配置审计

用户指南

文档版本 01

发布日期 2025-02-27

华为云计算技术有限公司

商标声明


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

注意

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

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

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，或Config暂不支持该服务或资源类型。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”页面默认展示在资源记录器配置的监控范围内且您拥有的全部资源信息。

图 1-1 资源清单默认页面

步骤3 您可以通过关闭“仅显示有资源的服务和区域”开关，并单击“更多服务”以查看配置审计支持服务的完整列表。

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。

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 1-3 查看资源概览和详情

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。
资源状态	通过资源状态对资源进行筛选。 资源状态分为以下两种： ● 保有中：资源正常使用中。 ● 已删除：资源已删除。
标签	直接在搜索框列表中选择一个标签键，然后再选择此标签键相关的一个标签值或所有标签值，资源列表将自动筛选并展示此标签关联的资源。

筛选条件	说明
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**开通企业中心**才可以使用，因此该筛选条件并非对每个用户可见。

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、资源状态、标签和企业项目筛选出您需要查看的资源。

图 1-4 筛选资源

----结束

1.1.4 导出资源列表

操作场景

在“资源清单”页面您可以导出资源列表中的资源信息。

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 单击列表左上方的“导出资源列表”按钮，导出列表中的资源信息。

导出资源列表功能仅会导出资源列表中展示资源的相关信息：

- 如未在“资源清单”页面进行任何筛选和搜索操作，由于资源列表默认展示Config支持且您拥有的全部资源，则将导出Config支持且您拥有的全部资源信息。
- 在“资源清单”页面通过选择服务、资源类型和区域来筛选资源，或通过在页面中部的搜索框进行更精细的资源搜索，则仅会导出筛选和搜索出的资源信息。如何筛选资源请参见**筛选资源**。

图 1-5 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上报Config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。

在规则列表上方的搜索框中，可以通过规则名称、规则ID、触发类型、最后一次评估时间和合规评估结果对规则进行筛选。

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 1-6 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。仅Config支持的资源关系才会在资源概览页的“关联资源”页签中显示，请参阅**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。

在每个关联资源的服务框中，支持按照资源ID或名称对资源进行搜索。

图 1-7 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，才会记录对接服务资源上报Config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。对接服务上报Config的资源属性和资源关系的变化，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。

说明

资源历史中记录的资源关系仅支持最大1000条资源关系。

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“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”来查看对接服务上报Config的资源属性的当前情况。

图 1-8 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且Config支持的云服务资源变更情况。

资源记录器可以为您提供以下功能：

- 当您开启并配置消息通知SMN主题后，在资源被创建、修改或删除时发送通知给您；
- 当您开启并配置消息通知SMN主题后，在Config支持的资源关系发生变更时发送通知；
- 当您开启并配置资源转储OBS桶和消息通知SMN主题后，对资源变更消息进行定期（6小时）存储；
- 当您开启并配置资源转储OBS桶后，对资源快照进行定期（24小时）存储。

资源记录器支持监控的资源请参阅**支持的服务和区域**。

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。其中主题是可选配置的，但如果您先配置了SMN主题，则也可以不配置资源转储（OBS桶）。
- 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。具体请参见**创建主题**、**添加订阅**和**请求订阅**。
- 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）。
- 当前每天仅支持最多开启和修改资源记录器10次，每天0点将重置此次数。
- 已对接Config的服务的资源数据同步到Config存在延迟，不同服务的延迟时间并不相同。对于已开启资源记录器且在监控范围内的资源，Config会在24小时内校正资源数据。如未开启资源记录器，或相关资源不在资源记录器配置的监控范围内，则Config不会校正这些资源的数据。

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、合规规则无法创建、修改、启用和触发规则评估、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。

当前每天仅支持最多开启和修改资源记录器10次，每天0点将重置此次数。

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的资源转储和主题功能后，当对接服务上报Config的资源变更（被创建、修改、删除等）、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 单击左侧导航栏的“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“确定”，资源记录器开启成功。

图 2-1 开启资源记录器

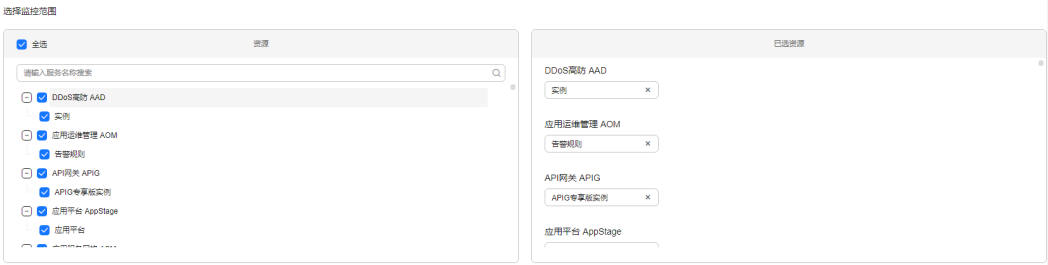
步骤5 选择资源的监控范围。

默认情况下，资源记录器的监控范围会覆盖当前Config支持的全部资源。您可以根据需要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。

说明

资源记录器默认收集Config服务的所有资源数据，不支持取消勾选的操作。

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。

如果您先配置了SMN主题，则也可以不配置资源转储（OBS桶）。

- **配置当前账号下OBS桶：**

  选择“您账号的桶”，然后在下拉列表中选择您账号下的OBS桶，用于存储资源变更消息及资源快照。如果您需要将资源变更消息及资源快照存储在OBS桶内的某个文件夹下，则在选择OBS桶后，还需输入“桶前缀”，该前缀指OBS桶内某个文件夹的名称。如您的账号下无OBS桶，则需先创建OBS桶，详见**创建桶**。

- **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，如果您需要将资源变更消息及资源快照存储在OBS桶内的某个文件夹下，则还需输入“桶前缀”，该前缀指OBS桶内某个文件夹的名称。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，此文件仅用于验证资源转储是否能够成功写入OBS桶。当界面出现报错信息时，如何处理请参见**为什么开启并配置资源记录器后，将数据转储至当前账号或其他账号的OBS桶时报错？**。

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。

如果您后续对数据保留周期进行了修改，此时新生成的资源数据将按照您新设置的保留周期进行存储，历史资源数据还将按照之前设置的数据保留周期进行存储。例如您先将数据保留周期设置为100天，此时生成的资源数据将保留100天，后续又将数据保留周期修改为30天，此时新生成的资源数据将保留30天，但修改数据保留周期之前生成的资源数据还是会保留100天。

图 2-4 配置数据保留周期

步骤8 （可选）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**创建主题**。

- **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，关于主题URN的详细信息请参见**基本概念**。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。

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**。

  如何为委托添加权限请参见**删除或修改委托**。
- **自定义授权：**您可自行在统一身份认证服务（IAM）中创建委托，并进行自定义授权，授权对象为云服务Config，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）的写入权限至少包含一个）。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**委托其他云服务管理资源**。

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“确定”，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“确定”，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。
  如未对待授权账号进行授权，则该账号将无法通过此SMN主题接收资源变更消息通知。
- **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。

桶策略的示例如下，配置该桶策略，将允许被授权账号的资源记录器将转储文件存放至本OBS桶的指定路径内，以下参数需要您根据实际使用场景手动替换：

- ${account_id}：需要被授权的账号的账号ID（domain_id）；
- ${agency_name}：被授权的委托名称，如果您使用快速授权方式，则该值为“rms_tracker_agency”；
- ${bucket_name}：用于存储文件的OBS桶的桶名；
- ${folder_name}：用于存储文件的OBS桶内文件夹的名称。如果您未设置OBS桶内文件夹，则需删除“/${folder_name}”。

```
{
  "Statement": [
    {
      "Sid": "org-bucket-policy",
      "Effect": "Allow",
      "Principal": {
        "ID": [
          "domain/${account_id}:agency/${agency_name}"
        ]
      },
      "Action": [
        "PutObject"
      ],
      "Resource": [
        "${bucket_name}/${folder_name}/RMSLogs/*/Snapshot/*",
        "${bucket_name}/${folder_name}/RMSLogs/*/Notification/*"
      ]
    }
  ]
}
```

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”、“查询密钥信息”和“解密数据密钥”。

2.3 基于组织批量配置资源记录器

操作场景

当前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。

如果您是组织管理员，您可以基于Terraform模板和RFS资源栈集批量为组织成员账号开启并配置资源记录器，而无需登录每个账号进行操作。在组织成员账号较多且均需使用Config服务的场景下，使用此功能将有助于您提升配置效率，减少复杂繁琐的操作。

本章节提供基于组织批量开启并配置资源记录器的操作流程和配置示例，帮助您快速了解和使用该功能。

操作流程

操作流程	说明
步骤一：启用RFS可信服务	在Organizations可信服务列表中启用“资源编排资源栈集服务（RF）”为可信服务。
步骤二：配置OBS桶策略	为OBS桶设置桶策略，授权组织内成员账号的资源记录器可将转储文件存放至此OBS桶。
步骤三：配置SMN主题策略	为SMN主题设置主题访问策略，授权组织内成员账号的资源记录器可通过此主题发送消息。
步骤四：创建RFS资源栈集	使用Terraform模板创建RFS资源栈集，向组织成员账号部署资源栈实例，用于启用和配置资源记录器。

约束与限制

- 当前单个RFS资源栈集最多仅支持开启100个组织成员账号的资源记录器。
- 仅组织管理员可以创建资源栈集。
- 创建资源栈集仅会在组织成员账号下部署资源栈，不会在组织管理员账号下部署资源栈。
- 当组织成员账号在资源栈集部署前已开启并配置了资源记录器，则通过资源栈集下发的配置不会覆盖成员账号当前的资源记录器配置。

步骤一：启用 RFS 可信服务

使用此功能前需先开启RFS可信服务，具体步骤如下：

步骤1 以组织管理员账号登录管理控制台，进入“组织 Organizations”服务。

步骤2 单击左侧导航栏的“可信服务”，进入“可信服务”页面。

步骤3 在列表中单击“资源编排资源栈集服务（RF）”操作列的“启用”。

步骤4 在弹出的确认框中单击“确定”，RFS可信服务启用成功。

图 2-9 启用可信服务

----结束

步骤二：配置 OBS 桶策略

说明

当您配置的资源转储OBS桶的桶策略为“公共读写”时，表示任何用户都可以对该OBS桶内对象进行读/写/删除操作，则无需执行此步骤。

开启资源记录器时需配置资源转储OBS桶，用于存储资源变更消息及资源快照。如无OBS桶，则需先**创建桶**。

在当前场景下，您需要为OBS桶设置桶策略，授权组织内成员账号的资源记录器可将转储文件存放至此OBS桶的指定路径内，具体请参见如下步骤：

步骤1 用授权账号登录管理控制台，进入OBS管理控制台。

授权账号指OBS桶所属的账号。

步骤2 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。

桶策略的示例如下，配置该桶策略，将允许被授权组织成员账号的资源记录器将转储文件存放至本OBS桶的指定路径内，以下参数需要您根据实际使用场景手动替换：

- ${account_id}：需要被授权的组织成员账号的账号ID（domain_id），多个账号ID之间以英文逗号分隔；
- ${agency_name}：被授权的自定义委托的名称。如何创建委托详见**委托其他云服务管理资源**，授权对象为云服务Config；
- ${bucket_name}：用于存储文件的OBS桶的桶名；
- ${folder_name}：用于存储文件的OBS桶内文件夹的名称。如果您未设置OBS桶内文件夹，则需删除“/${folder_name}”。

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

```
  {
    "Sid": "org-bucket-policy",
    "Effect": "Allow",
    "Principal": {
      "ID": [
        "domain/${account_id}:agency/${agency_name}"
      ]
    },
    "Action": [
      "PutObject"
    ],
    "Resource": [
      "${bucket_name}/${folder_name}/RMSLogs/*/Snapshot/*",
      "${bucket_name}/${folder_name}/RMSLogs/*/Notification/*"
    ]
  }
 ]
}
```

说明

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”中时，还需参见**资源变更消息和资源快照转储至OBS加密桶**设置密钥的跨账号权限，其中待授权账号需输入组织成员账号的账号ID（domain_id）。

----结束

步骤三：配置 SMN 主题策略

开启资源记录器时需配置SMN主题，当资源发生变更时，消息通知会推送消息到您所配置的SMN主题。如无SMN主题，则需先**创建主题**。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。

在当前场景下，您需要为SMN主题设置主题访问策略，授权组织内成员账号的资源记录器可通过此主题发送消息，具体请参见如下步骤：

步骤1 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。

授权账号指SMN主题所属的账号。

步骤2 参考**设置主题策略**对待授权账号授予相关SMN主题的权限。

其中“可发布消息的用户”选择“仅如下用户”，并依次输入组织成员账号的ID。

如未对某个成员账号进行授权，则该成员账号将无法通过此SMN主题接收资源变更消息通知。

----结束

步骤四：创建 RFS 资源栈集

步骤1 以组织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“资源编排服务 RFS”。

步骤3 单击左侧导航栏的“资源栈集”，进入“资源栈集”页面。

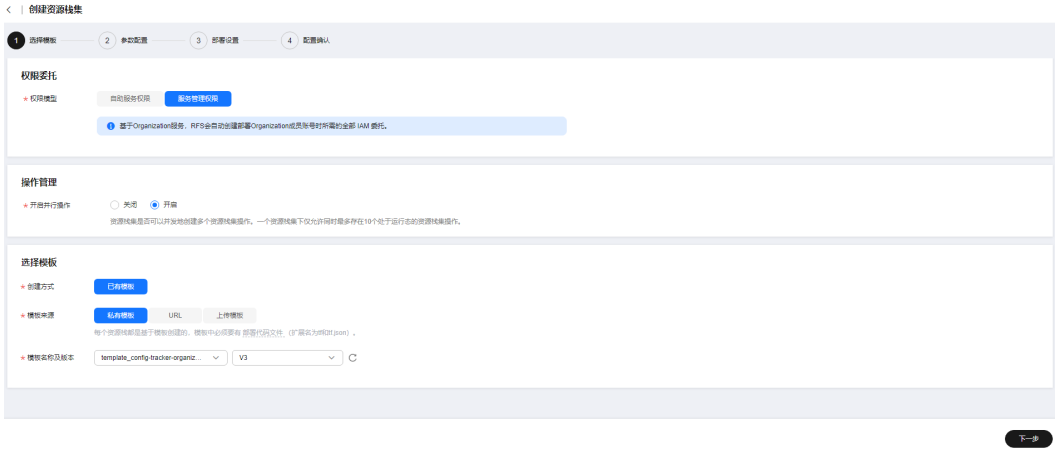
步骤4 单击页面右上角的“创建资源栈集”。

图 2-10 创建资源栈集

步骤5 进入“选择模板”页面，根据如下示例完成配置后，单击“下一步”。

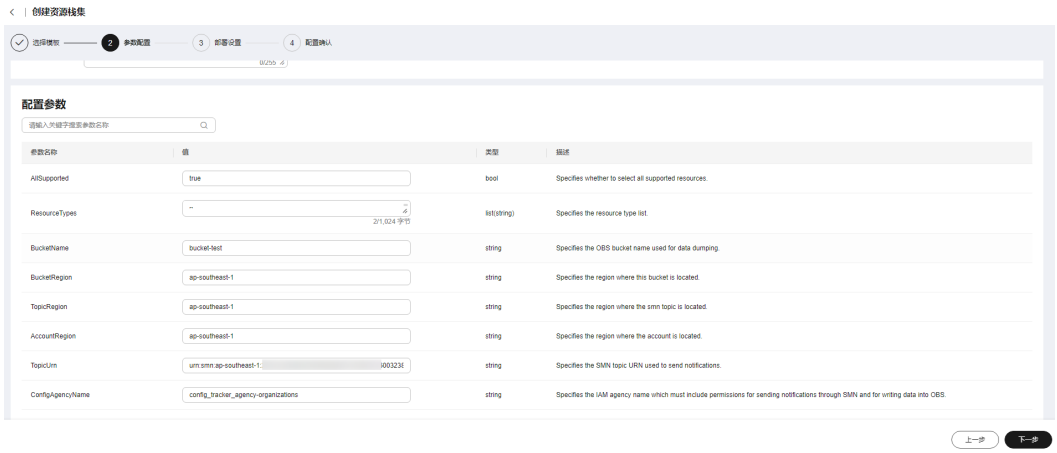
- 权限模型：选择“服务管理权限”。
- 开启并行操作：选择“关闭”或“开启”均可。 推荐选择“开启”，将提高资源栈的运行速度。
- 选择模板：根据需要选择任意模板来源。模板的内容请参见“**Terraform模板内容**”。

图 2-11 选择模板



步骤6 进入“参数配置”页面，根据如下示例完成配置后，单击“下一步”。

图 2-12 参数配置

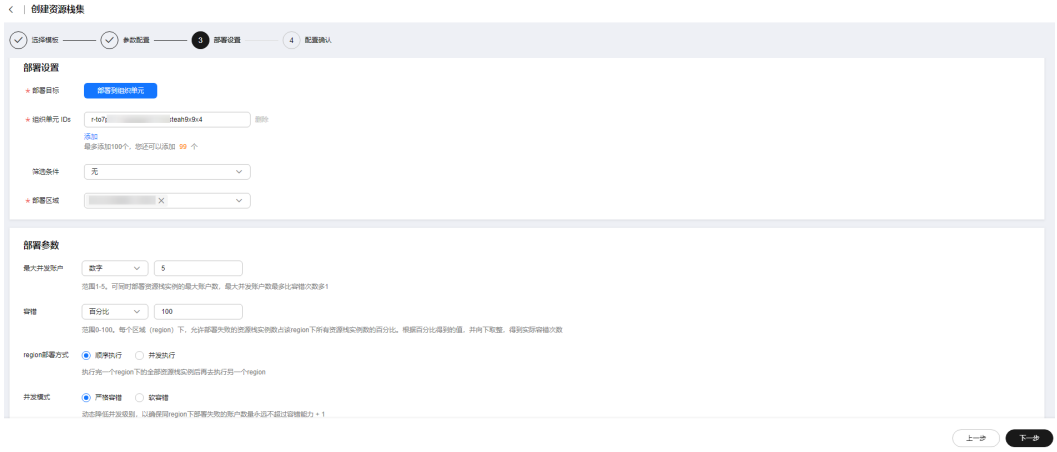


- 资源栈集名称：使用系统自动生成的名称或自定义，不可与已有资源栈集名称重复。
- 配置参数

- AllSupported：（必选，Bool类型）指定是否记录Config所有支持的资源类型，可选值为“true”和“false”。
- ResourceTypes：（可选，列表类型）指定资源类型列表。当AllSupported设置为“false”时，此处需输入具体的资源类型，例如["vpc.vpcs", "rds.instances"]。
- BucketName：（必选，字符串类型）指定用于资源转储的OBS桶的名称。
- BucketRegion：（必选，字符串类型）指定该OBS桶所在的区域。
- AccountRegion：（必选，字符串类型）指定账号所在的站点，输入cn-north-4表示组织内账号均属于中国站，输入ap-southeast-1表示组织内账号均属于国际站。
- TopicUrn：（必选，字符串类型）指定用于发送消息通知的SMN主题URN。
- TopicRegion：（必选，字符串类型）指定该SMN主题所在的区域。
- ConfigAgencyName：（必选，字符串类型）指定自定义IAM委托的名称。此委托必须包含可以让资源记录器正常工作的权限（调用SMN发送通知的权限和OBS的写入权限）。

步骤7 进入“部署设置”页面，根据如下示例完成配置后，单击“下一步”。

图 2-13 部署设置



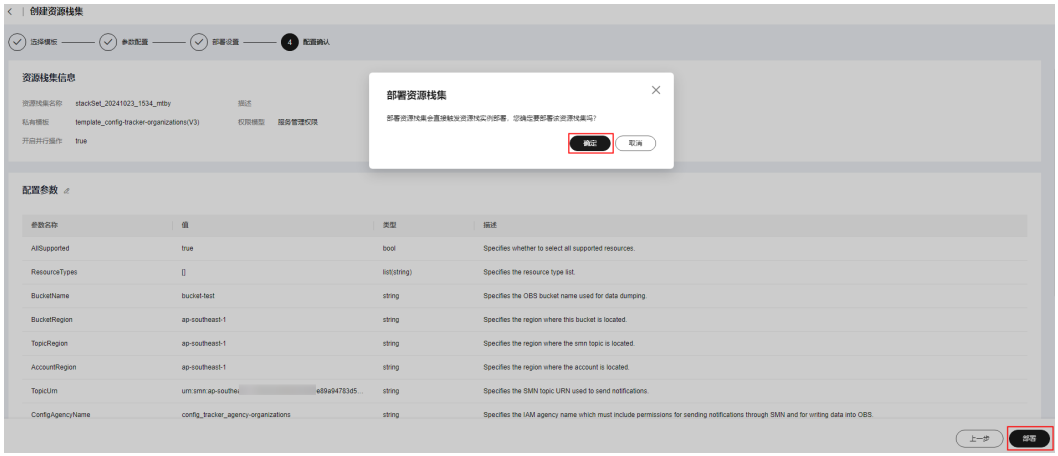
- 部署设置
  - 组织单元IDs：输入组织单元（OU）的ID。当指定根组织单元（Root）的ID时，表示资源栈集将部署于整个组织。
  - 筛选条件：根据需要筛选条件，用于筛选部署的账号。
  - 部署区域：选择资源栈集部署的区域。
- 部署参数
  - 最大并发账户：建议选择“数字”类型，值设置为5。
  - 容错：建议选择“百分比”类型，值设置为100。
  - Region部署方式和并发模式根据界面提示按需选择。

步骤8 进入“配置确认”界面，确认资源栈集配置无误后，单击“部署”。

步骤9 在弹出的确认框中单击“确定”，资源栈集部署成功。

资源栈集会向所选组织成员账号中均部署一个资源栈实例，部署完成后，组织成员账号的资源记录器将会被开启并基于Terraform模板内容进行配置。

图 2-14 部署资源栈集



说明

资源栈集创建并部署成功后，所部署的组织成员账号随时可以修改和关闭自身的资源记录器。您也可以随时**更新资源栈集**和**删除资源栈集**，删除资源栈集后，所部署成员账号的资源记录器均将被关闭。

----结束

Terraform 模板内容

Terraform模板示例如下，您可以使用此模板的内容创建RFS私有模板，或在本地保存为tf格式的文件，用于在创建资源栈集时选择此模板：

```
terraform {
  required_providers {
    huaweicloud = {
      source  = "huawei.com/provider/huaweicloud"
      version = ">=1.49.0"
    }
  }
}

provider "huaweicloud" {
}

variable "AllSupported" {
  description = "Specifies whether to select all supported resources."
  type        = bool
  default     = true

  validation {
    condition     = can(regex("^(true|false)$", var.AllSupported))
    error_message = "Must be true or false."
  }
}

variable "ResourceTypes" {
  description = "Specifies the resource type list. "
  type        = list(string)
  default     = []
}

variable "BucketName" {
  description = "Specifies the OBS bucket name used for data dumping."
  type        = string
}
```

```
variable "BucketRegion" {
  description = "Specifies the region where this bucket is located."
  type        = string
}

variable "TopicRegion" {
  description = "Specifies the region where the smn topic is located."
  type        = string
}

variable "AccountRegion" {
  description = "Specifies the region where the account is located."
  type        = string
}


variable "TopicUrn" {
  description = "Specifies the SMN topic URN used to send notifications."
  type        = string
}

variable "ConfigAgencyName" {
  description = "Specifies the IAM agency name which must include permissions for sending notifications
through SMN and for writing data into OBS."
  type        = string
}

data "huaweicloud_identity_projects" "CurrentAccountProject" {
  name = var.AccountRegion
}

resource "huaweicloud_identity_agency" "identity_agency" {
  name                  = var.ConfigAgencyName
  delegated_service_name = "op_svc_eps"
  all_resources_roles = ["SMN Administrator", "OBS Administrator", "KMS Administrator"]
}

resource "huaweicloud_rms_resource_recorder" "ConfigRecorder" {
  agency_name = var.ConfigAgencyName

  selector {
    all_supported  = var.AllSupported
    resource_types = var.ResourceTypes
  }

  obs_channel {
    bucket = var.BucketName
    region = var.BucketRegion
  }

  smn_channel {
    region = var.TopicRegion
    topic_urn = var.TopicUrn
    project_id = data.huaweicloud_identity_projects.CurrentAccountProject.projects[0].id
  }
  depends_on = [huaweicloud_identity_agency.identity_agency]
}
```

2.4 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的详细使用说明请参见**《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**。

2.5 资源快照存储

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。

无论是将资源快照文件存储至您账号的桶还是另一账号的桶，该文件在OBS桶内存放的路径均为：${bucket_name}/${bucket_prefix}/RMSLogs/${account_id}/Snapshot/${year}/${month}/*。此路径中的每个字段在控制台上均表示一个文件夹层级的名称，在OBS控制台进入相关桶的“对象”页面，然后按照上述路径所示查找资源快照存储文件，其中*表示文件名称。

资源快照存储文件的名称由账号ID、存储文件类型、OBS桶所在区域的ID、存储时间、随机生成的字符串、拆分文件的序号组成。每个文件最多存储2000个资源的信息，超出后将拆分为多个文件，此时文件名称中才会出现拆分文件的序号（例如part-1），“.json.gz”表示该文件的存储类型为JSON格式的压缩包。

文件名称示例如下：0926901ef980f2150fbdc001fdd23e80_Snapshot_me-east-1_ResourceSnapshot_2024-07-22T221441Z_90decead-b69b-4522-a090-657d8c299d40_part-1.json.gz。

关于OBS的详细使用说明请参见**列举对象**。

说明

当前用户的资源有保有中（Normal）和已删除（Deleted）两种状态，资源记录器仅会转储资源状态为保有中（Normal）的资源快照文件，不会转储状态为已删除（Deleted）的资源快照文件。

如果您想了解关于资源快照存储的后台代码示例，请参见**资源存储模型**。

2.6 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。

无论是将资源变更消息文件存储至您账号的桶还是另一账号的桶，该文件在OBS桶内存放的路径均为：${bucket_name}/${bucket_prefix}/RMSLogs/${account_id}/Notification/${year}/${month}/*"。此路径中的每个字段在控制台上均表示一个文件夹层级的名称，在OBS控制台进入相关桶的“对象”页面，然后按照上述路径所示查找资源变更消息存储文件，其中*表示文件名称。

资源变更消息存储文件的名称由账号ID、存储文件类型、OBS桶所在区域的ID、资源发生变更的服务和资源类型、存储时间组成。每个资源变更消息存储文件仅会存储一种资源的变更消息，如多个资源类型均有变更，则会分多个文件分别存储，“.json.gz”表示该文件的存储类型为JSON格式的压缩包。

文件名称示例如下：0926901ef980f2150fbdc001fdd23e80_Notification_me-east-1_NotificationChunk_OBS_BUCKETS_2024-07-24T214735Z_2024-07-24T214759Z.json.gz

关于OBS的详细使用说明请参见**列举对象**。

关于SMN的详细使用说明请参见**《消息通知服务用户指南》**。

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**。

2.7 资源记录器事件监控

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亚太-新加坡区域。

资源记录器目前支持的系统事件如下表所示：

表 2-1 资源记录器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	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

资源合规支持的配置审计（Config）事件请参见：**资源合规事件监控**。

3 资源合规

3.1 资源合规概述

概述

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。

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，您还可以添加组织类型的资源合规规则，直接作用于您组织内账号状态为“正常”的所有成员账号中。

针对合规规则评估出的不合规资源，合规修正功能可以帮助您设置基于合规规则的修正配置，通过关联RFS服务的私有模板或FunctionGraph服务的函数实例，按照您自定义的修正逻辑对不合规资源进行快速修正，确保您的云上资源持续合规。

约束与限制

- 每个账号最多可以添加500个合规规则（包括由组织合规规则和合规规则包创建的托管规则）。
- 添加、修改、启用合规规则和触发规则评估需要开启资源记录器，资源记录器处于关闭状态时，合规规则仅支持查看、停用和删除操作。

  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**。
- 添加、修改组织合规规则和触发规则评估需要开启资源记录器，资源记录器处于关闭状态时，组织合规规则仅支持查看和删除操作。
- 非组织内账号无法在Config控制台的“资源合规”页面中看到“组织规则”页签。
- 组织合规规则仅会下发至账号状态为“正常”的组织成员账号中，且组织成员账号需开启资源记录器，否则将导致部署异常。

- 当前仅用户自行创建的预定义或自定义合规规则支持修正配置，通过组织合规规则或合规规则包创建的托管合规规则不支持修正配置。
- 基于RFS服务私有模板执行修正的场景下，对应区域的资源栈应至少预留5个配额，否则执行修正可能会因配额不足导致失败。
- 一个合规规则上只能创建一个修正配置。
- 当合规规则存在修正配置，则必须删除修正配置并且停用规则后，才可删除此合规规则。
- 单个合规规则的修正配置最多支持用户手动添加100个修正例外资源，基于设置的修正重试规则被自动添加至修正例外的资源没有配额限制。

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：

- 如您未开启资源记录器，则资源合规规则无法评估任何资源数据。历史的合规规则评估结果依然存在。
- 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。

关于如何开启并配置资源记录器请参见：**配置资源记录器**。

3.2 资源合规规则

3.2.1 添加预定义合规规则

操作场景

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。
- 添加、修改、启用合规规则和触发规则评估需要开启资源记录器，资源记录器处于关闭状态时，合规规则仅支持查看、停用和删除操作。

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：

- 如您未开启资源记录器，则资源合规规则无法评估任何资源数据。历史的合规规则评估结果依然存在。
- 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。

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。

步骤5 基础配置完成后，单击页面右下角的“下一步”。

图 3-1 基础配置

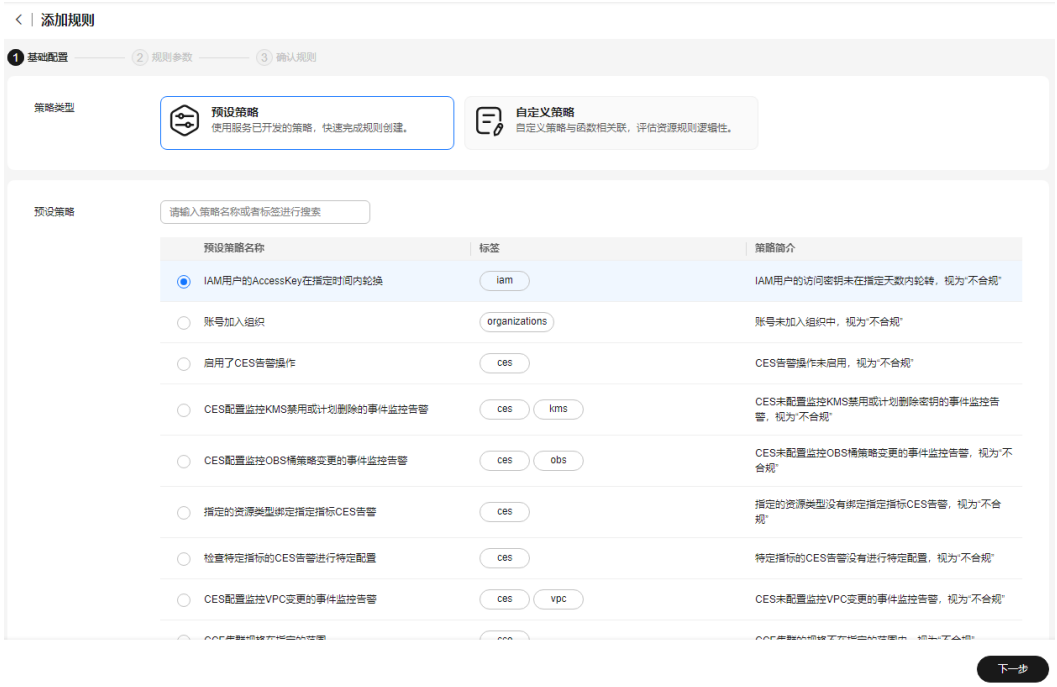


表 3-1 基础配置参数说明

参数	说明
策略类型	选择“预设策略”。 预设策略即服务已开发的策略，在下方的预设策略列表中直接选择所需预设策略，快速完成规则创建。支持输入策略名称或标签进行搜索。 预设策略详见**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，最大长度64个字符。
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。 目前对规则简介内容的字符类型不做限制，最大长度512个字符。

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”。

图 3-2 规则参数

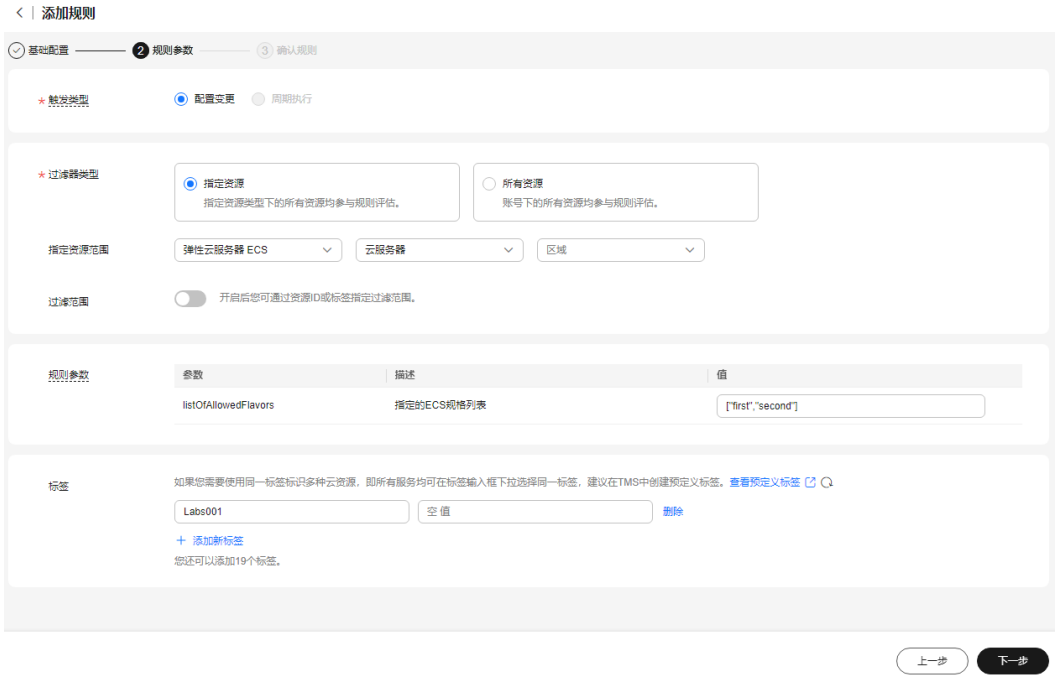


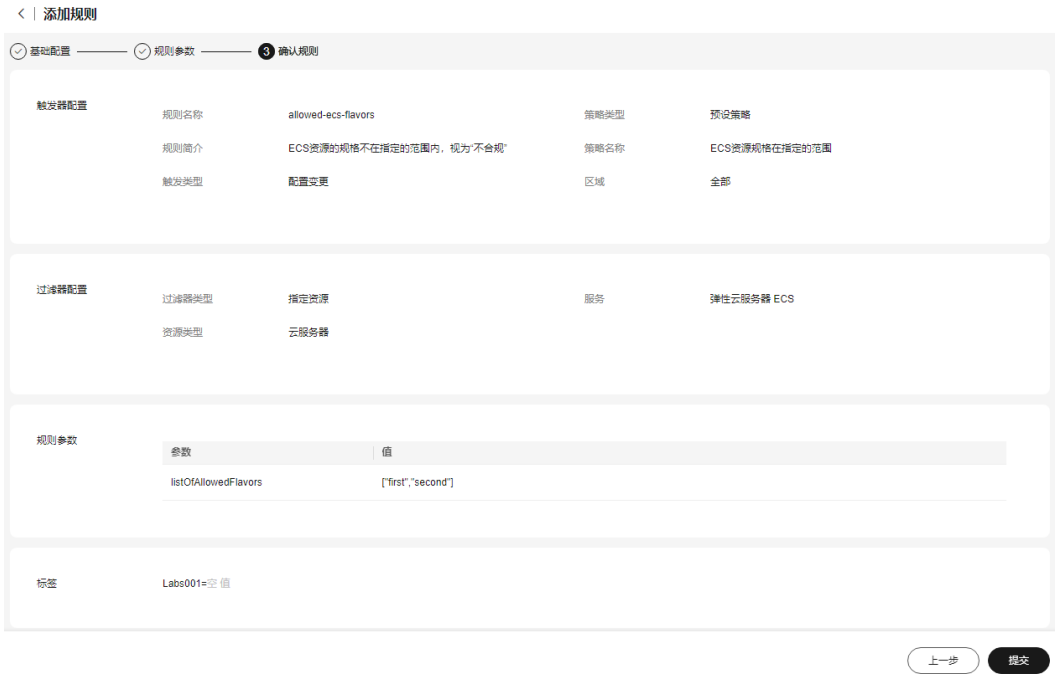
表 3-2 合规规则参数说明

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。 **说明** 预设策略的触发类型不支持修改，不同预设策略支持的触发类型不同。
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。

参数	说明
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。 **说明** ● 仅当“触发类型”为“配置变更”时支持指定服务和资源类型。 ● 当预设策略的“触发类型”为“周期执行”，且规则评估的资源类型非“account”时，支持指定资源所在的“区域”进行过滤。具体请以控制台显示为准或参见**预设策略列表**。
过滤范围（可选）	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。 当“触发类型”为“配置变更”时，您可以根据需要选择配置此参数。
周期频率	设置合规规则周期执行的频率。 可选项：1小时、3小时、6小时、12小时、24小时。 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”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“资源具有指定的标签”，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：已挂载的云硬盘开启加密（volumes-encrypted-check）。
标签	单击“添加新标签”，输入标签键和标签值，为合规规则添加标签。每个合规规则最多可以添加20个标签。 ● 标签键不能为空，可以包含任意语种的字母、数字和空格，以及_.:=+-@字符，但首尾不能包含空格，且不能以_sys_开头。长度不超过128个字符。 ● 标签值可以为空，可以包含任意语种的字母、数字和空格，以及_.:=+-@字符，但首尾不能包含空格。长度不超过255个字符。

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

3.2.2 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FunctionGraph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。

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**。

约束与限制

- 每个账号最多可以添加500个合规规则。
- 添加、修改、启用合规规则和触发规则评估需要开启资源记录器，资源记录器处于关闭状态时，合规规则仅支持查看、停用和删除操作。

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：

- 如您未开启资源记录器，则资源合规规则无法评估任何资源数据。历史的合规规则评估结果依然存在。
- 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。

关于如何开启并配置资源记录器请参见：**配置资源记录器**。

创建 FunctionGraph 函数

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“计算”下的“函数工作流 FunctionGraph”。

步骤3 在左侧的导航栏选择“函数 > 函数列表”。

步骤4 单击右上方的“创建函数”，进入“创建函数”页面。

步骤5 选择“创建空白函数”，“函数类型”选择“事件函数”，并配置函数名称、IAM委托等其他参数。

IAM委托授权给函数工作流（FunctionGraph），且需要包含权限“rms:policyStates:update”。

步骤6 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7 在代码框中写入评估函数内容，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8 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9 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。

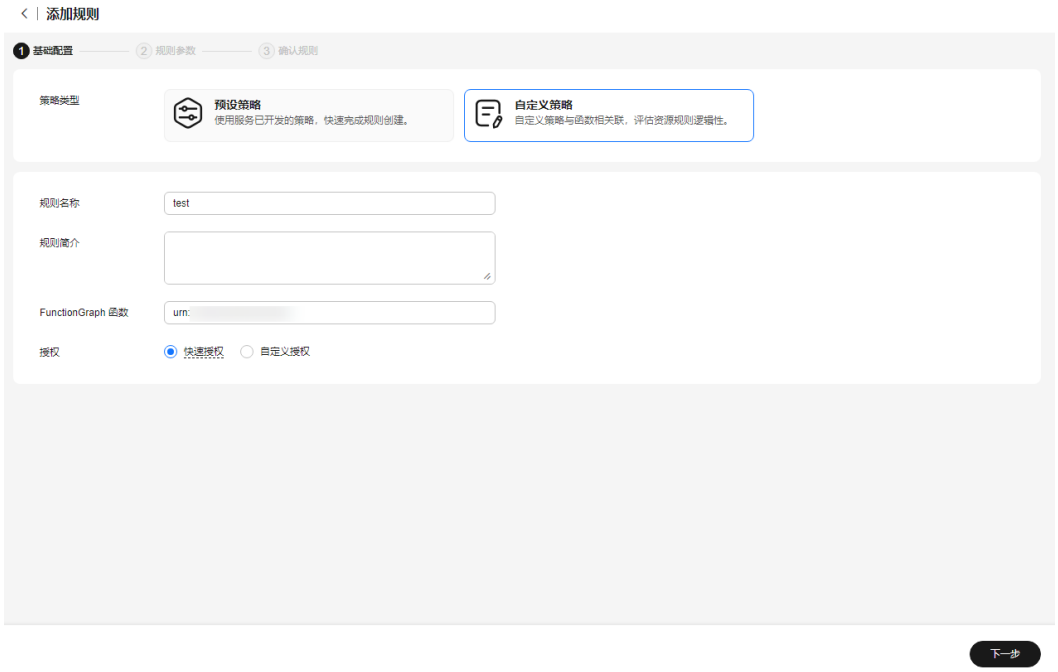
步骤4 单击页面中部的“添加规则”，进入“基础配置”页面。

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，配置完成后单击“下一步”。

表 3-3 基础配置参数说明

参数	说明
策略类型	选择“自定义策略”。 允许用户通过自定义策略来创建合规规则。
规则名称	合规规则的名称，不能与已存在的合规规则名称重复。 合规规则名称仅支持数字、字母、下划线和中划线，最大长度64个字符。
规则简介	合规规则的简介，目前对规则简介内容的字符类型不做限制，最大长度512个字符。
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**。 **说明** 如何获取FunctionGraph函数的URN可参考如下方法： • 进入函数工作流控制台，在左侧的导航栏选择“函数 > 函数列表”，单击列表中需使用函数操作列的“复制URN”即可获取。 • 进入函数工作流控制台，在左侧的导航栏选择“函数 > 函数列表”，单击列表中需使用函数的函数名称，进入函数详情页，在函数概述部分右侧显示“函数URN”。
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。 **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，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（调用函数工作流（FunctionGraph）的获取函数和异步执行函数的权限），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 基础配置



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”。

图 3-5 规则参数

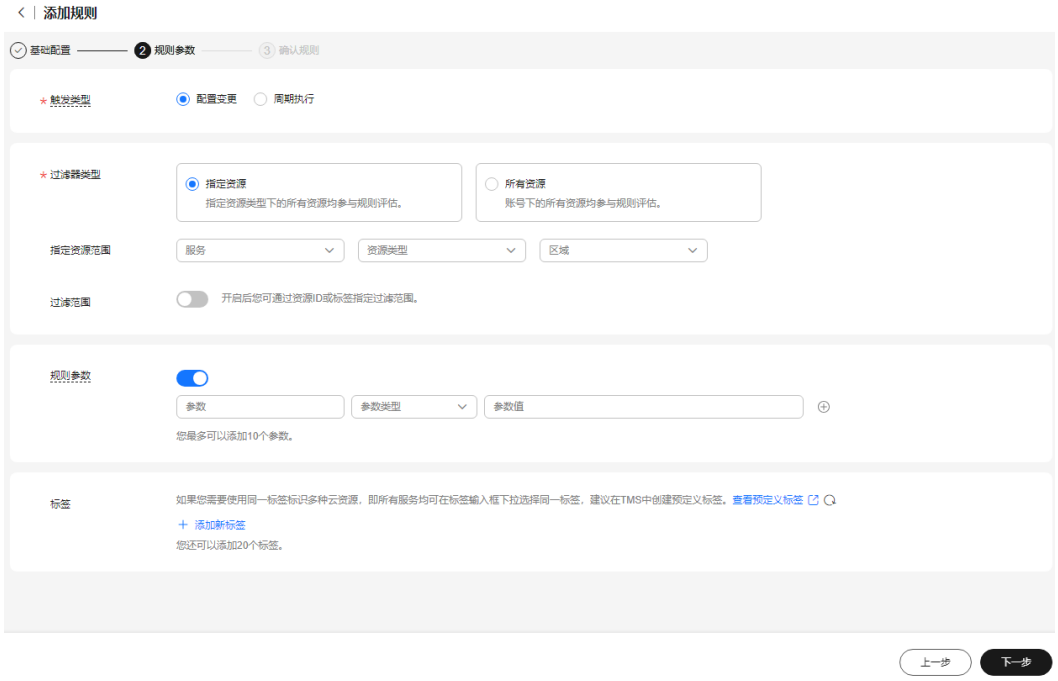


表 3-4 合规规则参数说明

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”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”，且“过滤器类型”为“指定资源”时需配置此参数。
过滤范围（可选）	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。 当“触发类型”为“配置变更”时，您可以根据需要选择配置此参数。
周期频率	设置合规规则周期执行的频率。 可选项：1小时、3小时、6小时、12小时、24小时。 仅当“触发类型”为“周期执行”时需配置此参数。
规则参数	自定义策略的规则参数最多可以设置10个，由您自行配置。
标签	单击“添加新标签”，输入标签键和标签值，为合规规则添加标签。每个合规规则最多可以添加20个标签。 ● 标签键不能为空，可以包含任意语种的字母、数字和空格，以及_.:=+-@字符，但首尾不能包含空格，且不能以_sys_开头。长度不超过128个字符。 ● 标签值可以为空，可以包含任意语种的字母、数字和空格，以及_.:=+-@字符，但首尾不能包含空格。长度不超过255个字符。

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。

说明

合规规则创建后会立即自动触发首次评估。

----结束

3.2.3 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、标签、修正配置和规则详情配置等信息。

规则的评估结果数据支持全部导出；在规则详情页的右上角，您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；在修正管理页签您可以查看和编辑此合规规则的修正配置；在标签页签您还可以查看和编辑合规规则的标签。

说明

添加、修改、启用合规规则和触发规则评估需要开启资源记录器，资源记录器处于关闭状态时，合规规则仅支持查看、停用和删除操作。

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。

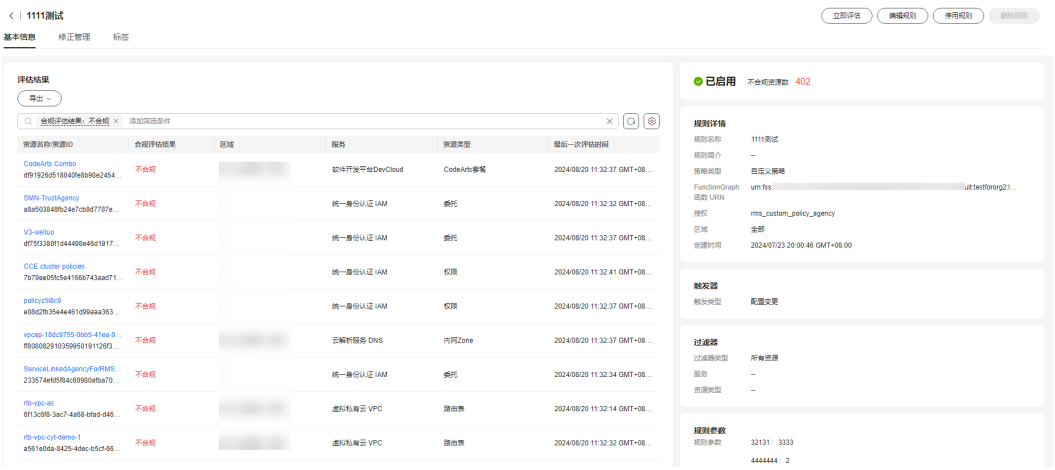
步骤5 在规则列表中单击合规规则的规则名称，进入规则详情的“基本信息”页。

“基本信息”页签左侧展示合规规则评估结果的详细信息，右侧展示合规规则的配置详情。左侧的评估结果列表默认展示合规评估结果为“不合规”的资源，您可以在列表上方的筛选框中通过合规评估结果、资源名称或资源ID对评估结果进行筛选检索，还支持导出全部评估结果数据。

“修正管理”页签展示此合规规则的修正配置详细信息，并支持编辑、删除修正配置，以及执行修正、添加/删除修正例外等操作。

“标签”页签展示此合规规则的标签信息，且支持编辑标签。

图 3-6 合规规则详情



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

3.2.4 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，具体请参见以下**操作步骤**。

约束与限制

- 每个账号最多可以添加500个合规规则。
- 添加、修改、启用合规规则和触发规则评估需要开启资源记录器，资源记录器处于关闭状态时，合规规则仅支持查看、停用和删除操作。

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：

- 如您未开启资源记录器，则资源合规规则无法评估任何资源数据。历史的合规规则评估结果依然存在。
- 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。

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”页签下的合规规则列表中，单击合规规则操作列的“立即评估”。

或者您也可以在规则详情页的右上角单击“立即评估”按钮执行此操作。

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 3-7 手动触发规则评估

----结束

3.2.5 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

- 添加、修改、启用合规规则和触发规则评估需要开启资源记录器，资源记录器处于关闭状态时，合规规则仅支持查看、停用和删除操作。
- 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 3-8 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。

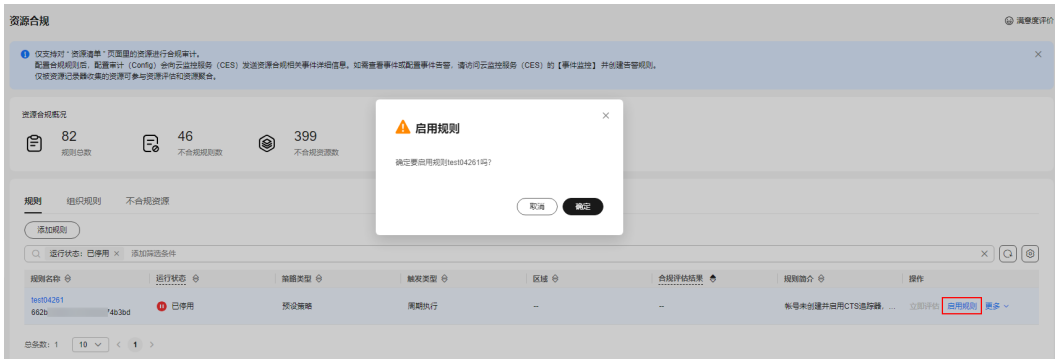
步骤4 在“规则”页签下的合规规则列表中，单击停用状态的合规规则操作列的“启用规则”。

步骤5 在弹出的确认框中，单击“确定”，启用此合规规则。

说明

合规规则被重新启用后会立即自动触发规则评估。

图 3-9 启用规则



----结束

修改合规规则

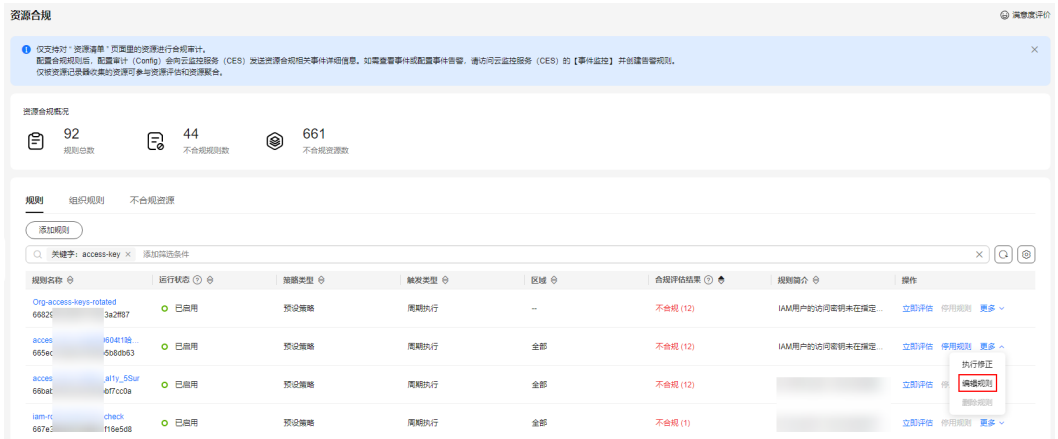
步骤1 登录管理控制台。

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 3-10 编辑规则



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

步骤6 进入“规则参数”页，修改规则相关配置后，单击“下一步”。

不同类型的策略支持修改的配置项存在差异，具体如下：

- 过滤器类型（规则“触发类型”为“配置变更”时支持修改）
- 资源范围（规则“触发类型”为“配置变更”时支持修改）
- 过滤范围（规则“触发类型”为“配置变更”时支持修改）
- 周期频率（规则“触发类型”为“周期频率”时支持修改）

- 规则参数（预定义合规规则仅支持修改规则参数的值，自定义合规规则支持增、删、改规则参数）

步骤7 确认规则修改无误后，单击“提交”。

说明

合规规则被修改后会立即自动触发规则评估。

----结束

删除合规规则

删除合规规则前需先停用该规则，如该规则已创建修正配置，则还需删除修正配置后才能删除合规规则。

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“更多>删除规则”。

图 3-11 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

3.2.6 自定义合规规则样例

3.2.6.1 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 time
import http.client
```

```
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.exceptions.exceptions import ConnectionException
from huaweicloudsdkcore.exceptions.exceptions import RequestTimeoutException
from huaweicloudsdkcore.exceptions.exceptions import ServiceResponseException
from huaweicloudsdkconfig.v1.region.config_region import ConfigRegion
from huaweicloudsdkconfig.v1.config_client import ConfigClient
from huaweicloudsdkconfig.v1 import PolicyResource, PolicyStateRequestBody
from huaweicloudsdkconfig.v1 import UpdatePolicyStateRequest

'''
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vpcId字段不是合规规则参数所指定的vpcId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").get("value") else "NonCompliant"


def update_policy_state(context, domain_id, evaluation):
    auth = GlobalCredentials(
        ak=context.getSecurityAccessKey(),
        sk=context.getSecuritySecretKey(),
        domain_id=domain_id
    ).with_security_token(context.getSecurityToken())
    client = ConfigClient.new_builder() \
        .with_credentials(credentials=auth) \
        .with_region(region=ConfigRegion.value_of(region_id="cn-north-4")) \
        .build()

    try:
        response = client.update_policy_state(evaluation)
        return 200
    except ConnectionException as e:
        print("A connect timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except RequestTimeoutException as e:
        print("A request timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except ServiceResponseException as e:
        print("There is service error, exception: ", e.status_code, e.error_msg)
        return e.status_code


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

    request_body = UpdatePolicyStateRequest(PolicyStateRequestBody(
        policy_resource = PolicyResource(
            resource_id = resource.get("id"),
            resource_name = resource.get("name"),
            resource_provider = resource.get("provider"),
            resource_type = resource.get("type"),
            region_id = resource.get("region_id"),
            domain_id = domain_id
        ),
        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"),
        evaluation_time = event.get("evaluation_time"),
        evaluation_hash = event.get("evaluation_hash")
```



```
    ))

    for retry in range(5):
        status_code = update_policy_state(context, domain_id, request_body)
        if status_code == http.client.TOO_MANY_REQUESTS:
            print("TOO_MANY_REQUESTS: retry again")
            time.sleep(1)
        elif status_code == http.client.OK:
            print("Update policyState successfully.")
            break
        else:
            print("Failed to update policyState.")
            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 time
import http.client
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.exceptions import exceptions
from huaweicloudsdkcore.exceptions.exceptions import ConnectionException
from huaweicloudsdkcore.exceptions.exceptions import RequestTimeoutException
from huaweicloudsdkcore.exceptions.exceptions import ServiceResponseException
from huaweicloudsdkconfig.v1.region.config_region import ConfigRegion
from huaweicloudsdkconfig.v1.config_client import ConfigClient
from huaweicloudsdkconfig.v1 import PolicyResource, PolicyStateRequestBody
from huaweicloudsdkconfig.v1 import UpdatePolicyStateRequest
from huaweicloudsdkiam.v3.region.iam_region import IamRegion
from huaweicloudsdkiam.v3 import IamClient, ShowDomainLoginPolicyRequest

"""
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。
该场景下，可能需要适当增加函数的执行超时时间和内存限制。
"""
def evaluate_compliance(context, domain_id):
    credentials = GlobalCredentials(
        ak=context.getSecurityAccessKey(),
        sk=context.getSecuritySecretKey(),
        domain_id=domain_id
    ).with_security_token(context.getSecurityToken())
    client = IamClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(IamRegion.value_of("cn-north-4")) \
        .build()

    try:
        request = ShowDomainLoginPolicyRequest()
        request.domain_id = domain_id
        response = client.show_domain_login_policy(request)
        session_timeout = response.login_policy.session_timeout
        print("session_timeout", session_timeout)
        if not session_timeout:
            return "NonCompliant"
        return "NonCompliant" if session_timeout > 30 else "Compliant"
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)


def update_policy_state(context, domain_id, evaluation):
    auth = GlobalCredentials(ak=context.getAccessKey(), sk=context.getSecretKey(), domain_id=domain_id)
    client = ConfigClient.new_builder() \
        .with_credentials(credentials=auth) \
```

```
        .with_region(region=ConfigRegion.value_of(region_id="cn-north-4")) \
        .build()
    try:
        response = client.update_policy_state(evaluation)
        return 200
    except ConnectionException as e:
        print("A connect timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except RequestTimeoutException as e:
        print("A request timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except ServiceResponseException as e:
        print("There is service error, exception: ", e.status_code, e.error_msg)
        return e.status_code

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

    request_body = UpdatePolicyStateRequest(PolicyStateRequestBody(
        policy_resource = PolicyResource(
            resource_id = resource.get("id"),
            resource_name = resource.get("name"),
            resource_provider = resource.get("provider"),
            resource_type = resource.get("type"),
            region_id = resource.get("region_id"),
            domain_id = domain_id
        ),
        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"),
        evaluation_time = event.get("evaluation_time"),
        evaluation_hash = event.get("evaluation_hash")
    ))

    for retry in range(5):
        status_code = update_policy_state(context, domain_id, request_body)
        if status_code == http.client.TOO_MANY_REQUESTS:
            print("TOO_MANY_REQUESTS: retry again")
            time.sleep(1)
        elif status_code == http.client.OK:
            print("Update policyState successfully.")
            break
        else:
            print("Failed to update policyState.")
            break
```

依赖包

如果依赖包缺失，则需要手动导入依赖包，详见**配置依赖包**。在上述示例中，使用到的依赖包为**huaweicloudsdkiam**和**huaweicloudsdkconfig**。

3.2.6.2 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
  }
}
```

3.3 组织合规规则

3.3.1 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账号状态为“正常”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。
- 添加、修改组织合规规则和触发规则评估需要开启资源记录器，资源记录器处于关闭状态时，组织合规规则仅支持查看和删除操作。
- 非组织内账号无法在Config控制台的“资源合规”页面中看到“组织规则”页签。
- 组织合规规则仅会下发至账号状态为“正常”的组织成员账号中，且组织成员账号需开启资源记录器，否则将导致部署异常。

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：

- 如您未开启资源记录器，则资源合规规则无法评估任何资源数据。历史的合规规则评估结果依然存在。
- 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。

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 3-12 基础配置

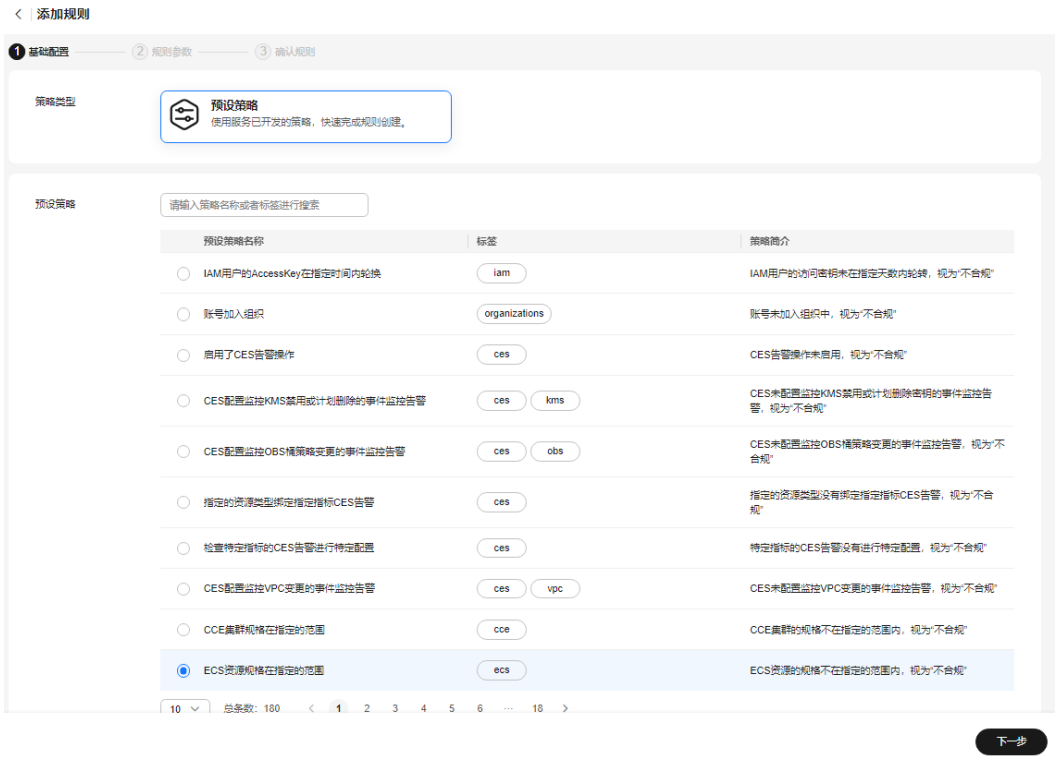


表 3-5 基础配置参数说明

参数	说明
策略类型	选择“预设策略”。 预设策略即服务已开发的策略，在下方的预设策略列表中直接选择所需预设策略，快速完成规则创建。支持输入策略名称或标签进行搜索。 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。

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。

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 3-13 规则参数

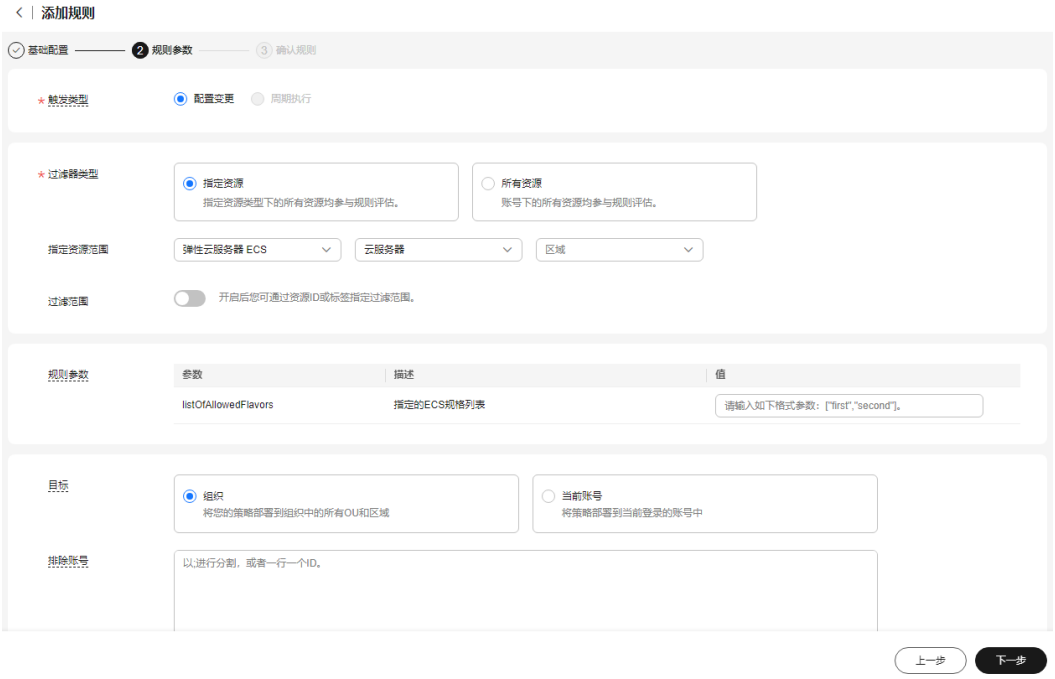


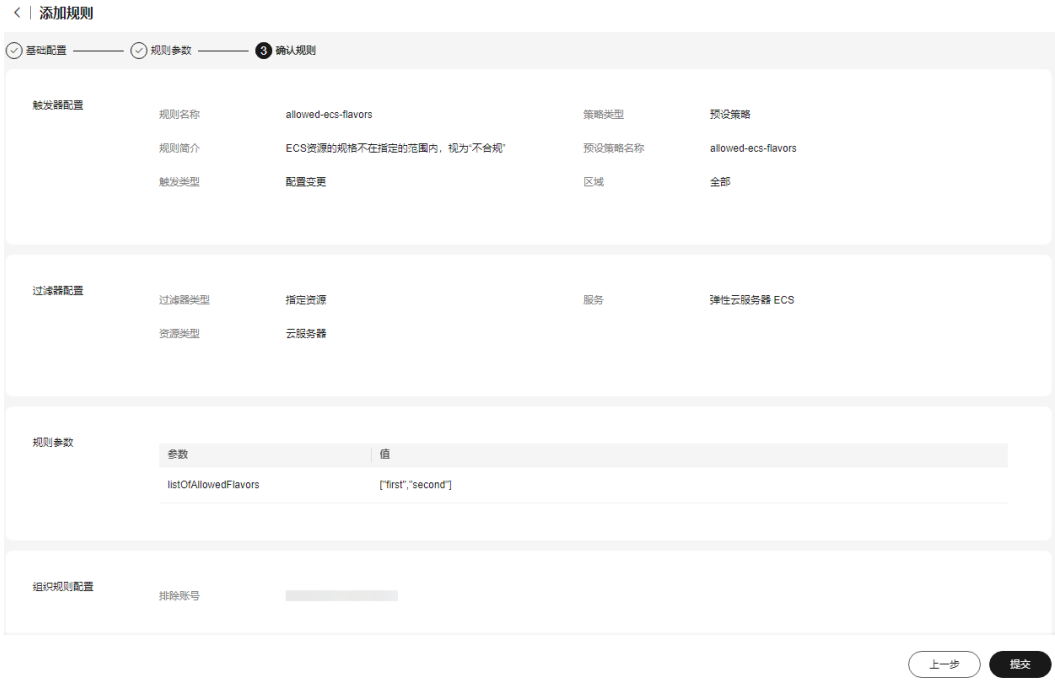
表 3-6 合规规则参数说明

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。

参数	说明
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。
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“资源具有指定的标签”，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：已挂载的云硬盘开启加密（volumes-encrypted-check）。
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 3-14 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**。

3.3.2 添加自定义组织合规规则

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，添加组织类型的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。添加组织类型的自定义合规规则还需通过RAM服务将FunctionGraph函数共享给组织成员账号。

本章节指导您如何通过自定义策略来添加组织类型的合规规则，主要包含如下步骤：

1. **创建FunctionGraph函数**；
2. **共享FunctionGraph函数**；
3. **添加自定义组织合规规则**；
4. **触发规则评估**。

约束与限制

- 每个账号最多可以添加500个合规规则。
- 添加、修改组织合规规则和触发规则评估需要开启资源记录器，资源记录器处于关闭状态时，组织合规规则仅支持查看和删除操作。
- 非组织内账号无法在Config控制台的“资源合规”页面中看到“组织规则”页签。
- 组织合规规则仅会下发至账号状态为“正常”的组织成员账号中，且组织成员账号需开启资源记录器，否则将导致部署异常。

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：

- 如您未开启资源记录器，则资源合规规则无法评估任何资源数据。历史的合规规则评估结果依然存在。
- 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。

关于如何开启并配置资源记录器请参见：**配置资源记录器**。

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

共享 FunctionGraph 函数

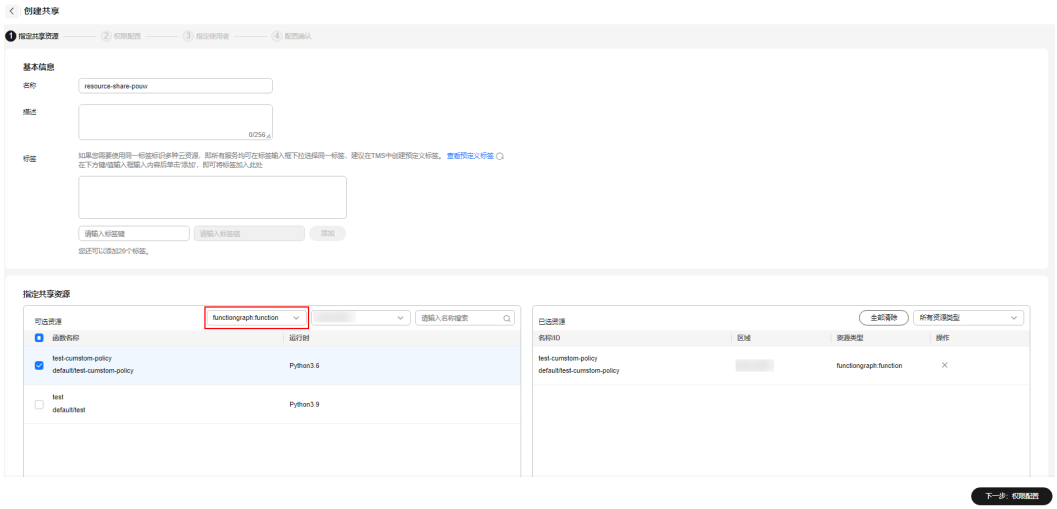
步骤1 以组织管理员账号或者Config服务的委托管理员账号登录管理控制台。

步骤2 单击页面左上角的 ☰，选择“管理与监管 > 资源访问管理”，进入“资源访问管理”页面。

步骤3 单击左侧的“我的共享”，选择“共享管理”。

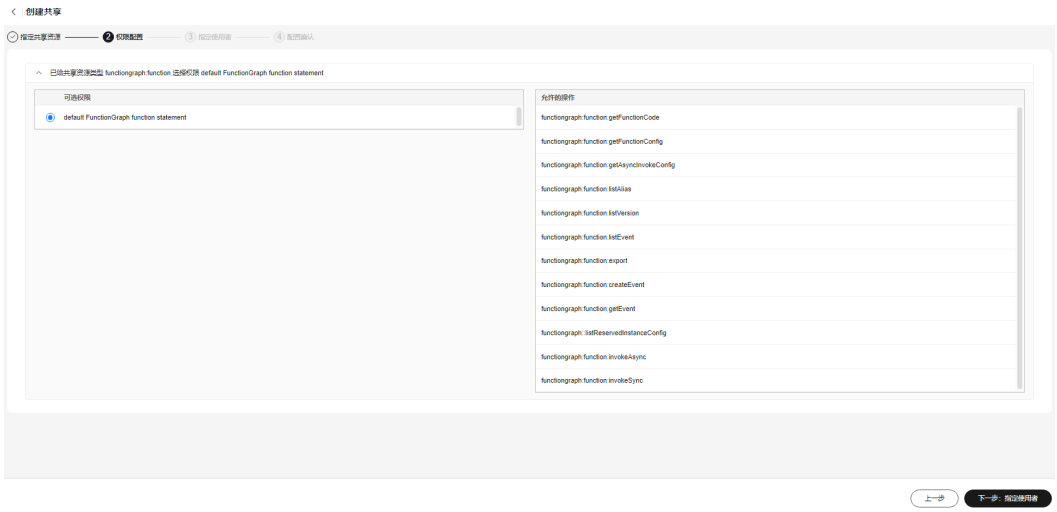
步骤4 单击页面右上角的“创建共享”，进入指定共享资源页面，配置基本信息并指定共享资源为“functiongraph:function”，选择已创建的FunctionGraph函数，单击页面右下角的“下一步：权限配置”。

图 3-15 指定共享资源



步骤5 进入“权限配置”页面，选择共享权限“default FunctionGraph function statement”，单击页面右下角的“下一步：指定使用者”。

图 3-16 权限配置



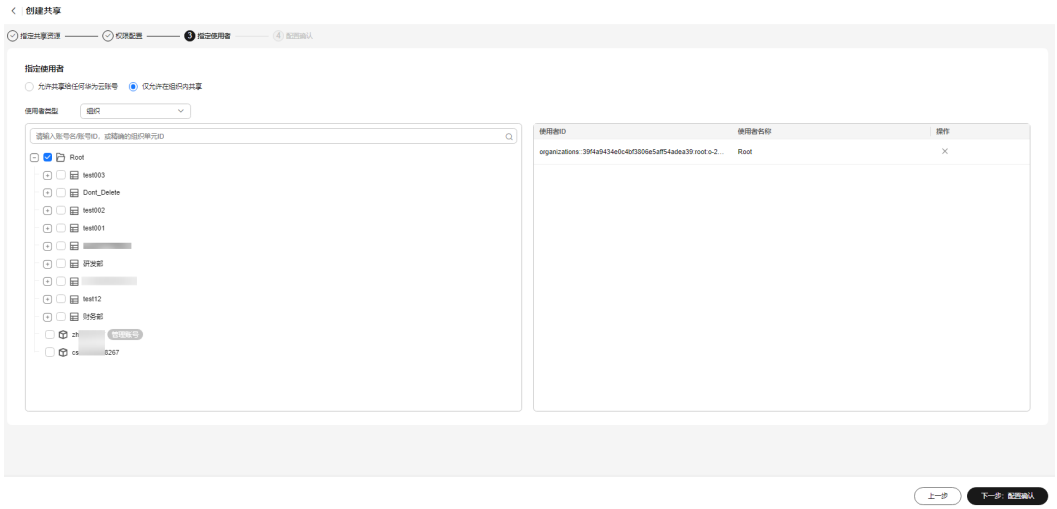
步骤6 进入“指定使用者”页面，指定共享资源的使用者，配置完成后，单击页面右下角的“下一步：配置确认”。

- 指定使用者：选择“仅允许在组织内共享”，表示指定的使用者必须为您组织内的成员。
- 使用者类型：选择“组织”，然后在下方的组织结构树中勾选根OU（即Root），表示将FunctionGraph函数共享给整个组织。

说明

如果您未打开“启用与组织共享资源”开关，使用者类型将无法选择“组织”，如何启用请参见**启用与组织共享资源**。

图 3-17 指定使用者



步骤7 进入“配置确认”页面，确认配置无误后，勾选同意“隐私声明”协议，单击页面右下角的“确定”，完成FunctionGraph函数的组织内共享。

----结束

添加自定义组织合规规则

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 选择“组织规则”页签，单击“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”，配置相关参数后单击“下一步”。

图 3-18 基础配置

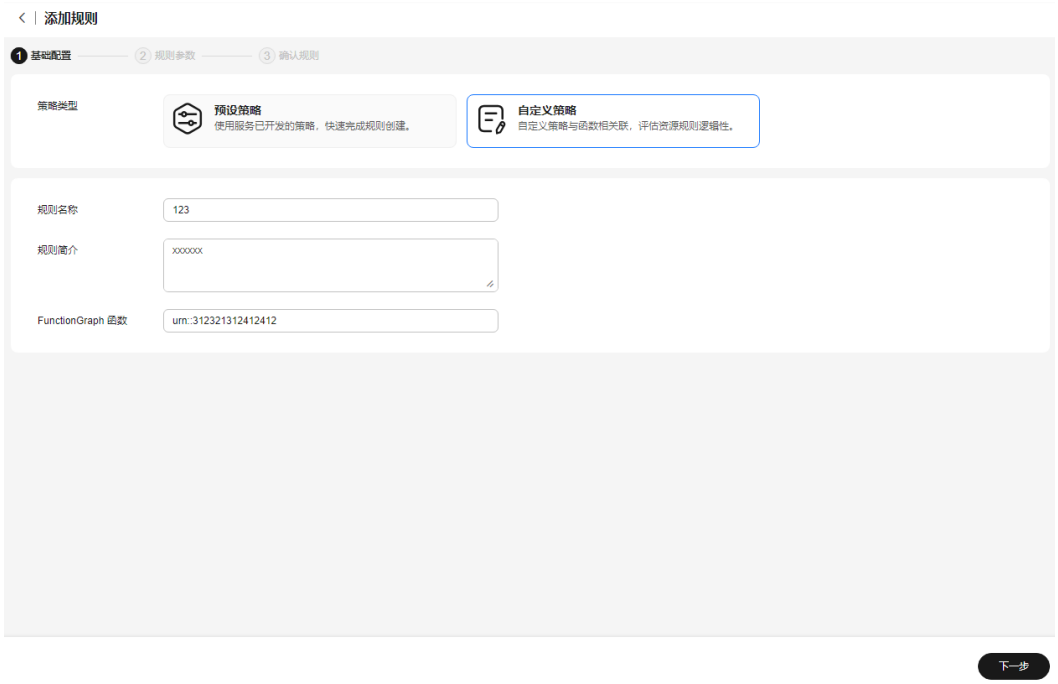


表 3-7 基础配置参数说明

参数	说明
策略类型	策略类型选择“自定义策略”。 允许用户通过自定义策略来创建合规规则。
规则名称	合规规则的名称，不能与已存在的合规规则名称重复。 合规规则名称仅支持数字、字母、下划线和中划线。
规则简介	合规规则的简介，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**。

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”。

图 3-19 规则参数

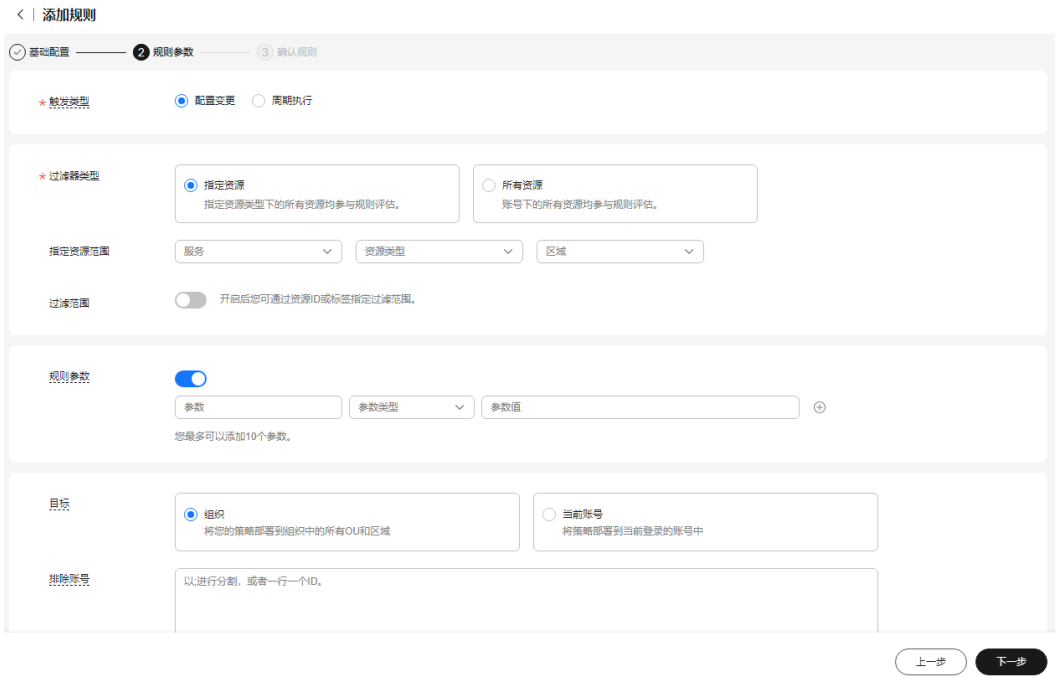


表 3-8 合规规则参数说明

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	自定义策略的规则参数最多可以设置10个，由您自行配置。
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，完成自定义组织合规规则的创建。

----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**。

3.3.3 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**、**查看部署至成员账号中的组织合规规则**和**组织合规规则的部署状态**三部分内容。

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 3-20 查看组织合规规则

步骤5 进入“规则详情页”，页面左侧显示此组织合规规则部署的成员账号列表及其相关信息和排除账号列表，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 3-21 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，系统将自动在此规则名称前添加“Org-”字段用于标识。

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

组织合规规则的部署状态

表 3-9 组织合规规则的部署状态

取值	状态	状态说明
CREATE_IN_PROGRESS	部署中	正在创建组织合规规则。
UPDATE_IN_PROGRESS	更新中	正在更新组织合规规则。
DELETE_IN_PROGRESS	删除中	正在删除组织合规规则。
CREATE_FAILED	部署异常	组织合规规则在该组织内的一个或多个成员账号中创建失败。
UPDATE_FAILED	更新失败	组织合规规则在该组织内的一个或多个成员账号中更新失败。
DELETE_FAILED	删除异常	组织合规规则在该组织内的一个或多个成员账号中删除失败。
CREATE_SUCCESSFUL	已部署	组织合规规则在该组织内的所有成员账号中创建成功。
UPDATE_SUCCESSFUL	更新成功	组织合规规则在该组织内的所有成员账号中更新成功。

3.3.4 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。

说明

添加、修改组织合规规则和触发规则评估需要开启资源记录器，资源记录器处于关闭状态时，组织合规规则仅支持查看和删除操作。

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 3-22 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

3.3.5 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。

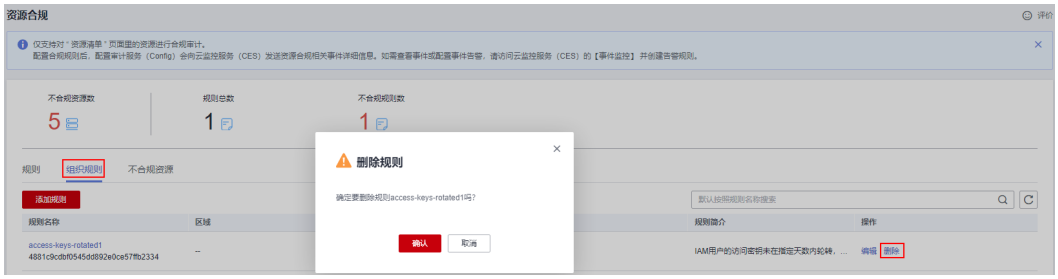
步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

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“删除规则”弹窗中，单击“确定”。

组织合规规则删除后，此组织合规规则在每个成员账号下所部署的合规规则将同时自动删除。

图 3-23 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。

3.3.6 自定义组织合规规则样例

3.3.6.1 示例函数(Python)

评估由配置变更触发的示例函数

Config服务检测到自定义组织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 time
import http.client
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.exceptions.exceptions import ConnectionException
from huaweicloudsdkcore.exceptions.exceptions import RequestTimeoutException
from huaweicloudsdkcore.exceptions.exceptions import ServiceResponseException
from huaweicloudsdkconfig.v1.region.config_region import ConfigRegion
from huaweicloudsdkconfig.v1.config_client import ConfigClient
from huaweicloudsdkconfig.v1 import PolicyResource, PolicyStateRequestBody
from huaweicloudsdkconfig.v1 import UpdatePolicyStateRequest

'''
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vpcId字段不是合规规则参数所指定的vpcId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(context, domain_id, evaluation):
    auth = GlobalCredentials(ak=context.getAccessKey(), sk=context.getSecretKey(), domain_id=domain_id)
    client = ConfigClient.new_builder() \
        .with_credentials(credentials=auth) \
        .with_region(region=ConfigRegion.value_of(region_id="cn-north-4")) \
        .build()

    try:
        response = client.update_policy_state(evaluation)
        return 200
    except ConnectionException as e:
        print("A connect timeout exception occurs while the Config performs some operations, exception: ",
```

```
e.error_msg)
        return e.status_code
    except RequestTimeoutException as e:
        print("A request timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except ServiceResponseException as e:
        print("There is service error, exception: ", e.status_code, e.error_msg)
        return e.status_code


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

    request_body = UpdatePolicyStateRequest(PolicyStateRequestBody(
        policy_resource = PolicyResource(
            resource_id = resource.get("id"),
            resource_name = resource.get("name"),
            resource_provider = resource.get("provider"),
            resource_type = resource.get("type"),
            region_id = resource.get("region_id"),
            domain_id = event.get("domain_id")
        ),
        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"),
        evaluation_time = event.get("evaluation_time"),
        evaluation_hash = event.get("evaluation_hash")
    ))

    for retry in range(5):
        status_code = update_policy_state(context, domain_id, request_body)
        if status_code == http.client.TOO_MANY_REQUESTS:
            print("TOO_MANY_REQUESTS: retry again")
            time.sleep(1)
        elif status_code == http.client.OK:
            print("Update policyState successfully.")
            break
        else:
            print("Failed to update policyState.")
            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组织合规规则，会调用函数的示例如下：

```
import time
import http.client
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.exceptions.exceptions import ConnectionException
from huaweicloudsdkcore.exceptions.exceptions import RequestTimeoutException
from huaweicloudsdkcore.exceptions.exceptions import ServiceResponseException
from huaweicloudsdkconfig.v1.region.config_region import ConfigRegion
from huaweicloudsdkconfig.v1.config_client import ConfigClient
from huaweicloudsdkconfig.v1 import PolicyResource, PolicyStateRequestBody
from huaweicloudsdkconfig.v1 import UpdatePolicyStateRequest
from huaweicloudsdkiam.v3.region.iam_region import IamRegion
from huaweicloudsdkiam.v3 import IamClient, ShowDomainLoginPolicyRequest

"""
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。
该场景下，可能需要适当增加函数的执行超时时间和内存限制。
"""
```

```
def evaluate_compliance(ak, sk, domain_id):
    credentials = GlobalCredentials(ak, sk)
    client = IamClient.new_builder() \
        .with_credentials(credentials) \
        .with_region(IamRegion.value_of("cn-north-4")) \
        .build()

    try:
        request = ShowDomainLoginPolicyRequest()
        request.domain_id = domain_id
        response = client.show_domain_login_policy(request)
        session_timeout = response.login_policy.session_timeout
        print("session_timeout", session_timeout)
        if not session_timeout:
            return "NonCompliant"
        return "NonCompliant" if session_timeout > 30 else "Compliant"
    except exceptions.ClientRequestException as e:
        print(e.status_code)
        print(e.request_id)
        print(e.error_code)
        print(e.error_msg)


def update_policy_state(context, domain_id, evaluation):
    auth = GlobalCredentials(ak=context.getAccessKey(), sk=context.getSecretKey(), domain_id=domain_id)
    client = ConfigClient.new_builder() \
        .with_credentials(credentials=auth) \
        .with_region(region=ConfigRegion.value_of(region_id="cn-north-4")) \
        .build()
    try:
        response = client.update_policy_state(evaluation)
        return 200
    except ConnectionException as e:
        print("A connect timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except RequestTimeoutException as e:
        print("A request timeout exception occurs while the Config performs some operations, exception: ",
e.error_msg)
        return e.status_code
    except ServiceResponseException as e:
        print("There is service error, exception: ", e.status_code, e.error_msg)
        return e.status_code

def handler(event, context):
    domain_id = "<manager_domain_id>"
    ak = "<user_ak">
    sk = "<user_sk>
    resource = event.get("invoking_event", {})
    if resource.get("name") != "Account":
        return
    compliance_state = evaluate_compliance(ak, sk, event.get("domain_id"))

    request_body = UpdatePolicyStateRequest(PolicyStateRequestBody(
        policy_resource = PolicyResource(
            resource_id = resource.get("id"),
            resource_name = resource.get("name"),
            resource_provider = resource.get("provider"),
            resource_type = resource.get("type"),
            region_id = resource.get("region_id"),
            domain_id = event.get("domain_id")
        ),
        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"),
        evaluation_time = event.get("evaluation_time"),
        evaluation_hash = event.get("evaluation_hash")
    ))
```

```
for retry in range(5):
    status_code = update_policy_state(context, domain_id, request_body)
    if status_code == http.client.TOO_MANY_REQUESTS:
        print("TOO_MANY_REQUESTS: retry again")
        time.sleep(1)
    elif status_code == http.client.OK:
        print("Update policyState successfully.")
        break
    else:
        print("Failed to update policyState.")
        break
```

依赖包

如果依赖包缺失，则需要手动导入依赖包，详见**配置依赖包**。在上述示例中，使用到的依赖包为**huaweicloudsdkiam**和**huaweicloudsdkconfig**。

3.3.6.2 事件

由配置变更触发的评估的示例事件

当触发规则时，Config服务会发送一个事件来调用该自定义组织合规规则的自定义策略的函数。

下面的事件演示自定义组织合规规则被某个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组织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
 }
}
```


3.4 查看不合规资源

操作场景

当您添加并运行多个合规规则进行资源合规评估时，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。

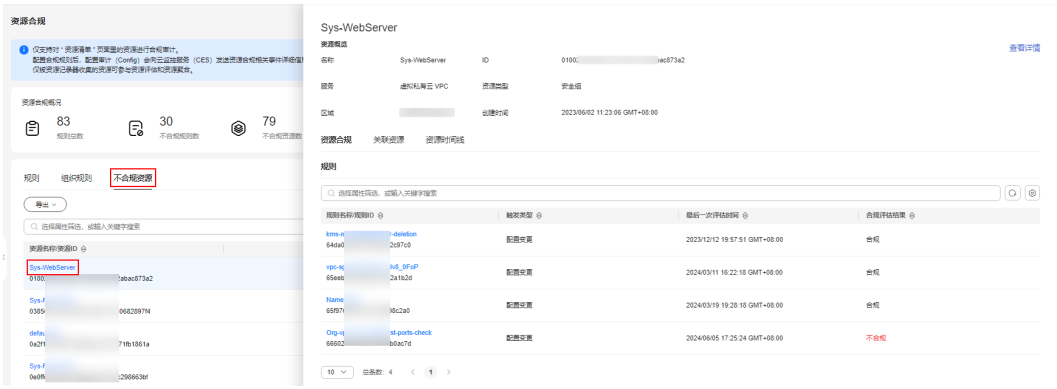
步骤3 单击左侧的“资源合规”，进入“资源合规”页面。

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。

在列表上方，支持通过多种条件对不合规资源进行检索，还支持导出全部不合规资源数据。

图 3-24 查看不合规资源



----结束

3.5 合规规则概念详解

3.5.1 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满足合规策略中的要求。

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（例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 3-10 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	合规策略的类型。 主要有以下类型： • builtin • custom	• 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。
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。

参数	定义	说明
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**。

3.5.2 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3-11**所示。

表 3-11 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。
tags	合规规则的标签列表	-	● 标签键：最大长度为128个unicode字符。 ● 标签值：最大长度为255个unicode字符。
created_by	合规规则的创建者	-	用户创建（custom）或服务关联委托方式创建。

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": []
    }
  }
  "tags": [],
  "created_by": "custom"
}
```

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"}
    }
  }
  "tags": [],
  "created_by": "custom"
}
```

3.5.3 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3-12**所示。

表 3-12 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	-
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
}
```

3.6 系统内置预设策略

3.6.1 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 3-13 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
	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
	资源在指定类型内	配置变更	全部资源
	不允许的资源类型	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
	CodeArts编译构建下的项目未设置参数加密	配置变更	codeartsbuild.CloudBuildServer

云服务	预设策略	触发方式	评估资源
MapReduce服务 MRS	MRS集群属于指定安全组	配置变更	mrs.mrs
	MRS集群属于指定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集群未绑定弹性公网IP	配置变更	mrs.mrs
	MRS集群开启KMS加密	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	account
Web应用防火墙 WAF	WAF防护域名配置防护策略	配置变更	waf.instance
	WAF防护策略配置防护规则	配置变更	waf.policy
	启用WAF实例域名防护	周期触发	account
	启用WAF防护策略地理位置访问控制规则	周期触发	account
	WAF实例启用拦截模式防护策略	配置变更	waf.instance
弹性负载均衡 ELB	ELB资源不具有弹性公网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
	监听器资源HTTPS重定向检查	配置变更	elb.listeners
	ELB资源使用多AZ部署	配置变更	elb.loadbalancers
	ELB负载均衡器配置访问日志	配置变更	elb.loadbalancers
弹性公网IP EIP	EIP带宽限制	配置变更	vpc.publicips

云服务	预设策略	触发方式	评估资源
	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
	弹性伸缩组未配置IPv6带宽	配置变更	as.scalingGroups
	弹性伸缩组VPC检查	配置变更	as.scalingGroups
高性能弹性文件服务 SFS Turbo	高性能弹性文件服务通过KMS进行加密	配置变更	sfsturbo.shares
	SFS Turbo资源在备份存储库中	配置变更	sfsturbo.shares
	SFS Turbo资源的备份时间检查	周期触发	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资源配置密钥对	配置变更	ecs.cloudservers
	ECS资源不能公网访问	配置变更	ecs.cloudservers
	检查ECS资源是否具有多个弹性公网IP	配置变更	ecs.cloudservers
	关机状态的ECS未进行任意操作的时间检查	周期触发	ecs.cloudservers

云服务	预设策略	触发方式	评估资源
	ECS资源附加IAM委托	配置变更	ecs.cloudservers
	ECS实例的镜像名称在指定的范围	配置变更	ecs.cloudservers
	ECS资源在备份存储库中	配置变更	ecs.cloudservers
	ECS云服务器的备份时间检查	周期触发	ecs.cloudservers
	ECS资源绑定服务主机代理防护	配置变更	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资源不存在弹性公网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实例不存在弹性公网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
	函数工作流的函数启用日志配置	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

云服务	预设策略	触发方式	评估资源
	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	account
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
	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
	DWS集群未绑定弹性公网IP	配置变更	dws.clusters
	DWS集群运维时间窗检查	配置变更	dws.clusters
	DWS集群VPC检查	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
	检查CSMS凭据轮转成功	配置变更	csms.secrets
	CSMS凭据启动自动轮转	配置变更	csms.secrets
	CSMS凭据使用指定KMS	配置变更	csms.secrets
	CSMS凭据在指定时间内轮转	周期触发	csms.secrets

云服务	预设策略	触发方式	评估资源
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策略中不授权KMS的禁止的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
	根用户存在可使用的访问密钥	周期触发	account
	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用户归属指定用户组	配置变更	iam.users
	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
	根用户开启MFA认证	周期触发	account
	IAM策略使用中	配置变更	iam.policies
	IAM权限使用中	配置变更	iam.roles
	IAM用户开启登录保护	周期触发	iam.users
	IAM委托绑定策略检查	配置变更	iam.agencies

云服务	预设策略	触发方式	评估资源
	IAM用户admin权限检查	配置变更	iam.users
	IAM用户不直接附加策略或权限	配置变更	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实例未绑定弹性公网IP	配置变更	dds.instances
	DDS实例端口检查	配置变更	dds.instances
	DDS实例数据库版本检查	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
	安全组非白名单端口检查	配置变更	vpc.securityGroups
	安全组连接到弹性网络接口	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

云服务	预设策略	触发方式	评估资源
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禁用或计划删除密钥的事件监控告警	周期触发	account
	CES配置监控OBS桶策略变更的事件监控告警	周期触发	account
	指定的资源类型绑定指定指标CES告警	周期触发	account
	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	account
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集群资源不具有弹性公网IP	配置变更	cce.clusters
	CCE集群规格在指定的范围	配置变更	cce.clusters
	CCE集群VPC检查	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	account
	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	account
	在指定区域创建并启用CTS追踪器	周期触发	account
	CTS追踪器符合安全最佳实践	周期触发	account
云数据库 RDS	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

云服务	预设策略	触发方式	评估资源
	RDS实例支持多可用区	配置变更	rds.instances
	RDS实例不具有弹性公网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
	RDS实例规格在指定的范围	配置变更	rds.instances
	RDS实例启用SSL加密通讯	配置变更	rds.instances
	RDS实例端口检查	配置变更	rds.instances
	RDS实例数据库引擎版本检查	配置变更	rds.instances
	RDS实例启用审计日志	配置变更	rds.instances
云数据库 GaussDB	GaussDB资源属于指定虚拟私有云ID	配置变更	gaussdb.instance
	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实例EIP检查	配置变更	gaussdb.instance
	GaussDB实例跨AZ部署检查	配置变更	gaussdb.instance
	GaussDB实例开启传输数据加密	配置变更	gaussdb.instance

云服务	预设策略	触发方式	评估资源
云数据库 TaurusDB	TaurusDB实例开启审计日志	配置变更	gaussdbformysql.instance
	TaurusDB实例开启备份	配置变更	gaussdbformysql.instance
	TaurusDB实例开启错误日志	配置变更	gaussdbformysql.instance
	TaurusDB实例开启慢日志	配置变更	gaussdbformysql.instance
	TaurusDB实例开启传输数据加密	配置变更	gaussdbformysql.instance
	TaurusDB实例跨AZ部署检查	配置变更	gaussdbformysql.instance
	TaurusDB实例EIP检查	配置变更	gaussdbformysql.instance
	TaurusDB实例VPC检查	配置变更	gaussdbformysql.instance
云数据库 GeminiDB	GeminiDB部署在单个可用区	配置变更	nosql.instances
	GeminiDB开启备份	配置变更	nosql.instances
	GeminiDB使用磁盘加密	配置变更	nosql.instances
	GeminiDB开启错误日志	配置变更	nosql.instances
	GeminiDB开启慢查询日志	配置变更	nosql.instances
云搜索服务 CSS	CSS集群启用安全模式	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集群支持安全模式	配置变更	css.clusters
	CSS集群未开启访问控制开关	配置变更	css.clusters
	CSS集群Kibana未开启访问控制开关	配置变更	css.clusters
	CSS集群开启慢日志	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
	云硬盘开启加密	配置变更	evs.volumes
	EVS资源在备份存储库保护中	配置变更	evs.volumes
	EVS资源的备份时间检查	周期触发	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
	检查私有根CA是否停用	周期触发	pca.ca
	私有证书管理服务算法检查	配置变更	pca.ca、pca.cert

云服务	预设策略	触发方式	评估资源
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.kafka
	DMS Kafka队列打开公网SSL加密访问	配置变更	dms.kafka
	DMS Kafka队列开启公网访问	配置变更	dms.kafka
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
	DMS RabbitMQ实例开启公网访问	配置变更	dms.rabbitmqs
分布式消息服务RocketMQ版	DMS RocketMQ实例打开SSL加密访问	配置变更	dms.reliabilitys
	DMS RocketMQ实例开启公网访问	配置变更	dms.reliabilitys
组织 Organizations	账号加入组织	周期触发	account
云防火墙 CFW	CFW防火墙配置防护策略	配置变更	cfw.cfw_instance
云备份 CBR	CBR备份被加密	配置变更	cbr.backup
	CBR备份策略执行频率检查	配置变更	cbr.policy
	CBR存储库最低保留天数	配置变更	cbr.vault
对象存储服务 OBS	OBS桶策略中不授权禁止的Action	配置变更	obs.buckets
	OBS桶策略中授权检查	配置变更	obs.buckets
	OBS桶策略授权约束	配置变更	obs.buckets
	OBS桶禁止公开读	配置变更	obs.buckets
	OBS桶禁止公开写	配置变更	obs.buckets
	OBS桶策略授权行为使用SSL加密	配置变更	obs.buckets
镜像服务 IMS	私有镜像开启加密	配置变更	ims.images
裸金属服务器 BMS	BMS资源使用密钥对登录	配置变更	bms.servers
图引擎服务 GES	GES图通过KMS加密	配置变更	ges.graphs

云服务	预设策略	触发方式	评估资源
	GES图开启LTS日志	配置变更	ges.graphs
	GES图支持跨AZ高可用	配置变更	ges.graphs

3.6.2 公共可用预设策略

3.6.2.1 资源名称满足正则表达式

规则详情

表 3-14 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。

3.6.2.2 资源具有所有指定的标签键

规则详情

表 3-15 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

参数	说明
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。

3.6.2.3 资源存在任一指定的标签

规则详情

表 3-16 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。

3.6.2.4 资源具有指定前后缀的标签键

规则详情

表 3-17 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

参数	说明
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。

3.6.2.5 资源标签非空

规则详情

表 3-18 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

3.6.2.6 资源具有指定的标签

规则详情

表 3-19 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

参数	说明
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。

3.6.2.7 资源属于指定企业项目 ID

规则详情

表 3-20 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。

3.6.2.8 资源在指定区域内

规则详情

表 3-21 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

参数	说明
规则参数	regions：指定区域列表，数组类型。全局资源的region为“global”。

3.6.2.9 资源在指定类型内

规则详情

表 3-22 规则详情

参数	说明
规则名称	resources-in-allowed-types
规则展示名	资源在指定类型内
规则描述	用户创建指定类型以外的资源，视为“不合规”。
标签	type
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	providerAndTypes：指定服务资源类型列表，形式应为['provider.type']。

3.6.2.10 不允许的资源类型

规则详情

表 3-23 规则详情

参数	说明
规则名称	resources-in-not-allowed-types
规则展示名	不允许的资源类型
规则描述	用户创建指定类型的资源，视为“不合规”。
标签	type
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	providerAndTypes：指定服务资源类型列表，形式应为['provider.type']。

3.6.3 API 网关 APIG

3.6.3.1 APIG 专享版实例配置安全认证类型

规则详情

表 3-24 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

3.6.3.2 APIG 专享版实例配置访问日志

规则详情

表 3-25 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

3.6.3.3 APIG 专享版实例域名均关联 SSL 证书

规则详情

表 3-26 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

3.6.4 部署 CodeArts Deploy

3.6.4.1 CodeArts 项目下的主机集群为可用状态

规则详情

表 3-27 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

3.6.4.2 CodeArts 编译构建下的项目未设置参数加密

规则详情

表 3-28 规则详情

参数	说明
规则名称	cloudbuildserver-encryption-parameter-check
规则展示名	CodeArts编译构建下的项目未设置参数加密
规则描述	CodeArts编译构建下的项目，如果设置未加密参数（除预定义参数外），则视为“不合规”。
标签	codeartsbuild
规则触发方式	配置变更
规则评估的资源类型	codeartsbuild.CloudBuildServer
规则参数	无

3.6.5 MapReduce 服务 MRS

3.6.5.1 MRS 集群属于指定安全组

规则详情

表 3-29 规则详情

参数	说明
规则名称	mrs-cluster-in-allowed-security-groups
规则展示名	MRS集群属于指定安全组
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。

3.6.5.2 MRS 集群属于指定 VPC

规则详情

表 3-30 规则详情

参数	说明
规则名称	mrs-cluster-in-vpc
规则展示名	MRS集群属于指定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：MRS集群使用的VPC ID。

应用场景

虚拟私有云（VPC）是您在云上的私有网络，可以为MRS构建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，确保MRS所有流量都安全地保留在虚拟私有云中，详见**虚拟私有云产品介绍**。

修复项指导

MRS集群创建完成后不支持切换虚拟私有云，请谨慎选择所属虚拟私有云。当前仅支持切换VPC子网，详见**切换MRS集群VPC子网**。

检测逻辑

- MRS集群的VPC不是指定的VPC，视为“不合规”。
- MRS集群使用的VPC是指定的VPC，视为“合规”。

3.6.5.3 MRS 集群开启 kerberos 认证

规则详情

表 3-31 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”。

参数	说明
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

3.6.5.4 MRS 集群使用多 AZ 部署

规则详情

表 3-32 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

3.6.5.5 MRS 集群未绑定弹性公网 IP

规则详情

表 3-33 规则详情

参数	说明
规则名称	mrs-cluster-no-public-ip
规则展示名	MRS集群未绑定弹性公网IP
规则描述	MRS集群绑定弹性公网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

参数	说明
规则参数	无

3.6.5.6 MRS 集群开启 KMS 加密

规则详情

表 3-34 规则详情

参数	说明
规则名称	mrs-cluster-encrypt-enable
规则展示名	MRS集群开启KMS加密
规则描述	MRS集群未开启KMS加密，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

3.6.6 NAT 网关 NAT

3.6.6.1 NAT 私网网关绑定指定 VPC 资源

规则详情

表 3-35 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。

3.6.7 VPC 终端节点 VPCEP

3.6.7.1 创建了指定服务名的终端节点

规则详情

表 3-36 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	account
规则参数	serviceName：指定服务名的终端节点。

3.6.8 Web 应用防火墙 WAF

3.6.8.1 WAF 防护域名配置防护策略

规则详情

表 3-37 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

3.6.8.2 WAF 防护策略配置防护规则

规则详情

表 3-38 规则详情

参数	说明
规则名称	waf-policy-not-empty
规则展示名	WAF防护策略配置防护规则
规则描述	WAF防护策略未配置防护规则，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.policy
规则参数	无

3.6.8.3 启用 WAF 实例域名防护

规则详情

表 3-39 规则详情

参数	说明
规则名称	waf-instance-enable-protect
规则展示名	启用WAF实例域名防护
规则描述	如果账号未配置并启用WAF防护策略的域名防护，视为“不合规”。
标签	waf
规则触发方式	周期触发
规则评估的资源类型	account
规则参数	无

3.6.8.4 启用 WAF 防护策略地理位置访问控制规则

规则详情

表 3-40 规则详情

参数	说明
规则名称	waf-policy-enable-geoip
规则展示名	启用WAF防护策略地理位置访问控制规则
规则描述	如果账号未配置并启用WAF防护策略的地理位置访问控制规则，视为“不合规”。
标签	waf
规则触发方式	周期触发
规则评估的资源类型	account
规则参数	无

3.6.8.5 WAF 实例启用拦截模式防护策略

规则详情

表 3-41 规则详情

参数	说明
规则名称	waf-instance-enable-block-policy
规则展示名	WAF实例启用拦截模式防护策略
规则描述	WAF实例未启用拦截模式防护策略，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

3.6.9 弹性负载均衡 ELB

3.6.9.1 ELB 资源不具有弹性公网 IP

规则详情

表 3-42 规则详情

参数	说明
规则名称	elb-loadbalancers-no-public-ip
规则展示名	ELB资源不具有弹性公网IP
规则描述	ELB资源具有弹性公网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

3.6.9.2 ELB 监听器配置指定预定义安全策略

规则详情

表 3-43 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**。

3.6.9.3 ELB 监听器配置 HTTPS 监听协议

规则详情

表 3-44 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

3.6.9.4 ELB 后端服务器权重检查

规则详情

表 3-45 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“SOURCE_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。

3.6.9.5 监听器资源 HTTPS 重定向检查

规则详情

表 3-46 规则详情

参数	说明
规则名称	elb-http-to-https-redirection-check
规则展示名	监听器资源HTTPS重定向检查
规则描述	检查HTTP监听器是否配置向HTTPS监听器的重定向，如果未配置，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.listeners
规则参数	无

3.6.9.6 ELB 资源使用多 AZ 部署

规则详情

表 3-47 规则详情

参数	说明
规则名称	elb-multiple-az-check
规则展示名	ELB资源使用多AZ部署
规则描述	检查负载均衡器是否已从多个可用分区注册实例。如果负载均衡器的实例注册在少于2个可用区，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

3.6.9.7 ELB 负载均衡器配置访问日志

规则详情

表 3-48 规则详情

参数	说明
规则名称	elb-logging-enabled
规则展示名	ELB负载均衡器配置访问日志
规则描述	弹性负载均衡器没有配置访问日志，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

应用场景

在您使用ELB期间，支持对采用HTTP/HTTPS/TLS监听器的负载均衡实例的访问日志进行记录，包括请求时间、客户端IP地址、请求路径和服务器响应等。

如果您遇到后端服务器导致的业务故障或异常，您可以查看访问弹性负载均衡的详细日志记录，分析负载均衡的响应状态码，快速定位异常的后端服务器。 详见 **访问日志**。

修复项指导

请根据指导 **配置访问日志** 。

检测逻辑

- 弹性负载均衡器没有配置访问日志，视为“不合规”。
- 弹性负载均衡器配置了访问日志，视为“合规”。

3.6.10 弹性公网 IP EIP

3.6.10.1 EIP 带宽限制

规则详情

表 3-49 规则详情

参数	说明
规则名称	eip-bandwidth-limit

参数	说明
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。

3.6.10.2 弹性公网 IP 未进行任何绑定

规则详情

表 3-50 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

3.6.10.3 EIP 在指定天数内绑定到资源实例

规则详情

表 3-51 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”。

参数	说明
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。

3.6.11 弹性伸缩 AS

3.6.11.1 弹性伸缩组均衡扩容

规则详情

表 3-52 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

3.6.11.2 弹性伸缩组使用弹性负载均衡健康检查

规则详情

表 3-53 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

参数	说明
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

3.6.11.3 弹性伸缩组启用多 AZ 部署

规则详情

表 3-54 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

3.6.11.4 弹性伸缩组未配置 IPv6 带宽

规则详情

表 3-55 规则详情

参数	说明
规则名称	as-group-ipv6-disabled
规则展示名	弹性伸缩组未配置IPv6带宽
规则描述	弹性伸缩组绑定IPv6共享带宽，视为“不合规”。
标签	as
规则触发方式	配置变更

参数	说明
规则评估的资源类型	as.scalingGroups
规则参数	无

3.6.11.5 弹性伸缩组 VPC 检查

规则详情

表 3-56 规则详情

参数	说明
规则名称	as-group-in-vpc
规则展示名	弹性伸缩组VPC检查
规则描述	AS弹性伸缩组绑定的VPC不在对应VPC列表，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	VpcIdList：指定允许绑定的VPC ID列表，数组类型。

应用场景

虚拟私有云（VPC）是您在云上的私有网络，可以为AS构建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，确保AS所有流量都安全地保留在虚拟私有云中，详见**虚拟私有云产品介绍**。

修复项指导

您可以通过网络配置，为不合规的AS弹性伸缩组绑定特定的虚拟私有云。

检测逻辑

- AS弹性伸缩组绑定的VPC不在对应VPC列表，视为“不合规”。
- AS弹性伸缩组绑定的VPC在对应VPC列表，视为“合规”。

3.6.12 高性能弹性文件服务 SFS Turbo

3.6.12.1 高性能弹性文件服务通过 KMS 进行加密

规则详情

表 3-57 规则详情

参数	说明
规则名称	sfsturbo-encrypted-check
规则展示名	高性能弹性文件服务通过KMS进行加密
规则描述	高性能弹性文件服务（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

3.6.12.2 SFS Turbo 资源在备份存储库中

规则详情

表 3-58 规则详情

参数	说明
规则名称	sfsturbo-protected-by-cbr
规则展示名	SFS Turbo资源在备份存储库中
规则描述	SFS Turbo资源没有关联备份存储库，视为“不合规”。
标签	cbr、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

3.6.12.3 SFS Turbo 资源的备份时间检查

规则详情

表 3-59 规则详情

参数	说明
规则名称	sfsturbo-last-backup-created
规则展示名	SFS Turbo资源的备份时间检查
规则描述	SFS Turbo资源最近一次备份创建时间超过参数要求，视为“不合规”。
标签	cbr、sfsturbo
规则触发方式	周期触发
规则评估的资源类型	sfsturbo.shares
规则参数	lastBackupAgeValue：SFS Turbo要求的备份时间间隔（以小时为单位）。

3.6.13 弹性云服务器 ECS

3.6.13.1 ECS 资源规格在指定的范围

规则详情

表 3-60 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。

3.6.13.2 ECS 实例的镜像 ID 在指定的范围

规则详情

表 3-61 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。

3.6.13.3 ECS 的镜像在指定 Tag 的 IMS 的范围内

规则详情

表 3-62 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。

3.6.13.4 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 3-63 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。

3.6.13.5 ECS 资源属于指定虚拟私有云 ID

规则详情

表 3-64 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：ECS实例使用的VPC ID。

应用场景

虚拟私有云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。您还可以在VPC中定义安全组、VPN、IP地址段、带宽等网络特性，方便管理、配置内部网络，进行安全、快捷的网络变更。同时，您可以自定义安全组内与组间弹性云服务器的访问规则，加强弹性云服务器的安全保护。

虚拟私有云更多信息，详见**虚拟私有云产品介绍**。

修复项指导

ECS弹性云服务器创建完成后不支持切换虚拟私有云，请谨慎选择所属虚拟私有云。

检测逻辑

- ECS实例使用的VPC不是指定的VPC，视为“不合规”。
- ECS实例使用的VPC是指定的VPC，视为“合规”。

3.6.13.6 ECS 资源配置密钥对

规则详情

表 3-65 规则详情

参数	说明
规则名称	ecs-instance-key-pair-login
规则展示名	ECS资源配置密钥对
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

3.6.13.7 ECS 资源不能公网访问

规则详情

表 3-66 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

参数	说明
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

3.6.13.8 检查 ECS 资源是否具有多个弹性公网 IP

规则详情

表 3-67 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资源是否具有多个弹性公网IP
规则描述	ECS资源具有多个弹性公网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

3.6.13.9 关机状态的 ECS 未进行任意操作的时间检查

规则详情

表 3-68 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

参数	说明
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。

3.6.13.10 ECS 资源附加 IAM 委托

规则详情

表 3-69 规则详情

参数	说明
规则名称	ecs-instance-agency-attach-iam-agency
规则展示名	ECS资源附加IAM委托
规则描述	ECS实例未附加IAM委托，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

3.6.13.11 ECS 实例的镜像名称在指定的范围

规则详情

表 3-70 规则详情

参数	说明
规则名称	allowed-images-by-name
规则展示名	ECS实例的镜像名称在指定的范围
规则描述	指定允许的镜像名称列表，ECS实例的镜像名称不在指定的范围内，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	imageNames：镜像名称列表，镜像名称检查方式为部分匹配。

检测逻辑

- ECS实例的镜像名称被参数范围内任意值匹配或部分匹配，视为“合规”。
- ECS实例的镜像名称不能被参数范围内任意值匹配或部分匹配，视为“不合规”。

3.6.13.12 ECS 资源在备份存储库中

规则详情

表 3-71 规则详情

参数	说明
规则名称	ecs-protected-by-cbr
规则展示名	ECS资源在备份存储库中
规则描述	ECS资源没有关联备份存储库，视为“不合规”。
标签	cbr、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

3.6.13.13 ECS 云服务器的备份时间检查

规则详情

表 3-72 规则详情

参数	说明
规则名称	ecs-last-backup-created
规则展示名	ECS云服务器的备份时间检查
规则描述	ECS云服务器最近一次备份创建时间超过参数要求，视为“不合规”。
标签	cbr、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	lastBackupAgeValue：ECS要求的备份时间间隔（以小时为单位）。

3.6.13.14 ECS 资源绑定服务主机代理防护

规则详情

表 3-73 规则详情

参数	说明
规则名称	ecs-attached-hss-agents-check
规则展示名	ECS资源绑定服务主机代理防护
规则描述	ECS实例未绑定HSS代理并启用防护，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

3.6.14 分布式缓存服务 DCS

3.6.14.1 DCS Memcached 资源支持 SSL

规则详情

表 3-74 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

3.6.14.2 DCS Memcached 资源属于指定虚拟私有云 ID

规则详情

表 3-75 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。

应用场景

虚拟私有云（VPC）是您在云上的私有网络，可以为DCS构建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，确保DCS所有流量都安全地保留在虚拟私有云中，详见**虚拟私有云产品介绍**。

修复项指导

您可以通过网络配置，为不合规的Memcached绑定特定的虚拟私有云。该资源已经停售，建议使用Redis实例，见**停售说明**。

检测逻辑

- Memcached使用的VPC不是指定的VPC，视为“不合规”。
- Memcached使用的VPC是指定的VPC，视为“合规”。

3.6.14.3 DCS Memcached 资源不存在弹性公网 IP

规则详情

表 3-76 规则详情

参数	说明
规则名称	dcs-memcached-no-public-ip
规则展示名	DCS Memcached资源不存在弹性公网IP

参数	说明
规则描述	DCS Memcached资源存在弹性公网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

3.6.14.4 DCS Memcached 资源需要密码访问

规则详情

表 3-77 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

3.6.14.5 DCS Redis 实例支持 SSL

规则详情

表 3-78 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

参数	说明
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

3.6.14.6 DCS Redis 实例高可用

规则详情

表 3-79 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

3.6.14.7 DCS Redis 实例属于指定虚拟私有云 ID

规则详情

表 3-80 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。

应用场景

虚拟私有云（VPC）是您在云上的私有网络，可以为DCS构建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，确保DCS所有流量都安全地保留在虚拟私有云中，详见**虚拟私有云产品介绍**。

修复项指导

您可以通过网络配置，为不合规的DCS资源绑定特定的虚拟私有云，详见**查看和修改DCS实例基本信息**。

检测逻辑

- Redis使用的VPC不是指定的VPC，视为“不合规”。
- Redis使用的VPC是指定的VPC，视为“合规”。

3.6.14.8 DCS Redis 实例不存在弹性公网 IP

规则详情

表 3-81 规则详情

参数	说明
规则名称	dcs-redis-no-public-ip
规则展示名	DCS Redis实例不存在弹性公网IP
规则描述	DCS Redis资源存在弹性公网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

3.6.14.9 DCS Redis 实例需要密码访问

规则详情

表 3-82 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

参数	说明
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

3.6.15 函数工作流 FunctionGraph

3.6.15.1 函数工作流的函数并发数在指定范围内

规则详情

表 3-83 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。

3.6.15.2 函数工作流使用指定 VPC

规则详情

表 3-84 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

参数	说明
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。

3.6.15.3 函数工作流的函数不允许访问公网

规则详情

表 3-85 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

3.6.15.4 检查函数工作流参数设置

规则详情

表 3-86 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

参数	说明
规则评估的资源类型	fgs.functions
规则参数	• runtimeList：允许的运行时列表，当前支持的运行时请参见**函数管理**，例如“Python3.6”。 • timout：执行超时时间，单位为秒。 • memorySize：函数实例内存规格限制，单位为MB。

检测逻辑

- 函数工作流的运行时不在参数允许的运行时列表内，视为“不合规”。
- 函数工作流的超时时间大于参数设置的超时时间，视为“不合规”。
- 函数工作流的内存限制大于参数设置的内存限制，视为“不合规”。
- 函数工作量不满足以上场景，视为“合规”。

3.6.15.5 函数工作流的函数启用日志配置

规则详情

表 3-87 规则详情

参数	说明
规则名称	function-graph-logging-enabled
规则展示名	函数工作流的函数启用日志配置
规则描述	函数工作流的函数未启用日志配置，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

3.6.16 内容分发网络 CDN

3.6.16.1 CDN 使用 HTTPS 证书

规则详情

表 3-88 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

3.6.16.2 CDN 回源方式使用 HTTPS

规则详情

表 3-89 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

3.6.16.3 CDN 安全策略检查

规则详情

表 3-90 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

3.6.16.4 CDN 使用自有证书

规则详情

表 3-91 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

3.6.17 配置审计 Config

3.6.17.1 账号开启资源记录器

规则详情

表 3-92 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	account
规则参数	无

3.6.18 数据仓库服务 DWS

3.6.18.1 DWS 集群启用 KMS 加密

规则详情

表 3-93 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

3.6.18.2 DWS 集群启用日志转储

规则详情

表 3-94 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

3.6.18.3 DWS 集群启用自动快照

规则详情

表 3-95 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

3.6.18.4 DWS 集群启用 SSL 加密连接

规则详情

表 3-96 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

3.6.18.5 DWS 集群未绑定弹性公网 IP

规则详情

表 3-97 规则详情

参数	说明
规则名称	dws-clusters-no-public-ip
规则展示名	DWS集群未绑定弹性公网IP
规则描述	DWS集群绑定弹性公网IP，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

3.6.18.6 DWS 集群运维时间窗检查

规则详情

表 3-98 规则详情

参数	说明
规则名称	dws-maintain-window-check
规则展示名	DWS集群运维时间窗检查
规则描述	DWS集群运维时间窗不满足配置，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	• maintainDay：运维时间窗日期。 • maintainStartTime：运维时间窗开始时间。

3.6.18.7 DWS 集群 VPC 检查

规则详情

表 3-99 规则详情

参数	说明
规则名称	dws-clusters-in-vpc
规则展示名	DWS集群VPC检查
规则描述	DWS集群绑定的VPC不在对应VPC列表，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	VpcIdList：指定允许绑定的VPC ID列表，数组类型。

应用场景

虚拟私有云（VPC）是您在云上的私有网络，可以为DWS构建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，确保DWS所有流量都安全地保留在虚拟私有云中，详见**虚拟私有云产品介绍**。

修复项指导

您可以通过网络配置，为不合规的DWS资源绑定特定的虚拟私有云。

检测逻辑

- DWS集群绑定的VPC不在对应VPC列表，视为“不合规”。
- DWS集群绑定的VPC在对应VPC列表，视为“合规”。

3.6.19 数据复制服务 DRS

3.6.19.1 数据复制服务实时灾备任务不使用公网网络

规则详情

表 3-100 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

3.6.19.2 数据复制服务实时迁移任务不使用公网网络

规则详情

表 3-101 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

参数	说明
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

3.6.19.3 数据复制服务实时同步任务不使用公网网络

规则详情

表 3-102 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

3.6.20 数据加密服务 DEW

3.6.20.1 KMS 密钥不处于“计划删除”状态

规则详情

表 3-103 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

参数	说明
规则评估的资源类型	kms.keys
规则参数	无

3.6.20.2 KMS 密钥启用密钥轮换

规则详情

表 3-104 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

3.6.20.3 检查 CSMS 凭据轮转成功

规则详情

表 3-105 规则详情

参数	说明
规则名称	csms-secrets-rotation-success-check
规则展示名	检查CSMS凭据轮转成功
规则描述	CSMS凭据轮转失败，视为“不合规”。
标签	csms
规则触发方式	配置变更
规则评估的资源类型	csms.secrets
规则参数	无

3.6.20.4 CSMS 凭据启动自动轮转

规则详情

表 3-106 规则详情

参数	说明
规则名称	csms-secrets-auto-rotation-enabled
规则展示名	CSMS凭据启动自动轮转
规则描述	CSMS凭据未启动自动轮转，视为“不合规”。
标签	csms
规则触发方式	配置变更
规则评估的资源类型	csms.secrets
规则参数	无

应用场景

CSMS凭据可以配置轮转，您可以使用轮转来将长期机密信息替换为短期机密信息。轮转机密信息可以限制非授权用户使用被泄露机密信息的时间。因此，您应该经常轮转您的机密信息。

修复项指导

请为您的凭据配置自动轮转，并选择合适的**轮转策略**和轮转周期。

检测逻辑

- CSMS凭据未启动自动轮转，视为“不合规”。
- CSMS凭据已启动自动轮转，视为“合规”。

3.6.20.5 CSMS 凭据使用指定 KMS

规则详情

表 3-107 规则详情

参数	说明
规则名称	csms-secrets-using-cmk
规则展示名	CSMS凭据使用指定KMS
规则描述	CSMS凭据未使用指定的KMS，视为“不合规”。
标签	csms

参数	说明
规则触发方式	配置变更
规则评估的资源类型	csms.secrets
规则参数	kmsIdList：允许使用的KMS的ID列表，数组类型。

3.6.20.6 CSMS 凭据在指定时间内轮转

规则详情

表 3-108 规则详情

参数	说明
规则名称	csms-secrets-periodic-rotation
规则展示名	CSMS凭据在指定时间内轮转
规则描述	CSMS凭据未在指定天数内轮转，视为“不合规”。
标签	csms
规则触发方式	周期触发
规则评估的资源类型	csms.secrets
规则参数	maxRotationDays：最大未轮转天数，默认值为90。

应用场景

CSMS凭据可以配置轮转，您可以使用轮转来将长期机密信息替换为短期机密信息。轮转机密信息可以限制非授权用户使用被泄露机密信息的时间。因此，您应该经常轮转您的机密信息。

修复项指导

请为您的凭据配置自动轮转，并选择合适的**轮转策略**和轮转周期。

检测逻辑

- 如果CSMS凭据创建时间和当前时间的间隔小于等于指定天数，无论是否轮转过，均视为“合规”。
- 如果CSMS凭据创建时间和当前时间的间隔大于指定天数，且CSMS凭据未在指定天数内轮转，视为“不合规”。
- 如果CSMS凭据创建时间和当前时间的间隔大于指定天数，且CSMS凭据在指定天数内轮转过，视为“合规”。

3.6.21 统一身份认证服务 IAM

3.6.21.1 IAM 用户的 AccessKey 在指定时间内轮换

规则详情

表 3-109 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用户的访问密钥未在指定天数内轮转，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：访问密钥最大更换天数，默认值为90。

应用场景

企业用户通常都会使用访问密钥（AK/SK）的方式对云上的资源进行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。

修复项指导

轮换访问密钥可以通过创建两个访问密钥进行，将两个访问密钥作为一主一备，一开始先使用主访问密钥一，一段时间后，使用备访问密钥二，然后在控制台删除主访问密钥一，并重新生成一个访问密钥，在您的应用程序中定期轮换使用，详见**定期修改身份凭证**。

检测逻辑

- IAM用户未配置AccessKey，视为“合规”。
- IAM用户为“停用”状态，视为“合规”。
- IAM用户为“启用”状态，且其AccessKey在指定时间内轮换，视为“合规”。
- IAM用户为“启用”状态，且其AccessKey在指定时间内未轮换，视为“不合规”。

3.6.21.2 IAM 策略中不授权 KMS 的禁止的 action

规则详情

表 3-110 规则详情

参数	说明
规则名称	iam-customer-policy-blocked-kms-actions
规则展示名	IAM策略中不授权KMS的禁止的action
规则描述	IAM策略中授权KMS的任一阻拦action，视为“不合规”。
标签	iam、access-analyzer-verified
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。

应用场景

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，防止非预期的身份拥有对数据的解密或加密能力。

修复项指导

用户可以根据合规评估结果修改IAM策略配置，详见**修改、删除自定义策略**。

检测逻辑

- IAM策略或权限未授予指定的KMS操作权限，视为“合规”。
- IAM策略或权限授予指定的KMS操作权限，视为“不合规”。

3.6.21.3 IAM 用户组添加了 IAM 用户

规则详情

表 3-111 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

参数	说明
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

应用场景

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，实现对用户的授权。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用户组中至少有一个IAM用户，空置的IAM用户组为管理盲区，可能存在管理风险。

修复项指导

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，详见**用户组添加/移除用户**。

检测逻辑

- IAM用户组未添加IAM用户，视为“不合规”。
- IAM用户组添加任意IAM用户，视为“合规”。

3.6.21.4 IAM 用户密码策略符合要求

规则详情

表 3-112 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

参数	说明
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。 **说明** 各密码强度的详细说明如下： • Strong（高）：至少包含大写字母、小写字母、数字、特殊字符和空格中的四种或三种字符类型，且长度在8到32之间。 • Medium（中）：至少包含大写字母、小写字母、数字、特殊字符和空格中的两种字符类型，且长度在8到32之间。 • Low（低）：至少包含大写字母、小写字母、数字、特殊字符和空格中的一种字符类型，且长度在8到32之间。

应用场景

确保IAM用户密码强度满足密码强度要求，详见**设置强密码策略**。

修复项指导

用户可以根据要求修改密码达到需要的密码强度，详见**修改IAM用户密码**。

检测逻辑

- IAM用户未设置密码，视为“合规”。
- IAM用户为“停用”状态，视为“合规”。
- IAM用户为“启用”状态且已设置密码，若密码强度满足密码强度要求，视为“合规”。
- IAM用户为“启用”状态且已设置密码，若密码强度不满足密码强度要求，视为“不合规”。

3.6.21.5 IAM 策略黑名单检查

规则详情

表 3-113 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、委托使用指定权限或策略，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

参数	说明
规则参数	blackListPolicyUrns：IAM权限或IAM策略的名称列表，不支持系统策略。

应用场景

为IAM用户、IAM用户组、IAM委托分配指定的权限，避免非必要权限带来的安全隐患，详见**授予最小权限**。

修复项指导

移除不合规的IAM用户、IAM用户组、IAM委托的对应权限。

检测逻辑

- IAM的用户、用户组、委托使用指定权限或策略，视为“不合规”。
- IAM的用户、用户组、委托未使用指定权限或策略，视为“合规”。

3.6.21.6 IAM 策略不具备 Admin 权限

规则详情

表 3-114 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自定义策略具有allow的全部云服务的全部权限(*:*:*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

应用场景

确保IAM用户、用户组或委托仅拥有所需操作的相关权限。为了提高账号资源的安全性，不创建允许“*”或“*:*”或“*:*:*”管理权限的自定义策略。

修复项指导

管理员可以修改不合规的IAM自定义策略，详见**修改、删除自定义策略**。

检测逻辑

- IAM自定义策略配置了Allow的全部云服务的全部权限(action为“*:*:*”或“*:*”或“*”)，视为“不合规”。
- IAM自定义策略未配置Allow的全部云服务的全部权限，视为“合规”。

3.6.21.7 IAM 自定义策略具备所有权限

规则详情

表 3-115 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的任意云服务的全部权限，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

应用场景

确保IAM用户或IAM委托操作仅限于所需的操作。为了提高账号资源的安全性，不创建允许某个云服务全部管理权限的自定义策略。

修复项指导

管理员可以在IAM页面修改不合规的IAM自定义策略，详见**修改、删除自定义策略**。

检测逻辑

- IAM自定义策略配置了Allow的任意一个云服务的全部权限，视为“不合规”。
- IAM自定义策略未配置Allow的任意一个云服务的全部权限，视为“合规”。

3.6.21.8 根用户存在可使用的访问密钥

规则详情

表 3-116 规则详情

参数	说明
规则名称	iam-root-access-key-check
规则展示名	根用户存在可使用的访问密钥
规则描述	根用户存在可使用的访问密钥，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	account
规则参数	无

应用场景

为了提高根用户的安全性，建议您仅使用密码登录控制台即可，不要给根用户创建访问密钥，避免因访问密钥泄露带来的信息安全风险。

修复项指导

删除或停用根用户下的访问密钥，详见**管理IAM用户访问密钥**。

检测逻辑

- 根用户未配置“启用”状态的访问密钥，视为“合规”。
- 根用户配置了“启用”状态的访问密钥，视为“不合规”。

3.6.21.9 IAM 用户访问模式

规则详情

表 3-117 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

参数	说明
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

应用场景

确保IAM用户不能同时通过控制台和API访问云服务，同时赋予一个IAM用户两种访问方式将增加安全风险。访问方式分为如下两种：

- 编程访问：启用访问密钥，用户仅能通过API、CLI、SDK等开发工具访问华为云服务。
- 管理控制台访问：启用登录密码，用户仅能登录华为云管理控制台访问云服务。

须知

请用户不要通过密码方式进行编程访问。

修复项指导

修改IAM用户，访问方式只允许编程访问和管理控制台访问中的一种，并确保一个IAM用户上只配置登录密码和访问密钥中的一种。

检测逻辑

- IAM用户为“停用”状态，视为“合规”。
- IAM用户为“启用”状态，且未同时开启“编程访问”和“管理控制台访问”，视为“合规”。
- IAM用户为“启用”状态，且未同时配置登录密码和访问密钥，视为“合规”。
- IAM用户不满足以上场景，视为“不合规”。

3.6.21.10 IAM 用户创建时设置 AccessKey

规则详情

表 3-118 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	对于从Console侧访问的IAM用户，其创建时设置访问密钥，视为“不合规”。

参数	说明
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

应用场景

为了提高账号资源的安全性，建议在设置初始IAM用户时，对具有控制台密码的IAM用户，不能设置访问密钥。

修复项指导

根据规则评估结果删除相关IAM用户被创建时设置的访问密钥。

检测逻辑

- IAM用户为“停用”状态，视为“合规”。
- IAM用户未开启“管理控制台访问”，视为“合规”。
- IAM用户不具有创建时就存在的访问密钥，视为“合规”。
- IAM用户不满足以上条件，视为“不合规”。

3.6.21.11 IAM 用户归属指定用户组

规则详情

表 3-119 规则详情

参数	说明
规则名称	iam-user-group-membership-check
规则展示名	IAM用户归属指定用户组
规则描述	IAM用户不属于指定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。

应用场景

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。

修复项指导

选择合适的用户组，将不合规的IAM用户添加到用户组中。如果确认该IAM用户后续不再使用，则可将其停用或删除。

检测逻辑

- IAM用户为“停用”状态，视为“合规”。
- IAM用户为“启用”状态，且规则参数为空列表，若IAM用户属于任意一个IAM用户组，视为“合规”。
- IAM用户为“启用”状态，且规则参数为空列表，若IAM用户不属于任意一个IAM用户组，视为“不合规”。
- IAM用户为“启用”状态，且规则参数非空列表，若IAM用户属于任意一个指定的IAM用户组，视为“合规”。
- IAM用户为“启用”状态，且规则参数非空列表，若IAM用户不属于任意一个指定视为IAM用户组，视为“不合规”。

3.6.21.12 IAM 用户在指定时间内有登录行为

规则详情

表 3-120 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，默认值为90。

应用场景

及时发现不活跃的IAM用户，用于减少闲置用户或降低密码泄露的风险，提升账号安全。

修复项指导

使用该闲置的IAM用户登录管理控制台，或删除该闲置的IAM用户，详见**IAM用户登录**或**删除IAM用户**。

检测逻辑

- IAM用户为“停用”状态，视为“合规”。
- IAM用户未开启“管理控制台访问”，视为“合规”。
- IAM用户为“启用”状态且开启“管理控制台访问”，若在指定时间内有登录行为，视为“合规”。
- IAM用户为“启用”状态且开启“管理控制台访问”，若在指定时间内没有登录行为，视为“不合规”。

3.6.21.13 IAM 用户开启 MFA

规则详情

表 3-121 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

应用场景

Multi-Factor Authentication（简称MFA）是一种非常简单的安全实践方法，建议您给华为账号以及您账号中具备较高权限的用户开启MFA功能，它能够在用户名和密码之外再额外增加一层保护。启用MFA后，用户登录控制台时，系统将要求用户输入用户名和密码（第一安全要素），以及来自其MFA设备的验证码（第二安全要素）。这些多重要素结合起来将为您的账户和资源提供更高的安全保护。

修复项指导

您需要在智能设备上安装一个虚拟MFA应用程序后（例如：Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。详见**如何绑定虚拟MFA**。

检测逻辑

- IAM用户为“停用”状态，视为“合规”。
- IAM用户为“启用”状态且开启了MFA认证，视为“合规”。
- IAM用户为“启用”状态且未开启MFA认证，视为“不合规”。

3.6.21.14 IAM 用户单访问密钥

规则详情

表 3-122 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

应用场景

IAM用户的访问密钥是单独的身份凭证，即IAM用户仅能使用自己的访问密钥进行API调用。为了提高账号资源的安全性，建议单个IAM用户仅有一个可用的活动访问密钥。

修复项指导

根据规则评估结果删除或停用IAM用户多余的访问密钥，详见**管理IAM用户访问密钥**。

检测逻辑

- IAM用户为“停用”状态，视为“合规”。
- IAM用户为“启用”状态且仅拥有一个“active”状态的访问密钥，视为“合规”。
- IAM用户为“启用”状态且拥有两个“active”状态的访问密钥，视为“不合规”。

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

规则详情

表 3-123 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

应用场景

Multi-Factor Authentication（简称MFA）是一种非常简单的安全实践方法，建议您给华为账号以及您账号中具备较高权限的用户开启MFA功能，它能够在用户名和密码之外再额外增加一层保护。启用MFA后，用户登录控制台时，系统将要求用户输入用户名和密码（第一安全要素），以及来自其MFA设备的验证码（第二安全要素）。这些多重要素结合起来将为您的账户和资源提供更高的安全保护。

修复项指导

您需要在智能设备上安装一个虚拟MFA应用程序后（例如：Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。详见**如何绑定虚拟MFA**。

检测逻辑

- IAM用户为“停用”状态，视为“合规”。
- IAM用户未开启“管理控制台访问”，视为“合规”。
- IAM用户为“启用”状态且开启“管理控制台访问”，若其已开启MFA认证，视为“合规”。
- IAM用户为“启用”状态且开启“管理控制台访问”，若其未开启MFA认证，视为“不合规”。

3.6.21.16 根用户开启 MFA 认证

规则详情

表 3-124 规则详情

参数	说明
规则名称	root-account-mfa-enabled
规则展示名	根用户开启MFA认证
规则描述	根用户未开启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	account
规则参数	无

应用场景

Multi-Factor Authentication（简称MFA）是一种非常简单的安全实践方法，建议您给华为账号以及您账号中具备较高权限的用户开启MFA功能，它能够在用户名和密码之外再额外增加一层保护。启用MFA后，用户登录控制台时，系统将要求用户输入用户名和密码（第一安全要素），以及来自其MFA设备的验证码（第二安全要素）。这些多重要素结合起来将为您的账户和资源提供更高的安全保护。

修复项指导

您需要在智能设备上安装一个虚拟MFA应用程序后（例如：Google Authenticator或Microsoft Authenticator），才能绑定虚拟MFA设备。详见**如何绑定虚拟MFA**。

检测逻辑

- 根用户已开启MFA认证，视为“合规”。
- 根用户未开启MFA认证，视为“不合规”。

3.6.21.17 IAM 策略使用中

规则详情

表 3-125 规则详情

参数	说明
规则名称	iam-policy-in-use
规则展示名	IAM策略使用中

参数	说明
规则描述	IAM策略未附加到IAM用户、用户组或委托，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.policies
规则参数	无

应用场景

避免长期存在未绑定的IAM策略，防止因管理疏漏引发计划外授权，从而导致恶意操作。

修复项指导

判断该IAM策略是否仍需使用，将其附加到预期的IAM用户、用户组或委托上，或删除该IAM策略。

检测逻辑

- IAM策略附加到IAM用户、用户组或委托，视为“合规”。
- IAM策略未附加到IAM用户、用户组或委托，视为“不合规”。

3.6.21.18 IAM 权限使用中

规则详情

表 3-126 规则详情

参数	说明
规则名称	iam-role-in-use
规则展示名	IAM权限使用中
规则描述	IAM权限未附加到IAM用户、用户组或委托，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
规则参数	无

应用场景

避免长期存在未绑定的IAM权限，防止因管理疏漏引发计划外授权，从而导致恶意操作。

修复项指导

判断该IAM权限是否仍需使用，将其附加到预期的IAM用户、用户组或委托上，或删除该IAM权限。

检测逻辑

- IAM权限附加到IAM用户、用户组或委托，视为“合规”。
- IAM权限未附加到IAM用户、用户组或委托，视为“不合规”。

3.6.21.19 IAM 用户开启登录保护

规则详情

表 3-127 规则详情

参数	说明
规则名称	iam-user-login-protection-enabled
规则展示名	IAM用户开启登录保护
规则描述	IAM用户未开启登录保护，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

应用场景

为了进一步提高账号安全性，有效避免钓鱼式攻击或者用户密码意外泄漏，建议账号或管理员为IAM用户开启登录保护。开启登录保护后，IAM用户登录时，除了在登录页面输入用户名和密码外（第一次身份验证），还需要在登录验证页面输入验证码（第二次身份验证），该功能是一种安全实践，建议开启登录保护，多次身份认证可以提高安全性。当前可以选择通过手机、邮箱、虚拟MFA进行登录验证。

修复项指导

账号或管理员为相关IAM用户开启的登录保护状态，详见**登录保护**。

检测逻辑

- IAM用户为“停用”状态，视为“合规”。

- IAM用户为“启用”状态且开启了任意验证方式的登录保护，视为“合规”。
- IAM用户为“启用”状态且未开启任意验证方式的登录保护，视为“不合规”。

3.6.21.20 IAM 委托绑定策略检查

规则详情

表 3-128 规则详情

参数	说明
规则名称	iam-agencies-managed-policy-check
规则展示名	IAM委托绑定策略检查
规则描述	IAM委托未绑定指定的IAM策略或权限，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.agencies
规则参数	• roleIdList：指定允许的权限ID列表，不支持系统权限。 • policyIdList：指定允许的策略ID列表，不支持系统身份策略。

应用场景

为IAM委托授予权限时，避免过大权限带来的安全隐患。账号中的委托仅授予能完成工作所需的必需权限，通过最小权限原则，可以帮助您安全地控制IAM委托对云资源的访问。

修复项指导

IAM委托绑定所有指定的IAM策略和权限，详见**分配委托权限**。

检测逻辑

- IAM委托未绑定所有指定的IAM策略和权限，视为“不合规”。
- IAM委托绑定所有指定的IAM策略和权限，视为“合规”。

3.6.21.21 IAM 用户 admin 权限检查

规则详情

表 3-129 规则详情

参数	说明
规则名称	iam-user-check-non-admin-group
规则展示名	IAM用户admin权限检查
规则描述	根用户以外的IAM用户加入admin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	无

应用场景

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

修复项指导

进入IAM的“admin”用户组，删除企业管理员以外的IAM用户，详见**用户组添加/移除用户**。

检测逻辑

- IAM用户为根用户，视为“合规”。
- IAM用户为“停用”状态，视为“合规”。
- 根用户以外的“启用”状态的IAM用户加入admin用户组，视为“不合规”。
- 根用户以外的“启用”状态的IAM用户未加入admin用户组，视为“合规”。

3.6.21.22 IAM 用户不直接附加策略或权限

规则详情

表 3-130 规则详情

参数	说明
规则名称	iam-user-no-policies-check
规则展示名	IAM用户不直接附加策略或权限
规则描述	IAM用户直接附加了策略或权限，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.users
规则参数	无

应用场景

给IAM用户授权时建议您使用“继承所选用户组的策略”的方式，而不是“直接给用户授权”。这可以降低访问管理的复杂性，并减少IAM用户无意中接收或保留过多权限的风险。详见**给IAM用户授权**。

修复项指导

请创建IAM用户组，并将策略挂载到该用户组，然后将用户添加到用户组，删除用户上直接附加的策略或权限。

检测逻辑

- IAM用户直接附加了IAM策略或IAM权限，视为“不合规”。
- IAM用户未直接附加IAM策略或IAM权限，视为“合规”。

3.6.22 文档数据库服务 DDS

3.6.22.1 DDS 实例开启 SSL

规则详情

表 3-131 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

参数	说明
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

3.6.22.2 DDS 实例属于指定实例类型

规则详情

表 3-132 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。

3.6.22.3 DDS 实例未绑定弹性公网 IP

规则详情

表 3-133 规则详情

参数	说明
规则名称	dds-instance-has-eip
规则展示名	DDS实例未绑定弹性公网IP
规则描述	DDS实例绑定弹性公网IP，视为“不合规”。
标签	dds
规则触发方式	配置变更

参数	说明
规则评估的资源类型	dds.instances
规则参数	无

3.6.22.4 DDS 实例端口检查

规则详情

表 3-134 规则详情

参数	说明
规则名称	dds-instance-port-check
规则展示名	DDS实例端口检查
规则描述	DDS实例的端口包含被禁止的端口，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	disabledPortsPatterns：指定禁止的DDS实例的端口列表，数组类型。

3.6.22.5 DDS 实例数据库版本检查

规则详情

表 3-135 规则详情

参数	说明
规则名称	dds-instance-engine-version-check
规则展示名	DDS实例数据库版本检查
规则描述	DDS实例数据库的版本低于指定版本，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	specifiedVersion：数据库指定的版本，建议按照对应版本号格式指定，例如4.2。

3.6.22.6 DDS 实例属于指定虚拟私有云 ID

规则详情

表 3-136 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。

3.6.23 消息通知服务 SMN

3.6.23.1 SMN 主题配置访问日志

规则详情

表 3-137 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

3.6.24 虚拟私有云 VPC

3.6.24.1 未与子网关联的网络 ACL

规则详情

表 3-138 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

3.6.24.2 默认安全组关闭出、入方向流量

规则详情

表 3-139 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

检测逻辑

- VPC安全组非默认安全组，视为“合规”。
- VPC的默认安全组关闭出、入方向的流量，视为“合规”。
- VPC的默认安全组未关闭出、入方向的流量，视为“不合规”。

说明

安全组内一般包含多个安全组规则，流量匹配时生效机制复杂，见**流量匹配安全组规则的顺序**。Config进行分析时会忽略策略为“拒绝”的安全组规则，而只关心您可能放通了哪些流量。

3.6.24.3 VPC 启用流日志

规则详情

表 3-140 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

3.6.24.4 安全组端口检查

规则详情

表 3-141 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或::/0，且开放所有的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

检测逻辑

- 当安全组入方向源地址未设置为0.0.0.0/0或::/0，或未开放所有的TCP/UDP端口时，视为“合规”。
- 当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放所有的TCP/UDP端口时，视为“不合规”。

说明

安全组内一般包含多个安全组规则，流量匹配时生效机制复杂，见**流量匹配安全组规则的顺序**。Config进行分析时会忽略策略为“拒绝”的安全组规则，而只关心您可能放通了哪些流量。

3.6.24.5 安全组入站流量限制指定端口

规则详情

表 3-142 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)或所有IPv6地址(::/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。

检测逻辑

- 当安全组的入站流量未放通参数指定端口的所有IPv4地址(0.0.0.0/0)和所有IPv6地址(::/0)，视为“合规”。
- 当安全组的入站流量放通参数指定端口的所有IPv4地址(0.0.0.0/0)或所有IPv6地址(::/0)，视为“不合规”。

说明

安全组内一般包含多个安全组规则，流量匹配时生效机制复杂，见**流量匹配安全组规则的顺序**。Config进行分析时会忽略策略为“拒绝”的安全组规则，而只关心您可能放通了哪些流量。

3.6.24.6 安全组入站流量限制 SSH 端口

规则详情

表 3-143 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或::/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

检测逻辑

- 当安全组的入站流量未放通TCP 22端口的所有IPv4地址(0.0.0.0/0)和所有IPv6地址(::/0)，视为“合规”。
- 当安全组的入站流量放通TCP 22端口的所有IPv4地址(0.0.0.0/0)或所有IPv6地址(::/0)，视为“不合规”。

说明

安全组内一般包含多个安全组规则，流量匹配时生效机制复杂，见**流量匹配安全组规则的顺序**。Config进行分析时会忽略策略为“拒绝”的安全组规则，而只关心您可能放通了哪些流量。

3.6.24.7 安全组非白名单端口检查

规则详情

表 3-144 规则详情

参数	说明
规则名称	vpc-sg-by-white-list-ports-check
规则展示名	安全组非白名单端口检查
规则描述	除指定的白名单端口外，其余端口的安全组策略为允许，视为“不合规”。
标签	vpc
规则触发方式	配置变更

参数	说明
规则评估的资源类型	vpc.securityGroups
规则参数	whiteListPorts：白名单端口列表。

检测逻辑

- 安全组入方向规则和出方向规则均不放通所有白名单端口以外端口的流量，视为“合规”。
- 安全组入方向规则或出方向规则放通任意白名单端口以外端口的流量，视为“不合规”。

说明

安全组内一般包含多个安全组规则，流量匹配时生效机制复杂，见**流量匹配安全组规则的顺序**。Config进行分析时会忽略策略为“拒绝”的安全组规则，而只关心您可能放通了哪些流量。

3.6.24.8 安全组连接到弹性网络接口

规则详情

表 3-145 规则详情

参数	说明
规则名称	vpc-sg-attached-ports
规则展示名	安全组连接到弹性网络接口
规则描述	检查非默认安全组是否连接到弹性网络接口（ports）。如果安全组未关联弹性网络接口（ports），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

3.6.25 虚拟专用网络 VPN

3.6.25.1 VPN 连接状态为“正常”

规则详情

表 3-146 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

3.6.26 云监控服务 CES

3.6.26.1 CES 启用告警操作

规则详情

表 3-147 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

3.6.26.2 CES 配置监控 KMS 禁用或计划删除密钥的事件监控告警

规则详情

表 3-148 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禁用或计划删除密钥的事件监控告警
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	account
规则参数	无

检测逻辑

- 账号未配置“计划删除密钥”或未配置“禁用密钥”的事件监控告警，视为“不合规”。
- 账号已配置“计划删除密钥”和“禁用密钥”的事件监控告警，视为“合规”。
- CES服务目前支持监控的系统事件请参见**事件监控支持的事件说明**。

3.6.26.3 CES 配置监控 OBS 桶策略变更的事件监控告警

规则详情

表 3-149 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	account
规则参数	无

检测逻辑

- 账号未配置“设置桶的策略”或未配置“删除桶policy配置”的事件监控告警，视为“不合规”。
- 账号已配置“设置桶的策略”和“删除桶policy配置”的事件监控告警，视为“合规”。
- CES服务目前支持监控的系统事件请参见**事件监控支持的事件说明**。

3.6.26.4 指定的资源类型绑定指定指标 CES 告警

规则详情

表 3-150 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	account
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。

3.6.26.5 检查特定指标的 CES 告警进行特定配置

规则详情

表 3-151 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。

3.6.26.6 CES 配置监控 VPC 变更的事件监控告警

规则详情

表 3-152 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	account
规则参数	无

检测逻辑

- 账号未配置“修改VPC”的事件监控告警，视为“不合规”。
- 账号已配置“修改VPC”的事件监控告警，视为“合规”。
- CES服务目前支持监控的系统事件请参见**事件监控支持的事件说明**。

3.6.27 云容器引擎 CCE

3.6.27.1 CCE 集群版本为处于维护的版本

规则详情

表 3-153 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
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

3.6.27.2 CCE 集群运行的非受支持的最旧版本

规则详情

表 3-154 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

3.6.27.3 CCE 集群资源不具有弹性公网 IP

规则详情

表 3-155 规则详情

参数	说明
规则名称	cce-endpoint-public-access
规则展示名	CCE集群资源不具有弹性公网IP
规则描述	CCE集群资源具有弹性公网IP，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

3.6.27.4 CCE 集群规格在指定的范围

规则详情

表 3-156 规则详情

参数	说明
规则名称	allowed-cce-flavors
规则展示名	CCE集群规格在指定的范围
规则描述	CCE集群的规格不在指定的范围内，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	listOfAllowedFlavors：指定的CCE规格列表，枚举值请参见**flavor**字段当前所支持的值，例如“cce.s1.small”。

检测逻辑

- CCE集群的规格在参数配置的范围内，视为“合规”。
- CCE集群的规格不在参数配置的范围内，视为“不合规”。

3.6.27.5 CCE 集群 VPC 检查

规则详情

表 3-157 规则详情

参数	说明
规则名称	cce-cluster-in-vpc
规则展示名	CCE集群VPC检查
规则描述	CCE集群绑定的VPC不在对应VPC列表，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	VpcIdList：指定允许绑定的VPC ID列表，数组类型。

应用场景

虚拟私有云（VPC）是您在云上的私有网络，可以为CCE构建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，确保CCE所有流量都安全地保留在虚拟私有云中，详见**虚拟私有云产品介绍**。

修复项指导

您可以通过网络配置，为不合规的CCE集群绑定特定的虚拟私有云，详见**修改CCE集群配置**。

检测逻辑

- CCE集群绑定的VPC不在对应VPC列表，视为“不合规”。
- CCE集群绑定的VPC在对应VPC列表，视为“合规”。

3.6.28 云审计服务 CTS

3.6.28.1 CTS 追踪器通过 KMS 进行加密

规则详情

表 3-158 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

参数	说明
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

应用场景

确保CTS追踪器转储归档的审计事件到OBS桶时，数据是被加密的。

修复项指导

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。

检测逻辑

- 无论是否为启用状态，CTS追踪器未配置KMS加密，视为“不合规”。
- 无论是否为启用状态，CTS追踪器配置KMS加密，视为“合规”。

使用约束

组织追踪器的场景下，在成员账号上使用该合规规则时，由于Config收集组织管理员下发的追踪器资源存在时延，合规评估结果的更新可能存在最多不超过24小时的滞后。

3.6.28.2 CTS 追踪器启用事件分析

规则详情

表 3-159 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追踪器未转储到LTS，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

应用场景

云审计服务记录了用户对云服务资源新建、修改、删除等操作的详细信息，控制台的事件列表中会保存最近7天的操作记录。如果需要将操作记录保存7天以上，则需要配置事件转储至LTS功能，云审计服务会定期将操作记录同步保存到用户定义的LTS日志流中进行长期保存。

修复项指导

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，并将当前用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，详见**配置云审计事件转储至LTS并查看**。

检测逻辑

- 无论是否为启用状态，CTS追踪器配置转储到LTS，视为“合规”。
- 无论是否为启用状态，CTS追踪器未配置转储到LTS，视为“不合规”。

使用约束

组织追踪器的场景下，在成员账号上使用该合规规则时，由于Config收集组织管理员下发的追踪器资源存在时延，合规评估结果的更新可能存在最多不超过24小时的滞后。

3.6.28.3 CTS 追踪器追踪指定的 OBS 桶

规则详情

表 3-160 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	account
规则参数	trackBucket：指定的OBS桶名称，字符串类型。

应用场景

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，即针对用户对OBS桶中的数据的操作日志，例如上传、下载等。

修复项指导

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，详见**配置追踪器**。

检测逻辑

- 配置数据类追踪器追踪OBS桶时，只追踪“读操作”或“写操作”，也视为追踪该OBS桶。
- 账号下存在“启用”状态的CTS追踪器追踪指定的OBS桶，视为“合规”。
- 账号下所有“启用”状态的CTS追踪器均未追踪指定的OBS桶，视为“不合规”。
- 账号下不存在“启用”状态的CTS追踪器，视为“不合规”。

3.6.28.4 CTS 追踪器打开事件文件校验

规则详情

表 3-161 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

应用场景

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，从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。

修复项指导

在CTS追踪器的配置转储页面打开“文件校验”开关，即可开启事件文件完整性校验功能，详见**开启事件文件完整性校验功能**。

检测逻辑

- 无论是否为启用状态，CTS追踪器打开事件文件校验，视为“合规”。
- 无论是否为启用状态，CTS追踪器未打开事件文件校验，视为“不合规”。

使用约束

组织追踪器的场景下，在成员账号上使用该合规规则时，由于Config收集组织管理员下发的追踪器资源存在时延，合规评估结果的更新可能存在最多不超过24小时的滞后。

3.6.28.5 创建并启用 CTS 追踪器

规则详情

表 3-162 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	账号未创建并启用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	account
规则参数	无

应用场景

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，即针对用户对OBS桶中的数据的操作日志，例如上传、下载等。

修复项指导

用户首次进入云审计服务时，在追踪器页面单击“开通云审计服务”，系统会自动为您创建一个名为system的管理类事件追踪器，详见**创建追踪器**。

检测逻辑

- 账号未创建CTS追踪器，视为“不合规”。
- 账号已创建CTS追踪器，但均未启用，视为“不合规”。
- 账号已创建并启用CTS追踪器，视为“合规”。

使用约束

组织追踪器的场景下，在成员账号上使用该合规规则时，由于Config收集组织管理员下发的追踪器资源存在时延，合规评估结果的更新可能存在最多不超过24小时的滞后。

3.6.28.6 在指定区域创建并启用 CTS 追踪器

规则详情

表 3-163 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	account
规则参数	regionList：指定的Region列表，数组类型。

应用场景

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。

修复项指导

用户首次进入云审计服务时，在追踪器页面单击“开通云审计服务”，系统会自动为您创建一个名为system的管理类事件追踪器，详见**创建追踪器**。

检测逻辑

- 账号在指定区域均已创建“启用”状态的CTS追踪器，视为“合规”。
- 账号在任意指定的区域，未创建“启用”状态的CTS追踪器，视为“不合规”。

使用约束

组织追踪器的场景下，在成员账号上使用该合规规则时，由于Config收集组织管理员下发的追踪器资源存在时延，合规评估结果的更新可能存在最多不超过24小时的滞后。

3.6.28.7 CTS 追踪器符合安全最佳实践

规则详情

表 3-164 规则详情

参数	说明
规则名称	cts-tracker-enabled-security
规则展示名	CTS追踪器符合安全最佳实践
规则描述	不存在满足安全最佳实践的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	account
规则参数	regions：区域列表，如果为空列表，则表示任意区域。

应用场景

云审计服务，是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。需要满足安全最佳实践以避免日志文件丢失、被篡改或泄露。

- 文件校验: 可以检验转储至OBS桶的数据是否被篡改，保障事件文件的完整性。
- 加密事件文件: 云审计支持对事件文件加密存储。
- 转储到LTS: 当“转储到LTS”开关打开时，表示操作事件将转储到日志流中。

修复项指导

云审计服务管理控制台支持对已创建的追踪器增加文件校验、加密事件文件、LTS转储等相关配置，详见**配置追踪器**。

检测逻辑

- 如果CTS追踪器配置文件校验、加密事件文件、转储到LTS，视其满足CTS的安全最佳实践。
- 若规则参数列表为空，账号中存在至少一个符合安全最佳实践的“启用”状态的CTS追踪器，视为“合规”。
- 若规则参数列表为空，账号中不存在符合安全最佳实践的“启用”状态的CTS追踪器，视为“不合规”。
- 若规则参数列表非空，相关区域存在至少一个符合安全最佳实践的“启用”状态的CTS追踪器，视为“合规”。
- 若规则参数列表非空，相关区域均不存在符合安全最佳实践的“启用”状态的CTS追踪器，视为“不合规”。

使用约束

组织追踪器的场景下，在成员账号上使用该合规规则时，由于Config收集组织管理员下发的追踪器资源存在时延，合规评估结果的更新可能存在最多不超过24小时的滞后。

3.6.29 云数据库 RDS

3.6.29.1 RDS 实例开启备份

规则详情

表 3-165 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

3.6.29.2 RDS 实例开启错误日志

规则详情

表 3-166 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

3.6.29.3 RDS 实例开启慢日志

规则详情

表 3-167 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

3.6.29.4 RDS 实例支持多可用区

规则详情

表 3-168 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

3.6.29.5 RDS 实例不具有弹性公网 IP

规则详情

表 3-169 规则详情

参数	说明
规则名称	rds-instance-no-public-ip
规则展示名	RDS实例不具有弹性公网IP
规则描述	RDS资源具有弹性公网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

3.6.29.6 RDS 实例开启存储加密

规则详情

表 3-170 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

3.6.29.7 RDS 实例属于指定虚拟私有云 ID

规则详情

表 3-171 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：RDS实例使用的VPC ID。

应用场景

虚拟私有云（VPC）是您在云上的私有网络，可以为RDS构建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，确保RDS所有流量都安全地保留在虚拟私有云中，详见**虚拟私有云产品介绍**。

修复项指导

RDS实例创建后，暂不支持直接通过控制台更换VPC和子网。但您可以通过已有RDS的全量备份恢复到新实例的方法切换到目标VPC和子网。具体操作请参考**恢复备份**。

检测逻辑

- RDS实例使用的VPC不是指定的VPC，视为“不合规”。
- RDS实例使用的VPC是指定的VPC，视为“合规”。

3.6.29.8 RDS 实例配备日志

规则详情

表 3-172 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”。

参数	说明
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

3.6.29.9 RDS 实例规格在指定的范围

规则详情

表 3-173 规则详情

参数	说明
规则名称	allowed-rds-flavors
规则展示名	RDS实例规格在指定的范围
规则描述	RDS实例的规格不在指定的范围内，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	listOfAllowedFlavors：指定的RDS规格列表。

3.6.29.10 RDS 实例启用 SSL 加密通讯

规则详情

表 3-174 规则详情

参数	说明
规则名称	rds-instance-ssl-enable
规则展示名	RDS实例启用SSL加密通讯
规则描述	RDS实例未启用SSL加密通讯，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

参数	说明
规则参数	无

3.6.29.11 RDS 实例端口检查

规则详情

表 3-175 规则详情

参数	说明
规则名称	rds-instance-port-check
规则展示名	RDS实例默认端口检查
规则描述	RDS实例的端口包含被禁止的端口，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	• blockedPortsForMysql：指定MySQL数据库禁止的端口列表，数组类型。 • blockedPortsForMariadb：指定MariaDB数据库禁止的端口列表，数组类型。 • blockedPortsForPostgresql：指定PostgreSQL数据库禁止的端口列表，数组类型。 • blockedPortsForSqlserver：SQLServer数据库禁止的端口列表，数组类型。

3.6.29.12 RDS 实例数据库引擎版本检查

规则详情

表 3-176 规则详情

参数	说明
规则名称	rds-instance-engine-version-check
规则展示名	RDS实例数据库引擎版本检查
规则描述	RDS实例数据库引擎的版本低于指定版本，视为“不合规”。
标签	rds

参数	说明
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	• mysqlVersion：MySQL类型的数据库引擎指定的版本，建议按照对应版本号格式指定，例如8.0.28。 • postgresqlVersion：PostgreSQL类型的数据库引擎指定的版本，建议按照对应版本号格式指定，例如10.16。 • mariadbVersion：MariaDB类型的数据库引擎指定的版本，建议按照对应版本号格式指定，例如10.5。 • sqlserverVersion：SQLServer类型的数据库引擎指定的版本，建议按照对应版本号格式指定，例如2017。

3.6.29.13 RDS 实例启用审计日志

规则详情

表 3-177 规则详情

参数	说明
规则名称	rds-instance-enable-auditLog
规则展示名	RDS实例启用审计日志
规则描述	未启用审计日志或审计日志保存天数不足的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	keepDays：审计日志需要保存的天数。

3.6.30 云数据库 GaussDB

3.6.30.1 GaussDB 资源属于指定虚拟私有云 ID

规则详情

表 3-178 规则详情

参数	说明
规则名称	gaussdb-instance-in-vpc
规则展示名	GaussDB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GaussDB实例，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：GaussDB使用的VPC ID。

应用场景

虚拟私有云（VPC）是您在云上的私有网络，可以为GaussDB构建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，确保GaussDB所有流量都安全地保留在虚拟私有云中，详见**虚拟私有云产品介绍**。

修复项指导

GaussDB实例暂不支持直接通过控制台更换VPC。但您可以通过已有GaussDB的全量备份恢复到新实例的方法切换到目标VPC。具体操作请参考**数据恢复**。

检测逻辑

- GaussDB实例使用的VPC不是指定的VPC，视为“不合规”。
- GaussDB实例使用的VPC是指定的VPC，视为“合规”。

3.6.30.2 GaussDB 实例开启审计日志

规则详情

表 3-179 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实例，视为“不合规”。

参数	说明
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

3.6.30.3 GaussDB 实例开启自动备份

规则详情

表 3-180 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实例，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

3.6.30.4 GaussDB 实例开启错误日志

规则详情

表 3-181 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实例，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

参数	说明
规则参数	无

3.6.30.5 GaussDB 实例开启慢日志

规则详情

表 3-182 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实例，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

3.6.30.6 GaussDB 实例 EIP 检查

规则详情

表 3-183 规则详情

参数	说明
规则名称	gaussdb-instance-no-public-ip-check
规则展示名	GaussDB实例EIP检查
规则描述	GaussDB实例如绑定EIP，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

3.6.30.7 GaussDB 实例跨 AZ 部署检查

规则详情

表 3-184 规则详情

参数	说明
规则名称	gaussdb-instance-multiple-az-check
规则展示名	GaussDB实例跨AZ部署检查
规则描述	GaussDB实例未跨AZ部署，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

3.6.30.8 GaussDB 实例开启传输数据加密

规则详情

表 3-185 规则详情

参数	说明
规则名称	gaussdb-instance-ssl-enable
规则展示名	GaussDB实例开启传输数据加密
规则描述	GaussDB实例未启用SSL数据传输加密，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

3.6.31 云数据库 TaurusDB

3.6.31.1 TaurusDB 实例开启慢日志

规则详情

表 3-186 规则详情

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

3.6.31.2 TaurusDB 实例开启错误日志

规则详情

表 3-187 规则详情

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

3.6.31.3 TaurusDB 实例开启备份

规则详情

表 3-188 规则详情

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

3.6.31.4 TaurusDB 实例开启审计日志

规则详情

表 3-189 规则详情

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

3.6.31.5 TaurusDB 实例开启传输数据加密

规则详情

表 3-190 规则详情

参数	说明
规则名称	gaussdb-mysql-instance-ssl-enable
规则展示名	TaurusDB实例开启传输数据加密
规则描述	TaurusDB实例未启用SSL数据传输加密，视为“不合规”。
标签	taurusdb
规则触发方式	配置变更
规则评估的资源类型	gaussdbformysql.instance
规则参数	无

3.6.31.6 TaurusDB 实例跨 AZ 部署检查

规则详情

表 3-191 规则详情

参数	说明
规则名称	gaussdb-mysql-instance-multiple-az-check
规则展示名	TaurusDB实例跨AZ部署检查
规则描述	TaurusDB实例未跨AZ部署，视为“不合规”。
标签	taurusdb
规则触发方式	配置变更
规则评估的资源类型	gaussdbformysql.instance
规则参数	无

3.6.31.7 TaurusDB 实例 EIP 检查

规则详情

表 3-192 规则详情

参数	说明
规则名称	gaussdb-mysql-instance-no-public-ip-check
规则展示名	TaurusDB实例EIP检查
规则描述	TaurusDB实例如绑定EIP，视为“不合规”。
标签	taurusdb
规则触发方式	配置变更
规则评估的资源类型	gaussdbformysql.instance
规则参数	无

3.6.31.8 TaurusDB 实例 VPC 检查

规则详情

表 3-193 规则详情

参数	说明
规则名称	gaussdb-mysql-instance-in-vpc
规则展示名	TaurusDB实例VPC检查
规则描述	TaurusDB实例绑定的VPC不在对应VPC列表，视为“不合规”。
标签	taurusdb
规则触发方式	配置变更
规则评估的资源类型	gaussdbformysql.instance
规则参数	VpcIdList：指定允许绑定的VPC ID列表，数组类型。

应用场景

虚拟私有云（VPC）是您在云上的私有网络，可以为TaurusDB实例构建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，确保TaurusDB实例所有流量都安全地保留在虚拟私有云中，详见**虚拟私有云产品介绍**。

修复项指导

TaurusDB实例创建完成后不支持切换虚拟私有云，请谨慎选择所属虚拟私有云。详见**购买TaurusDB实例**中关于虚拟私有云部分的介绍。

检测逻辑

- TaurusDB实例绑定的VPC不在对应VPC列表，视为“不合规”。
- TaurusDB实例绑定的VPC在对应VPC列表，视为“合规”。

3.6.32 云数据库 GeminiDB

3.6.32.1 GeminiDB 开启慢查询日志

规则详情

表 3-194 规则详情

参数	说明
规则名称	gaussdb-nosql-support-slow-log
规则展示名	GeminiDB开启慢查询日志
规则描述	GeminiDB不开启慢查询日志，视为“不合规”。
标签	gemini db
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

3.6.32.2 GeminiDB 开启错误日志

规则详情

表 3-195 规则详情

参数	说明
规则名称	gaussdb-nosql-enable-error-log
规则展示名	GeminiDB开启错误日志
规则描述	GeminiDB未开启错误日志，视为“不合规”。
标签	gemini db
规则触发方式	配置变更

参数	说明
规则评估的资源类型	nosql.instances
规则参数	无

3.6.32.3 GeminiDB 使用磁盘加密

规则详情

表 3-196 规则详情

参数	说明
规则名称	gaussdb-nosql-enable-disk-encryption
规则展示名	GeminiDB使用磁盘加密
规则描述	GeminiDB未使用磁盘加密，视为“不合规”。
标签	gemini db
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

3.6.32.4 GeminiDB 开启备份

规则详情

表 3-197 规则详情

参数	说明
规则名称	gaussdb-nosql-enable-backup
规则展示名	GeminiDB开启备份
规则描述	GeminiDB未开启备份，视为“不合规”。
标签	gemini db
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

3.6.32.5 GeminiDB 部署在单个可用区

规则详情

表 3-198 规则详情

参数	说明
规则名称	gaussdb-nosql-deploy-in-single-az
规则展示名	GeminiDB部署在单个可用区
规则描述	GeminiDB部署在单个可用区中，视为“不合规”。
标签	gemini db
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

3.6.33 云搜索服务 CSS

3.6.33.1 CSS 集群启用安全模式

规则详情

表 3-199 规则详情

参数	说明
规则名称	css-cluster-authority-enable
规则展示名	CSS集群启用安全模式
规则描述	CSS集群未启用安全模式，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

应用场景

CSS集群内部的权限控制是通过安全集群实现的，当集群开启安全模式后，访问集群时需要进行身份认证，通过Kibana可以给集群创建用户进行授权。确保CSS集群启用了认证，详见**身份认证与访问控制**。

修复项指导

部分集群支持开启安全模式。用户可以通过**安全模式修改**API接口启用安全模式。

检测逻辑

- CSS集群未启用安全模式，视为“不合规”。
- CSS集群启用安全模式，视为“合规”。

3.6.33.2 CSS 集群启用快照

规则详情

表 3-200 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

应用场景

为避免数据丢失，您可以将集群的索引数据进行备份，当数据发生丢失或者想找回某一时间段数据时，您可以通过恢复索引操作快速获得数据。索引的备份是通过创建集群快照实现。第一次备份时，建议将所有索引数据进行备份。

修复项指导

在“集群快照”管理页面，单击“集群快照开关”右侧开关，打开集群快照功能，详见**设置自动创建快照**。

检测逻辑

- CSS集群未开启快照，视为“不合规”。
- CSS集群开启了快照，视为“合规”。

3.6.33.3 CSS 集群开启磁盘加密

规则详情

表 3-201 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

应用场景

由于可能存在敏感数据，请启用磁盘加密以保护相关数据。

修复项指导

当前CSS服务暂时不支持磁盘加密功能，请避免在CSS服务中存储敏感数据。

检测逻辑

- CSS集群未开启磁盘加密，视为“不合规”。
- CSS集群开启了磁盘加密，视为“合规”。

3.6.33.4 CSS 集群启用 HTTPS

规则详情

表 3-202 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

参数	说明
规则评估的资源类型	css.clusters
规则参数	无

应用场景

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。详见**切换安全模式下的协议**。

修复项指导

CSS集群的安全模式启用时，开启HTTPS访问，访问集群将进行通讯加密。用户可以通过**安全模式修改**API接口启用安全模式。

检测逻辑

- CSS集群未启用安全模式，视为“不合规”。
- CSS集群启用安全模式但未开启HTTPS访问，视为“不合规”。
- CSS集群启用安全模式并且开启HTTPS访问，视为“合规”。

3.6.33.5 CSS 集群绑定指定 VPC 资源

规则详情

表 3-203 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。

应用场景

虚拟私有云（VPC）是您在云上的私有网络，可以为CSS构建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，确保CSS所有流量都安全地保留在虚拟私有云中，详见**虚拟私有云产品介绍**。

修复项指导

您可以通过网络配置，为不合规的CSS集群绑定特定的虚拟私有云。

检测逻辑

- CSS集群绑定的VPC不在对应VPC列表，视为“不合规”。
- CSS集群绑定的VPC在对应VPC列表，视为“合规”。

3.6.33.6 CSS 集群具备多 AZ 容灾

规则详情

表 3-204 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

应用场景

为防止数据丢失，并确保在服务中断情况下能降低集群的停机时间，从而增强集群的高可用性，CSS服务支持跨可用区（即多可用区）部署。用户可以在同一个区域内选择两个或三个不同的可用区进行集群部署。详见**规划集群可用区**。

修复项指导

在创建集群时，如果用户选择了两个或三个可用区，CSS服务将自动开启跨AZ的高可用性特性，确保节点在这些可用区内均匀分配。

检测逻辑

- CSS集群单AZ部署，视为“不合规”。
- CSS集群多AZ部署，视为“合规”。

3.6.33.7 CSS 集群具备多实例容灾

规则详情

表 3-205 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

应用场景

为防止数据丢失，并确保在服务中断情况下能降低集群的停机时间，从而增强集群的高可用性，请确保CSS集群的实例个数大于等于2个。

修复项指导

针对实例个数不足的CSS集群，**扩容集群**中实例数量。

检测逻辑

- CSS集群节点数量为1个，视为“不合规”。
- CSS集群节点数量大于1个，视为“合规”。

3.6.33.8 CSS 集群不能公网访问

规则详情

表 3-206 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

参数	说明
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

应用场景

确保CSS集群不能公网访问。由于敏感数据可能存在，请关闭CSS集群的公网访问。详见**配置公网访问**。

修复项指导

用户可以通过**关闭公网访问**API接口阻止CSS集群被公网访问。

检测逻辑

- CSS集群开启公网访问，视为“不合规”。
- CSS集群未开启公网访问，视为“合规”。

3.6.33.9 CSS 集群支持安全模式

规则详情

表 3-207 规则详情

参数	说明
规则名称	css-cluster-security-mode-enable
规则展示名	CSS集群支持安全模式
规则描述	CSS集群不支持安全模式，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

应用场景

非安全模式的集群无需安全认证即可访问，采用HTTP协议明文传输数据。建议确认访问环境的安全性，勿将访问接口暴露到公网环境上。安全模式的集群需要通过安全认证才能访问，且支持对集群进行授权、加密等功能。采用HTTPS协议进行通信加密，使数据更安全。详见**更改Elasticsearch集群安全模式**。

修复项指导

部分集群版本不支持开启安全模式，请使用支持安全模式的版本，如Elasticsearch 7.10.2等。

检测逻辑

- CSS集群不支持安全模式，视为“不合规”。
- CSS集群支持安全模式，视为“合规”。

3.6.33.10 CSS 集群未开启访问控制开关

规则详情

表 3-208 规则详情

参数	说明
规则名称	css-cluster-not-enable-white-list
规则展示名	CSS集群未开启访问控制开关
规则描述	CSS集群未开启访问控制开关，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

应用场景

如果关闭访问控制开关，则允许任何IP通过公网IP访问集群。如果开启访问控制开关，则只允许白名单列表中的IP通过公网IP访问集群。详见**配置公网访问**。

修复项指导

用户可以通过接口**开启公网访问控制白名单**配置合适的访问控制白名单。

检测逻辑

- CSS集群未开启公网访问，视为“合规”。
- CSS集群开启了公网访问但未开启访问控制开关，视为“不合规”。
- CSS集群开启了公网访问且开启了访问控制开关，视为“合规”。

3.6.33.11 CSS 集群 Kibana 未开启访问控制开关

规则详情

表 3-209 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未开启访问控制开关
规则描述	CSS集群Kibana未开启访问控制开关，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

应用场景

如果关闭访问控制开关，则允许任何IP通过公网IP访问集群Kibana。如果开启访问控制开关，则只允许白名单列表中的IP通过公网IP访问集群Kibana。详见**通过公网地址访问Kibana登录Elasticsearch集群**。

修复项指导

用户可以通过接口**开启Kibana公网访问**配置合适的访问控制白名单。

检测逻辑

- CSS集群Kibana未开启公网访问，视为“合规”。
- CSS集群Kibana开启了公网访问但未开启访问控制开关，视为“不合规”。
- CSS集群Kibana开启了公网访问且开启了访问控制开关，视为“合规”。

3.6.33.12 CSS 集群开启慢日志

规则详情

表 3-210 规则详情

参数	说明
规则名称	css-cluster-slowLog-enable
规则展示名	CSS集群开启慢日志
规则描述	CSS集群未开启慢日志，视为“不合规”。

参数	说明
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

应用场景

Elasticsearch和OpenSearch集群备份的日志文件主要包括废弃操作日志、运行日志、慢索引日志、慢查询日志，用户可以使用日志定位问题，详见**查询和管理Elasticsearch集群日志**。

修复项指导

CSS集群默认记录慢日志，用户可以将其转储在OBS桶中，详见**修改日志基础配置**。

检测逻辑

- CSS集群未开启慢日志，视为“不合规”。
- CSS集群开启慢日志，视为“合规”。

3.6.34 云硬盘 EVS

3.6.34.1 云硬盘的类型在指定的范围内

规则详情

表 3-211 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。

3.6.34.2 云硬盘创建后在指定天数内绑定资源实例

规则详情

表 3-212 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。

3.6.34.3 云硬盘闲置检测

规则详情

表 3-213 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

3.6.34.4 已挂载的云硬盘开启加密

规则详情

表 3-214 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

3.6.34.5 云硬盘开启加密

规则详情

表 3-215 规则详情

参数	说明
规则名称	volumes-encrypted-check-by-default
规则展示名	云硬盘开启加密
规则描述	云硬盘未进行加密，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

3.6.34.6 EVS 资源在备份存储库保护中

规则详情

表 3-216 规则详情

参数	说明
规则名称	evs-protected-by-cbr
规则展示名	EVS资源在备份存储库保护中
规则描述	EVS磁盘没有关联备份存储库，视为“不合规”。
标签	cbr、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

3.6.34.7 EVS 资源的备份时间检查

规则详情

表 3-217 规则详情

参数	说明
规则名称	evs-last-backup-created
规则展示名	EVS资源的备份时间检查
规则描述	EVS磁盘最近一次备份创建时间超过参数要求，视为“不合规”。
标签	cbr、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	lastBackupAgeValue：EVS要求的备份时间间隔（以小时为单位）。

3.6.35 云证书管理服务 CCM

3.6.35.1 检查私有 CA 是否过期

规则详情

表 3-218 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在指定时间内过期，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。

3.6.35.2 检查私有证书是否过期

规则详情

表 3-219 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。

3.6.35.3 检查私有根 CA 是否停用

规则详情

表 3-220 规则详情

参数	说明
规则名称	pca-certificate-authority-root-disable
规则展示名	检查私有根CA是否停用
规则描述	私有根CA未停用，视为“不合规”。
标签	pca
规则触发方式	配置变更
规则评估的资源类型	pca.ca
规则参数	无

3.6.35.4 私有证书管理服务算法检查

规则详情

表 3-221 规则详情

参数	说明
规则名称	pca-algorithm-check
规则展示名	私有证书管理服务算法检查
规则描述	私有证书管理服务使用了禁止的密钥算法或签名哈希算法，视为“不合规”。
标签	pca
规则触发方式	配置变更
规则评估的资源类型	pca.ca、pca.cert
规则参数	• blockedKeyAlgorithm：禁止使用的密钥算法列表，数组类型，如 ["SM2", "RSA2048", "EC256"]。 • blockedSignatureAlgorithm：禁止使用的签名算法，数组类型，如 ["SHA256"]。

应用场景

私有CA和私有证书的加密或签名的安全性与使用的算法直接相关，随着算力越来越便宜，为了保护您的资源的安全性，建议您使用足够安全的算法。

修复项指导

请释放使用未满足您合规要求的资源，并购买满足安全算法要求的**私有CA**或**私有证书**。

检测逻辑

- 私有证书管理服务的私有CA或私有证书使用禁止的密钥算法或签名哈希算法，视为“不合规”。
- 私有证书管理服务的私有CA或私有证书未使用禁止的密钥算法或签名哈希算法，视为“合规”。

3.6.36 分布式消息服务 Kafka 版

3.6.36.1 DMS Kafka 队列打开内网 SSL 加密访问

规则详情

表 3-222 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 kafka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.kafka
规则参数	无

3.6.36.2 DMS Kafka 队列打开公网 SSL 加密访问

规则详情

表 3-223 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 kafka队列未打开公网SSL加密访问，视为“不合规”。

参数	说明
标签	dms
规则触发方式	配置变更
规则评估的资源类型	dms.kafka
规则参数	无

3.6.36.3 DMS Kafka 队列开启公网访问

规则详情

表 3-224 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 kafka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.kafka
规则参数	无

3.6.37 分布式消息服务 RabbitMQ 版

3.6.37.1 DMS RabbitMq 队列打开 SSL 加密访问

规则详情

表 3-225 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

参数	说明
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

3.6.37.2 DMS RabbitMQ 实例开启公网访问

规则详情

表 3-226 规则详情

参数	说明
规则名称	dms-rabbitmq-public-access-enabled-check
规则展示名	DMS RabbitMQ实例开启公网访问
规则描述	DMS RabbitMQ实例开启公网访问，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.rabbitmqs
规则参数	无

应用场景

您需要通过公网地址访问RabbitMQ实例时，开启实例的公网访问功能，并设置弹性IP地址。当业务不再使用公网访问功能时，需关闭实例的公网访问功能，避免将DMS RabbitMQ实例直接暴露到公网。

修复项指导

请关闭公网访问，避免将DMS RabbitMQ实例直接暴露到公网。

检测逻辑

- DMS RabbitMQ实例开启公网访问，视为“不合规”。
- DMS RabbitMQ实例未开启公网访问，视为“合规”。

3.6.38 分布式消息服务 RocketMQ 版

3.6.38.1 DMS RocketMQ 实例打开 SSL 加密访问

规则详情

表 3-227 规则详情

参数	说明
规则名称	dms-rocketmq-not-enable-ssl
规则展示名	DMS RocketMQ实例打开SSL加密访问
规则描述	DMS RocketMQ实例未打开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

3.6.38.2 DMS RocketMQ 实例开启公网访问

规则详情

表 3-228 规则详情

参数	说明
规则名称	dms-reliability-public-access-enabled-check
规则展示名	DMS RocketMQ实例开启公网访问
规则描述	DMS RocketMQ实例开启公网访问，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.reliabilitys
规则参数	无

应用场景

您需要通过公网地址访问RocketMQ实例时，开启实例的公网访问功能，并设置弹性IP地址。当业务不再使用公网访问功能时，需关闭实例的公网访问功能，避免将DMS RocketMQ实例直接暴露到公网。

修复项指导

请关闭公网访问，避免将DMS RocketMQ实例直接暴露到公网。

检测逻辑

- DMS RocketMQ实例开启公网访问，视为“不合规”。
- DMS RocketMQ实例未开启公网访问，视为“合规”。

3.6.39 组织 Organizations

3.6.39.1 账号加入组织

规则详情

表 3-229 规则详情

参数	说明
规则名称	account-part-of-organizations
规则展示名	账号加入组织
规则描述	账号未加入组织中，视为“不合规”。
标签	organizations
规则触发方式	周期触发
规则评估的资源类型	account
规则参数	domainId：账号所属组织的组织管理员账号ID，空字符串表示任意账号ID。

3.6.40 云防火墙 CFW

3.6.40.1 CFW 防火墙配置防护策略

规则详情

表 3-230 规则详情

参数	说明
规则名称	cfw-policy-not-empty
规则展示名	CFW防火墙配置防护策略
规则描述	CFW防火墙未配置防护策略，视为“不合规”。

参数	说明
标签	cfw
规则触发方式	配置变更
规则评估的资源类型	cfw.cfw_instance
规则参数	无

3.6.41 云备份 CBR

3.6.41.1 CBR 备份被加密

规则详情

表 3-231 规则详情

参数	说明
规则名称	cbr-backup-encrypted-check
规则展示名	CBR备份被加密
规则描述	CBR服务的备份未被加密，视为“不合规”。
标签	cbr
规则触发方式	配置变更
规则评估的资源类型	cbr.backup
规则参数	无

3.6.41.2 CBR 备份策略执行频率检查

规则详情

表 3-232 规则详情

参数	说明
规则名称	cbr-policy-minimum-frequency-check
规则展示名	CBR备份策略执行频率检查
规则描述	CBR备份策略执行频率低于设定值，视为“不合规”。
标签	cbr

参数	说明
规则触发方式	配置变更
规则评估的资源类型	cbr.policy
规则参数	requiredFrequency：备份频率，请输入备份的时间间隔（以小时为单位）。

检测逻辑

- CBR服务的备份策略未启用，视为“合规”。
- CBR服务的备份策略执行的最大时间间隔小于等于参数要求，视为“合规”。
- CBR服务的备份策略执行的最大时间间隔大于参数要求，视为“不合规”。

3.6.41.3 CBR 存储库最低保留天数

规则详情

表 3-233 规则详情

参数	说明
规则名称	cbr-vault-minimum-retention-check
规则展示名	CBR存储库最低保留天数
规则描述	CBR存储库未绑定策略或绑定的策略按天数保留且保留天数低于设定值，视为“不合规”。
标签	cbr
规则触发方式	配置变更
规则评估的资源类型	cbr.vault
规则参数	requiredRetentionDays：所需保留期（以天为单位）。

3.6.42 对象存储服务 OBS

3.6.42.1 OBS 桶策略中不授权禁止的 Action

规则详情

表 3-234 规则详情

参数	说明
规则名称	obs-bucket-blacklisted-actions-prohibited
规则展示名	OBS桶策略中不授权禁止的Action
规则描述	OBS桶策略中授权任意禁止的Action给外部身份，视为“不合规”。
标签	obs、access-analyzer-verified
规则触发方式	配置变更
规则评估的资源类型	obs.buckets
规则参数	blockedActionsPatterns：禁止的action列表。

应用场景

桶策略是作用于所配置的OBS桶及桶内对象的，OBS桶拥有者通过桶策略可为IAM用户或其他账号授权桶及桶内对象的操作权限，详见**桶策略**。桶策略应当仅授予刚好能完成工作所需的权限，通过最小权限原则，可以帮助您安全地控制对OBS桶及桶内对象的访问。

修复项指导

通过**可视化视图**或**JSON视图**修改桶策略内容，避免桶策略授权非预期的action操作。

检测逻辑

- OBS桶策略未授予的本华为云账号以外的身份指定操作权限，视为“合规”。
- OBS桶策略授予的本华为云账号以外的身份指定操作权限，视为“不合规”。

3.6.42.2 OBS 桶策略中授权检查

规则详情

表 3-235 规则详情

参数	说明
规则名称	obs-bucket-policy-grantee-check
规则展示名	OBS桶策略中授权检查
规则描述	OBS桶策略授权了不被允许的访问行为，视为“不合规”。

参数	说明
标签	obs、access-analyzer-verified
规则触发方式	配置变更
规则评估的资源类型	obs.buckets
规则参数	• principal：授权的身份列表，例如：["domain/aaaa:user/111111", "domain/bbbb"]。 • sourceIp：授权的sourceIp列表，例如：["192.168.0.0/16"]。 • sourceVpc：授权的sourceVpc列表，需填入请求发起的VPC ID，例如["vpcidaaaa"]。 • sourceVpce：授权的sourceVpce列表，需填入请求发起的VPC终端节点ID，例如["vpceidaaaa"]。 注：上述字段的格式均需与OBS桶策略中的principal或condition的格式一致。

应用场景

桶策略是作用于所配置的OBS桶及桶内对象的，OBS桶拥有者通过桶策略可为IAM用户或其他账号授权桶及桶内对象的操作权限，详见**桶策略**。桶策略应当仅授予刚好能完成工作所需的权限，通过最小权限原则，可以帮助您安全地控制对OBS桶及桶内对象的访问。

修复项指导

通过**可视化视图**或**JSON视图**修改桶策略内容，避免桶策略授权非预期的身份或网络。

检测逻辑

- OBS桶策略授予的访问权限受您提供的访问身份和网络限制约束，视为“合规”。
- OBS桶策略授予的访问权限不受您提供的访问身份和网络限制约束，视为“不合规”。
- 规则参数中的格式，与OBS桶策略的相关字段格式一致。

3.6.42.3 OBS 桶策略授权约束

规则详情

表 3-236 规则详情

参数	说明
规则名称	obs-bucket-policy-not-more-permissive
规则展示名	OBS桶策略授权约束

参数	说明
规则描述	OBS桶策略授权了控制策略以外的访问行为，视为“不合规”。
标签	obs、access-analyzer-verified
规则触发方式	配置变更
规则评估的资源类型	obs.buckets
规则参数	controlPolicy：允许的访问边界策略。 **说明** • 规则参数示例1：桶策略只授权对象的操作权限，不授权桶的操作权限。 {"Statement": [{"Action": ["*Object*"], "Resource": ["*/*"], "Effect": "Allow", "Principal": {"ID": ["*"]}}]} • 规则参数示例2：桶策略只授权华为云账号的身份，不授权联合身份用户或匿名用户。 {"Statement": [{"Action": ["*"], "Resource": ["*"], "Effect": "Allow", "Principal": {"ID": ["domain/*"]}}]}

应用场景

桶策略是作用于所配置的OBS桶及桶内对象的，OBS桶拥有者通过桶策略可为IAM用户或其他账号授权桶及桶内对象的操作权限，详见**桶策略**。桶策略应当仅授予刚好能完成工作所需的权限，通过最小权限原则，可以帮助您安全地控制对OBS桶及桶内对象的访问。

修复项指导

通过**可视化视图**或**JSON视图**修改桶策略内容，避免桶策略授权非预期的身份或网络。

检测逻辑

- OBS桶策略授权controlPolicy以外的访问，视为“不合规”。
- OBS桶策略未授权controlPolicy以外的访问，视为“合规”。

3.6.42.4 OBS 桶禁止公开读

规则详情

表 3-237 规则详情

参数	说明
规则名称	obs-bucket-public-read-policy-check
规则展示名	OBS桶禁止公开读
规则描述	OBS桶可以被公开读，视为“不合规”。

参数	说明
标签	obs、access-analyzer-verified
规则触发方式	配置变更
规则评估的资源类型	obs.buckets
规则参数	无

应用场景

桶策略是作用于所配置的OBS桶及桶内对象的，OBS桶拥有者通过桶策略可为IAM用户或其他账号授权桶及桶内对象的操作权限，详见**桶策略**。桶策略应当仅授予刚好能完成工作所需的权限，通过最小权限原则，可以帮助您安全地控制对OBS桶及桶内对象的访问。

修复项指导

通过**可视化视图**或**JSON视图**修改桶策略内容，避免桶策略授权非预期的读操作。

检测逻辑

- OBS桶策略允许本账号以外的身份执行“读”相关的操作，视为“不合规”。
- OBS桶ACL允许本账号或日志投递用户组以外的身份执行“读”相关的操作，视为“不合规”。
- OBS桶不满足以上场景，视为“合规”。

3.6.42.5 OBS 桶禁止公开写

规则详情

表 3-238 规则详情

参数	说明
规则名称	obs-bucket-public-write-policy-check
规则展示名	OBS桶禁止公开写
规则描述	OBS桶可以被公开写，视为“不合规”。
标签	obs、access-analyzer-verified
规则触发方式	配置变更
规则评估的资源类型	obs.buckets
规则参数	无

应用场景

桶策略是作用于所配置的OBS桶及桶内对象的，OBS桶拥有者通过桶策略可为IAM用户或其他账号授权桶及桶内对象的操作权限，详见**桶策略**。桶策略应当仅授予刚好能完成工作所需的权限，通过最小权限原则，可以帮助您安全地控制对OBS桶及桶内对象的访问。

修复项指导

通过**可视化视图**或**JSON视图**修改桶策略内容，避免桶策略授权非预期的写操作。

检测逻辑

- OBS桶策略允许本账号以外的身份执行“写”相关的操作，视为“不合规”。
- OBS桶ACL允许本账号或日志投递用户组以外的身份执行“写”相关的操作，视为“不合规”。
- OBS桶不满足以上场景，视为“合规”。

3.6.42.6 OBS 桶策略授权行为使用 SSL 加密

规则详情

表 3-239 规则详情

参数	说明
规则名称	obs-bucket-ssl-requests-only
规则展示名	OBS桶策略授权行为使用SSL加密
规则描述	OBS桶策略授权了无需SSL加密的行为，视为“不合规”。
标签	obs、access-analyzer-verified
规则触发方式	配置变更
规则评估的资源类型	obs.buckets
规则参数	无

应用场景

确保您的数据在传输到OBS过程中不被窃取和篡改。

修复项指导

为避免客户端误使用HTTP协议进行OBS业务操作，建议通过桶策略中的SecureTransport条件进行限制，限制是否必须使用HTTPS协议发起请求对该桶进行操作。SecureTransport配置为True时，发起的请求必须使用SSL加密。如何配置桶策略中Condition以及SecureTransport条件，详情见**桶策略参数说明**。

建议您在桶策略中补充如下condition，以确保实现上述目的： "Condition": {"Bool": {"g:SecureTransport": ["true"]}}。

检测逻辑

- OBS桶策略不允许未SSL加密的请求，视为“合规”。
- OBS桶策略允许未SSL加密的请求，视为“不合规”。
- 根据SecureTransport或g:SecureTransport条件是否限制了桶策略所有授权的请求，来判定OBS桶策略是否禁止未SSL加密的请求。

3.6.43 镜像服务 IMS

3.6.43.1 私有镜像开启加密

规则详情

表 3-240 规则详情

参数	说明
规则名称	ims-images-enable-encryption
规则展示名	私有镜像开启加密
规则描述	私有镜像未开启加密，视为“不合规”。
标签	ims
规则触发方式	配置变更
规则评估的资源类型	ims.images
规则参数	无

3.6.44 裸金属服务器 BMS

3.6.44.1 BMS 资源使用密钥对登录

规则详情

表 3-241 规则详情

参数	说明
规则名称	bms-key-pair-security-login
规则展示名	BMS资源使用密钥对登录
规则描述	裸金属服务器未启用密钥对安全登录，视为“不合规”。
标签	bms
规则触发方式	配置变更

参数	说明
规则评估的资源类型	bms.servers
规则参数	无

3.6.45 图引擎服务 GES

3.6.45.1 GES 图通过 KMS 加密

规则详情

表 3-242 规则详情

参数	说明
规则名称	ges-graphs-encrypted-check
规则展示名	GES图通过KMS加密
规则描述	GES图未通过KMS加密，视为“不合规”。
标签	ges
规则触发方式	配置变更
规则评估的资源类型	ges.graphs
规则参数	无

应用场景

由于可能存在敏感数据，应当确保图引擎服务（GES）已通过KMS进行加密。加密可帮助您保护数据的机密性，从而降低未经授权的用户访问数据的风险。

修复项指导

在创建图实例时，您应当使用KMS对图实例进行加密，详见**自定义创建图**。

检测逻辑

- GES图未通过KMS进行加密，视为“不合规”。
- GES图通过KMS进行加密，视为“合规”。

3.6.45.2 GES 图开启 LTS 日志

规则详情

表 3-243 规则详情

参数	说明
规则名称	ges-graphs-lts-enable
规则展示名	GES图开启LTS日志
规则描述	GES图未开启LTS日志，视为“不合规”。
标签	ges
规则触发方式	配置变更
规则评估的资源类型	ges.graphs
规则参数	无

应用场景

若您有查看和监控业务日志的需求，可以通过开启LTS服务来查看业务运行日志。

修复项指导

在LTS服务创建日志组和对应的日志流，并在GES服务开启LTS，详见**对接LTS**。

检测逻辑

- GES图未开启LTS日志，视为“不合规”。
- GES图开启了LTS日志，视为“合规”。

3.6.45.3 GES 图支持跨 AZ 高可用

规则详情

表 3-244 规则详情

参数	说明
规则名称	ges-graphs-multi-az-support
规则展示名	GES图支持跨AZ高可用
规则描述	GES图不支持跨AZ高可用，视为“不合规”。
标签	ges
规则触发方式	配置变更

参数	说明
规则评估的资源类型	ges.graphs
规则参数	无

应用场景

建议您创建跨AZ高可用部署的图实例，以提供不同可用区之间的故障转移能力和高可用性。

修复项指导

在创建图实例时，您应当开启跨AZ高可用，详见**自定义创建图**。

检测逻辑

- GES图不支持跨AZ高可用，视为“不合规”。
- GES图支持跨AZ高可用，视为“合规”。

3.7 资源合规事件监控

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亚太-新加坡区域。

资源合规目前支持的系统事件如下表所示：

表 3-245 资源合规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

资源记录器支持的配置审计（Config）事件请参见：**资源记录器事件监控**。

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账号状态为“正常”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。
- 组织合规规则包仅会下发至账号状态为“正常”的组织成员账号中，且组织成员账号需开启资源记录器，否则将导致部署异常。

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“示例模板”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“上传模板”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；若该值为“--”，则代表合规规则包未评估到任何资源。

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、更新和删除行为最终是通过RFS服务的资源栈来实现的。资源栈是资源编排服务的概念，详见**资源栈**。

状态：

表 4-1 合规规则包的部署状态

取值	状态	状态说明
CREATE_SUCCESSFUL	已部署	合规规则包已部署成功，合规规则均创建成功。
CREATE_IN_PROGRESS	部署中	合规规则包正在部署中，合规规则正在创建中。
CREATE_FAILED	部署异常	合规规则包部署失败。
DELETE_IN_PROGRESS	删除中	合规规则包正在删除中，合规规则正在删除中。
DELETE_FAILED	删除异常	合规规则包删除失败。
ROLLBACK_SUCCESSFUL	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。

取值	状态	状态说明
ROLLBACK_IN_PROGRESS	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。
ROLLBACK_FAILED	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。
UPDATE_SUCCESSFUL	更新成功	合规规则包修改并更新成功。
UPDATE_IN_PROGRESS	更新中	合规规则包修改更新中。
UPDATE_FAILED	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（RFS）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。

当您不选择进行自定义授权时，Config将通过服务关联委托的方式自动获取RFS的相关权限。如您需要自行控制委托权限的范围，可选择进行自定义授权，提前在统一身份认证服务（IAM）中创建委托，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）**。

说明

如果您通过存储在OBS桶中的合规规则包模板创建合规规则包，请配置合适的IAM策略和OBS桶策略，以确保模板内容可以正常获取，详情请参考**OBS**和**RFS**的文档。

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。

- 创建或修改合规规则包需要开启资源记录器，资源记录器处于关闭状态时，合规规则包仅支持查看和删除操作。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。

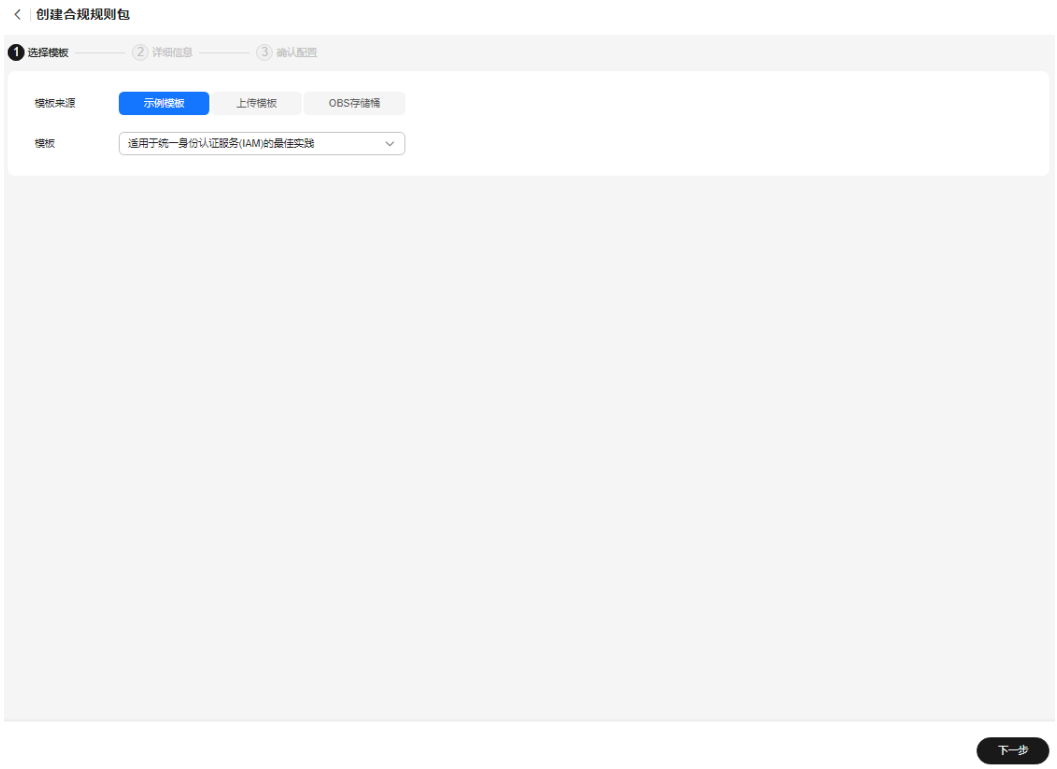
  模板文件格式和文件内容格式均为JSON，不支持tf格式和zip格式的文件内容，该文件的后缀需为.tf.json，具体请参见：**自定义合规规则包**。

- OBS存储桶：自定义合规规则包模板存储在OBS桶的位置。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，合规规则包的详细参数配置完成后，单击“下一步”。

图 4-4 详细信息

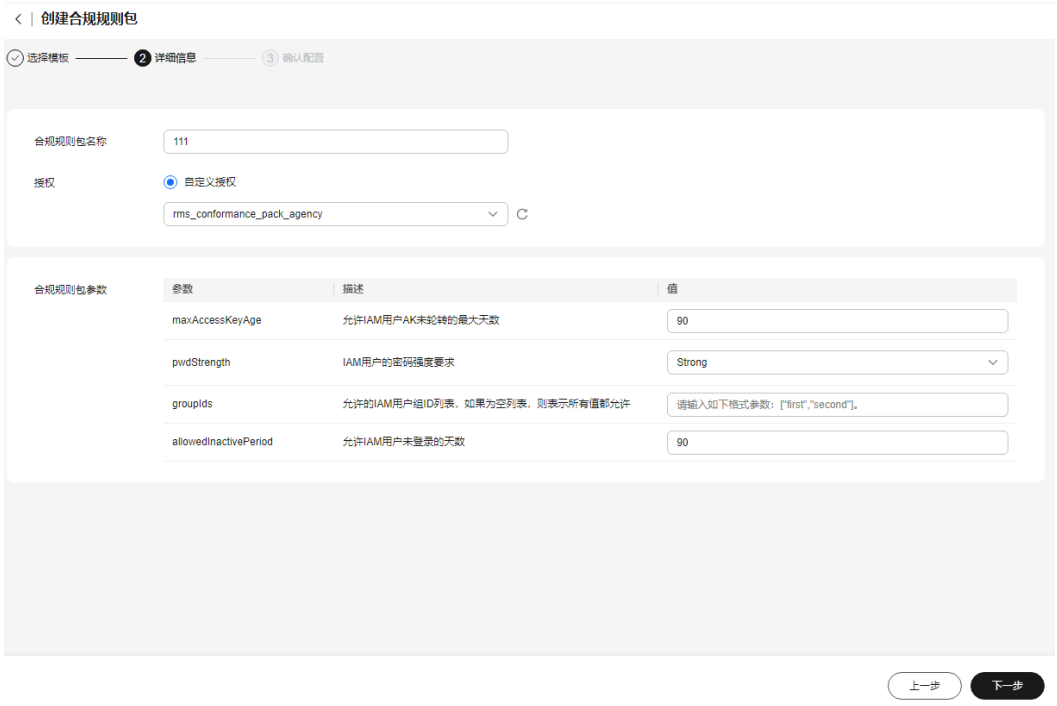
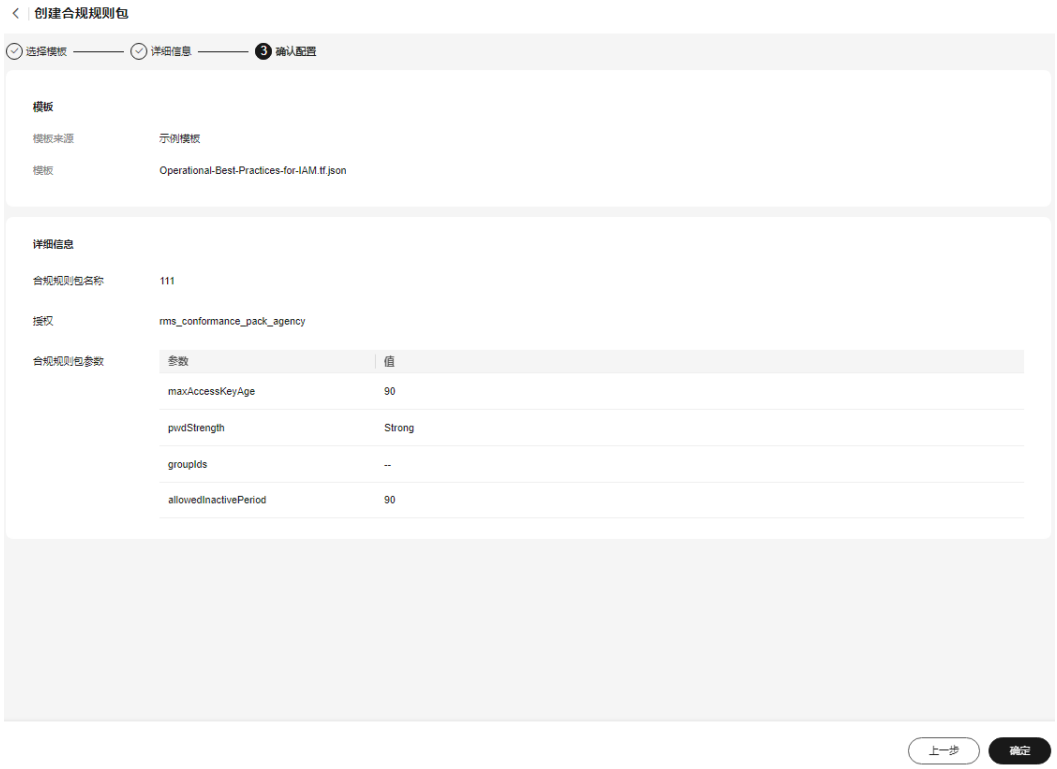


表 4-2 详细信息配置说明

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。
（可选）授权	此处的授权为**委托授权**，当您不选择自定义授权时，Config将通过服务关联委托的方式自动获取RFS的相关权限。如您需要自行控制委托权限的范围，可选择进行自定义授权，提前在统一身份认证服务（IAM）中创建委托，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），然后在下拉框中选择委托。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 查看合规规则包详情

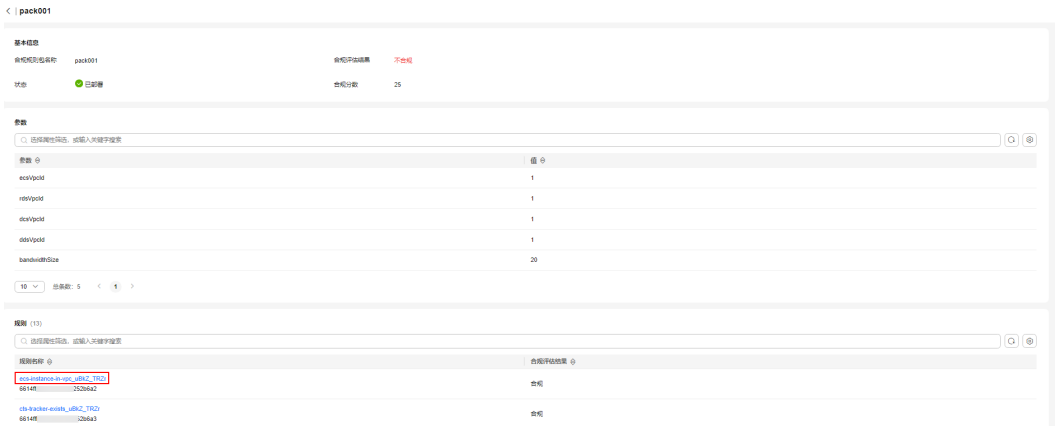


表 4-3 合规规则包的部署状态

取值	状态	状态说明
CREATE_SUCCESSFUL	已部署	合规规则包已部署成功，合规规则均创建成功。
CREATE_IN_PROGRESS	部署中	合规规则包正在部署中，合规规则正在创建中。
CREATE_FAILED	部署异常	合规规则包部署失败。

取值	状态	状态说明
DELETE_IN_PROGRESS	删除中	合规规则包正在删除中，合规规则正在删除中。
DELETE_FAILED	删除异常	合规规则包删除失败。
ROLLBACK_SUCCESSFUL	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。
ROLLBACK_IN_PROGRESS	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。
ROLLBACK_FAILED	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。
UPDATE_SUCCESSFUL	更新成功	合规规则包修改并更新成功。
UPDATE_IN_PROGRESS	更新中	合规规则包修改更新中。
UPDATE_FAILED	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。

说明

创建或修改合规规则包需要开启资源记录器，资源记录器处于关闭状态时，合规规则包仅支持查看和删除操作。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 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。

图 4-7 修改合规规则包

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”。

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。

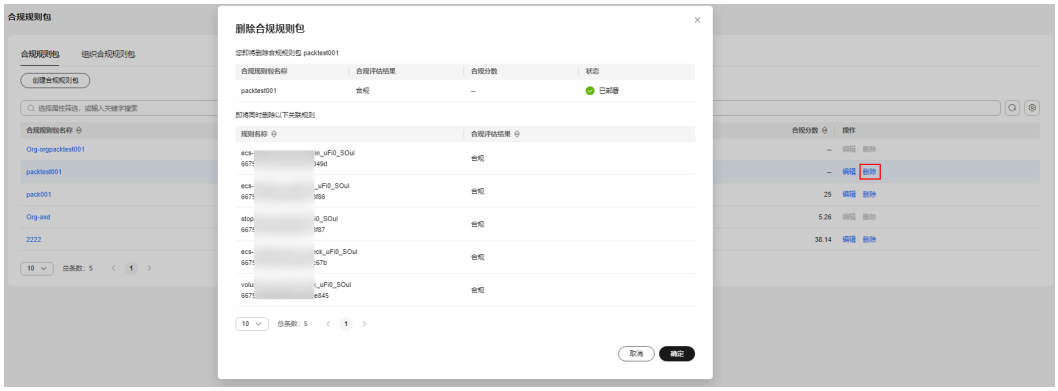
步骤3 单击页面左侧的“合规规则包”，进入“合规规则包”页面。

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账号状态为“正常”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，所部署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。
- 创建或修改组织合规规则包需要开启资源记录器，资源记录器处于关闭状态时，组织合规规则包仅支持查看和删除操作。具体请参见**配置资源记录器**。
- 非组织内账号无法在Config控制台的“合规规则包”页面中看到“组织合规规则包”页签。
- 组织合规规则包仅会下发至账号状态为“正常”的组织成员账号中，且组织成员账号需开启资源记录器，否则将导致部署异常。

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。

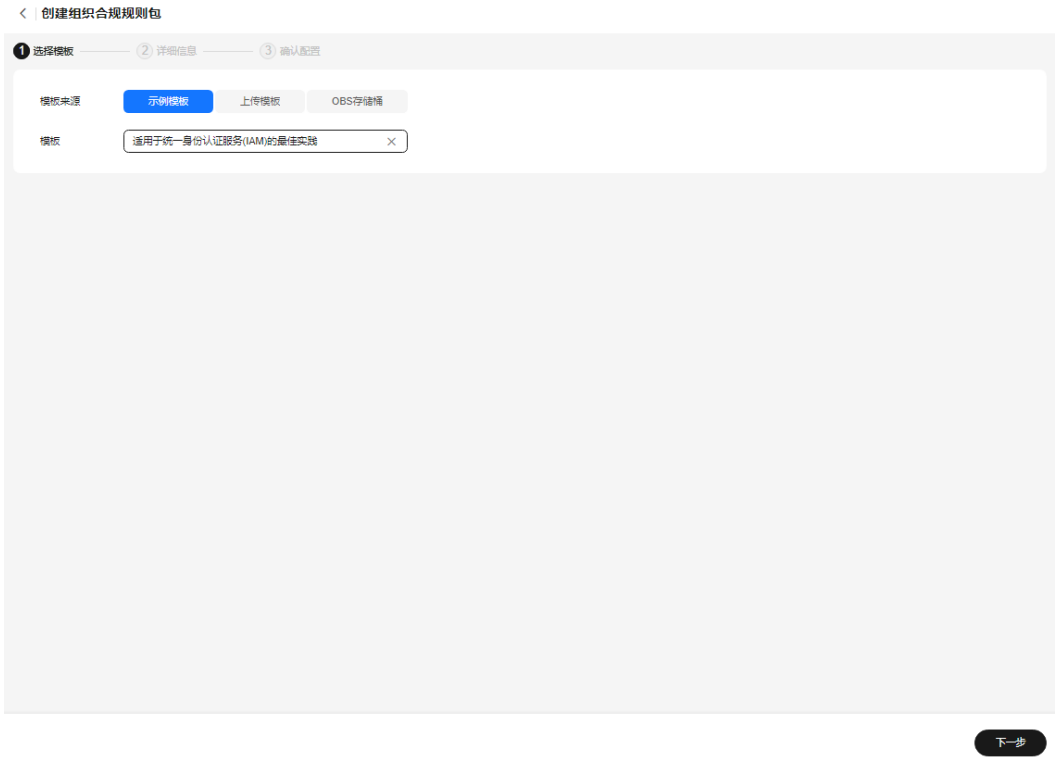
  关于每个示例模板包含的具体合规规则请参见：**合规规则包示例模板**。
- 本地模板：从本地上传模板文件，您可以根据自身的需求编写合规规则包的模板文件，然后上传并使用。

  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存储在OBS桶的位置。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

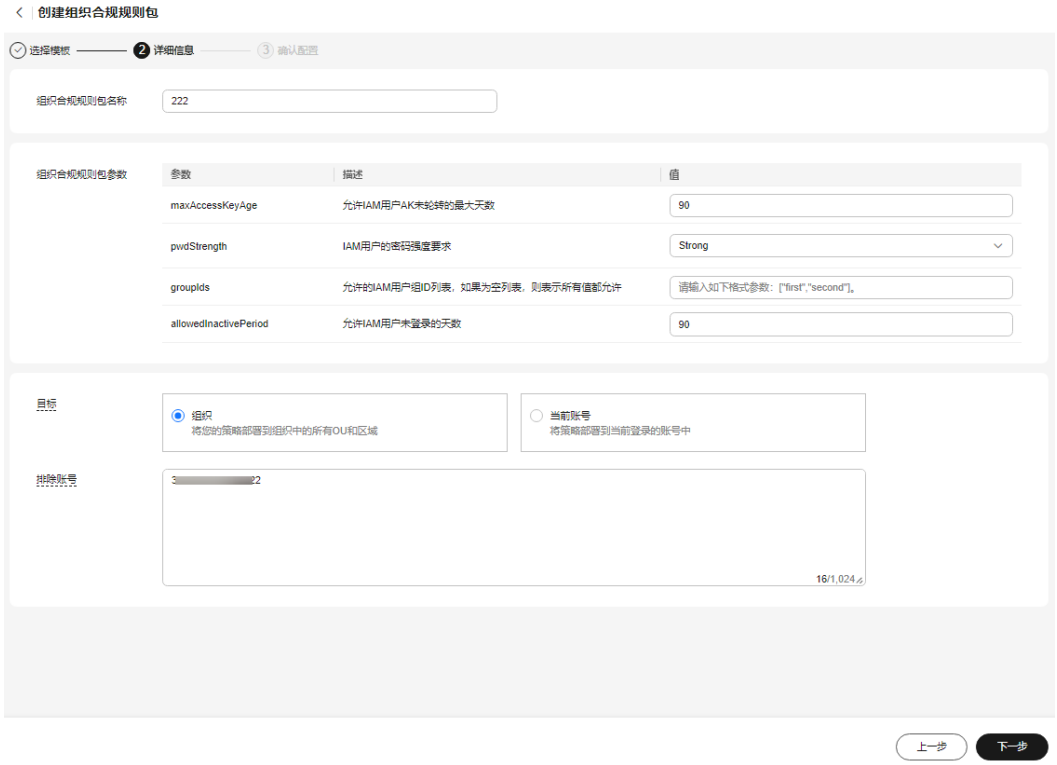
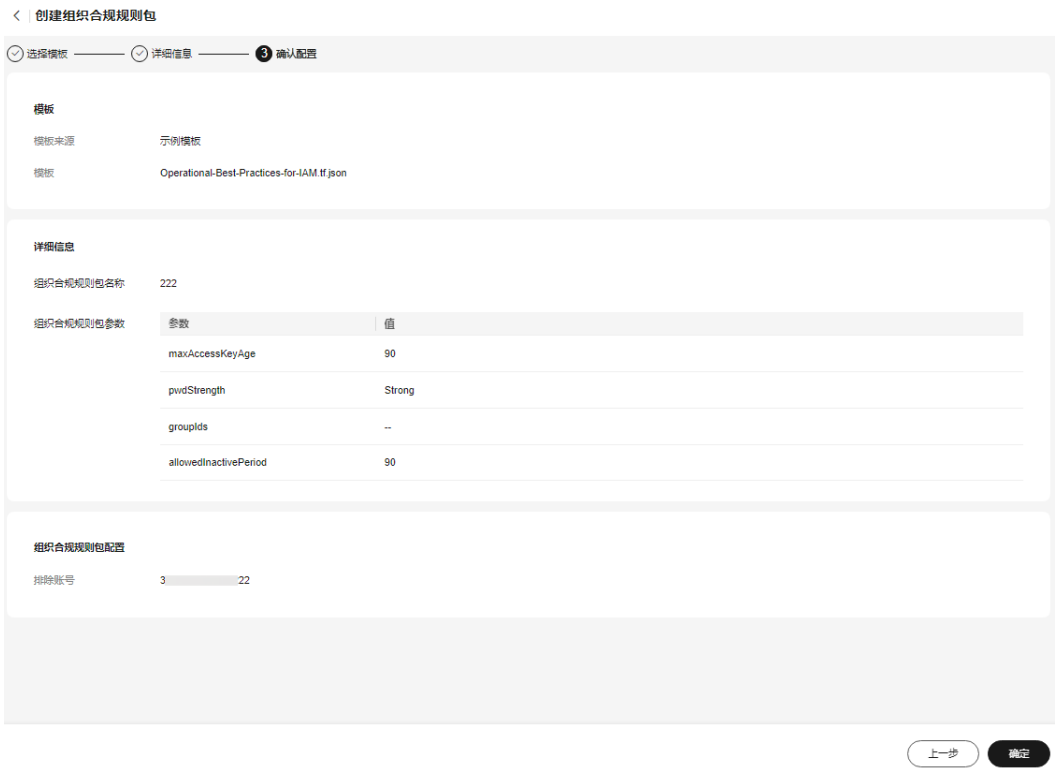


表 4-4 详细信息配置说明

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**、**查看部署至成员账号中的组织合规规则包**和**组织合规规则包的部署状态**三部分内容。

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。

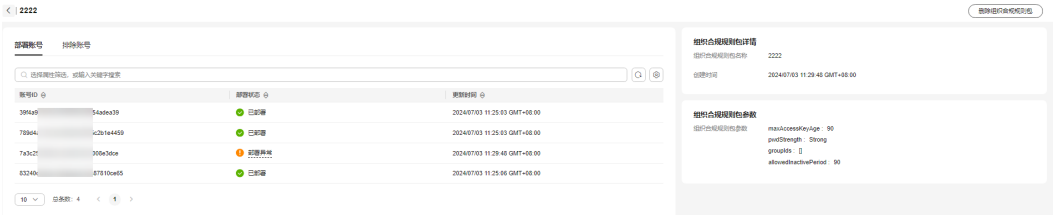
步骤3 单击页面左侧的“合规规则包”，进入“合规规则包”页面。

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 查看组织合规规则包详情



----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-”字段用于标识。

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

组织合规规则包的部署状态

表 4-5 组织合规规则包的部署状态

取值	状态	状态说明
CREATE_IN_PROGRESS	部署中	正在创建组织合规规则包。
UPDATE_IN_PROGRESS	更新中	正在更新组织合规规则包。
DELETE_IN_PROGRESS	删除中	正在删除组织合规规则包。
CREATE_FAILED	部署异常	组织合规规则包在该组织内的一个或多个成员账号中创建失败。
UPDATE_FAILED	更新失败	组织合规规则包在该组织内的一个或多个成员账号中更新失败。
DELETE_FAILED	删除异常	组织合规规则包在该组织内的一个或多个成员账号中删除失败。
CREATE_SUCCESSFUL	已部署	组织合规规则包在该组织内的所有成员账号中创建成功。
UPDATE_SUCCESSFUL	更新成功	组织合规规则包在该组织内的所有成员账号中更新成功。

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，您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。

说明

创建或修改组织合规规则包需要开启资源记录器，资源记录器处于关闭状态时，组织合规规则包仅支持查看和删除操作。具体请参见**配置资源记录器**。

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”。

图 4-15 修改组织合规规则包

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”。

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。

说明

如果您通过存储在OBS桶中的合规规则包模板创建合规规则包，请配置合适的IAM策略和OBS桶策略，以确保模板内容可以正常获取，详情请参考**OBS**和**RFS**的文档。

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": "1.66.2"
    }
  }
}
```

其中version必须选择1.66.2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": "1.66.2"
    }
  }
 }
}
```

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": "1.66.2"
        }
    }
  }
}
```

4.5 合规规则包示例模板

4.5.1 示例模板概述

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
- 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
- 网络及数据安全最佳实践
- 适用于Landing Zone基础场景的最佳实践
- 架构安全支柱运营最佳实践
- 网络和内容交付服务运营最佳实践
- 适用于空闲资产管理的最佳实践
- 多可用区架构最佳实践
- 资源稳定性最佳实践
- 适用于API网关（APIG）的最佳实践
- 适用于云容器引擎（CCE）的最佳实践
- 适用于内容分发网络（CDN）的最佳实践
- 适用于函数工作流（FunctionGraph）的最佳实践
- 适用于云数据库（GaussDB）的最佳实践
- 适用于云数据库（GeminiDB）的最佳实践
- 适用于MapReduce服务（MRS）的最佳实践
- NIST审计标准最佳实践
- 新加坡金融行业的最佳实践
- 安全身份和合规性运营最佳实践
- 华为云安全配置基线指南的标准合规包（level 1）
- 华为云安全配置基线指南的标准合规包（level 2）
- 静态数据加密最佳实践
- 数据传输加密最佳实践
- 适用于云备份（CBR）的最佳实践
- 适用于云搜索服务（CSS）的最佳实践
- 适用于分布式缓存服务（DCS）的最佳实践
- 适用于分布式消息服务（DMS）的最佳实践
- 适用于数据仓库服务（DWS）的最佳实践

- 适用于云数据库（TaurusDB）的最佳实践
- 适用于对象存储服务（OBS）的最佳实践
- 适用于VPC安全组的最佳实践
- 适用于Web应用防火墙（WAF）的最佳实践

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 4-6

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。	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。	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连接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连接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。
8.1.3.1	b）应能够对非授权设备私自连接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，此类账号需要原则和访问控制。

建议项编号	建议项说明	华为云合规规则	指导
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，此类账号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来减少账号被盗用的事件。
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。

建议项编号	建议项说明	华为云合规规则	指导
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	规则描述
access-keys-rotated	IAM用户的AccessKey在指定时间内轮换	iam	IAM用户的访问密钥未在指定天数内轮转，视为“不合规”.

合规规则	规则中文名称	涉及云服务	规则描述
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	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”
css-cluster-https-required	CSS集群启用HTTPS	css	CSS集群未启用https，视为“不合规”
css-cluster-in-vpc	CSS集群绑定指定VPC资源	css	CSS集群未与指定的vpc资源绑定，视为“不合规”
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未启用事件分析，视为“不合规”
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	CTS追踪器未打开事件文件校验，视为“不合规”
cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建CTS追踪器，视为“不合规”
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs，vpc	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	ECS资源具有公网IP，视为“不合规”
eip-unbound-check	弹性公网IP未进行任何绑定	vpc	弹性公网IP未进行任何绑定，视为“不合规”
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
function-graph-concurrency-check	函数工作流的函数并发数在指定范围内	fgs	FunctionGraph函数并发数不在指定的范围内，视为“不合规”
iam-group-has-users-check	IAM用户组添加了IAM用户	iam	IAM用户组未添加任意IAM用户，视为“不合规”
iam-password-policy	IAM用户密码策略符合要求	iam	IAM用户密码强度不满足密码强度要求，视为“不合规”
iam-root-access-key-check	IAM账号存在可使用的访问密钥	iam	账号存在可使用的访问密钥，视为“不合规”
iam-user-group-membership-check	IAM用户归属指定用户组	iam	IAM用户不属于指定IAM用户组，视为“不合规”
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	IAM用户在指定时间范围内无登录行为，视为“不合规”
iam-user-mfa-enabled	IAM用户开启MFA	iam	IAM用户未开启MFA认证，视为“不合规”
kms-rotation-enabled	KMS密钥启用密钥轮换	kms	KMS密钥未启用密钥轮换，视为“不合规”
mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	通过Console密码登录的IAM用户未开启MFA认证，视为“不合规”
mrs-cluster-in-vpc	MRS集群属于指定VPC	mrs	指定虚拟私有云ID，不属于此VPC的MRS集群，视为“不合规”
mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS集群未开启kerberos认证，视为“不合规”
mrs-cluster-no-public-ip	MRS集群未绑定弹性公网IP	mrs	MRS集群绑定弹性公网IP，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
private-nat-gateway-authorized-vpc-only	NAT私网网关绑定指定VPC资源	nat	NAT私网网关未与指定的VPC资源绑定，视为“不合规”
rds-instance-multi-az-support	RDS实例支持多可用区	rds	RDS实例仅支持一个可用区，视为“不合规”
rds-instance-no-public-ip	RDS实例不具有弹性公网IP	rds	RDS资源具有弹性公网IP，视为“不合规”
root-account-mfa-enabled	根账号开启MFA认证	iam	根账号未开启MFA认证，视为“不合规”
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	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”
volume-unused-check	云硬盘闲置检测	evs	云硬盘未挂载给任何云服务器，视为“不合规”
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs，evs	已挂载的云硬盘未进行加密，视为“不合规”
vpc-acl-unused-check	未与子网关联的网络ACL	vpc	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”
vpc-flow-logs-enabled	VPC启用流日志	vpc	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”
vpc-sg-ports-check	安全组端口检查	vpc	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”
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”

合规规则	规则中文名称	涉及云服务	规则描述
waf-instance-policy-not-empty	WAF防护域名配置防护策略	waf	WAF防护域名未配置防护策略，视为“不合规”

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	规则描述
access-keys-rotated	IAM用户的AccessKey在指定时间内轮换	iam	IAM用户的访问密钥未在指定天数内轮转，视为“不合规”
alarm-kms-disable-or-delete-key	CES配置监控KMS禁用或计划删除密钥的事件监控告警	ces, kms	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”
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	CES未配置监控OBS桶策略变更的事件监控告警，视为“不合规”
alarm-vpc-change	CES配置监控VPC变更的事件监控告警	ces, vpc	CES未配置监控VPC变更的事件监控告警，视为“不合规”
css-cluster-https-required	CSS集群启用HTTPS	css	CSS集群未启用https，视为“不合规”
css-cluster-in-vpc	CSS集群绑定指定VPC资源	css	CSS集群未与指定的vpc资源绑定，视为“不合规”
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未转储到LTS，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	CTS追踪器未打开事件文件校验，视为“不合规”
cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建并启用CTS追踪器，视为“不合规”
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs, vpc	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	ECS资源具有弹性公网IP，视为“不合规”
eip-unbound-check	弹性公网IP未进行任何绑定	vpc	弹性公网IP未进行任何绑定，视为“不合规”
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”
iam-group-has-users-check	IAM用户组添加了IAM用户	iam	IAM用户组未添加任意IAM用户，视为“不合规”
iam-password-policy	IAM用户密码策略符合要求	iam	IAM用户密码强度不满足密码强度要求，视为“不合规”
iam-root-access-key-check	根用户存在可使用的访问密钥	iam	根用户存在可使用的访问密钥，视为“不合规”
iam-user-console-and-api-access-at-creation	IAM用户创建时设置AccessKey	iam	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”
iam-user-group-membership-check	IAM用户归属指定用户组	iam	IAM用户不属于指定IAM用户组，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	IAM用户在指定时间范围内无登录行为，视为“不合规”
iam-user-mfa-enabled	IAM用户开启MFA	iam	IAM用户未开启MFA认证，视为“不合规”
iam-user-single-access-key	IAM用户单访问密钥	iam	IAM用户拥有多个处于“active”状态的访问密钥，视为“不合规”
mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	通过console密码登录的IAM用户未开启MFA认证，视为“不合规”
mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS集群未开启kerberos认证，视为“不合规”
mrs-cluster-no-public-ip	MRS集群未绑定弹性公网IP	mrs	MRS集群绑定弹性公网IP，视为“不合规”
private-nat-gateway-authorized-vpc-only	NAT私网网关绑定指定VPC资源	nat	NAT私网网关未与指定的VPC资源绑定，视为“不合规”
rds-instance-multi-az-support	RDS实例支持多可用区	rds	RDS实例仅支持一个可用区，视为“不合规”
rds-instance-no-public-ip	RDS实例不具有弹性公网IP	rds	RDS资源具有弹性公网IP，视为“不合规”
root-account-mfa-enabled	根用户开启MFA认证	iam	根用户未开启MFA认证，视为“不合规”
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	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”
volume-unused-check	云硬盘闲置检测	evs	云硬盘未挂载给任何云服务器，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs, evs	已挂载的云硬盘未进行加密，视为“不合规”
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”
bms-key-pair-security-login	BMS资源使用密钥对登录	bms	裸金属服务器未启用密钥对安全登录，视为“不合规”
cbr-backup-encrypted-check	CBR备份被加密	cbr	CBR服务的备份未被加密，视为“不合规”
cfw-policy-not-empty	CFW防火墙配置防护策略	cfw	CFW防火墙未配置防护策略，视为“不合规”
csms-secrets-auto-rotation-enabled	CSMS凭据启动自动轮转	csms	CSMS凭据未启动自动轮转，视为“不合规”
csms-secrets-rotation-success-check	检查CSMS凭据轮转成功	csms	CSMS凭据轮转失败，视为“不合规”
csms-secrets-using-cmk	CSMS凭据使用指定KMS	csms	CSMS凭据未使用指定的KMS，视为“不合规”

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	规则描述
access-keys-rotated	IAM用户的AccessKey在指定时间内轮换	iam	IAM用户的访问密钥未在指定天数内轮转，视为“不合规”.
iam-group-has-users-check	IAM用户组添加了IAM用户	iam	IAM用户组未添加任意IAM用户，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
iam-password-policy	IAM用户密码策略符合要求	iam	IAM用户密码强度不满足密码强度要求，视为“不合规”
iam-root-access-key-check	IAM账号存在可使用的访问密钥	iam	账号存在可使用的访问密钥，视为“不合规”
iam-user-console-and-api-access-at-creation	IAM用户创建时设置AccessKey	iam	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”
iam-user-group-membership-check	IAM用户归属指定用户组	iam	IAM用户不属于指定IAM用户组，视为“不合规”
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	IAM用户在指定时间范围内无登录行为，视为“不合规”
iam-user-mfa-enabled	IAM用户开启MFA	iam	IAM用户未开启MFA认证，视为“不合规”
iam-user-single-access-key	IAM用户单访问密钥	iam	IAM用户拥有多个处于“active”状态的访问密钥，视为“不合规”
mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	通过Console密码登录的IAM用户未开启MFA认证，视为“不合规”
root-account-mfa-enabled	根账号开启MFA认证	iam	根账号未开启MFA认证，视为“不合规”
iam-policy-in-use	IAM策略使用中	iam	IAM策略未附加到IAM用户、用户组或委托，视为“不合规”
iam-role-in-use	IAM权限使用中	iam	IAM权限未附加到IAM用户、用户组或委托，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
iam-user-login-protection-enabled	IAM用户开启登录保护	iam	IAM用户未开启登录保护，视为“不合规”
iam-user-no-policies-check	IAM用户不直接附加策略或权限	iam	IAM用户直接附加了策略或权限，视为“不合规”
iam-user-check-non-admin-group	IAM用户admin权限检查	iam	根用户以外的IAM用户加入admin用户组，视为“不合规”

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	规则描述
alarm-action-enabled-check	启用了CES告警操作	ces	CES告警操作未启用，视为“不合规”
alarm-kms-disable-or-delete-key	CES配置监控KMS禁用或计划删除密钥的事件监控告警	ces，kms	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”
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	CES未配置监控OBS桶策略变更的事件监控告警，视为“不合规”
alarm-vpc-change	CES配置监控VPC变更的事件监控告警	ces，vpc	CES未配置监控VPC变更的事件监控告警，视为“不合规”

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	规则描述
as-capacity-rebalancing	弹性伸缩组均衡扩容	as	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”
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	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”
as-multiple-az	弹性伸缩组启用多AZ部署	as	弹性伸缩组没有启用多AZ部署，视为“不合规”
ecs-instance-key-pair-login	ECS资源配置密钥对	ecs	ECS未配置密钥对，视为“不合规”
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	ECS资源具有弹性公网IP，视为“不合规”
ecs-multiple-public-ip-check	检查ECS资源是否具有多个弹性公网IP	ecs	ECS资源具有多个弹性公网IP，视为“不合规”
eip-bandwidth-limit	EIP带宽限制	eip	弹性IP实例可用带宽小于指定参数值，视为“不合规”
function-graph-concurrency-check	函数工作流的函数并发数在指定范围内	fgs	FunctionGraph函数并发数不在指定的范围内，视为“不合规”
function-graph-public-access-prohibited	函数工作流的函数不允许访问公网	fgs	函数工作流的函数允许访问公网，视为“不合规”
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	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”
volume-unused-check	云硬盘闲置检测	evs	云硬盘未挂载给任何云服务器，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs，evs	已挂载的云硬盘未进行加密，视为“不合规”
as-group-ipv6-disabled	弹性伸缩组未配置IPv6带宽	as	弹性伸缩组绑定IPv6共享带宽，视为“不合规”

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	规则描述
ecs-instance-key-pair-login	ECS资源配置密钥对	ecs	ECS未配置密钥对，视为“不合规”
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	ECS资源具有弹性公网IP，视为“不合规”
ecs-multiple-public-ip-check	检查ECS资源是否具有多个弹性公网IP	ecs	ECS资源具有多个弹性公网IP，视为“不合规”
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	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”
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs，evs	已挂载的云硬盘未进行加密，视为“不合规”
ecs-attached-hss-agents-check	ECS资源绑定服务主机代理防护	ecs	ECS实例未绑定HSS代理并启用防护，视为“不合规”
ecs-instance-agency-attach-iam-agency	ECS资源附加IAM委托	ecs	ECS实例未附加IAM委托，视为“不合规”
ecs-last-backup-created	ECS云服务器的备份时间检查	cbr, ecs	ECS云服务器最近一次备份创建时间超过参数要求，视为“不合规”

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	规则描述
elb-loadbalancers-no-public-ip	ELB资源不具有弹性公网IP	elb	ELB资源具有弹性公网IP，视为“不合规”
elb-predefined-security-policy-https-check	ELB监听器配置指定预定义安全策略	elb	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“
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”
elb-http-to-https-redirection-check	监听器资源HTTPS重定向检查	elb	检查HTTP监听器是否配置了向HTTPS监听器的重定向，如果未配置，视为“不合规”
elb-multiple-az-check	ELB资源使用多AZ部署	elb	检查负载均衡器是否已从多个可用分区注册实例。如果负载均衡器的实例注册在少于2个可用区，视为“不合规”

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	规则描述
alarm-action-enabled-check	启用了CES告警操作	ces	CES告警操作未启用，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
alarm-kms-disable-or-delete-key	CES配置监控KMS禁用或计划删除密钥的事件监控告警	ces，kms	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”
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	CES未配置监控OBS桶策略变更的事件监控告警，视为“不合规”
alarm-vpc-change	CES配置监控VPC变更的事件监控告警	ces，vpc	CES未配置监控VPC变更的事件监控告警，视为“不合规”
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未启用事件分析，视为“不合规”
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	CTS追踪器未打开事件文件校验，视为“不合规”
cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建CTS追踪器，视为“不合规”
tracker-config-enabled-check	账号开启资源记录器	config	如果账号未开启资源记录器，视为“不合规”

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	规则描述
rds-instance-enable-backup	RDS实例开启备份	rds	未开启备份的RDS资源，视为“不合规”
rds-instance-enable-errorLog	RDS实例开启错误日志	rds	未开启错误日志的RDS资源，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
rds-instance-enable-slowLog	RDS实例开启慢日志	rds	未开启慢日志的RDS资源，视为“不合规”
rds-instance-multi-az-support	RDS实例支持多可用区	rds	RDS实例仅支持一个可用区，视为“不合规”
rds-instance-no-public-ip	RDS实例不具有弹性公网IP	rds	RDS资源具有弹性公网IP，视为“不合规”
rds-instances-enable-kms	RDS实例开启存储加密	rds	未开启存储加密的RDS资源，视为“不合规”
rds-instance-enable-auditLog	RDS实例启用审计日志	rds	未启用审计日志或审计日志保存天数不足的rds资源，视为“不合规”
rds-instance-engine-version-check	RDS实例数据库引擎版本检查	rds	RDS实例数据库引擎的版本低于指定版本，视为“不合规”
rds-instance-port-check	RDS实例默认端口检查	rds	RDS实例的端口包含被禁止的端口，视为“不合规”
rds-instance-ssl-enable	RDS实例启用SSL加密通讯	rds	RDS实例未启用SSL加密通讯，视为“不合规”

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	规则描述
as-capacity-rebalancing	弹性伸缩组均衡扩容	as	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”

合规规则	规则中文名称	涉及云服务	规则描述
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	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”
as-multiple-az	弹性伸缩组启用多AZ部署	as	弹性伸缩组没有启用多AZ部署，视为“不合规”
as-group-ipv6-disabled	弹性伸缩组未配置IPv6带宽	as	弹性伸缩组绑定IPv6共享带宽，视为“不合规”

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	规则描述
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未启用事件分析，视为“不合规”
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	CTS追踪器未打开事件文件校验，视为“不合规”
cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建CTS追踪器，视为“不合规”

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	规则描述
cce-cluster-end-of-maintenance-version	CCE集群版本为处于维护的版本	cce	CCE集群版本为停止维护的版本，视为“不合规”
cce-cluster-oldest-supported-version	CCE集群运行的非受支持的最旧版本	cce	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”
cce-endpoint-public-access	CCE集群资源不具有弹性公网IP	cce	CCE集群资源具有弹性公网IP，视为“不合规”
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”
mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS集群未开启kerberos认证，视为“不合规”
mrs-cluster-no-public-ip	MRS集群未绑定弹性公网IP	mrs	MRS集群绑定弹性公网IP，视为“不合规”
sfsturbo-encrypted-check	高性能弹性文件服务通过KMS进行加密	sfsturbo	高性能弹性文件服务(SFS Turbo)未通过KMS进行加密，视为“不合规”

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	规则描述
css-cluster-disk-encryption-check	CSS集群开启磁盘加密	css	CSS集群未开启磁盘加密，视为“不合规”
css-cluster-https-required	CSS集群启用HTTPS	css	CSS集群未启用https，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
css-cluster-no-public-zone	CSS集群不能公网访问	css	CSS集群开启公网访问，视为“不合规”
css-cluster-security-mode-enable	CSS集群支持安全模式	css	CSS集群不支持安全模式，视为“不合规”
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	CTS追踪器未打开事件文件校验，视为“不合规”
cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建CTS追踪器，视为“不合规”
dcs-redis-no-public-ip	DCS Redis实例不存在弹性公网IP	dcs	DCS Redis资源存在弹性公网IP，视为“不合规”
dcs-redis-password-access	DCS Redis实例需要密码访问	dcs	DCS Redis资源不需要密码访问，视为“不合规”
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	ECS资源具有弹性公网IP，视为“不合规”
elb-loadbalancers-no-public-ip	ELB资源不具有弹性公网IP	elb	ELB资源具有弹性公网IP，视为“不合规”
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”
iam-password-policy	IAM用户密码策略符合要求	iam	IAM用户密码强度不满足密码强度要求，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	IAM用户在指定时间范围内无登录行为，视为“不合规”
iam-user-mfa-enabled	IAM用户开启MFA	iam	IAM用户未开启MFA认证，视为“不合规”
rds-instance-no-public-ip	RDS实例不具有弹性公网IP	rds	RDS资源具有弹性公网IP，视为“不合规”
root-account-mfa-enabled	根账号开启MFA认证	iam	根账号未开启MFA认证，视为“不合规”
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs，evs	已挂载的云硬盘未进行加密，视为“不合规”
vpc-flow-logs-enabled	VPC启用流日志	vpc	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”
vpc-sg-ports-check	安全组端口检查	vpc	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”

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	规则描述
css-cluster-in-vpc	CSS集群绑定指定VPC资源	css	CSS集群未与指定的VPC资源绑定，视为“不合规”
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	数据复制服务实时灾备任务使用公网网络，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
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	数据复制服务实时迁移任务使用公网网络，视为“不合规”
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	数据复制服务实时同步任务使用公网网络，视为“不合规”
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs，vpc	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	ECS资源具有弹性公网IP，视为“不合规”
function-graph-inside-vpc	函数工作流使用指定VPC	fgs	函数工作流未使用指定VPC，视为“不合规”
function-graph-public-access-prohibited	函数工作流的函数不允许访问公网	fgs	函数工作流的函数允许访问公网，视为“不合规”
mrs-cluster-no-public-ip	MRS集群未绑定弹性公网IP	mrs	MRS集群绑定弹性公网IP，视为“不合规”
rds-instance-no-public-ip	RDS实例不具有弹性公网IP	rds	RDS资源具有弹性公网IP，视为“不合规”

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如下表所示：

表 4-21 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
alarm-action-enabled-check	启用了CES告警操作	ces	CES告警操作未启用，视为“不合规”
apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	APIG专享版实例未配置访问日志，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	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”
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未启用事件分析，视为“不合规”
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	CTS追踪器未打开事件文件校验，视为“不合规”
cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建CTS追踪器，视为“不合规”
dws-enable-log-dump	DWS集群启用日志转储	dws	DWS集群未启用日志转储，视为“不合规”
function-graph-concurrency-check	函数工作流的函数并发数在指定范围内	fgs	FunctionGraph函数并发数不在指定的范围内，视为“不合规”
multi-region-cts-tracker-exists	在指定区域创建并启用CTS追踪器	cts	账号未在指定region列表创建CTS追踪器，视为“不合规”
rds-instance-logging-enabled	RDS实例配备日志	rds	未配备任何日志的RDS资源，视为“不合规”
vpc-flow-logs-enabled	VPC启用流日志	vpc	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”

4.5.18 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如下表所示：

表 4-22 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	APIG专享版实例未配置访问日志，视为“不合规”
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	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”
cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未启用事件分析，视为“不合规”
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”
cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建CTS追踪器，视为“不合规”
dws-enable-kms	DWS集群启用KMS加密	dws	DWS集群未启用KMS加密，视为“不合规”
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs, vpc	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”
function-graph-concurrency-check	函数工作流的函数并发数在指定范围内	fgs	FunctionGraph函数并发数不在指定的范围内，视为“不合规”
gaussdb-nosql-enable-disk-encryption	GeminiDB使用磁盘加密	gaussdb nosql	GeminiDB未使用磁盘加密，视为“不合规”
kms-not-scheduled-for-deletion	KMS密钥不处于“计划删除”状态	kms	KMS密钥处于“计划删除“状态，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
multi-region-cts-tracker-exists	在指定区域创建并启用CTS追踪器	cts	账号未在指定region列表创建CTS追踪器，视为“不合规”
rds-instance-enable-backup	RDS实例开启备份	rds	未开启备份的RDS资源，视为“不合规”
rds-instance-multi-az-support	RDS实例支持多可用区	rds	RDS实例仅支持一个可用区，视为“不合规”
rds-instances-enable-kms	RDS实例开启存储加密	rds	未开启存储加密的RDS资源，视为“不合规”
sfsturbo-encrypted-check	高性能弹性文件服务通过KMS进行加密	sfsturbo	高性能弹性文件服务(SFS Turbo)未通过KMS进行加密，视为“不合规”
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs，evs	已挂载的云硬盘未进行加密，视为“不合规”
vpc-flow-logs-enabled	VPC启用流日志	vpc	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”
vpn-connections-active	VPN连接状态为“正常”	vpnaas	确保VPN连接状态正常。

4.5.19 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 4-23 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。

建议项编号	建议项说明	合规规则	指导
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 4-24 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 4-25 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 4-26 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。

4.5.20 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。

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 4-27 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，确保高性能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，以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GeminiDB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，以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，确保高性能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GeminiDB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GeminiDB开启备份。

4.5.21 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 4-28 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ECS实例是否具有多个公网IP。拥有多个弹性公网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，确保高性能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，以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。

4.5.22 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 4-29 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，确保高性能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GeminiDB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，以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。

4.5.23 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 4-30 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，以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ECS实例是否具有多个弹性公网IP。拥有多个弹性公网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，确保高性能弹性文件服务（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，以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，以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，确保高性能弹性文件服务（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。

4.5.24 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如下表所示：

表 4-31 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	APIG专享版实例未配置访问日志，视为“不合规”
apig-instances-ssl-enabled	APIG专享版实例域名均关联SSL证书	apig	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”。
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	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”
css-cluster-disk-encryption-check	CSS集群开启磁盘加密	css	CSS集群未开启磁盘加密，视为“不合规”
css-cluster-https-required	CSS集群启用HTTPS	css	CSS集群未启用https，视为“不合规”
css-cluster-in-vpc	CSS集群绑定指定VPC资源	css	CSS集群未与指定的vpc资源绑定，视为“不合规”
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未启用事件分析，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	CTS追踪器未打开事件文件校验，视为“不合规”
cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建CTS追踪器，视为“不合规”
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	数据复制服务实时灾备任务使用公网网络，视为“不合规”
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	数据复制服务实时迁移任务使用公网网络，视为“不合规”
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	数据复制服务实时同步任务使用公网网络，视为“不合规”
dws-enable-log-dump	DWS集群启用日志转储	dws	DWS集群未启用日志转储，视为“不合规”
dws-enable-snapshot	DWS集群启用自动快照	dws	DWS集群未启用自动快照，视为“不合规”
dws-enable-ssl	DWS集群启用SSL加密连接	dws	DWS集群未启用SSL加密连接，视为“不合规”
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs，vpc	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	ECS资源具有弹性公网IP，视为“不合规”
eip-unbound-check	弹性公网IP未进行任何绑定	vpc	弹性公网IP未进行任何绑定，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
eip-use-in-specified-days	EIP在指定天数内绑定到资源实例	eip	EIP创建指定天数内未使用，视为“不合规”
elb-predefined-security-policy-https-check	ELB监听器配置指定预定义安全策略	elb	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“
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”
function-graph-public-access-prohibited	函数工作流的函数不允许访问公网	fgs	函数工作流的函数允许访问公网，视为“不合规”
gaussdb-nosql-enable-backup	GeminiDB开启备份	gaussdb nosql	GeminiDB未开启备份，视为“不合规”
gaussdb-nosql-enable-disk-encryption	GeminiDB使用磁盘加密	gaussdb nosql	GeminiDB未使用磁盘加密，视为“不合规”
iam-customer-policy-blocked-kms-actions	IAM策略中不存在KMS的任一阻拦action	iam	IAM策略存在允许的任一KMS阻拦的action，视为“不合规”
iam-password-policy	IAM用户密码策略符合要求	iam	IAM用户密码强度不满足密码强度要求，视为“不合规”
iam-policy-no-statements-with-admin-access	IAM策略不具备Admin权限	iam	IAM策略admin权限(*:*:*或*:*或*)，视为“不合规”
iam-role-has-all-permissions	IAM自定义策略具备所有权限	iam	IAM自定义策略具有allow的*:*权限，视为“不合规”
iam-root-access-key-check	IAM账号存在可使用的访问密钥	iam	账号存在可使用的访问密钥，视为“不合规”
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	IAM用户在指定时间范围内无登录行为，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
iam-user-mfa-enabled	IAM用户开启MFA	iam	IAM用户未开启MFA认证，视为“不合规”
kms-not-scheduled-for-deletion	KMS密钥不处于“计划删除”状态	kms	KMS密钥处于“计划删除“状态，视为“不合规”
mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	通过Console密码登录的IAM用户未开启MFA认证，视为“不合规”
mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS集群未开启kerberos认证，视为“不合规”
mrs-cluster-no-public-ip	MRS集群未绑定弹性公网IP	mrs	MRS集群绑定弹性公网IP，视为“不合规”
multi-region-cts-tracker-exists	在指定区域创建并启用CTS追踪器	cts	账号未在指定region列表创建CTS追踪器，视为“不合规”
pca-certificate-authority-expiration-check	检查私有CA是否过期	pca	私有CA在指定时间内过期，视为“不合规”
pca-certificate-expiration-check	检查私有证书是否过期	pca	私有证书没有标记在指定时间内到期，视为“不合规”
private-nat-gateway-authorized-vpc-only	NAT私网网关绑定指定VPC资源	nat	NAT私网网关未与指定的VPC资源绑定，视为“不合规”
rds-instance-enable-backup	RDS实例开启备份	rds	未开启备份的RDS资源，视为“不合规”
rds-instance-multi-az-support	RDS实例支持多可用区	rds	RDS实例仅支持一个可用区，视为“不合规”
rds-instance-no-public-ip	RDS实例不具有弹性公网IP	rds	RDS资源具有弹性公网IP，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
rds-instances-enable-kms	RDS实例开启存储加密	rds	未开启存储加密的RDS资源，视为“不合规”
root-account-mfa-enabled	根账号开启MFA认证	iam	根账号未开启MFA认证，视为“不合规”
sfsturbo-encrypted-check	高性能弹性文件服务通过KMS进行加密	sfsturbo	高性能弹性文件服务(SFS Turbo)未通过KMS进行加密，视为“不合规”
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	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”
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs，evs	已挂载的云硬盘未进行加密，视为“不合规”
vpc-acl-unused-check	未与子网关联的网络ACL	vpc	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”
vpc-default-sg-closed	默认安全组关闭出、入方向流量	vpc	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”
vpc-flow-logs-enabled	VPC启用流日志	vpc	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”
vpc-sg-ports-check	安全组端口检查	vpc	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”
vpc-sg-restricted-common-ports	安全组入站流量限制指定端口	vpc	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”

合规规则	规则中文名称	涉及云服务	规则描述
vpc-sg-restricted-ssh	安全组入站流量限制SSH端口	vpc	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”
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”

4.5.25 网络及数据安全最佳实践

本文为您介绍网络及数据安全最佳实践的应用场景以及合规包中的默认规则。

应用场景

该合规规则包从网络和数据安全等方面进行检测，帮助用户的信息资产免受网络攻击和数据泄露的威胁。关于网络及数据安全的相关要求请参见**CIS Control v8**。

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**CIS Control v8**中参考文档的章节编号，供您查阅参考。

表 4-32 网络及数据安全最佳实践合规包默认规则说明

建议项编号	合规规则	规则中文名称	涉及云服务	规则描述
1.1	ecs-in-allowed-security-groups	绑定指定标签的ECS关联在指定安全组ID列表内	ecs	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”
1.1	eip-unbound-check	弹性公网IP未进行任何绑定	vpc	弹性公网IP未进行任何绑定，视为“不合规”
1.1	eip-use-in-specified-days	EIP在指定天数内绑定到资源实例	eip	EIP创建后在指定天数内未使用，视为“不合规”

建议项编号	合规规则	规则中文名称	涉及云服务	规则描述
1.1	stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	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”
1.1	vpc-acl-unused-check	未与子网关联的网络ACL	vpc	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”
2.2	cce-cluster-oldest-supported-version	CCE集群运行的非受支持的最旧版本	cce	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”
3.3	css-cluster-in-vpc	CSS集群绑定指定VPC资源	css	CSS集群未与指定的虚拟私有云资源绑定，视为“不合规”
3.3	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	数据复制服务实时灾备任务使用公网网络，视为“不合规”
3.3	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	数据复制服务实时迁移任务使用公网网络，视为“不合规”
3.3	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	数据复制服务实时同步任务使用公网网络，视为“不合规”
3.3	ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs、vpc	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”
3.3	ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	ECS资源具有弹性公网IP，视为“不合规”
3.3	function-graph-inside-vpc	函数工作流使用指定VPC	fgs	函数工作流未使用指定VPC，视为“不合规”
3.3	function-graph-public-access-prohibited	函数工作流的函数不允许访问公网	fgs	函数工作流的函数允许访问公网，视为“不合规”

建议项编号	合规规则	规则中文名称	涉及云服务	规则描述
3.3	iam-customer-policy-blocked-kms-actions	IAM策略中不存在KMS的任一阻拦action	iam、access-analyzer-verified	IAM策略中授权KMS的任一阻拦action，视为“不合规”
3.3	iam-group-has-users-check	IAM用户组添加了IAM用户	iam	IAM用户组未添加任意IAM用户，视为“不合规”
3.3	iam-policy-no-statements-with-admin-access	IAM策略不具备Admin权限	iam	IAM策略中存在admin权限（Action为*:*:*或*:*或*），视为“不合规”
3.3	iam-role-has-all-permissions	IAM自定义策略具备所有权限	iam	IAM自定义策略具有allow的云服务的全部权限，视为“不合规”
3.3	iam-root-access-key-check	IAM账号存在可使用的访问密钥	iam	账号有可使用的AK/SK访问密钥，视为“不合规”
3.3	iam-user-group-membership-check	IAM用户归属指定用户组	iam	IAM用户不属于指定IAM用户组，视为“不合规”
3.3	iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	IAM用户在指定时间范围内无登录行为，视为“不合规”
3.3	mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS集群未开启kerberos认证，视为“不合规”
3.3	mrs-cluster-no-public-ip	MRS集群未绑定弹性公网IP	mrs	MRS集群绑定弹性公网IP，视为“不合规”
3.3	rds-instance-no-public-ip	RDS实例不具有弹性公网IP	rds	RDS资源具有弹性公网IP，视为“不合规”
3.3	bms-key-pair-security-login	BMS资源使用密钥对登录	bms	裸金属服务器未启用密钥对安全登录，视为“不合规”
3.1	apig-instances-ssl-enabled	APIG专享版实例域名均关联SSL证书	apig	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”

建议项编号	合规规则	规则中文名称	涉及云服务	规则描述
3.1	css-cluster-disk-encryption-check	CSS集群开启磁盘加密	css	CSS集群未开启磁盘加密，视为“不合规”
3.1	css-cluster-https-required	CSS集群启用HTTPS	css	CSS集群未启用HTTPS，视为“不合规”
3.1	dws-enable-ssl	DWS集群启用SSL加密连接	dws	DWS集群未启用SSL加密连接，视为“不合规”
3.1	elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”
3.11	cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
3.11	dws-enable-kms	DWS集群启用KMS加密	dws	DWS集群未启用KMS加密，视为“不合规”
3.11	gaussdb-nosql-enable-disk-encryption	GeminiDB使用磁盘加密	gemini db	GeminiDB未使用磁盘加密，视为“不合规”
3.11	rds-instances-enable-kms	RDS实例开启存储加密	rds	未开启存储加密的RDS资源，视为“不合规”
3.11	sfsturbo-encrypted-check	高性能弹性文件服务通过KMS进行加密	sfsturbo	高性能弹性文件服务（SFS Turbo）未通过KMS进行加密，视为“不合规”
3.11	volumes-encrypted-check	已挂载的云硬盘开启加密	evs、ecs	已挂载的云硬盘未进行加密，视为“不合规”
3.11	cbr-backup-encrypted-check	CBR备份被加密	cbr	CBR服务的备份未被加密，视为“不合规”
3.14	apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	APIG专享版实例未配置访问日志，视为“不合规”
3.14	cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未启用事件分析，视为“不合规”
3.14	cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”
3.14	cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建CTS追踪器，视为“不合规”

建议项编号	合规规则	规则中文名称	涉及云服务	规则描述
3.14	multi-region-cts-tracker-exists	在指定区域创建并启用CTS追踪器	cts	账号未在指定Region列表创建CTS追踪器，视为“不合规”
3.14	rds-instance-logging-enabled	RDS实例配备日志	rds	未配备任何日志的RDS资源，视为“不合规”
3.14	vpc-flow-logs-enabled	VPC启用流日志	vpc	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”
4.1	access-keys-rotated	IAM用户的AccessKey在指定时间内轮换	iam	IAM用户的AK/SK访问密钥未在指定天数内更换，视为“不合规”
4.1	evs-use-in-specified-days	云硬盘创建后在指定天数内绑定资源实例	evs	云硬盘创建后在指定天数内未使用，视为“不合规”
4.1	stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	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”
4.1	volume-unused-check	云硬盘闲置检测	evs	云硬盘未挂载给任何云服务器，视为“不合规”
4.6	apig-instances-ssl-enabled	APIG专享版实例域名均关联SSL证书	apig	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”
4.6	css-cluster-https-required	CSS集群启用HTTPS	css	CSS集群未启用HTTPS，视为“不合规”
4.6	dws-enable-ssl	DWS集群启用SSL加密连接	dws	DWS集群未启用SSL加密连接，视为“不合规”
4.6	elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”
4.7	iam-root-access-key-check	IAM账号存在可使用的访问密钥	iam	账号有可使用的AK/SK访问密钥，视为“不合规”
5.2	iam-password-policy	IAM用户密码策略符合要求	iam	IAM用户密码强度不满足密码强度要求，视为“不合规”

建议项编号	合规规则	规则中文名称	涉及云服务	规则描述
5.2	iam-user-mfa-enabled	IAM用户开启MFA	iam	IAM用户未开启MFA认证，视为“不合规”
5.2	mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	通过Console密码登录的IAM用户未开启MFA认证，视为“不合规”
5.2	root-account-mfa-enabled	根账号开启MFA认证	iam	账号未开启MFA认证，视为“不合规”
5.3	iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	IAM用户在指定时间范围内无登录行为，视为“不合规”
5.4	iam-policy-no-statements-with-admin-access	IAM策略不具备Admin权限	iam	IAM策略中存在admin权限（Action为*:*:*或*:*或*），视为“不合规”
5.4	iam-root-access-key-check	IAM账号存在可使用的访问密钥	iam	账号有可使用的AK/SK访问密钥，视为“不合规”
6.4	iam-user-mfa-enabled	IAM用户开启MFA	iam	IAM用户未开启MFA认证，视为“不合规”
6.4	mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	通过Console密码登录的IAM用户未开启MFA认证，视为“不合规”
6.4	root-account-mfa-enabled	根账号开启MFA认证	iam	账号未开启MFA认证，视为“不合规”
8.2	apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	APIG专享版实例未配置访问日志，视为“不合规”
8.2	cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未启用事件分析，视为“不合规”
8.2	cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”
8.2	cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建CTS追踪器，视为“不合规”
8.2	multi-region-cts-tracker-exists	在指定区域创建并启用CTS追踪器	cts	账号未在指定Region列表创建CTS追踪器，视为“不合规”
8.2	rds-instance-logging-enabled	RDS实例配备日志	rds	未配备任何日志的RDS资源，视为“不合规”

建议项编号	合规规则	规则中文名称	涉及云服务	规则描述
8.2	vpc-flow-logs-enabled	VPC启用流日志	vpc	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”
8.5	apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	APIG专享版实例未配置访问日志，视为“不合规”
8.5	cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未启用事件分析，视为“不合规”
8.5	cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”
8.5	cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建CTS追踪器，视为“不合规”
8.5	multi-region-cts-tracker-exists	在指定区域创建并启用CTS追踪器	cts	账号未在指定Region列表创建CTS追踪器，视为“不合规”
8.5	rds-instance-logging-enabled	RDS实例配备日志	rds	未配备任何日志的RDS资源，视为“不合规”
8.5	vpc-flow-logs-enabled	VPC启用流日志	vpc	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”
8.9	cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未启用事件分析，视为“不合规”
11.2	dws-enable-snapshot	DWS集群启用自动快照	dws	DWS集群未启用自动快照，视为“不合规”
11.2	gaussdb-instance-enable-backup	GaussDB实例开启自动备份	gaussdb	未开启资源备份的GaussDB实例，视为“不合规”
11.2	gaussdb-mysql-instance-enable-backup	TaurusDB实例开启备份	taurusdb	未开启备份的TaurusDB实例，视为“不合规”
11.2	gaussdb-nosql-enable-backup	GeminiDB开启备份	gemini db	GeminiDB未开启备份，视为“不合规”
11.2	rds-instance-enable-backup	RDS实例开启备份	rds	未开启备份的RDS资源，视为“不合规”
11.3	rds-instances-enable-kms	RDS实例开启存储加密	rds	未开启存储加密的RDS资源，视为“不合规”

建议项编号	合规规则	规则中文名称	涉及云服务	规则描述
11.3	volumes-encrypted-check	已挂载的云硬盘开启加密	evs、ecs	已挂载的云硬盘未进行加密，视为“不合规”
11.4	dws-enable-snapshot	DWS集群启用自动快照	dws	DWS集群未启用自动快照，视为“不合规”
11.4	gaussdb-instance-enable-backup	GaussDB实例开启自动备份	gaussdb	未开启资源备份的GaussDB实例，视为“不合规”
11.4	gaussdb-mysql-instance-enable-backup	TaurusDB实例开启备份	taurusdb	未开启备份的TaurusDB实例，视为“不合规”
11.4	gaussdb-nosql-enable-backup	GeminiDB开启备份	gemini db	GeminiDB未开启备份，视为“不合规”
11.4	rds-instance-enable-backup	RDS实例开启备份	rds	未开启备份的RDS资源，视为“不合规”
12.2	css-cluster-in-vpc	CSS集群绑定指定VPC资源	css	CSS集群未与指定的虚拟私有云资源绑定，视为“不合规”
12.2	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	数据复制服务实时灾备任务使用公网网络，视为“不合规”
12.2	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	数据复制服务实时迁移任务使用公网网络，视为“不合规”
12.2	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	数据复制服务实时同步任务使用公网网络，视为“不合规”
12.2	ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs、vpc	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”
12.2	ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	ECS资源具有弹性公网IP，视为“不合规”
12.2	function-graph-inside-vpc	函数工作流使用指定VPC	fgs	函数工作流未使用指定VPC，视为“不合规”
12.2	function-graph-public-access-prohibited	函数工作流的函数不允许访问公网	fgs	函数工作流的函数允许访问公网，视为“不合规”
12.2	mrs-cluster-no-public-ip	MRS集群未绑定弹性公网IP	mrs	MRS集群绑定弹性公网IP，视为“不合规”

建议项编号	合规规则	规则中文名称	涉及云服务	规则描述
12.2	pca-certificate-authority-expiration-check	检查私有CA是否过期	pca	私有CA在指定时间内过期，视为“不合规”
12.2	pca-certificate-expiration-check	检查私有证书是否过期	pca	私有证书没有标记在指定时间内到期，视为“不合规”
12.2	rds-instance-multi-az-support	RDS实例支持多可用区	rds	RDS实例仅支持一个可用区，视为“不合规”
12.2	rds-instance-no-public-ip	RDS实例不具有弹性公网IP	rds	RDS资源具有弹性公网IP，视为“不合规”
12.2	vpc-default-sg-closed	默认安全组关闭出、入方向流量	vpc	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”
12.2	vpc-sg-ports-check	安全组端口检查	vpc	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”
12.2	vpc-sg-restricted-common-ports	安全组入站流量限制指定端口	vpc	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”
12.2	vpc-sg-restricted-ssh	安全组入站流量限制SSH端口	vpc	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”
12.2	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”
12.3	apig-instances-ssl-enabled	APIG专享版实例域名均关联SSL证书	apig	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”
12.3	css-cluster-https-required	CSS集群启用HTTPS	css	CSS集群未启用HTTPS，视为“不合规”
12.3	dws-enable-ssl	DWS集群启用SSL加密连接	dws	DWS集群未启用SSL加密连接，视为“不合规”
12.3	elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”

建议项编号	合规规则	规则中文名称	涉及云服务	规则描述
12.6	apig-instances-ssl-enabled	APIG专享版实例域名均关联SSL证书	apig	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”
12.6	css-cluster-https-required	CSS集群启用HTTPS	css	CSS集群未启用HTTPS，视为“不合规”
12.6	dws-enable-ssl	DWS集群启用SSL加密连接	dws	DWS集群未启用SSL加密连接，视为“不合规”
12.6	elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”
13.6	vpc-flow-logs-enabled	VPC启用流日志	vpc	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”

4.5.26 适用于 Landing Zone 基础场景的最佳实践

本文为您介绍适用于Landing Zone基础场景的最佳实践的业务背景以及合规包中的默认规则。

业务背景

为满足客户更好的管理云的诉求，华为云基于华为公司多年自身企业治理经验以及帮助企业实现数字化转型的成功实践，系统性提出Landing Zone解决方案。Landing Zone解决方案旨在为企业构筑一套可持续扩展、安全、合规的云上运行环境，天然契合金融行业的上云与数字化转型痛点诉求。Landing Zone解决方案从多账号组织管理、网络规划、身份与权限、数据边界、安全防护、合规审计、运维监控和成本管理多个维度按照最佳实践指导企业搭建上云环境。

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

该示例模板中对应的合规规则的说明如下表所示：

表 4-33 适用于 Landing Zone 基础场景的最佳实践合规包默认规则说明

规则目标	合规规则	规则中文名称
组织单元和账号设计	account-part-of-organizations	账号加入组织
组织单元和账号设计	iam-user-group-membership-check	IAM用户归属指定用户组
组织单元和账号设计	iam-group-has-users-check	IAM用户组添加了IAM用户
统一身份权限	root-account-mfa-enabled	根账号开启MFA认证
统一身份权限	mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证
统一身份权限	iam-root-access-key-check	IAM账号存在可使用的访问密钥
统一身份权限	iam-user-single-access-key	IAM用户单访问密钥
统一身份权限	iam-password-policy	IAM用户密码策略符合要求
统一身份权限	access-keys-rotated	IAM用户的AccessKey在指定时间内轮换
统一身份权限	iam-user-last-login-check	IAM用户在指定时间内有登录行为
统一身份权限	iam-policy-no-statements-with-admin-access	IAM策略不具备Admin权限
统一网络架构	eip-unbound-check	弹性公网IP未进行任何绑定
统一网络架构	elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议
统一网络架构	vpc-acl-unused-check	未与子网关联的网络ACL
统一网络架构	vpc-sg-restricted-ssh	安全组入站流量限制SSH端口
统一网络架构	vpc-default-sg-closed	默认安全组关闭出、入方向流量
统一网络架构	vpc-sg-ports-check	安全组端口检查
统一网络架构	vpn-connections-active	VPN连接状态为“正常”
统一运维监控	alarm-obs-bucket-policy-change	CES配置监控OBS桶策略变更的事件监控告警

规则目标	合规规则	规则中文名称
统一运维监控	alarm-vpc-change	CES配置监控VPC变更的事件监控告警
统一运维监控	alarm-kms-disable-or-delete-key	CES配置监控KMS禁用或计划删除密钥的事件监控告警
统一合规审计	cts-lts-enable	CTS追踪器启用事件分析
统一合规审计	cts-support-validate-check	CTS追踪器打开事件文件校验
统一合规审计	cts-kms-encrypted-check	CTS追踪器通过KMS进行加密
统一合规审计	multi-region-cts-tracker-exists	在指定区域创建并启用CTS追踪器
统一安全管控	cce-endpoint-public-access	CCE集群资源不具有弹性公网IP
统一安全管控	ecs-instance-no-public-ip	ECS资源不能公网访问
统一安全管控	rds-instance-no-public-ip	RDS实例不具有弹性公网IP
统一安全管控	pca-certificate-authority-expiration-check	检查私有CA是否过期
统一安全管控	pca-certificate-expiration-check	检查私有证书是否过期
统一安全管控	volumes-encrypted-check	已挂载的云硬盘开启加密
统一安全管控	rds-instances-enable-kms	RDS实例开启存储加密
可靠架构	rds-instance-enable-backup	RDS实例开启备份
可靠架构	rds-instance-multi-az-support	RDS实例支持多可用区
可靠架构	volume-unused-check	云硬盘闲置检测

4.5.27 架构安全支柱运营最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-34 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
access-keys-rotated	IAM用户的AccessKey在指定时间内轮换	iam	IAM用户的访问密钥未在指定天数内轮转，视为“不合规”
pca-certificate-authority-expiration-check	检查私有CA是否过期	pca	私有CA在指定时间内过期，视为“不合规”
pca-certificate-expiration-check	检查私有证书是否过期	pca	私有证书在指定时间内到期，视为“不合规”
apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	APIG专享版实例未配置访问日志，视为“不合规”
apig-instances-ssl-enabled	APIG专享版实例域名均关联SSL证书	apig	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”
cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未转储到LTS，视为“不合规”
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	CTS追踪器未打开事件文件校验，视为“不合规”
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”
ecs-multiple-public-ip-check	检查ECS资源是否具有多个公网IP	ecs	ECS资源具有多个弹性公网IP，视为“不合规”
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	ECS资源具有弹性公网IP，视为“不合规”
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	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”

合规规则	规则中文名称	涉及云服务	规则描述
evs-use-in-specified-days	云硬盘创建后在指定天数内绑定资源实例	evs	创建的EVS在指定天数后仍未绑定到资源实例，视为“不合规”
volume-unused-check	云硬盘闲置检测	evs	云硬盘未挂载给任何云服务器，视为“不合规”
cce-cluster-end-of-maintenance-version	CCE集群版本为处于维护的版本	cce	CCE集群版本为停止维护的版本，视为“不合规”
cce-cluster-oldest-supported-version	CCE集群运行的非受支持的最旧版本	cce	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”
sfsturbo-encrypted-check	高性能弹性文件服务通过KMS进行加密	sfsturbo	高性能弹性文件服务(SFS Turbo)未通过KMS进行加密，视为“不合规”
css-cluster-in-vpc	CSS集群绑定指定VPC资源	css	CSS集群未与指定的vpc资源绑定，视为“不合规”
css-cluster-disk-encryption-check	CSS集群开启磁盘加密	css	CSS集群未开启磁盘加密，视为“不合规”
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”
mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS集群未开启kerberos认证，视为“不合规”
mrs-cluster-no-public-ip	MRS集群未绑定弹性公网IP	mrs	MRS集群绑定弹性公网IP，视为“不合规”
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs, evs	已挂载的云硬盘未进行加密，视为“不合规”
iam-customer-policy-blocked-kms-actions	IAM策略中不授权KMS的禁止的action	iam, access-analyzer-verified	IAM策略中授权KMS的任一阻拦action，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
iam-group-has-users-check	IAM用户组添加了IAM用户	iam	IAM用户组未添加任意IAM用户，视为“不合规”
iam-password-policy	IAM用户密码策略符合要求	iam	IAM用户密码强度不满足密码强度要求，视为“不合规”
iam-policy-no-statements-with-admin-access	IAM策略不具备Admin权限	iam	IAM自定义策略具有allow的全部云服务的全部权限(*:*:*或*:*或*)，视为“不合规”
iam-role-has-all-permissions	IAM自定义策略具备所有权限	iam	IAM自定义策略具有allow的任意云服务的全部权限，视为“不合规”
iam-root-access-key-check	根用户存在可使用的访问密钥	iam	根用户存在可使用的访问密钥，视为“不合规”
iam-user-group-membership-check	IAM用户归属指定用户组	iam	IAM用户不属于指定IAM用户组，视为“不合规”
iam-user-mfa-enabled	IAM用户开启MFA	iam	IAM用户未开启MFA认证，视为“不合规”
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	IAM用户在指定时间范围内无登录行为，视为“不合规”
vpc-sg-restricted-ssh	安全组入站流量限制SSH端口	vpc	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放TCP 22端口，视为“不合规”
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs, vpc	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”
kms-not-scheduled-for-deletion	KMS密钥不处于“计划删除”状态	kms	KMS密钥处于“计划删除“状态，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
function-graph-public-access-prohibited	函数工作流的函数不允许访问公网	fgs	函数工作流的函数允许访问公网，视为“不合规”
function-graph-inside-vpc	函数工作流使用指定VPC	fgs	函数工作流未使用指定VPC，视为“不合规”
mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	通过console密码登录的IAM用户未开启MFA认证，视为“不合规”
css-cluster-https-required	CSS集群启用HTTPS	css	CSS集群未启用https，视为“不合规”
rds-instance-no-public-ip	RDS实例不具有弹性公网IP	rds	RDS资源具有弹性公网IP，视为“不合规”
rds-instance-logging-enabled	RDS实例配备日志	rds	未配备任何日志的rds资源，视为“不合规”
rds-instances-enable-kms	RDS实例开启存储加密	rds	未开启存储加密的rds资源，视为“不合规”
dws-enable-kms	DWS集群启用KMS加密	dws	DWS集群未启用KMS加密，视为“不合规”
gaussdb-nosql-enable-disk-encryption	GeminiDB使用磁盘加密	gemini db	GeminiDB未使用磁盘加密，视为“不合规”
dws-enable-ssl	DWS集群启用SSL加密连接	dws	DWS集群未启用SSL加密连接，视为“不合规”
vpc-sg-restricted-common-ports	安全组入站流量限制指定端口	vpc	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)或所有IPv6地址(::/0)，视为“不合规”
root-account-mfa-enabled	根用户开启MFA认证	iam	根用户未开启MFA认证，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
vpc-default-sg-closed	默认安全组关闭出、入方向流量	vpc	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”
vpc-flow-logs-enabled	VPC启用流日志	vpc	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”
vpc-acl-unused-check	未与子网关联的网络ACL	vpc	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”
vpc-sg-ports-check	安全组端口检查	vpc	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放了所有的TCP或UDP端口时，视为“不合规”
waf-instance-policy-not-empty	WAF防护域名配置防护策略	waf	WAF防护域名未配置防护策略，视为“不合规”
pca-certificate-authority-root-disable	检查私有根CA是否停用	pca	私有根CA未停用，视为“不合规”

4.5.28 网络和内容交付服务运营最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-35 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	APIG专享版实例未配置访问日志，视为“不合规”
apig-instances-ssl-enabled	APIG专享版实例域名均关联SSL证书	apig	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	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”
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”
vpc-sg-restricted-ssh	安全组入站流量限制SSH端口	vpc	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放TCP 22端口，视为“不合规”
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs, vpc	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”
private-nat-gateway-authorized-vpc-only	NAT私网网关绑定指定VPC资源	nat	NAT私网网关未与指定的VPC资源绑定，视为“不合规”
vpc-sg-restricted-common-ports	安全组入站流量限制指定端口	vpc	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)或所有IPv6地址(::/0)，视为“不合规”
vpc-default-sg-closed	默认安全组关闭出、入方向流量	vpc	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”
vpc-flow-logs-enabled	VPC启用流日志	vpc	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”
vpc-acl-unused-check	未与子网关联的网络ACL	vpc	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”

合规规则	规则中文名称	涉及云服务	规则描述
vpc-sg-ports-check	安全组端口检查	vpc	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放了所有的TCP或UDP端口时，视为“不合规”
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”

4.5.29 适用于空闲资产管理的最佳实践

业务背景

适用于空闲资产管理的最佳实践用于检测常见的云资源在购买后是否被闲置，涉及弹性公网IP、弹性云服务器、云硬盘等云产品。资源购买后未使用会导致企业成本的浪费，建议及时发现并治理。

默认规则

该示例模板中对应的合规规则的说明如下表所示：

表 4-36 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	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”
eip-use-in-specified-days	弹性公网IP在指定天数内绑定到资源实例	vpc	创建的弹性公网IP在指定天数后仍未绑定到资源实例，视为“不合规”
evs-use-in-specified-days	云硬盘创建后在指定天数内绑定资源实例	evs	创建的EVS在指定天数后仍未绑定到资源实例，视为“不合规”
eip-unbound-check	弹性公网IP未进行任何绑定	vpc	弹性公网IP未进行任何绑定，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
iam-group-has-users-check	IAM用户组添加了IAM用户	iam	IAM用户组未添加任意IAM用户，视为“不合规”
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	IAM用户在指定时间范围内无登录行为，视为“不合规”
volume-unused-check	云硬盘闲置检测	evs	云硬盘未挂载给任何云服务器，视为“不合规”
vpc-acl-unused-check	未与子网关联的网络ACL	vpc	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”
cce-cluster-end-of-maintenance-version	CCE集群版本为处于维护的版本	cce	CCE集群版本为停止维护的版本，视为“不合规”

4.5.30 多可用区架构最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-37 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
css-cluster-multiple-az-check	CSS集群具备多AZ容灾	css	CSS集群没有多az容灾，视为“不合规”
gaussdb-nosql-deploy-in-single-az	GeminiDB部署在单个可用区	gemini db	GeminiDB部署在单个可用区中，视为“不合规”
as-multiple-az	弹性伸缩组启用多AZ部署	as	弹性伸缩组没有启用多AZ部署，视为“不合规”
mrs-cluster-multiAZ-deployment	MRS集群使用多AZ部署	mrs	MRS集群没有多az部署，视为“不合规”
rds-instance-multi-az-support	RDS实例支持多可用区	rds	RDS实例仅支持一个可用区，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
dcs-redis-high-tolerance	DCS Redis实例高可用	dcs	dcs redis资源不是高可用时，视为“不合规”
elb-multiple-az-check	ELB资源使用多AZ部署	elb	检查负载均衡器是否已从多个可用分区注册实例。如果负载均衡器的实例注册在少于2个可用区，视为“不合规”
gaussdb-instance-multiple-az-check	GaussDB实例跨AZ部署检查	gaussdb	gaussdb资源未跨AZ部署，视为“不合规”
gaussdb-mysql-instance-multiple-az-check	TaurusDB实例跨AZ部署检查	taurus db	TaurusDB实例未跨AZ部署，视为“不合规”

4.5.31 资源稳定性最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-38 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
css-cluster-multiple-az-check	CSS集群具备多AZ容灾	css	CSS集群没有多az容灾，视为“不合规”
gaussdb-nosql-deploy-in-single-az	GeminiDB部署在单个可用区	gemini db	GeminiDB部署在单个可用区中，视为“不合规”
as-multiple-az	弹性伸缩组启用多AZ部署	as	弹性伸缩组没有启用多AZ部署，视为“不合规”
mrs-cluster-multiAZ-deployment	MRS集群使用多AZ部署	mrs	MRS集群没有多az部署，视为“不合规”
rds-instance-multi-az-support	RDS实例支持多可用区	rds	RDS实例仅支持一个可用区，视为“不合规”
dcs-redis-high-tolerance	DCS Redis实例高可用	dcs	dcs redis资源不是高可用时，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
allowed-rds-flavors	RDS实例规格在指定的范围	rds	RDS实例的规格不在指定的范围内，视为“不合规”
allowed-images-by-name	ECS实例的镜像名称在指定的范围	ecs	指定允许的镜像名称列表，ECS实例的镜像名称不在指定的范围内，视为“不合规”
allowed-images-by-id	ECS实例的镜像ID在指定的范围	ecs, ims	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”
function-graph-concurrency-check	函数工作流的函数并发数在指定范围内	fgs	FunctionGraph函数并发数不在指定的范围内，视为“不合规”
function-graph-settings-check	检查函数工作流参数设置	fgs	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”
dds-instance-hamode	DDS实例属于指定实例类型	dds	指定实例类型，不属于此的DDS实例资源，视为“不合规”
allowed-cce-flavors	CCE集群规格在指定的范围	cce	CCE集群的规格不在指定的范围内，视为“不合规”
allowed-ecs-flavors	ECS资源规格在指定的范围	ecs	ECS资源的规格不在指定的范围内，视为“不合规”

4.5.32 适用于 API 网关（APIG）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-39 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
apig-instances-authorization-type-configured	APIG专享版实例配置安全认证类型	apig	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”
apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	APIG专享版实例未配置访问日志，视为“不合规”
apig-instances-ssl-enabled	APIG专享版实例域名均关联SSL证书	apig	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”

4.5.33 适用于云容器引擎（CCE）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-40 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
allowed-cce-flavors	CCE集群规格在指定的范围	cce	CCE集群的规格不在指定的范围内，视为“不合规”
cce-cluster-end-of-maintenance-version	CCE集群版本为处于维护的版本	cce	CCE集群版本为停止维护的版本，视为“不合规”
cce-cluster-oldest-supported-version	CCE集群运行的非受支持的最旧版本	cce	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”
cce-endpoint-public-access	CCE集群资源不具有弹性公网IP	cce	CCE集群资源具有弹性公网IP，视为“不合规”

4.5.34 适用于内容分发网络（CDN）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-41 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
cdn-enable-https-certificate	CDN使用HTTPS证书	cdn	CDN未使用HTTPS，视为“不合规”
cdn-origin-protocol-no-http	CDN回源方式使用HTTPS	cdn	CDN回源方式未使用HTTPS，视为“不合规”
cdn-security-policy-check	CDN安全策略检查	cdn	CDN使用TLSv1.2以下的版本，视为“不合规”
cdn-use-my-certificate	CDN使用自有证书	cdn	CDN使用了自有证书，视为“不合规”

4.5.35 适用于函数工作流（FunctionGraph）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-42 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
function-graph-concurrency-check	函数工作流的函数并发数在指定范围内	fgs	FunctionGraph函数并发数不在指定的范围内，视为“不合规”
function-graph-inside-vpc	函数工作流使用指定VPC	fgs	函数工作流未使用指定VPC，视为“不合规”
function-graph-public-access-prohibited	函数工作流的函数不允许访问公网	fgs	函数工作流的函数允许访问公网，视为“不合规”
function-graph-settings-check	检查函数工作流参数设置	fgs	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”
function-graph-logging-enabled	函数工作流的函数启用日志配置	fgs	函数工作流的函数未启用日志配置，视为“不合规”

4.5.36 适用于云数据库（GaussDB）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-43 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
gaussdb-instance-enable-auditLog	GaussDB实例开启审计日志	gaussdb	未开启审计日志的gaussdb资源，视为“不合规”
gaussdb-instance-enable-backup	GaussDB实例开启自动备份	gaussdb	未开启资源备份的gaussdb资源，视为“不合规”
gaussdb-instance-enable-errorLog	GaussDB实例开启错误日志	gaussdb	未开启错误日志的gaussdb资源，视为“不合规”
gaussdb-instance-enable-slowLog	GaussDB实例开启慢日志	gaussdb	未开启慢日志的gaussdb资源，视为“不合规”
gaussdb-instance-in-vpc	GaussDB资源属于指定虚拟私有云ID	gaussdb	指定虚拟私有云ID，不属于此VPC的gaussdb资源，视为“不合规”
gaussdb-instance-multiple-az-check	GaussDB实例跨AZ部署检查	gaussdb	gaussdb资源未跨AZ部署，视为“不合规”
gaussdb-instance-no-public-ip-check	GaussDB实例弹性公网IP检查	gaussdb	gaussdb实例如绑定弹性公网IP，视为“不合规”
gaussdb-instance-ssl-enable	GaussDB实例开启传输数据加密	gaussdb	gaussdb实例未启用SSL数据传输加密，视为“不合规”

4.5.37 适用于云数据库（GeminiDB）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-44 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
gaussdb-nosql-deploy-in-single-az	GeminiDB部署在单个可用区	gemini db	GeminiDB部署在单个可用区中，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
gaussdb-nosql-enable-backup	GeminiDB开启备份	gemini db	GeminiDB未开启备份，视为“不合规”
gaussdb-nosql-enable-disk-encryption	GeminiDB使用磁盘加密	gemini db	GeminiDB未使用磁盘加密，视为“不合规”
gaussdb-nosql-enable-error-log	GeminiDB开启错误日志	gemini db	GeminiDB未开启错误日志，视为“不合规”
gaussdb-nosql-support-slow-log	GeminiDB开启慢查询日志	gemini db	GeminiDB不开启慢查询日志，视为“不合规”

4.5.38 适用于 MapReduce 服务（MRS）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-45 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
mrs-cluster-in-allowed-security-groups	MRS集群属于指定安全组	mrs	指定安全组id，不属于此安全组的mrs资源，视为“不合规”
mrs-cluster-in-vpc	MRS集群属于指定VPC	mrs	指定虚拟私有云ID，不属于此VPC的mrs资源，视为“不合规”
mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS集群未开启kerberos认证，视为“不合规”
mrs-cluster-multiAZ-deployment	MRS集群使用多AZ部署	mrs	MRS集群没有多az部署，视为“不合规”
mrs-cluster-no-public-ip	MRS集群未绑定弹性公网IP	mrs	MRS集群绑定弹性公网IP，视为“不合规”
mrs-cluster-encrypt-enable	MRS集群开启kms加密	mrs	MRS集群未开启kms加密，视为“不合规”

4.5.39 NIST 审计标准最佳实践

应用场景

基于NIST的部分要求，对华为云上资源的合规性进行检测。

默认规则

该示例模板中对应的合规规则的说明如下表所示：

表 4-46 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
access-keys-rotated	IAM用户的AccessKey在指定时间内轮换	iam	IAM用户的访问密钥未在指定天数内轮转，视为“不合规”
apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	APIG专享版实例未配置访问日志，视为“不合规”
apig-instances-ssl-enabled	APIG专享版实例域名均关联SSL证书	apig	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	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”
css-cluster-disk-encryption-check	CSS集群开启磁盘加密	css	CSS集群未开启磁盘加密，视为“不合规”
css-cluster-in-vpc	CSS集群绑定指定VPC资源	css	CSS集群未与指定的vpc资源绑定，视为“不合规”
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未转储到LTS，视为“不合规”
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	CTS追踪器未打开事件文件校验，视为“不合规”
cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建并启用CTS追踪器，视为“不合规”
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	数据复制服务实时灾备任务使用公网网络，视为“不合规”
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	数据复制服务实时迁移任务使用公网网络，视为“不合规”
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	数据复制服务实时同步任务使用公网网络，视为“不合规”
dws-enable-kms	DWS集群启用KMS加密	dws	DWS集群未启用KMS加密，视为“不合规”
dws-enable-snapshot	DWS集群启用自动快照	dws	DWS集群未启用自动快照，视为“不合规”
dws-enable-ssl	DWS集群启用SSL加密连接	dws	DWS集群未启用SSL加密连接，视为“不合规”
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs, vpc	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	ECS资源具有弹性公网IP，视为“不合规”
eip-unbound-check	弹性公网IP未进行任何绑定	vpc	弹性公网IP未进行任何绑定，视为“不合规”
eip-use-in-specified-days	弹性公网IP在指定天数内绑定到资源实例	vpc	创建的弹性公网IP在指定天数后仍未绑定到资源实例，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”
evs-use-in-specified-days	云硬盘创建后在指定天数内绑定资源实例	evs	创建的EVS在指定天数后仍未绑定到资源实例，视为“不合规”
function-graph-inside-vpc	函数工作流使用指定VPC	fgs	函数工作流未使用指定VPC，视为“不合规”
function-graph-public-access-prohibited	函数工作流的函数不允许访问公网	fgs	函数工作流的函数允许访问公网，视为“不合规”
gaussdb-nosql-enable-backup	GeminiDB开启备份	gemini db	GeminiDB未开启备份，视为“不合规”
iam-customer-policy-blocked-kms-actions	IAM策略中不授权KMS的禁止的action	iam, access-analyzer-verified	IAM策略中授权KMS的任一阻拦action，视为“不合规”
iam-group-has-users-check	IAM用户组添加了IAM用户	iam	IAM用户组未添加任意IAM用户，视为“不合规”
iam-password-policy	IAM用户密码策略符合要求	iam	IAM用户密码强度不满足密码强度要求，视为“不合规”
iam-policy-no-statements-with-admin-access	IAM策略不具备Admin权限	iam	IAM自定义策略具有allow的全部云服务的全部权限(*:*:*或*:*或*)，视为“不合规”
iam-role-has-all-permissions	IAM自定义策略具备所有权限	iam	IAM自定义策略具有allow的任意云服务的全部权限，视为“不合规”
iam-root-access-key-check	根用户存在可使用的访问密钥	iam	根用户存在可使用的访问密钥，视为“不合规”
iam-user-group-membership-check	IAM用户归属指定用户组	iam	IAM用户不属于指定IAM用户组，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
iam-user-mfa-enabled	IAM用户开启MFA	iam	IAM用户未开启MFA认证，视为“不合规”
kms-not-scheduled-for-deletion	KMS密钥不处于“计划删除”状态	kms	KMS密钥处于“计划删除“状态，视为“不合规”
kms-rotation-enabled	KMS密钥启用密钥轮换	kms	KMS密钥未启用密钥轮换，视为“不合规”
mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	通过console密码登录的IAM用户未开启MFA认证，视为“不合规”
mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS集群未开启kerberos认证，视为“不合规”
mrs-cluster-no-public-ip	MRS集群未绑定弹性公网IP	mrs	MRS集群绑定弹性公网IP，视为“不合规”
multi-region-cts-tracker-exists	在指定区域创建并启用CTS追踪器	cts	账号未在指定region列表创建并启用CTS追踪器，视为“不合规”
private-nat-gateway-authorized-vpc-only	NAT私网网关绑定指定VPC资源	nat	NAT私网网关未与指定的VPC资源绑定，视为“不合规”
rds-instance-enable-backup	RDS实例开启备份	rds	未开启备份的rds资源，视为“不合规”
rds-instance-multi-az-support	RDS实例支持多可用区	rds	RDS实例仅支持一个可用区，视为“不合规”
rds-instance-no-public-ip	RDS实例不具有弹性公网IP	rds	RDS资源具有弹性公网IP，视为“不合规”
root-account-mfa-enabled	根用户开启MFA认证	iam	根用户未开启MFA认证，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
sfsturbo-encrypted-check	高性能弹性文件服务通过KMS进行加密	sfsturbo	高性能弹性文件服务(SFS Turbo)未通过KMS进行加密，视为“不合规”
stopped-ecs-date-diff	关机状态的ECS未进行任意操作的时间检查	ecs	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”
volume-unused-check	云硬盘闲置检测	evs	云硬盘未挂载给任何云服务器，视为“不合规”
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs, evs	已挂载的云硬盘未进行加密，视为“不合规”
vpc-acl-unused-check	未与子网关联的网络ACL	vpc	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”
vpc-default-sg-closed	默认安全组关闭出、入方向流量	vpc	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”
vpc-sg-ports-check	安全组端口检查	vpc	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放了所有的TCP或UDP端口时，视为“不合规”
vpc-sg-restricted-common-ports	安全组入站流量限制指定端口	vpc	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)或所有IPv6地址(::/0)，视为“不合规”
vpc-sg-restricted-ssh	安全组入站流量限制SSH端口	vpc	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放TCP 22端口，视为“不合规”
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”

4.5.40 新加坡金融行业的最佳实践

应用场景

新加坡金融管理局针对云计算的监管预期，制定了MAS准则，用于规范金融机构的实践，关于该指南的更多信息，请参见**Technology Risk Management Guidelines**。

默认规则

该示例模板中对应的合规规则的说明如下表所示：

表 4-47 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
access-keys-rotated	IAM用户的AccessKey在指定时间内轮换	iam	IAM用户的访问密钥未在指定天数内轮转，视为“不合规”
account-part-of-organizations	账号加入组织	organizations	账号未加入组织中，视为“不合规”
pca-certificate-authority-expiration-check	检查私有CA是否过期	pca	私有CA在指定时间内过期，视为“不合规”
pca-certificate-expiration-check	检查私有证书是否过期	pca	私有证书在指定时间内到期，视为“不合规”
elb-http-to-https-redirection-check	监听器资源HTTPS重定向检查	elb	检查HTTP监听器是否配置了向HTTPS监听器的重定向，如果未配置，视为“不合规”
apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	APIG专享版实例未配置访问日志，视为“不合规”
apig-instances-ssl-enabled	APIG专享版实例域名均关联SSL证书	apig	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
as-group-elb-healthcheck-required	弹性伸缩组使用弹性负载均衡健康检查	as	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”
as-group-ipv6-disabled	弹性伸缩组未配置IPv6带宽	as	弹性伸缩组绑定IPv6共享带宽，视为“不合规”
cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未转储到LTS，视为“不合规”
cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建并启用CTS追踪器，视为“不合规”
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	CTS追踪器未打开事件文件校验，视为“不合规”
cts-obs-bucket-track	CTS追踪器追踪指定的OBS桶	cts	账号下的所有CTS追踪器未追踪指定的OBS桶，视为“不合规”
cts-tracker-enabled-security	CTS追踪器符合安全最佳实践	cts	不存在满足安全最佳实践的CTS追踪器，视为“不合规”
kms-rotation-enabled	KMS密钥启用密钥轮换	kms	KMS密钥未启用密钥轮换，视为“不合规”
cloudbuildserver-encryption-parameter-check	CodeArts编译构建下的项目未设置参数加密	codeartsbuild	CodeArts编译构建下的项目，如果设置了未加密参数（除了预定义参数），视为“不合规”
rds-instance-enable-backup	RDS实例开启备份	rds	未开启备份的rds资源，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
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	数据复制服务实时灾备任务使用公网网络，视为“不合规”
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	数据复制服务实时迁移任务使用公网网络，视为“不合规”
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	数据复制服务实时同步任务使用公网网络，视为“不合规”
volumes-encrypted-check-by-default	云硬盘开启加密	evs	云硬盘未进行加密，视为“不合规”
ecs-instance-no-public-ip	ECS资源不能公网访问	ecs	ECS资源具有弹性弹性公网IP，视为“不合规”
ecs-instance-agency-attach-iam-agency	ECS资源附加IAM委托	ecs	ECS实例未附加IAM委托，视为“不合规”
sfsturbo-encrypted-check	高性能弹性文件服务通过KMS进行加密	sfsturbo	高性能弹性文件服务(SFS Turbo)未通过KMS进行加密，视为“不合规”
css-cluster-in-vpc	CSS集群绑定指定VPC资源	css	CSS集群未与指定的vpc资源绑定，视为“不合规”
css-cluster-disk-encryption-check	CSS集群开启磁盘加密	css	CSS集群未开启磁盘加密，视为“不合规”
elb-multiple-az-check	ELB资源使用多AZ部署	elb	检查负载均衡器是否已从多个可用分区注册实例。如果负载均衡器的实例注册在少于2个可用区，视为“不合规”
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS集群未开启kerberos认证，视为“不合规”
mrs-cluster-no-public-ip	MRS集群未绑定弹性公网IP	mrs	MRS集群绑定弹性公网IP，视为“不合规”
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs, evs	已挂载的云硬盘未进行加密，视为“不合规”
iam-customer-policy-blocked-kms-actions	IAM策略中不授权KMS的禁止的action	iam, access-analyzer-verified	IAM策略中授权KMS的任一阻拦action，视为“不合规”
iam-group-has-users-check	IAM用户组添加了IAM用户	iam	IAM用户组未添加任意IAM用户，视为“不合规”
iam-password-policy	IAM用户密码策略符合要求	iam	IAM用户密码强度不满足密码强度要求，视为“不合规”
iam-policy-no-statements-with-admin-access	IAM策略不具备Admin权限	iam	IAM自定义策略具有allow的全部云服务的全部权限(*:*:*或*:*或*)，视为“不合规”
iam-role-has-all-permissions	IAM自定义策略具备所有权限	iam	IAM自定义策略具有allow的任意云服务的全部权限，视为“不合规”
iam-root-access-key-check	根用户存在可使用的访问密钥	iam	根用户存在可使用的访问密钥，视为“不合规”
iam-user-group-membership-check	IAM用户归属指定用户组	iam	IAM用户不属于指定IAM用户组，视为“不合规”
iam-user-mfa-enabled	IAM用户开启MFA	iam	IAM用户未开启MFA认证，视为“不合规”
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	IAM用户在指定时间范围内无登录行为，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
vpc-sg-restricted-ssh	安全组入站流量限制SSH端口	vpc	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放TCP 22端口，视为“不合规”
ecs-instance-in-vpc	ECS资源属于指定虚拟私有云ID	ecs, vpc	指定虚拟私有云ID，不属于此VPC的ECS资源，视为“不合规”
kms-not-scheduled-for-deletion	KMS密钥不处于“计划删除”状态	kms	KMS密钥处于“计划删除“状态，视为“不合规”
function-graph-public-access-prohibited	函数工作流的函数不允许访问公网	fgs	函数工作流的函数允许访问公网，视为“不合规”
function-graph-inside-vpc	函数工作流使用指定VPC	fgs	函数工作流未使用指定VPC，视为“不合规”
mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	通过console密码登录的IAM用户未开启MFA认证，视为“不合规”
css-cluster-https-required	CSS集群启用HTTPS	css	CSS集群未启用https，视为“不合规”
rds-instance-no-public-ip	RDS实例不具有弹性公网IP	rds	RDS资源具有弹性公网IP，视为“不合规”
rds-instance-logging-enabled	RDS实例配备日志	rds	未配备任何日志的rds资源，视为“不合规”
rds-instance-multi-az-support	RDS实例支持多可用区	rds	RDS实例仅支持一个可用区，视为“不合规”
rds-instances-enable-kms	RDS实例开启存储加密	rds	未开启存储加密的rds资源，视为“不合规”
dws-enable-snapshot	DWS集群启用自动快照	dws	DWS集群未启用自动快照，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
gaussdb-instance-enable-backup	GaussDB实例开启自动备份	gaussdb	未开启资源备份的gaussdb资源，视为“不合规”
gaussdb-mysql-instance-enable-backup	TaurusDB实例开启备份	taurusdb	未开启备份的TaurusDB资源，视为“不合规”
gaussdb-nosql-enable-backup	GeminiDB开启备份	gemini db	GeminiDB未开启备份，视为“不合规”
dws-enable-kms	DWS集群启用KMS加密	dws	DWS集群未启用KMS加密，视为“不合规”
gaussdb-nosql-enable-disk-encryption	GeminiDB使用磁盘加密	gemini db	GeminiDB未使用磁盘加密，视为“不合规”
dws-maintain-window-check	DWS集群运维时间窗检查	dws	DWS集群运维时间窗不满足配置，视为“不合规”
dws-clusters-no-public-ip	DWS集群未绑定弹性公网IP	dws	DWS集群绑定弹性公网IP，视为“不合规”
dws-enable-ssl	DWS集群启用SSL加密连接	dws	DWS集群未启用SSL加密连接，视为“不合规”
vpc-sg-restricted-common-ports	安全组入站流量限制指定端口	vpc	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)或所有IPv6地址(::/0)，视为“不合规”
root-account-mfa-enabled	根用户开启MFA认证	iam	根用户未开启MFA认证，视为“不合规”
csms-secrets-rotation-success-check	检查CSMS凭据轮转成功	csms	CSMS凭据轮转失败，视为“不合规”
vpc-default-sg-closed	默认安全组关闭出、入方向流量	vpc	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”

合规规则	规则中文名称	涉及云服务	规则描述
vpc-flow-logs-enabled	VPC启用流日志	vpc	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”
vpc-sg-ports-check	安全组端口检查	vpc	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放了所有的TCP或UDP端口时，视为“不合规”
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”

4.5.41 安全身份和合规性运营最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-48 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
access-keys-rotated	IAM用户的AccessKey在指定时间内轮换	iam	IAM用户的访问密钥未在指定天数内轮转，视为“不合规”
pca-certificate-authority-expiration-check	检查私有CA是否过期	pca	私有CA在指定时间内过期，视为“不合规”
pca-certificate-expiration-check	检查私有证书是否过期	pca	私有证书在指定时间内到期，视为“不合规”
apig-instances-execution-logging-enabled	APIG专享版实例配置访问日志	apig	APIG专享版实例未配置访问日志，视为“不合规”
cts-lts-enable	CTS追踪器启用事件分析	cts	CTS追踪器未转储到LTS，视为“不合规”
cts-tracker-exists	创建并启用CTS追踪器	cts	账号未创建并启用CTS追踪器，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
cts-support-validate-check	CTS追踪器打开事件文件校验	cts	CTS追踪器未打开事件文件校验，视为“不合规”
kms-rotation-enabled	KMS密钥启用密钥轮换	kms	KMS密钥未启用密钥轮换，视为“不合规”
iam-customer-policy-blocked-kms-actions	IAM策略中不授权KMS的禁止的action	iam, access-analyzer-verified	IAM策略中授权KMS的任一阻拦action，视为“不合规”
iam-group-has-users-check	IAM用户组添加了IAM用户	iam	IAM用户组未添加任意IAM用户，视为“不合规”
iam-password-policy	IAM用户密码策略符合要求	iam	IAM用户密码强度不满足密码强度要求，视为“不合规”
iam-policy-no-statements-with-admin-access	IAM策略不具备Admin权限	iam	IAM自定义策略具有allow的全部云服务的全部权限(*:*:*或*:*或*)，视为“不合规”
iam-role-has-all-permissions	IAM自定义策略具备所有权限	iam	IAM自定义策略具有allow的任意云服务的全部权限，视为“不合规”
iam-root-access-key-check	根用户存在可使用的访问密钥	iam	根用户存在可使用的访问密钥，视为“不合规”
iam-user-group-membership-check	IAM用户归属指定用户组	iam	IAM用户不属于指定IAM用户组，视为“不合规”
iam-user-mfa-enabled	IAM用户开启MFA	iam	IAM用户未开启MFA认证，视为“不合规”
iam-user-last-login-check	IAM用户在指定时间内有登录行为	iam	IAM用户在指定时间范围内无登录行为，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
vpc-sg-restricted-ssh	安全组入站流量限制SSH端口	vpc	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放TCP 22端口，视为“不合规”
kms-not-scheduled-for-deletion	KMS密钥不处于“计划删除”状态	kms	KMS密钥处于“计划删除“状态，视为“不合规”
mfa-enabled-for-iam-console-access	Console侧密码登录的IAM用户开启MFA认证	iam	通过console密码登录的IAM用户未开启MFA认证，视为“不合规”
rds-instance-logging-enabled	RDS实例配备日志	rds	未配备任何日志的rds资源，视为“不合规”
vpc-sg-restricted-common-ports	安全组入站流量限制指定端口	vpc	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)或所有IPv6端口(::/0)，视为“不合规”
root-account-mfa-enabled	根用户开启MFA认证	iam	根用户未开启MFA认证，视为“不合规”
vpc-default-sg-closed	默认安全组关闭出、入方向流量	vpc	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”
vpc-sg-ports-check	安全组端口检查	vpc	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放了所有的TCP或UDP端口时，视为“不合规”

4.5.42 华为云安全配置基线指南的标准合规包（level 1）

本文为您介绍华为云安全配置基线指南的标准合规包（level 1）的应用场景以及合规包中的默认规则。

应用场景

华为云安全配置基线指南为您提供重要云服务的基线配置指导，开启云上服务安全建设的第一步，更多信息见**华为云信任中心**。

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**华为云安全配置基线指南**文档的章节编号，供您查阅参考。

表 4-49 华为云安全配置基线指南的标准合规包（level 1）默认规则说明

建议项编号	建议项说明	合规规则	规则中文名称	涉及云服务	规则描述
C.CS.FOUNDATION.G_1.R_1	确保管理员账号禁用 AK/SK	iam-root-access-key-check	根用户存在可使用的访问密钥	iam	根用户存在可使用的访问密钥，视为“不合规”
C.CS.FOUNDATION.G_1.R_2	确保管理员账号已启用 MFA	root-account-mfa-enabled	根用户开启MFA认证	iam	根用户未开启MFA认证，视为“不合规”
C.CS.FOUNDATION.G_1.R_14	确保不创建允许“*:*”管理权限的 IAM 策略	iam-policy-no-statements-with-admin-access	IAM策略不具备Admin权限	iam	IAM自定义策略具有allow的全部云服务的全部权限(*:*:*或*:*或*)，视为“不合规”
C.CS.FOUNDATION.G_2.R_1	启用 CTS	multi-region-cts-tracker-exists	在指定区域创建并启用CTS追踪器	cts	账号未在指定region列表创建并启用CTS追踪器，视为“不合规”
C.CS.FOUNDATION.G_2.R_15	开启日志文件完整性校验	cts-support-validate-check	CTS追踪器打开事件文件校验	cts	CTS追踪器未打开事件文件校验，视为“不合规”
C.CS.FOUNDATION.G_3_3.R_1	禁止使用 CCE 已经 EOS 的 K8S 集群版本	cce-cluster-end-of-maintenance-version	CCE集群版本为处于维护的版本	cce	CCE集群版本为停止维护的版本，视为“不合规”

建议项编号	建议项说明	合规规则	规则中文名称	涉及云服务	规则描述
C.CS.FOUNDATION.G_3_3.R_6	集群节点不要暴露到公网	cce-endpoint-public-access	CCE集群资源不具有弹性公网IP	cce	CCE集群资源具有弹性公网IP，视为“不合规”
C.CS.FOUNDATION.G_4.R_1	确保限制 SSH 的 Internet 公网访问	vpc-sg-restricted-ssh	安全组入站流量限制SSH端口	vpc	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放TCP 22端口，视为“不合规”
C.CS.FOUNDATION.G_4.R_4	确保安全组不允许源地址 0.0.0.0/0 访问远程管理端口及高危端口	vpc-sg-restricted-common-ports	安全组入站流量限制指定端口	vpc	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)或所有IPv6地址(::/0)，视为“不合规”
C.CS.FOUNDATION.G_5_1.R_2	禁用匿名访问	obs-bucket-policy-not-more-permissive	OBS桶策略授权约束	obs	OBS桶策略授权了控制策略以外的访问行为，视为“不合规”
C.CS.FOUNDATION.G_5_1.R_5	使用桶策略限制对 OBS 桶的访问必须使用 HTTPS 协议	obs-bucket-ssl-requests-only	OBS桶策略授权行为使用SSL加密	obs	OBS桶策略授权了无需SSL加密的行为，视为“不合规”
C.CS.FOUNDATION.G_6_1.R_1	开启加密通信	rds-instance-ssl-enable	RDS实例启用SSL加密通讯	rds	RDS实例未启用SSL加密通讯，视为“不合规”
C.CS.FOUNDATION.G_6_1.R_5	避免绑定 EIP 直接通过互联网访问	rds-instance-no-public-ip	RDS实例不具有弹性公网IP	rds	RDS资源具有弹性公网IP，视为“不合规”
C.CS.FOUNDATION.G_6_2.R_1	开启加密通信	dds-instance-enable-ssl	DDS实例开启SSL	dds	DDS实例未开启SSL，视为“不合规”

建议项编号	建议项说明	合规规则	规则中文名称	涉及云服务	规则描述
C.CS.FOUNDATION.G_6_2.R_7	禁止使用默认端口	dds-instance-port-check	DDS实例端口检查	dds	DDS实例的端口包含被禁止的端口，视为“不合规”
C.CS.FOUNDATION.G_6_2.R_8	补丁升级	dds-instance-engine-version-check	DDS实例数据库版本检查	dds	低于指定版本的DDS实例，视为“不合规”
C.CS.FOUNDATION.G_6_3.R_2	开启备份功能设置合理的备份策略	rds-instance-enable-backup	RDS实例开启备份	rds	未开启备份的rds资源，视为“不合规”
C.CS.FOUNDATION.G_6_3.R_4	禁止使用默认端口	rds-instance-port-check	RDS实例默认端口检查	rds	RDS实例的端口包含被禁止的端口，视为“不合规”
C.CS.FOUNDATION.G_6_3.R_8	数据库版本更新到最新版本	rds-instance-engine-version-check	RDS实例数据库引擎版本检查	rds	RDS实例数据库引擎的版本低于指定版本，视为“不合规”
C.CS.FOUNDATION.G_7_2.R_1	开启 Kerberos 认证	mrs-cluster-kerberos-enabled	MRS集群开启kerberos认证	mrs	MRS集群未开启kerberos认证，视为“不合规”
C.CS.FOUNDATION.G_7_2.R_3	集群 EIP 安全组管控	mrs-cluster-no-public-ip	MRS集群未绑定弹性公网IP	mrs	MRS集群绑定弹性公网IP，视为“不合规”
C.CS.FOUNDATION.G_7_2.R_3	集群 EIP 安全组管控	mrs-cluster-in-vpc	MRS集群属于指定VPC	mrs	指定虚拟私有云ID，不属于此VPC的mrs资源，视为“不合规”
C.CS.FOUNDATION.G_7_3.R_6	开启 SSL 加密传输功能	dws-enable-ssl	DWS集群启用SSL加密连接	dws	DWS集群未启用SSL加密连接，视为“不合规”
C.CS.FOUNDATION.G_8.R_1	启用 Web 应用防火墙功能	waf-instance-enable-protect	启用WAF实例域名防护	waf	如果账号未配置并启用WAF防护策略的域名防护，视为“不合规”

建议项编号	建议项说明	合规规则	规则中文名称	涉及云服务	规则描述
C.CS.FOUNDATION.G_8.R_2	配置 WAF 地理位置访问策略	waf-policy-enable-geoip	启用WAF防护策略地理位置访问控制规则	waf	如果账号不存在启用地理位置访问控制规则的waf服务防护策略，视为“不合规”
C.CS.FOUNDATION.G_8.R_5	启用 WAF 对 Web 基础防护的拦截模式	waf-instance-enable-block-policy	启用WAF实例启用拦截模式防护策略	waf	WAF实例未启用拦截模式防护策略，视为“不合规”
C.CS.FOUNDATION.G_8.R_7	启用企业主机安全 HSS（基础版/专业版/企业版/旗舰版）	ecs-attached-hss-agents-check	ECS资源绑定服务主机代理防护	ecs	ECS实例未绑定HSS代理并启用防护，视为“不合规”

4.5.43 华为云安全配置基线指南的标准合规包（level 2）

本文为您介绍华为云安全配置基线指南的标准合规包（level 2）的应用场景以及合规包中的默认规则。

应用场景

华为云安全配置基线指南为您提供重要云服务的基线配置指导，开启云上服务安全建设的第一步，更多信息见**华为云信任中心**。

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**华为云安全配置基线指南**文档的章节编号，供您查阅参考。

表 4-50 华为云安全配置基线指南的标准合规包（level 2）默认规则说明

建议项编号	建议项说明	合规规则	规则中文名称	涉及云服务	规则描述
C.CS.FOUNDATION.G_1.R_3	确保不创建管理员权限的 IAM 用户	iam-user-check-non-admin-group	IAM用户admin权限检查	iam	根用户以外的IAM用户加入admin用户组，视为“不合规”
C.CS.FOUNDATION.G_1.R_9	启用用户登录保护	iam-user-login-protection-enabled	IAM用户开启登录保护	iam	IAM用户未开启登录保护，视为“不合规”
C.CS.FOUNDATION.G_1.R_12	设置初始 IAM 用户时，避免对具有控制台密码的用户设置访问密钥	iam-user-console-and-api-access-at-creation	IAM用户创建时设置AccessKey	iam	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”
C.CS.FOUNDATION.G_1.R_13	确保任何单个 IAM 用户仅有一个可用的活动访问密钥	iam-user-single-access-key	IAM用户单访问密钥	iam	IAM用户拥有多个处于“active”状态的访问密钥，视为“不合规”
C.CS.FOUNDATION.G_2.R_5	启用 VPC 流量日志功能	vpc-flow-logs-enabled	VPC启用流日志	vpc	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”
C.CS.FOUNDATION.G_2.R_11	启用 Function Graph 函数日志功能	function-graph-logging-enabled	函数工作流的函数启用日志配置	fgs	函数工作流的函数未启用日志配置，视为“不合规”
C.CS.FOUNDATION.G_2.R_16	开启日志文件加密存储	cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
C.CS.FOUNDATION.G_3_1.R_1	使用密钥对安全登录 ECS	ecs-instance-key-pair-login	ECS资源配置密钥对	ecs	ECS未配置密钥对，视为“不合规”

建议项编号	建议项说明	合规规则	规则中文名称	涉及云服务	规则描述
C.CS.FOUNDATION.G_3_1.R_4	确保私有镜像开启了加密	ims-images-enable-encryption	私有镜像开启加密	ims	私有镜像未开启加密，视为“不合规”
C.CS.FOUNDATION.G_3_2.R_1	使用密钥对安全登录 BMS	bms-key-pair-security-login	BMS资源使用密钥对登录	bms	裸金属服务器未启用密钥对安全登录，视为“不合规”
C.CS.FOUNDATION.G_5_1.R_4	使用双端固定对 OBS 的资源进行权限控制	obs-bucket-policy-grantee-check	OBS桶策略中授权检查	obs	OBS桶策略授权了不被允许的访问行为，视为“不合规”
C.CS.FOUNDATION.G_5_2.R_1	确保云硬盘是加密的	volumes-encrypted-check	已挂载的云硬盘开启加密	ecs, evs	已挂载的云硬盘未进行加密，视为“不合规”
C.CS.FOUNDATION.G_5_3.R_1	确保SFS Turbo文件系统是加密的	sfsturbo-encrypted-check	高性能弹性文件服务通过KMS进行加密	sfsturbo	高性能弹性文件服务(SFS Turbo)未通过KMS进行加密，视为“不合规”
C.CS.FOUNDATION.G_5_4.R_1	承载备份数据的云硬盘选择加密盘	cbr-backup-encrypted-check	CBR备份被加密	cbr	CBR服务的备份未被加密，视为“不合规”
C.CS.FOUNDATION.G_5_4.R_4	开启强制备份	ecs-protected-by-cbr	ECS资源在备份存储库中	cbr, ecs	ECS资源没有关联备份存储库，视为“不合规”
C.CS.FOUNDATION.G_5_4.R_4	开启强制备份	evs-protected-by-cbr	EVS资源在备份存储库保护中	cbr, evs	EVS磁盘没有关联备份存储库，视为“不合规”
C.CS.FOUNDATION.G_5_4.R_4	开启强制备份	sfsturbo-protected-by-cbr	SFSturbo资源在备份存储库中	cbr, sfsturbo	SFSturbo资源没有关联备份存储库，视为“不合规”

建议项编号	建议项说明	合规规则	规则中文名称	涉及云服务	规则描述
C.CS.FOUNDATION.G_6_1.R_7	开启数据库审计日志	rds-instance-enable-auditLog	RDS实例启用审计日志	rds	未启用审计日志或审计日志保存天数不足的rds资源，视为“不合规”
C.CS.FOUNDATION.G_6_4.R_5	开启数据库审计日志	gaussdb-instance-enable-auditLog	GaussDB实例开启审计日志	gaussdb	未开启审计日志的gaussdb资源，视为“不合规”
C.CS.FOUNDATION.G_6_4.R_5	开启数据库审计日志	gaussdb-mysql-instance-enable-auditlog	TaurusDB实例开启审计日志	taurusdb	未开启审计日志的TaurusDB资源，视为“不合规”
C.CS.FOUNDATION.G_6_4.R_7	开启备份功能设置合理的备份策略	gaussdb-instance-enable-backup	GaussDB实例开启自动备份	gaussdb	未开启资源备份的gaussdb资源，视为“不合规”
C.CS.FOUNDATION.G_7_3.R_1	开启集群数据加密功能	dws-enable-kms	DWS集群启用KMS加密	dws	DWS集群未启用KMS加密，视为“不合规”
C.CS.FOUNDATION.G_7_3.R_4	开启 DWS 数据库审计日志转储	dws-enable-log-dump	DWS集群启用日志转储	dws	DWS集群未启用日志转储，视为“不合规”

4.5.44 静态数据加密最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-51 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
cbr-backup-encrypted-check	CBR备份被加密	cbr	CBR服务的备份未被加密，视为“不合规”
css-cluster-disk-encryption-check	CSS集群开启磁盘加密	css	CSS集群未开启磁盘加密，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
cts-kms-encrypted-check	CTS追踪器通过KMS进行加密	cts	CTS追踪器未通过KMS进行加密，视为“不合规”
dws-enable-kms	DWS集群启用KMS加密	dws	DWS集群未启用KMS加密，视为“不合规”
gaussdb-nosql-enable-disk-encryption	GeminiDB使用磁盘加密	gemini db	GeminiDB未使用磁盘加密，视为“不合规”
ims-images-enable-encryption	私有镜像开启加密	ims	私有镜像未开启加密，视为“不合规”
kms-rotation-enabled	KMS密钥启用密钥轮换	kms	KMS密钥未启用密钥轮换，视为“不合规”
mrs-cluster-encrypt-enable	MRS集群开启kms加密	mrs	MRS集群未开启kms加密，视为“不合规”
rds-instances-enable-kms	RDS实例开启存储加密	rds	未开启存储加密的rds资源，视为“不合规”
sfsturbo-encrypted-check	高性能弹性文件服务通过KMS进行加密	sfsturbo	高性能弹性文件服务(SFS Turbo)未通过KMS进行加密，视为“不合规”
volumes-encrypted-check	已挂载的云硬盘开启加密	ecs, evs	已挂载的云硬盘未进行加密，视为“不合规”

4.5.45 数据传输加密最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-52 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
apig-instances-ssl-enabled	APIG专享版实例域名均关联SSL证书	apig	APIG专享版实例如果有域名未关联SSL证书，则视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
cdn-enable-https-certificate	CDN使用HTTPS证书	cdn	CDN未使用HTTPS，视为“不合规”
cdn-origin-protocol-no-http	CDN回源方式使用HTTPS	cdn	CDN回源方式未使用HTTPS，视为“不合规”
css-cluster-https-required	CSS集群启用HTTPS	css	CSS集群未启用https，视为“不合规”
css-cluster-security-mode-enable	CSS集群支持安全模式	css	CSS集群不支持安全模式，视为“不合规”
dcs-memcached-enable-ssl	DCS Memcached资源支持SSL	dcs	dcs memcached资源可以公网访问，但不支持SSL时，视为“不合规”
dcs-redis-enable-ssl	DCS Redis实例支持SSL	dcs	dcs redis资源可以公网访问，但不支持SSL时，视为“不合规”
dds-instance-enable-ssl	DDS实例开启SSL	dds	DDS实例未开启SSL，视为“不合规”
dms-kafka-not-enable-private-ssl	DMS Kafka队列打开内网SSL加密访问	dms	DMS kafka队列未打开内网SSL加密访问，视为“不合规”
dms-kafka-not-enable-public-ssl	DMS Kafka队列打开公网SSL加密访问	dms	DMS kafka队列未打开公网SSL加密访问，视为“不合规”
dms-rabbitmq-not-enable-ssl	DMS RabbitMq队列打开SSL加密访问	dms	DMS rabbitmqs队列未打开SSL加密访问，视为“不合规”
dms-rocketmq-not-enable-ssl	DMS RocketMQ打开SSL加密访问	dms	DMS RockctMQ未打开SSL加密访问，视为“不合规”
dws-enable-ssl	DWS集群启用SSL加密连接	dws	DWS集群未启用SSL加密连接，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
elb-http-to-https-redirection-check	监听器资源HTTPS重定向检查	elb	检查HTTP监听器是否配置了向HTTPS监听器的重定向，如果未配置，视为“不合规”
elb-tls-https-listeners-only	ELB监听器配置HTTPS监听协议	elb	负载均衡器的任一监听器未配置HTTPS监听协议，视为“不合规”
gaussdb-instance-ssl-enable	GaussDB实例开启传输数据加密	gaussdb	gaussdb实例未启用SSL数据传输加密，视为“不合规”
gaussdb-mysql-instance-ssl-enable	TaurusDB实例开启传输数据加密	taurusdb	TaurusDB实例未启用SSL数据传输加密，视为“不合规”
obs-bucket-ssl-requests-only	OBS桶策略授权行为使用SSL加密	obs	OBS桶策略授权了无需SSL加密的行为，视为“不合规”
rds-instance-ssl-enable	RDS实例启用SSL加密通讯	rds	RDS实例未启用SSL加密通讯，视为“不合规”

4.5.46 适用于云备份（CBR）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-53 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
cbr-backup-encrypted-check	CBR备份被加密	cbr	CBR服务的备份未被加密，视为“不合规”
cbr-policy-minimum-frequency-check	CBR备份策略执行频率检查	cbr	CBR备份策略执行频率低于设定值，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
cbr-vault-minimum-retention-check	CBR存储库最低保留天数	cbr	存储库未绑定策略或绑定的策略按天数保留且保留天数低于设定值，视为“不合规”
ecs-protected-by-cbr	ECS资源在备份存储库中	cbr, ecs	ECS资源没有关联备份存储库，视为“不合规”
evs-protected-by-cbr	EVS资源在备份存储库保护中	cbr, evs	EVS磁盘没有关联备份存储库，视为“不合规”
sfsturbo-protected-by-cbr	SFSturbo资源在备份存储库中	cbr, sfsturbo	SFSturbo资源没有关联备份存储库，视为“不合规”
ecs-last-backup-created	ECS云服务器的备份时间检查	cbr, ecs	ECS云服务器最近一次备份创建时间超过参数要求，视为“不合规”
evs-last-backup-created	EVS资源的备份时间检查	cbr, evs	EVS磁盘最近一次备份创建时间超过参数要求，视为“不合规”
sfsturbo-last-backup-created	SFSturbo资源的备份时间检查	cbr, sfsturbo	SFS turbo资源最近一次备份创建时间超过参数要求，视为“不合规”

4.5.47 适用于云搜索服务（CSS）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-54 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
css-cluster-backup-available	CSS集群启用快照	css	CSS集群未启用快照，视为“不合规”
css-cluster-disk-encryption-check	CSS集群开启磁盘加密	css	CSS集群未开启磁盘加密，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
css-cluster-https-required	CSS集群启用HTTPS	css	CSS集群未启用https，视为“不合规”
css-cluster-not-enable-white-list	CSS集群未开启访问控制开关	css	CSS集群未开启访问控制开关，视为“不合规”
css-cluster-kibana-not-enable-white-list	CSS集群Kibana未开启访问控制开关	css	CSS集群Kibana未开启访问控制开关，视为“不合规”
css-cluster-multiple-az-check	CSS集群具备多AZ容灾	css	CSS集群没有多az容灾，视为“不合规”
css-cluster-no-public-zone	CSS集群不能公网访问	css	CSS集群开启公网访问，视为“不合规”
css-cluster-security-mode-enable	CSS集群支持安全模式	css	CSS集群不支持安全模式，视为“不合规”
css-cluster-slowLog-enable	CSS集群开启慢日志	css	CSS集群未开启慢日志，视为“不合规”

4.5.48 适用于分布式缓存服务（DCS）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-55 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
dcs-redis-enable-ssl	DCS Redis实例支持SSL	dcs	dcs redis资源可以公网访问，但不支持SSL时，视为“不合规”
dcs-redis-high-tolerance	DCS Redis实例高可用	dcs	dcs redis资源不是高可用时，视为“不合规”
dcs-redis-no-public-ip	DCS Redis实例不存在弹性公网IP	dcs	dcs redis资源存在弹性公网IP，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
dcs-redis-password-access	DCS Redis实例需要密码访问	dcs	dcs redis资源不需要密码访问，视为“不合规”

4.5.49 适用于分布式消息服务（DMS）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-56 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
dms-kafka-not-enable-private-ssl	DMS Kafka队列打开内网SSL加密访问	dms	DMS kafka队列未打开内网SSL加密访问，视为“不合规”
dms-kafka-not-enable-public-ssl	DMS Kafka队列打开公网SSL加密访问	dms	DMS kafka队列未打开公网SSL加密访问，视为“不合规”
dms-kafka-public-access-enabled-check	DMS Kafka队列开启公网访问	dms	DMS kafka队列开启公网访问，视为“不合规”
dms-rabbitmq-not-enable-ssl	DMS RabbitMq队列打开SSL加密访问	dms	DMS rabbitmqs队列未打开SSL加密访问，视为“不合规”
dms-rocketmq-not-enable-ssl	DMS RockctMQ打开SSL加密访问	dms	DMS RockctMQ未打开SSL加密访问，视为“不合规”
dms-rabbitmq-public-access-enabled-check	DMS RabbitMQ实例开启公网访问	dms	DMS RabbitMQ实例开启公网访问，视为“不合规”
dms-reliability-public-access-enabled-check	DMS RocketMQ实例开启公网访问	dms	DMS RocketMQ实例开启公网访问，视为“不合规”

4.5.50 适用于数据仓库服务（DWS）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-57 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
dws-clusters-no-public-ip	DWS集群未绑定弹性公网IP	dws	DWS集群绑定弹性公网IP，视为“不合规”
dws-enable-kms	DWS集群启用KMS加密	dws	DWS集群未启用KMS加密，视为“不合规”
dws-enable-ssl	DWS集群启用SSL加密连接	dws	DWS集群未启用SSL加密连接，视为“不合规”
dws-enable-log-dump	DWS集群启用日志转储	dws	DWS集群未启用日志转储，视为“不合规”
dws-enable-snapshot	DWS集群启用自动快照	dws	DWS集群未启用自动快照，视为“不合规”
dws-maintain-window-check	DWS集群运维时间窗检查	dws	DWS集群运维时间窗不满足配置，视为“不合规”

4.5.51 适用于云数据库（TaurusDB）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-58 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
gaussdb-mysql-instance-enable-auditlog	TaurusDB实例开启审计日志	taurusdb	未开启审计日志的TaurusDB资源，视为“不合规”
gaussdb-mysql-instance-enable-backup	TaurusDB实例开启备份	taurusdb	未开启备份的TaurusDB资源，视为“不合规”
gaussdb-mysql-instance-enable-errorlog	TaurusDB实例开启错误日志	taurusdb	未开启错误日志的TaurusDB资源，视为“不合规”
gaussdb-mysql-instance-enable-slowlog	TaurusDB实例开启慢日志	taurusdb	未开启慢日志的TaurusDB资源，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
gaussdb-mysql-instance-multiple-az-check	TaurusDB实例跨AZ部署检查	taurusdb	TaurusDB实例未跨AZ部署，视为“不合规”
gaussdb-mysql-instance-no-public-ip-check	TaurusDB实例弹性公网IP检查	taurusdb	TaurusDB实例如绑定弹性公网IP，视为“不合规”
gaussdb-mysql-instance-ssl-enable	TaurusDB实例开启传输数据加密	taurusdb	TaurusDB实例未启用SSL数据传输加密，视为“不合规”

4.5.52 适用于对象存储服务（OBS）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-59 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
obs-bucket-public-read-policy-check	OBS桶禁止公开读	obs	桶可以被公开读，视为“不合规”
obs-bucket-public-write-policy-check	OBS桶禁止公开写	obs	桶可以被公开写，视为“不合规”
obs-bucket-ssl-requests-only	OBS桶策略授权行为使用SSL加密	obs	OBS桶策略授权了无需SSL加密的行为，视为“不合规”

4.5.53 适用于 VPC 安全组的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-60 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
vpc-default-sg-closed	默认安全组关闭出、入方向流量	vpc	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”

合规规则	规则中文名称	涉及云服务	规则描述
vpc-sg-attached-ports	安全组连接到弹性网络接口	vpc	检查非默认安全组是否连接到弹性网络接口(ports)。如果安全组未关联弹性网络接口（ports），视为“不合规”
vpc-sg-ports-check	安全组端口检查	vpc	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放了所有的TCP或UDP端口时，视为“不合规”
vpc-sg-restricted-ssh	安全组入站流量限制SSH端口	vpc	当安全组入方向源地址设置为0.0.0.0/0或::/0，且开放TCP 22端口，视为“不合规”
vpc-sg-by-white-list-ports-check	安全组非白名单端口检查	vpc	除指定的白名单端口外，其余端口的安全组策略为允许，视为“不合规”

4.5.54 适用于 Web 应用防火墙（WAF）的最佳实践

该示例模板中对应的合规规则的说明如下表所示：

表 4-61 合规包示例模板说明

合规规则	规则中文名称	涉及云服务	规则描述
waf-instance-enable-block-policy	启用WAF实例启用拦截模式防护策略	waf	WAF实例未启用拦截模式防护策略，视为“不合规”
waf-instance-enable-protect	启用WAF实例域名防护	waf	如果账号未配置并启用WAF防护策略的域名防护，视为“不合规”
waf-instance-policy-not-empty	WAF防护域名配置防护策略	waf	WAF防护域名未配置防护策略，视为“不合规”

合规规则	规则中文名称	涉及云服务	规则描述
waf-policy-enable-geoip	启用WAF防护策略地理位置访问控制规则	waf	如果账号不存在启用地理位置访问控制规则的waf服务防护策略，视为“不合规”
waf-policy-not-empty	WAF防护策略配置防护规则	waf	WAF防护策略未配置防护规则，视为“不合规”

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 新建自定义查询

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：

- **新建自定义查询**
- **基于预设查询创建自定义查询**
- **高级查询配置样例**

新建自定义查询

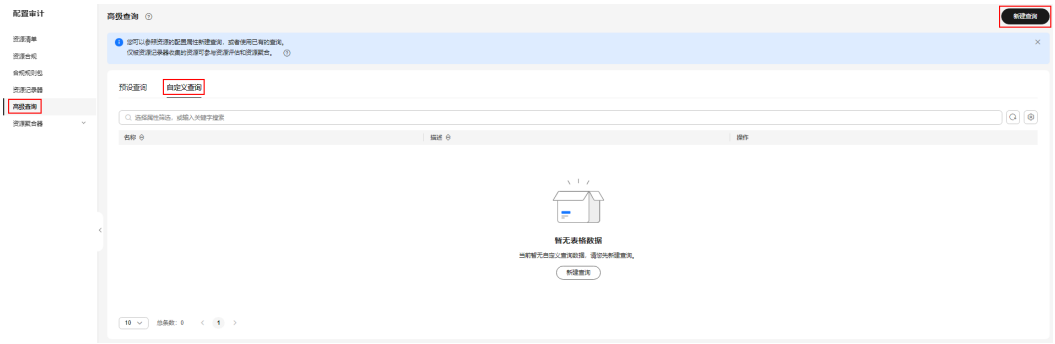
步骤1 登录管理控制台。

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”。

图 5-1 新建查询



步骤5 在“查询编辑器”的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，最大长度64个字符。

步骤7 单击“确定”，保存成功。

图 5-2 保存查询

说明

如果自定义查询达到限额时，您将无法单击“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”。但此时您依然可以单击“运行”，直接运行查询并查看和导出查询结果。

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 单击查询结果列表上方的“导出”，选择要导出的文件格式（CSV格式或JSON格式），可导出查询结果。

步骤10 单击“历史执行记录”，可查看该查询历史执行的时间和查询语句等信息。

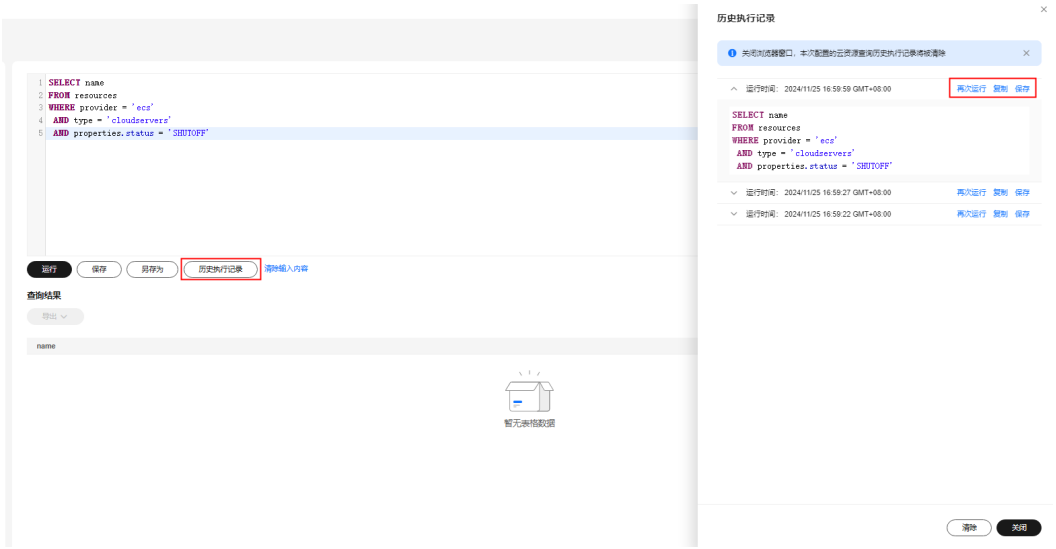
您可以基于历史执行记录进行如下操作：

- 再次运行：直接基于历史查询语句再次运行查询。
- 复制：复制历史查询语句。
- 保存：直接将历史查询语句保存为新的自定义查询。

说明

当您关闭浏览器窗口或登出账号后，高级查询的历史执行记录将被清除。

图 5-3 历史执行记录



----结束

基于预设查询创建自定义查询

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，此处以另存预设查询为例进行说明。

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 5-4 使用预设查询

步骤3 在“查询编辑器”的输入框中修改查询语句。

详细请参见**高级查询配置样例**。

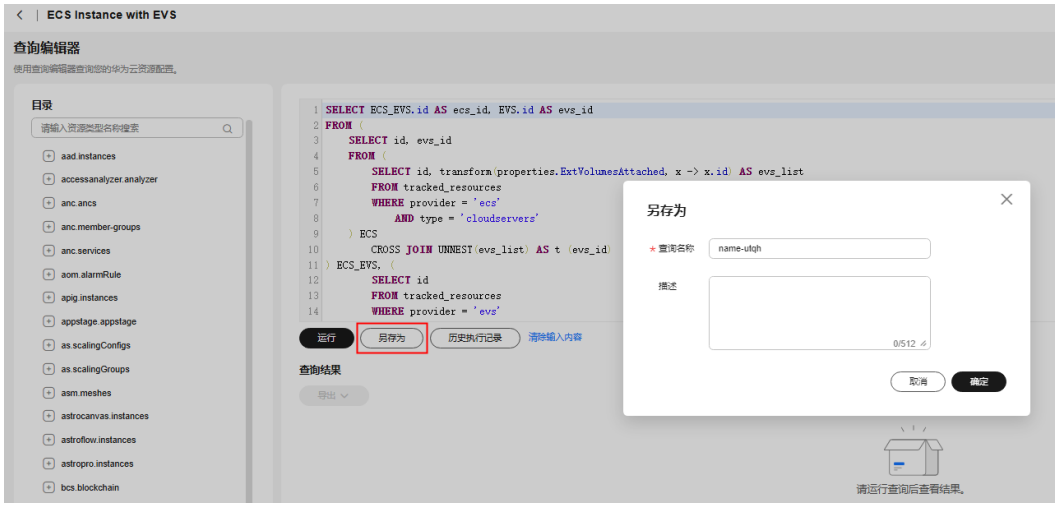
步骤4 单击“另存为”，配置查询名称和描述。

步骤5 在弹框中，单击“确定”。

通过另存预设查询操作产生的新查询，将更新在自定义查询列表中。

您也可以基于该查询的历史执行记录将其保存为新的自定义查询，具体请参见**历史执行记录**。

图 5-5 另存预设查询



----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
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

资源参数	参数类型	含义
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。

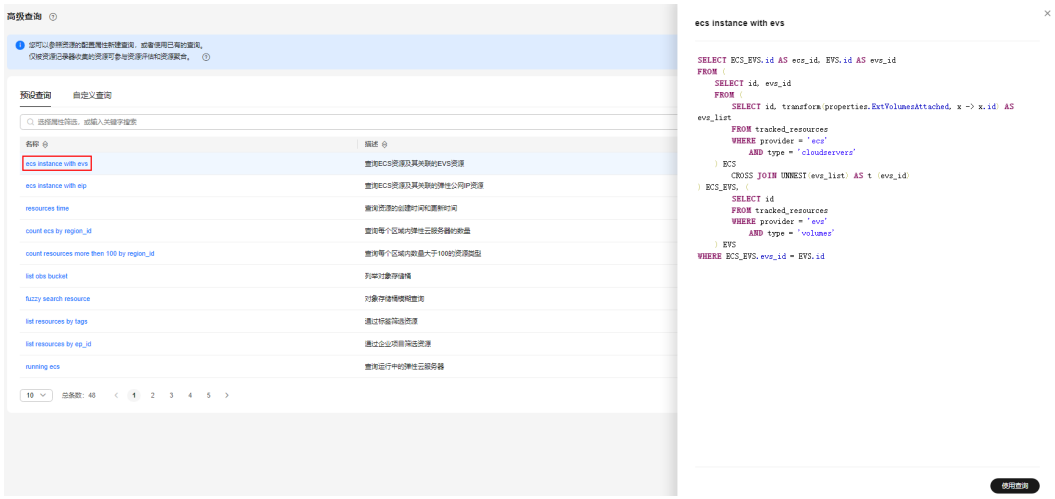
“高级查询”页面默认展示预设查询列表，您可以选择“自定义查询”页签，查看自定义查询列表。

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 5-6 查看查询详情



----结束

5.5 修改自定义查询

操作场景

如果您需要修改某个自定义查询的查询语句、名称和描述，可按如下操作修改查询。

说明

预设查询支持修改查询语句、名称和描述后另存为新的自定义查询，具体请参见**基于预设查询创建自定义查询**。

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。

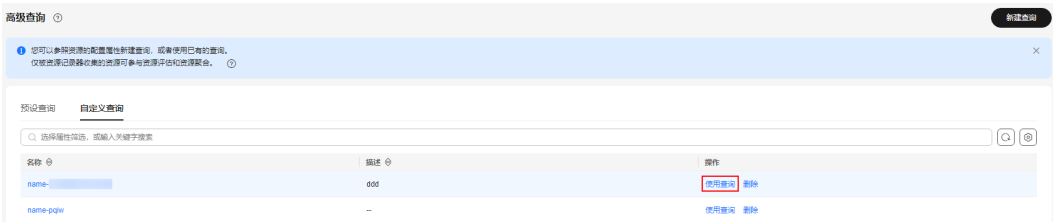
步骤3 单击页面左侧的“高级查询”，进入“高级查询”页面。

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 5-7 修改自定义查询



步骤6 在“查询编辑器”的输入框中修改查询语句。

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，最大长度64个字符。

----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。

说明

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 5-8 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24小时内最多只能创建1次组织类型资源聚合器，创建的组织类型资源聚合器被删除后在24小时内无法再次创建。
- 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。
- 组织类型的资源聚合器仅会聚合组织下账号状态为“正常”的成员账号的数据。

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。

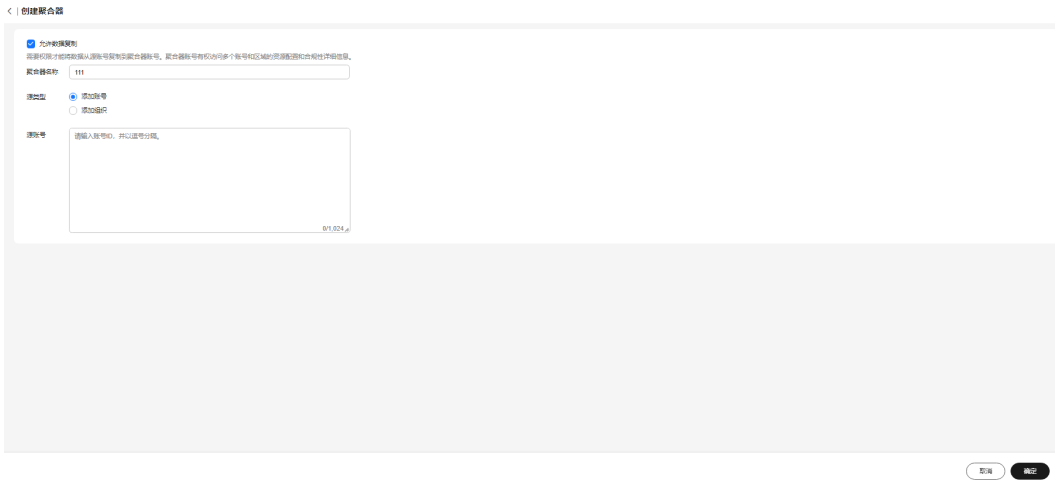
步骤3 单击页面左侧的“资源聚合器”，在下拉列表中选择“聚合器”，进入“聚合器”页面。

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账号状态为“正常”的成员账号的数据，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。

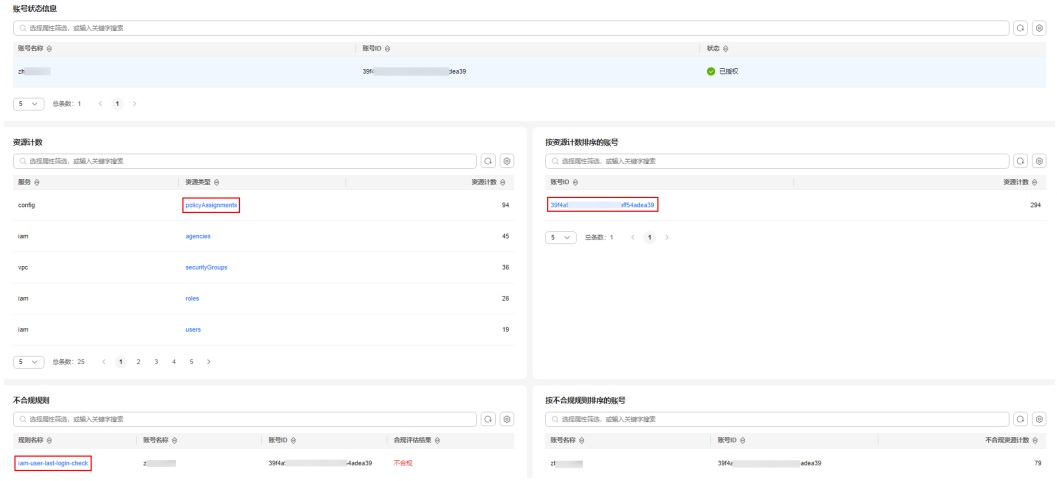
步骤5 在列表中单击需要查看的聚合器名称，进入资源聚合器详情页，查看该资源聚合器的详细信息。

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。

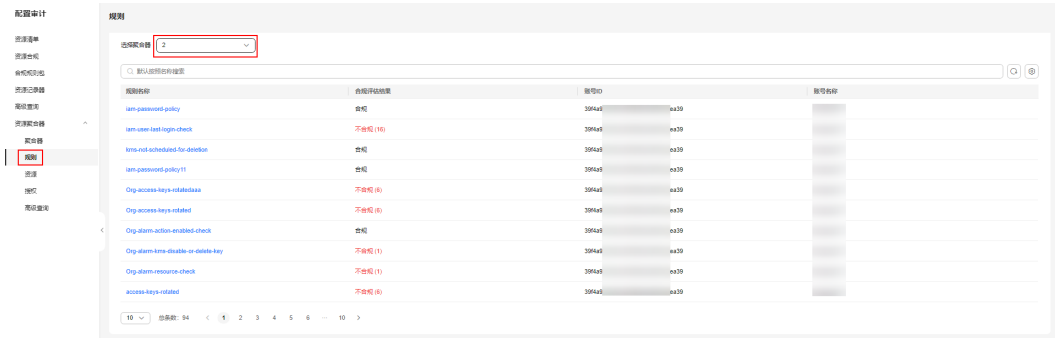
步骤3 单击页面左侧的“资源聚合器”，在下拉列表中选择“规则”，进入“规则”页面。

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。

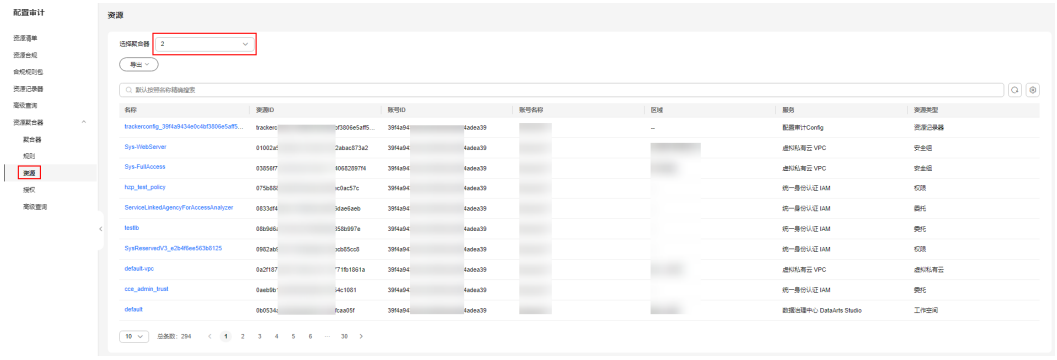
步骤3 单击页面左侧的“资源聚合器”，在下拉列表中选择“资源”，进入“资源”页面。

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及其相关信息，并支持导出全部资源数据。

在页面上方的搜索框中可使用资源名称、资源ID、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。
- 资源聚合器的高级查询能力暂时不支持 checksum 和 provisioning_state 两个属性。

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”处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，最大长度64个字符。

步骤7 单击“确定”，保存成功。

图 6-10 保存查询

说明

如果自定义查询达到限额时，您将无法单击“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”。但此时您依然可以单击“运行”，直接运行查询并查看和导出查询结果。

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 单击查询结果列表上方的“导出”，选择要导出的文件格式（CSV格式或JSON格式），可导出查询结果。

步骤10 单击“历史执行记录”，可查看该查询历史执行的时间和查询语句等信息。

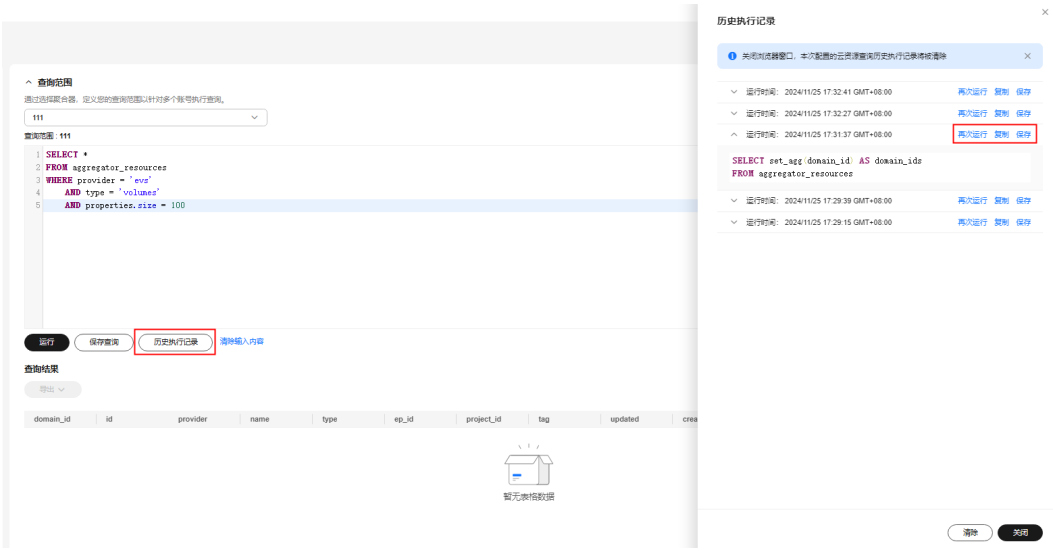
您可以基于历史执行记录进行如下操作：

- 再次运行：直接基于历史查询语句再次运行查询。
- 复制：复制历史查询语句。
- 保存：直接将历史查询语句保存为新的自定义查询。

说明

当您关闭浏览器窗口或登出账号后，高级查询的历史执行记录将被清除。

图 6-11 历史执行记录



----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**基于预设查询创建自定义查询**。
- 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
创建合规规则	policy	createPolicyAssignments
删除合规规则	policy	deletePolicyAssignment
更新合规规则	policy	updatePolicyAssignment
触发规则评估	policy	runEvaluation
停用合规规则	policy	disablePolicyAssignment
启用合规规则	policy	enablePolicyAssignment
创建或更新合规规则修正配置	policy	createOrUpdateRemediationConfiguration
删除合规规则修正配置	policy	deleteRemediationConfiguration
手动运行合规规则修正执行	policy	runRemediationExecution

操作名称	资源类型	事件名称
批量创建合规规则修正例外	policy	batchCreateRemediationExceptions
批量删除合规规则修正例外	policy	batchDeleteRemediationExceptions
更新合规评估结果	policyState	updatePolicyState
配置或修改资源记录器	trackerConfig	createOrUpdateTrackerConfig
关闭资源记录器	trackerConfig	deleteTrackerConfig
创建高级查询	storedQuery	createStoredQuery
更新高级查询	storedQuery	updateStoredQuery
删除高级查询	storedQuery	deleteStoredQuery
创建组织合规规则	organizationPolicyAssignments	createOrganizationPolicyAssignment
更新组织合规规则	organizationPolicyAssignments	updateOrganizationPolicyAssignment
删除组织合规规则	organizationPolicyAssignments	deleteOrganizationPolicyAssignment
创建资源聚合器授权	authorization	createAggregationAuthorization
删除资源聚合器授权	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
删除聚合器账号中挂起的授权请求	aggregationRequests	deletePendingAggregationRequest
创建合规规则包	conformancePacks	createConformancePack
删除合规规则包	conformancePacks	deleteConformancePack
更新合规规则包	conformancePacks	updateConformancePack
创建组织合规规则包	organizationConformancePacks	createOrganizationConformancePack
删除组织合规规则包	organizationConformancePacks	deleteOrganizationConformancePack

操作名称	资源类型	事件名称
更新组织合规规则包	organizationConformancePacks	updateOrganizationConformancePack
批量添加资源标签	policy	tagResource
批量删除资源标签	policy	unTagResource

7.2 在 CTS 事件列表查看云审计事件

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)或云日志服务(LTS)，才可在OBS桶或LTS日志组里面查看历史事件信息。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。
- 云审计控制台对用户的操作事件日志保留7天，过期自动删除，不支持人工删除。

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。
- 企业项目ID：输入企业项目ID。
- 访问密钥ID：输入访问密钥ID（包含临时访问凭证和永久访问密钥）。
- 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7天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

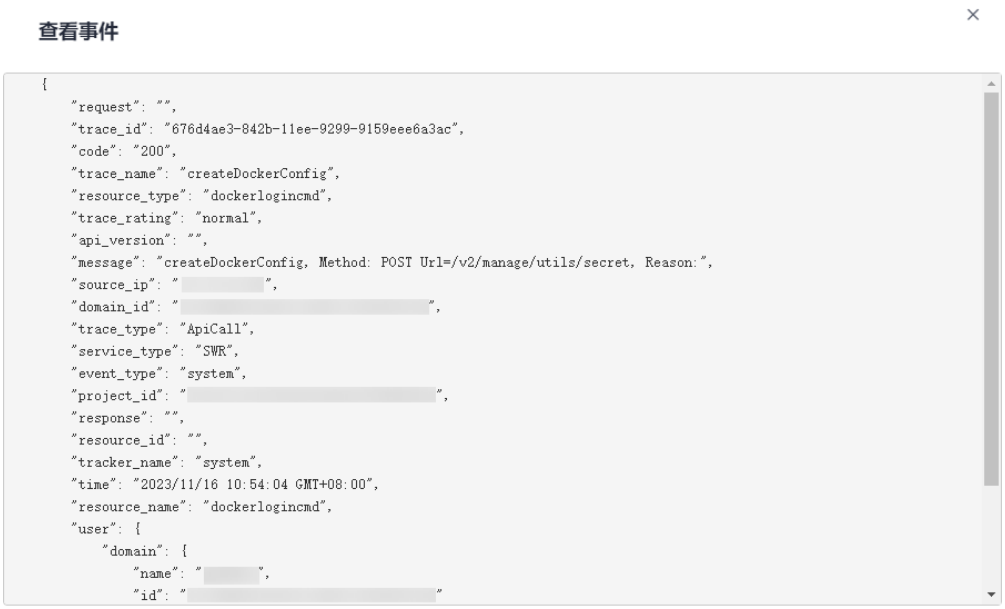
1. 登录管理控制台。
2. 单击左上角，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
   - 事件类型、云服务、资源类型和筛选类型，在下拉框中选择查询条件。
     - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。

- 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1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。

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支持的服务和区域请以控制台界面显示为准，具体如下：

步骤1 登录管理控制台，进入“配置审计 Config”服务。

步骤2 在“资源清单”页面单击“已支持的服务和区域”。

图 8-1 查看 Config 支持的服务和区域

步骤3 进入“已支持的服务和区域”页面，列表中显示当前Config已支持的服务、资源类型和区域等信息。

步骤4 在列表上方的搜索框中可输入服务或资源类型名称进行搜索，还支持基于资源所在区域进行筛选。

----结束

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
			企业主机安全 HSS	主机代理
			MapReduce服务 MRS	弹性大数据服务
		包含（contains）	云备份	存储库
		绑定（isAttachedTo）	虚拟私有云 VPC	弹性公网IP
			云备份 CBR	备份
			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
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

服务	资源类型	关系类型	相关云服务	相关资源类型
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
		包含（contains）	弹性负载均衡 ELB	转发策略
		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

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	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
	转发策略	被包含（isContainedIn）	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
			虚拟私有云 VPC	VPC流日志
			虚拟私有云 VPC	弹性公网IP
	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
		被包含（isContainedIn）	虚拟私有云 VPC	弹性网卡
	VPC流日志	被包含（isContainedIn）	虚拟私有云 VPC	子网
			虚拟私有云 VPC	弹性网卡
			虚拟私有云 VPC	虚拟私有云
	弹性网卡	包含（contains）	虚拟私有云 VPC	VPC流日志
			虚拟私有云 VPC	安全组
	子网	包含（contains）	虚拟私有云 VPC	VPC流日志
	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
			虚拟私有云 VPC	虚拟私有云
		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

服务	资源类型	关系类型	相关云服务	相关资源类型
云硬盘 EVS	磁盘	包含（contains）	云备份 CBR	存储库
		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
			云备份 CBR	备份
			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
云数据库 GeminiDB	实例	包含（contains）	云数据库 GeminiDB	节点
	节点	被包含（isContainedIn）	云数据库 GeminiDB	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

服务	资源类型	关系类型	相关云服务	相关资源类型
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
统一身份认证服务 IAM	委托	关联（isAssociatedWith）	统一身份认证服务 IAM	策略
			统一身份认证服务 IAM	权限
	用户组	包含（contains）	统一身份认证服务 IAM	用户
		关联（isAssociatedWith）	统一身份认证服务 IAM	策略
			统一身份认证服务 IAM	权限
	策略	关联（isAssociatedWith）	统一身份认证服务 IAM	委托
			统一身份认证服务 IAM	用户组
			统一身份认证服务 IAM	用户
	权限	关联（isAssociatedWith）	统一身份认证服务 IAM	委托
			统一身份认证服务 IAM	用户组
			统一身份认证服务 IAM	用户
	用户	关联（isAssociatedWith）	统一身份认证服务 IAM	策略
			统一身份认证服务 IAM	权限
		被包含（isContainedIn）	统一身份认证服务 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

服务	资源类型	关系类型	相关云服务	相关资源类型
	合规规则	被包含（isContainedIn）	配置审计 Config	合规规则包
云备份 CBR	备份	绑定（isAttachedTo）	弹性云服务器 ECS	云服务器
			云硬盘 EVS	磁盘
			高性能弹性文件服务 SFS Turbo	SFS Turbo
	策略	绑定（isAttachedTo）	云备份 CBR	存储库
	存储库	绑定（isAttachedTo）	云备份 CBR	策略
		被包含（isContainedIn）	弹性云服务器 ECS	云服务器
			云硬盘 EVS	磁盘
			高性能弹性文件服务 SFS Turbo	SFS Turbo
文档数据库服务 DDS	实例	包含（contains）	文档数据库服务 DDS	节点
	节点	被包含（isContainedIn）	文档数据库服务 DDS	实例
企业主机安全 HSS	主机代理	包含（contains）	弹性云服务器 ECS	云服务器
Web应用防火墙 WAF	网站	被包含（isContainedIn）	Web应用防火墙 WAF	防护策略
	防护策略	包含（contains）	Web应用防火墙 WAF	网站
高性能弹性文件服务 SFS Turbo	SFS Turbo	包含（contains）	云备份	存储库
	SFS Turbo	绑定（isAttachedTo）	云备份	备份

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）
高性能弹性文件服务 SFS Turbo	SFS Turbo（sfsturbo.shares）
弹性负载均衡 ELB	• 负载均衡器（elb.loadbalancers） • 监听器（elb.listeners）
消息通知服务 SMN	主题（smn.topic）

服务	资源类型
分布式消息服务 DMS	• Kafka实例（dms.kafka） • 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）
硬件开发工具链平台云服务 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

8.4.1 资源变更的消息通知模型

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。此处的消息通知类型为“ResourceChanged”。
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。

参数	参数类型	描述
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.regionid1a.xxxxxx.com/v2/059b5e0a2500d5552fa1c00adada8c06/os-vendor-
volumes/3e62c0e6-e779-469e-b0f2-35743f6229d1"
        },
        {
         "rel": "bookmark",
         "href": "https://evs.regionid1a.xxxxxx.com/059b5e0a2500d5552fa1c00adada8c06/os-vendor-
volumes/3e62c0e6-e779-469e-b0f2-35743f6229d1"
        }
       ],
       "volHostAttrHost": "regionid1a-pod01.regionid1a#0",
       "multiattach": false,
       "status": "available"
      },
      "region_id": "regionid1a",
      "project_id": "059b5e0a2500d5552fa1c00adada8c06",
      "project_name": "regionid1a",
      "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"
}
```


8.4.2 资源关系变更的消息通知模型

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。此处的消息通知类型为“ResourceRelationChanged”。

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）。
from_resource_id	String	起始资源ID（仅当起始资源存在时展示）。
from_resource_type	String	起始资源类型（仅当起始资源存在时展示）。
relation_type	String	资源关系（仅当起始资源存在时展示）。

资源关系变更消息通知示例

```
{
  "detail" : {
    "resource_id" : "675d78fd****377b067be0531",
    "resource_type" : "config.policyAssignments",
    "event_type" : "CHANGE",
    "capture_time" : "2024-12-14T12:31:59.201Z",
    "from_resource_id" : "e336ffcfc2ab****4bf892423739c7125",
    "from_resource_type" : "config.conformancePacks",
    "relation_type" : "isContainedIn"
  },
  "notification_type" : "ResourceRelationChanged",
  "notification_creation_time" : "2024-12-14T12:31:59.404Z",
  "domain_id" : "017f09bdc0194******80082147f41a8"
}
```

8.4.3 资源快照存储完成的消息通知模型

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。此处的消息通知类型为“SnapshotArchiveCompleted”。
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 8-9 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	资源快照存储的OBS桶内对象的路径。

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": "regionid1a",
    "bucket_name": "test",
    "object_keys": [
      "RMSLogs/059b5c937100d3e40ff0c00a7675a0a0/Snapshot/
2020/8/11/059b5c937100d3e40ff0c00a7675a0a0_Snapshot_regionid1a_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"
}
```

8.4.4 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。此处的消息通知类型为“NotificationArchiveCompleted”。
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	资源变更消息所在区域ID。
bucket_name	String	资源变更消息所在OBS桶名。
object_key	String	资源变更消息存储的OBS桶内对象的路径。

资源变更消息存储完成的消息通知示例

```
{
    "detail": {
        "region_id": "regionid1a",
        "bucket_name": "test",
        "object_key": "RMSLogs/059b5c937100d3e40ff0c00a7675a0a0/Notification/2020/12/10/
NotificationChunk/
059b5c937100d3e40ff0c00a7675a0a0_Notification_regionid1a_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 存储模型

8.5.1 资源快照存储模型

资源快照存储模型

表 8-12 资源快照存储模型

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。

参数	参数类型	描述
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。
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。

资源快照存储示例

```
{
  "items": [
    {
      "resource": {
        "id": "c25ee8b3-c907-4cd4-9869-6c4b07c61a0b",
        "name": "rse-cdk-07-cdk-3sbz",
        "provider": "vpc",
        "type": "securityGroups",
        "region_id": "regionid1a",
        "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"
}
```


8.5.2 资源变更消息存储模型

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。

表 8-17 notification_items 参数

参数	参数类型	描述
notification_type	String	消息通知类型。此处的消息通知类型为“ResourceChanged”。
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。

参数	参数类型	描述
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。
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": "regionid1a",
               "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"
      }
   ]
}
```

8.6 ResourceQL 语法

8.6.1 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 8-20 支持的数据类型

类型名	类型英文
整型	int/integer
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 8-21 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cloudservcer包含字段flavor，而vpc的publicips包含字段bandwidth。

各个资源类型properties内支持的字段以及类型可以通过配置审计控制台和API接口两种方式查看，具体请参见**如何获取各对接云服务上报Config的资源属性?** 。

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'
```


8.6.2 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
```

8.6.3 函数列表

ResourceQL支持以下函数：

表 8-22 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。
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 8-23 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 8-24 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	返回数组a的平均值。
array_distinct(a) → array	返回数组a去重后的新数组。

函数	功能描述
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_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。
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。

函数	功能描述
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 8-25 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。
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 8-26 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。