      },
      {
        "value": "${resource().properties.metadata.systemEncrypted}",
        "comparator": "equals",
        "pattern": "0"
      }
    ]
  }
}
```

8.7.3 表达式

在上一节提到value和pattern字段中，你不但可以填写常值，还可以编写表达式。表达式被${}包含，表达式中可以使用下列函数：

表 8-20 字符串函数

函数	参数	返回值	功能描述
base64()	string	string	对给定字符串进行base64编码。
base64ToString()	string	string	对一个base64编码的字符串解码。
concat()	string, string	string	拼接两个字符串。
contains()	string, string	bool	判断参数二是否是参数一的子串。
empty()	string	bool	判断字符串是否为空串。
endsWith()	string, string	bool	判断参数一是否以参数二结尾。

函数	参数	返回值	功能描述
indexOf()	string, string	int	返回参数二在参数一中第一次出现的位置，如果没有出现返回-1。
lastIndexOf()	string, string	int	返回参数二在参数一中最后一次出现的位置，如果没有出现返回-1。
length()	string	int	返回字符串长度。
replace()	string, string, string	string	将参数一中所有出现参数二的部分以参数三替换。
startsWith()	string, string	bool	判断参数一是否以参数二开头。
toLower()	string	string	将字符串中的英文字符都转换为小写。
toUpper()	string	string	将字符串中的英文字符都转换为大写。
equals()	string, string	bool	判断两个字符串是否相等。
greater()	string, string	bool	判断参数一是否大于参数二。
greaterOrEquals()	string, string	bool	判断参数一是否不小于参数二。
less()	string, string	bool	判断参数一是否小于参数二。
lessOrEquals()	string, string	bool	判断参数一是否不大于参数二。
split()	string, string	array	返回将参数一以参数二为分隔符分割后的结果。
substring()	string, int, int	string	获取参数一的子串，子串的开始位置由参数二指定，长度由参数三指定。

表 8-21 数值函数

函数	参数	返回值	功能描述
add()	int, int	int	将两个整数相加。
max()	int, int	int	取两个整数中的较大值。
min()	int, int	int	取两个整数中的较小值。
sub()	int, int	int	计算参数一减去参数二后的结果。
equals()	int, int	bool	判断两个整数是否相等。
greater()	int, int	bool	判断参数一是否大于参数二。

函数	参数	返回值	功能描述
greaterOrEquals()	int, int	bool	判断参数一是否不小于参数二。
less()	int, int	bool	判断参数一是否小于参数二。
lessOrEquals()	int, int	bool	判断参数一是否不大于参数二。

表 8-22 数组函数

函数	参数	返回值	功能描述
concat()	array, array	array	拼接两个数组。
contains()	array, any	bool	判断参数二是否在数组参数一中。
empty()	array	bool	判断数组是否为空。
first()	array	any	返回数组中的第一个元素。
last()	array	any	返回数组中的最后一个元素。
length()	array	int	返回数组长度。

表 8-23 对象函数

函数	参数	返回值	功能描述
contains()	object, string	bool	判断参数一是否包含键值参数二。
getValue()	object, string	any	获取参数一中参数二键值对应的值。
empty()	object	bool	判断对象是否为空。
length()	object	int	返回对象中的键值数量。

表 8-24 逻辑函数

函数	参数	返回值	功能描述
if()	bool, any, any	any	判断参数一是否为真，如果为真返回参数二，否则返回参数三。

函数	参数	返回值	功能描述
and()	bool, bool	bool	判断参数一和参数二是否都为真。
or()	bool, bool	bool	判断参数一和参数二是否至少一个为真。
not()	bool	bool	将输入的布尔值取反。

表 8-25 资源合规相关函数

函数	参数	返回值	功能描述
resource()	无	object	返回当前评估资源的结构体。
parameters()	string	any	返回在parameters部分定义的一个参数。

除了函数计算以外，表达式中还支持下列语法：

- "."连接符：你可以使用"."连接符来访问一个object中的一个字段，如resource().properties.metadata.systemEncrypted。
- "CASE WHEN"语句：

```
CASE WHEN condition1 THEN value1
    WHEN condition2 THEN value2
    ...
    ELSE defaultValue END
```

8.8 ResourceQL 语法

8.8.1 语法概览

ResourceQL能够提供类似SQL的服务来灵活地查询您的云资源。

```
SELECT name, created, updated FROM resources WHERE region_id = 'regionid1'
```

语句不区分大小写，即'SELECT COUNT(*)' 和'select CoUnT(*)'没有区别。用单引号表示字符串字面量。

ResourceQL支持以下7种数据类型。其中数组类型用'[]'来索引某个位置（标号从'1'开始）。

表 8-26 支持的数据类型

类型名	类型英文
整型	int/integer

类型名	类型英文
浮点型	float/double
布尔型	boolean
数组型	array
字符串	string
字典型	object
时刻型	date

您的所有云资源构成了一张表，表名固定为resouces。您的资源聚合器下的资源构成了一张表，表名固定为aggregator_resources。表中每一行记录了一条数据，每一列约定如下：

表 8-27 resources 参数含义

资源参数	参数类型	含义
id	String	资源ID。
name	String	资源名称。
provider	String	云服务名称。
type	String	资源类型。
region_id	String	区域ID。
project_id	String	项目ID。
ep_id	String	企业项目ID。
checksum	String	资源详情校验码。
created	Date	资源创建时间。
updated	Date	资源更新时间。
provisioning_state	String	资源操作状态。
tag	Array(Map<String,String>)	资源Tag。
properties	Map<String,Object>	资源详细属性。

资源聚合器表aggregator_resources则额外支持资源参数domain_id，类型为String，含义为账号ID。

不同类型的资源可以用'provider'和'type'来区分，它们对应的'properties'字段的结构也就不一样。 例如，ecs的cloudservers拥有包含23个字段的'properties'，而vpc仅有包含3个字段的'properties'。

各个资源类型properties内支持的字段以及类型可以在配置审计控制台的新建查询页面查看，具体请参见**新建查询**。

对于某个具体的资源类型，我们可以用'.'嵌套的方式去查询'properties'下的具体字段。例如，弹性云服务器的'properties'里有'status'和'addresses'字段，可以用如下语句查询正在运行的弹性云服务器及其地址。

```
SELECT name, created, updated, properties.addresses FROM resources
    WHERE provider = 'ecs' AND type = 'cloudservers' AND properties.status = 'ACTIVE'
```

8.8.2 语法文档

符号约定

本节把需要原样输入的单词用大写表示，需要原样输入的字符用单引号括起来。

'[x]'表示语句'x'可以出现一次或不出现。

'(x)'表示语句'x'是个整体。'(x, ...)'表示语句'x'可以出现一次或多次，多次之间用逗号连接。

'|'表示所有可能的替代情况。

'expression'表示任意表达式。特殊地，'bool_expression'表示任意布尔表达式。

'identifier'表示一个合法的标识符。由字符'0-9,a-z,A-Z,_'组成，且不能以数字开头。

'column_name'表示一个合法的字段名。它可以是一个'identifier'或多个嵌套，如'A.id'。

'table_name'表示一个合法的表名。ResourceQL语法规定'table_name'必须为'resources'。

用双引号括起来的单位会被认为是一个整体。例如，若需表示带有特殊字符的列名，需在其前后加双引号。

查询的基本语法

```
[WITH (with_item, ...)]
SELECT [DISTINCT | ALL] (select_item, ...)
[FROM (from_item, ...)]
[WHERE bool_expression]
[GROUP BY [DISTINCT | ALL] (expression, ...)]
[HAVING booleanExpression]
[ORDER BY (expression [ASC | DESC] [NULLS (FIRST | LAST)], ...)]
[LIMIT number]
```

'select_item'支持对字段名进行重命名和运算，也支持全选。

```
select_item = (expression [[AS] column_name_aias]) | *
```

'from_item'支持join函数和嵌套子查询，且支持对表名进行重命名。

```
from_item = table_name [[AS] table_name_aias]
        | (from_item join_type from_item [(ON bool_expression) | USING(column_name, ...)])
        | '(' query ')'
```

'with_item'用来定制模板化询问，以方便后续多次调用。

```
with_item = identifier AS '(' query ')'
```

例如，查询每个区域内数量大于100的资源类型，可以使用如下语句：


```
WITH counts AS (
   SELECT region_id, provider, type, count(*) AS number FROM resources
   GROUP BY region_id, provider, type
) SELECT * FROM counts WHERE number > 100
```

数值运算和布尔运算

ResourceQL支持对整型和浮点型进行二元数学运算，运算符包括'+,-,*,/,%'。

相同类型的值之间可以比较，比较符包括'<,>,<=,>=,=,<>,!='（最后两个符号都表示“不等于”）。数值之间比的是大小，字符串之间比的是字典序。数值和集合之间也可以进行比较，此时比较符右侧为'ALL | SOME | ANY'中的一种，用来限定比较范围。'ALL'表示集合里所有元素都要满足，'SOME/ANY'表示至少一个元素满足即可。

```
expression ('=' | '<>' | '!=' | '<' | '>' | '<=' | '>=')
expression
expression ('=' | '<>' | '!=' | '<' | '>' | '<=' | '>=')
[ALL | SOME | ANY] '(' query ')'
```

'bool_expression'表示任意布尔表达式（运算后返回True或False），包括以下几种语法：

```
NOT bool_expression
bool_expression (AND | OR) bool_expression
expression [NOT] BETWEEN expression AND expression
expression [NOT] IN '(' query ')'
EXISTS '(' query ')'
expression [NOT] LIKE pattern [ESCAPE escape_characters]
expression IS [NOT] NULL
expression IS [NOT] DISTINCT FROM expression
```

特别地，运算符'||'会对左右两边的值进行连接并返回连接后的新值，左右两侧类型相同且均为数组或字符串。

时间类型

ResourceQL支持查询时间类型的字段。查询结果会折算成零时区并以ISODate的标准格式返回，保留至毫秒。

时间类型可以用比较运算符连接。如果想使用表示时间的字面量，请写作timestamp 'time'的形式。其中的'time'可以是任意的ISODate格式或者常用时间格式。以下的'time'写法都是被允许的。

2019-06-17T12:55:42.233Z

2019-06-17T12:55:42Z

2019-06-17 12:55:42

2019-06-17T12:55:42.00 + 08:00

2019-06-17 05:55:40 - 06:00

2019-06-17

2019

如果不加时区则默认为零时区，不加24小时时刻则默认为0:00，不加月份则默认为1月1日。

例如，把2020年9月12日12:55:00以来创建的资源按更新时间降序排序，可以使用如下语句：


```
select name, created, updated from resources
where created >= timestamp '2020-09-12T12:55:00Z'
order by updated DESC
```

模糊查询

```
string LIKE pattern [ESCAPE escape_characters]
```

'LIKE'用来判断字符串是否符合某种pattern。如果pattern里想表达'%'或者'_'这两种字符的字面量，可以在'ESCAPE'后指定转义符（如'#'），在pattern里写成'#%'和'#_'即可。

通配符'%'表示匹配0或多个字符。

通配符'_'表示正好匹配一个字符。

对象存储桶的模糊查询，可以写成如下形式：

```
SELECT name, id FROM resources
   WHERE provider = 'obs' AND type = 'buckets' AND name LIKE '%figure%'
```

或

```
SELECT name, id FROM resources
   WHERE provider = 'obs' AND type = 'buckets' AND name LIKE '%figure#_%' ESCAPE '#'
```

条件函数

CASE关键字可以根据情况选择不同的返回值。它有以下两种用法。

- 计算给定表达式expression的值，根据不同的值返回对应的结果。
- 依次计算每一个bool_expression的值，找到第一条符合要求的expression并返回对应的结果。

```
CASE expression
   WHEN value1 THEN result1
   [WHEN value2 THEN result2]
   [...]
   [ELSE result]
END
CASE
   WHEN condition1 THEN result1
   WHEN condition2 THEN result2
   [...]
   [ELSE result]
END
```

IF关键字的用法有以下两种。

- 'IF(bool_expression, value)'：如果布尔表达式值为真就返回'value'，否则返回NULL。
- 'IF(bool_expression, value1, value2)'：如果布尔表达式值为真就返回'value1'，否则返回 'value2'。

用函数来简化查询

ResourceQL提供丰富的函数来简化查询。详细函数说明请参见**函数列表**。

ResourceQL支持lambda表达式。某些函数的参数可能是另一个函数，此时用lambda表达式就很方便。

例如，查询与所有ECS关联的EVS，可以使用如下的语句：


```
SELECT ECS.id AS ecs_id, EVS.id AS evs_id FROM
   (SELECT id, transform(properties.ExtVolumesAttached, x -> x.id) AS evs_list
   FROM resources WHERE provider = 'ecs' AND type = 'cloudservers') ECS
   (SELECT id FROM resources WHERE provider = 'evs' AND type = 'volumes') EVS
   WHERE contains(ecs.evs_list, evs.id)
```

其中'contains(a, element) →boolean'：可以判断某元素是否出现在数组a中。

'transform(array(T), function(T, S))→array(S)'能够把某个类型的数组变换成另一个类型的数组。

Join 和 Unnest

ResourceQL支持'JOIN'和'UNNEST'。'JOIN'分为以下四种类型。

- [INNER] JOIN
- LEFT [OUTER] JOIN
- RIGHT [OUTER] JOIN
- FULL [OUTER] JOIN

'JOIN'后需紧跟'USING(...)'或'ON <bool_expression>'。

'USING'用来指定参与join的若干个列名。

'ON'接受一个布尔表达式，若值为真则合并。出于性能考虑，布尔表达式的合取范式里需保证至少有一个等式，且该等式左右两端的运算内容被左右两张表独立提供。

'JOIN'前可以冠上'NATURAL'关键词表示自然连接，这样后面不用'USING'或'ON'连接。

'UNNEST'能把数组解包成表，加上'WITH ORDINALITY'会有一个自动计数的列，格式如下：

```
table_name CROSS JOIN UNNEST '(' (expression, ...) ')' [WITH ORDINALITY]
```

注意，'CROSS JOIN'只能用于和 'UNNEST'连接，ResourceQL不支持其他格式的'CROSS JOIN'。

上述查询ECS和EVS关联的例子还可以写成如下形式：

```
SELECT ECS_EVS.id AS ecs_id, EVS.id AS evs_id FROM
   (SELECT id, evs_id FROM (SELECT id, transform(properties.ExtVolumesAttached, x ->x.id) AS evs_list
      FROM resources WHERE provider = 'ecs' AND type = 'cloudservers') ECS
    CROSS JOIN UNNEST(evs_list) AS t (evs_id)) ECS_EVS,
    (SELECT id FROM resources WHERE provider = 'evs' AND type = 'volumes') EVS
    WHERE ECS_EVS.evs_id = EVS.id
```

8.8.3 函数列表

ResourceQL支持以下函数：

表 8-28 数学运算函数

函数	功能描述
abs(x)	返回x的绝对值。
ceil/ceiling(x)	把小数x向上取整。

函数	功能描述
floor(x)	把小数x向下取整。
pow/power(x, p) → double	计算x^p。
round(x)	把小数x四舍五入取整。
round(x, d)	把小数x四舍五入保留d位小数。
sign(x)	返回x的符号，正数是1负数是-1。

表 8-29 字符串函数

函数	功能描述
concat(str1, str2, ..., strn) → string	合并字符串。
chr(n) → string	把数字n转化成对应的unicode字符。
codepoint(str) → int	把unicode字符转化成数字。
length(str) → int	返回字符串的长度。
lower/upper(str) → string	把字符串变换成全小写/大写。
replace(str, sub) → string	把字符串str里所有sub子串都删除。
replace(str, sub, replace) → string	把字符串str里所有sub子串都替换成replace。
reverse(str) → string	把字符串str翻转。
split(str, delimiter) → array	把字符串str按照delimiter切割成数组。
strpos(str, sub) → int	返回str里第一次出现sub的下标。下标从1开始，不存在返回0。
strpos(str, sub, n) -> int	返回str里第n次出现sub的下标。下标从1开始，不存在返回0。
strrpos(str, sub) → int	返回str里倒数第一次出现sub的下标。下标从1开始，不存在返回0。
strrpos(str, sub, n) -> int	返回str里倒数第n次出现sub的下标。下标从1开始，不存在返回0 。
substr(str, start) → string	返回str里从start开始的子串。
substr(str, start, length) → string	返回str里从start开始，长度为length的子串。
trim/lstrim/rstrim(str)	把str里开头和结尾/开头/结尾的空白字符删掉。

表 8-30 数组函数

函数	功能描述
all_match(array(T), function(T, boolean)) → boolean	询问每个函数是否都满足给定函数。
any_match(array(T), function(T, boolean)) → boolean	询问是否存在元素满足给定函数。
array_average(a) → double	询问是否存在元素满足给定函数。
array_distinct(a) → array	返回数组a去重后的新数组。
array_duplicates(a) → array	返回数组a里出现次数超过一次的元素构成的新数组。
array_frequency(a) → map	统计数组中每个元素出现的次数并返回对应的map。
array_has_duplicates(a) → boolean	查询数组中是否有重复元素。
array_intersect(a, b) → array	对数组a和b的元素求个交集。
array_join(x, delimiter) → string	把数组元素连接成字符串，中间用delimiter来分隔。
array_join(x, delimiter[, null_replacement]) → string	把数组元素连接成字符串，中间用delimiter来分隔，null元素用null_replacement填充。
array_max/array_min(a)	返回数组a的最大值/最小值。
array_position(a, element) → int	查询element在数组a中的位置。如果不存在返回0。
array_position(a, element, instance) → int	查询element在数组a中的位置。如果不存在返回0。如果'instance>0'，返回第'instance' 出现的位置；如果'instance < 0'，返回倒数'instance'位置。
array_remove(a, element) → array	把数组a中等于element的元素都删除。
array_sort(a) → array	返回数组a排序后的新数组。
array_sort(array(T), function(<T, T>, int)) → array	返回数组a排序后的新数组。需要提供一个二元比较函数，(-1,0,1) 分别表示小于等于和大于。
array_sum(a)	返回数组a的元素和。
array_overlap(a, b) → boolean	询问a和b的交集是否为不为空。
array_union(a, b) → array	返回a和b的并集的数组。
array_except(x, y) → array	返回x中但不在y中的元素数组。
cardinality(a) → int	返回数组a的大小。
concat(a1, a2, ...) → array	合并数组，等价于'||'运算符。

函数	功能描述
contains(a, element) → boolean	判断element是否出现在数组a中。
element_at(a, index)	返回数组a中的第index个元素。如果'index < 0'将从后往前找。
filter(array(T), function(T, boolean)) → array(T)	筛选满足条件的元素组成新数组。
none_match(array(T), function(T, boolean)) → boolean	询问是否所有元素都不满足给定函数。
reverse(a) → array	把数组a前后取反。
sequence(start, stop, step)	和python的range效果类似。
shuffle(a) → array	把数组a的元素打乱。
slice(a, start, length) → array	截取数组a从start开始长度为length的子串。
transform(array(T), function(T, S)) → array(S)	把原数组变换成另一个数组。

表 8-31 聚合函数

函数	功能描述
arbitrary(x)	返回任意一个非NULL的元素（如果存在的话）。
array_agg(x) → array	把元素合并成一个数组返回。
avg(x)→ double	返回算术平均数。
bool_and/bool_or(x) → boolean	对每个元素执行布尔AND/OR。
coalesce(value1, value2, ...)	返回第一个非NULL的元素。会被短路。
count(*)/count(x) → int	计数。
greatest(value1, value2, ..., valueN)	返回给定同类型权值里最大的权值。
histogram(x) → map	返回一个map，统计了x里每个不同的权值以及他们对应的个数。
least(value1, value2, ..., valueN)	返回给定同类型权值里最小的权值。
max/min(x, n=1)	返回元素里的最大/小值，第n大/小值。
max_by/min_by(x, y, n=1)	根据元素y的最大/小值或第n大/小值，返回对应的元素x。
geometric_mean(x) → double	返回几何平均数。
set_agg(x) → array	把元素去重后合并成一个数组返回。

函数	功能描述
set_union(x) → array	把每个读入的数组的元素求并，返回并集的数组。
sum(x)	返回和。
multimap_agg(key, value)	返回从输入键/值对创建的多重映射。
map_agg(key, value)	返回从输入键/值对创建的映射。

表 8-32 时间函数

函数	功能描述
now() → date	获取当前时间。
date_diff(unit, timestamp1, timestamp2) → int	返回timestamp2-timestamp1在unit下的时间间隔，unit的可选值：millisecond、second、minute、hour、day、week、month、quarter、year。
date_parse(string, format) → timestamp	通过指定格式format，将字符串转为时间格式。

9 修订记录

版本日期	变更说明
2023-12-13	第十七次正式发布。 本次变更如下： **系统内置预设策略**章节内容优化。
2023-11-20	第十六次正式发布。 新增： ● **组织合规规则包**相关内容。 ● **跨账号授权**新增资源记录器支持转储到加密的OBS桶的相关内容。
2023-10-11	第十五次正式发布。 新增： ● **查看资源合规**章节。 ● **查看不合规资源**章节。
2023-08-18	第十四次正式发布。 新增**合规规则包**特性：合规规则包是多个合规规则的集合，帮助您统一创建和管理合规规则，并统一查询合规性数据。
2023-06-07	第十三次正式发布。 本次变更如下： 服务名称变更：“资源管理服务 RMS”更名为“配置审计 Config”。
2023-04-12	第十二次正式发布。 新增： ● **组织合规规则**章节。 ● **查看聚合的合规规则**章节。 ● **高级查询**章节。

版本日期	变更说明
2023-03-10	第十一次正式发布。 本次变更如下： ● “我的资源”特性更名为“资源清单”。
2023-02-17	第十次正式发布。 新增： ● **事件监控**章节。 ● **资源聚合器**章节。
2022-12-30	第九次正式发布。 新增“自定义策略”特性： ● **添加自定义合规规则**； ● **示例函数(Python)**； ● **事件**。
2022-08-24	第八次正式发布。 新增**跨账号授权**：配置资源记录器时支持跨账号授予SMN主题和OBS桶权限。
2022-04-06	第七次正式发布。 新增：“高级查询”特性： ● **高级查询**：高级查询概述，高级查询使用限制，新建查询，查看查询，修改查询，删除查询。 ● **ResourceQL语法**：语法概览，语法文档，函数列表。
2021-09-09	第六次正式发布。 新增：**“资源清单”页面中怎么无法删除资源？**章节。
2021-07-16	第五次正式发布。 本次变更如下： Console产品目录变更：中文“管理与部署”入口更名为“管理与监管”，英文“计算”入口更名。
2020-12-28	第四次正式发布。 新增： ● **云审计-记录配置审计**章节。 ● **支持云审计的关键操作**。 ● **查询审计事件**。
2020-12-16	第三次正式发布。 新增：**常见问题**。

版本日期	变更说明
2020-12-14	第二次正式发布。 新增：“资源变更消息存储”特性： ● **资源变更消息存储**； ● **资源变更消息存储完成的消息通知模型**； ● **资源变更消息存储模型**。
2020-11-30	第一次正式发布。 ● **资源清单**：查看资源，筛选资源，导出资源，查看资源关系，查看资源历史。 ● **资源记录器**：开启资源记录器，配置资源记录器，修改资源记录器。 ● **资源合规**：添加合规规则，触发合规规则，编辑合规规则。

