#### 资源治理服务

最佳实践

文档版本01发布日期2025-01-22





#### 版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可,任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部,并不得以任何形式传播。

#### 商标声明

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

#### 注意

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

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

#### 华为云计算技术有限公司

地址: 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编: 550029

网址: <u>https://www.huaweicloud.com/</u>



目录

1 使用 Config 创建合规规则	1
2 使用 Config 查询资源详情、资源关系和资源历	远4
3 通过 CES 实现不合规资源的告警通知	7
4 通过高级查询自定义查询资源并下载	
5 使用 Config 查找未绑定指定标签的资源	12
6 通过 Config 实现资源的多维度合规审计	14
7 通过 Config 实现资源自动化管理	

### 】 使用 Config 创建合规规则

#### 示例简介

该示例展示了如何通过Java版本SDK为Config服务创建合规规则和查询合规规则。

**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。

#### 开发前准备

- 1. 获取华为云开发工具包(SDK),您也可以查看安装JAVA SDK。
- 您需要拥有华为云账号以及该账号对应的 Access Key(AK)和 Secret Access Key (SK),请在华为云控制台"我的凭证 > 访问密钥"页面上创建和查看您的 AK/SK。具体请参见访问密钥。
- 3. 配置审计 Config SDK, 支持 Java JDK 1.8 及其以上版本。

#### 安装 SDK

您可以通过Maven方式获取和安装SDK,您只需要在Java项目的pom.xml文件中加入 相应的依赖项即可 。 具体的SDK版本号请参见<mark>SDK开发中心</mark> 。

#### <dependency>

- <groupId>com.huaweicloud.sdk</groupId>
- <artifactId>huaweicloud-sdk-config</artifactId>
- <version>{sdk-version}</version> </dependency>

#### 代码示例

public class CreatePolicyAssignmentDemo {
 public static void main(String[] args) {
 // 认证用的ak和sk直接写到代码中有很大的安全风险,建议在配置文件或者环境变量中密文存放,使用时
解密,确保安全;
 // 本示例以ak和sk保存在环境变量中来实现身份验证为例,运行本示例前请先在本地环境中设置环境变量
HUAWEICLOUD\_SDK\_AK和HUAWEICLOUD\_SDK\_SK。
 String ak = System.getenv("HUAWEICLOUD\_SDK\_AK");
 String sk = System.getenv("HUAWEICLOUD\_SDK\_SK");
 String regionId = "<region id>";
 HttpConfig config = HttpConfig.getDefaultHttpConfig();
 config.withIgnoreSSLVerification(true);
 ICredential auth = new GlobalCredentials().withAk(ak).withSk(sk);
 ConfigClient client = ConfigClient.newBuilder().withHttpConfig(config).withCredential(auth)
 .withRegion(ConfigRegion.valueOf(regionId)).build();
 }
}

```
CreatePolicyAssignmentsRequest createRequest = new CreatePolicyAssignmentsRequest()
        .withBody(new
PolicyAssignmentRequestBody().withPolicyAssignmentType(PolicyAssignmentRequestBody.PolicyAssignment
TypeEnum.BUILTIN)
          .withName("<Your policy_assignment_name>").withDescription("<Your
policy_assignment_description>")
          .withPolicyFilter(new PolicyFilterDefinition()).withPolicyDefinitionId("<Your
policy_definition_id>"));
     try {
       CreatePolicyAssignmentsResponse createResponse = client.createPolicyAssignments(createRequest);
       System.out.println(createResponse.toString());
       ShowPolicyAssignmentRequest showPolicyAssignmentRequest = new
ShowPolicyAssignmentRequest()
          .withPolicyAssignmentId(createResponse.getId());
       ShowPolicyAssignmentResponse showResponse =
client.showPolicyAssignment(showPolicyAssignmentRequest);
       System.out.println(showResponse.toString());
     } catch (ConnectionException | RequestTimeoutException | ServiceResponseException ex) {
       System.out.println(ex);
     }
  }
}
```

返回结果示例

class CreatePolicyAssignmentsResponse {
 policyAssignmentType: "policyAssignmentType"
 id: "id"
 name: "name"
 description: "description"
 policyFilter: class PolicyFilterDefinition {}
 period: "period"
 state: "state"
 created: "created"
 updated: "updated"
 policyDefinitionId: "policyDefinitionId"
 customPolicy: "customPolicy"
 parameters: {}
 createdBy: "createdBy"

}

class ShowPolicyAssignmentResponse {
 policyAssignmentType: "policyAssignmentType"
 id: "id"
 name: "name"
 description: "description"
 policyFilter: class PolicyFilterDefinition {}
 period: "period"
 state: "state"
 created: "created"
 updated: "updated"
 policyDefinitionId: "policyDefinitionId"
 customPolicy: "customPolicy"
 parameters: {}
 createdBy: "createdBy"

#### 参考

更多信息请参考资源合规概述。

#### 修订记录

发布日期	文档版本	修订说明	
2024-12-25	1.0	文档首次发布	

# 2 使用 Config 查询资源详情、资源关系和资源

#### 示例简介

该示例展示了如何通过Java版本SDK查询资源详情、资源关系和资源历史。

- 资源清单 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。
- 2. 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。
- 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。

#### 开发前准备

- 1. 获取华为云开发工具包(SDK),您也可以查看安装JAVA SDK。
- 您需要拥有华为云账号以及该账号对应的 Access Key(AK)和 Secret Access Key (SK),请在华为云控制台"我的凭证 > 访问密钥"页面上创建和查看您的 AK/SK。具体请参见访问密钥。
- 3. 配置审计 Config SDK, 支持 Java JDK 1.8 及其以上版本。

#### 安装 SDK

您可以通过Maven方式获取和安装SDK,您只需要在Java项目的pom.xml文件中加入 相应的依赖项即可 。 具体的SDK版本号请参见<mark>SDK开发中心</mark> 。

<dependency>

- <groupId>com.huaweicloud.sdk</groupId>
- <artifactId>huaweicloud-sdk-config</artifactId>
- <version>{sdk-version}</version> </dependency>

#### 代码示例

public class ShowResourceRelationDemo {

public static void main(String[] args) {

// 认证用的ak和sk直接写到代码中有很大的安全风险,建议在配置文件或者环境变量中密文存放,使用时 解密,确保安全;

// 本示例以ak和sk保存在环境变量中来实现身份验证为例,运行本示例前请先在本地环境中设置环境变量HUAWEICLOUD\_SDK\_AK和HUAWEICLOUD\_SDK\_SK。

```
String ak = System.getenv("HUAWEICLOUD_SDK_AK");
  String sk = System.getenv("HUAWEICLOUD_SDK_SK");
  String regionId = "<region id>";
  HttpConfig config = HttpConfig.getDefaultHttpConfig();
  config.withIgnoreSSLVerification(true);
  ICredential auth = new GlobalCredentials().withAk(ak).withSk(sk);
  ConfigClient client = ConfigClient.newBuilder().withHttpConfig(config).withCredential(auth)
     .withRegion(ConfigRegion.valueOf(regionId)).build();
  try {
     String resourceId = "<resource id>";
     // 查询资源详情
     ShowResourceDetailRequest resourceDetailRequest = new ShowResourceDetailRequest()
        .withResourceId(resourceId);
     System.out.println(client.showResourceDetail(resourceDetailRequest));
     // 查询资源关系
     ShowResourceRelationsRequest resourceRelationsRequest = new ShowResourceRelationsRequest()
        .withResourceId(resourceId)
        .withDirection(ShowResourceRelationsRequest.DirectionEnum.IN);
     System.out.println(client.showResourceRelations(resourceRelationsRequest).toString());
     // 查询资源历史
     ShowResourceHistoryRequest resourceHistoryRequest = new ShowResourceHistoryRequest()
        .withResourceId(resourceId);
     System.out.println(client.showResourceHistory(resourceHistoryRequest).toString());
  } catch (ConnectionException | RequestTimeoutException | ServiceResponseException ex) {
     System.out.println(ex);
  }
}
```

#### 返回结果示例

}

```
class ShowResourceDetailResponse {
  id: 81fi****a864
  name: zh****ng
  provider: iam
  type: users
  regionId: global
  projectId:
  projectName:
  epId: 0
  epName: default
  checksum: 522u****e689
  created: 2023-09-18T12:56:30.000Z
  updated: 2023-09-18T12:56:30.000Z
  provisioningState: Succeeded
  state: Normal
  tags: {}
  properties: {pwd_status=false, pwd_strength=high, group_list=[f588****54c5], role_list=[],
last_login_time=2023-09-18T12:57:45Z, virtual_mfa_device=false, login_protect={enabled=false},
credentials=[], policy_list=[], access_mode=default, is_root_user=false, enabled=true}
class ShowResourceRelationsResponse {
  relations: [class ResourceRelation {
     relationType: contains
     fromResourceType: iam.groups
     toResourceType: iam.users
     fromResourceId: f587****54c5
     toResourceld: 81fa****a864
  }]
  pageInfo: class PageInfo {
     currentCount: 1
     nextMarker: null
  }
}
```

class ShowResourceHistoryResponse {

```
items: [class HistoryItem {
     domainId: 39f4****ea39
     resourceld: 81fa****a864
     resourceType: iam.users
     captureTime: 2023-09-21T15:39:27.632Z
     status: ResourceChanged.CREATE
     relations: [class ResourceRelation {
        relationType: isContainedIn
        fromResourceType: iam.users
        toResourceType: iam.groups
        fromResourceld: 81fa****a864
toResourceld: b04e****8dd2
     }]
     resource: class ResourceEntity {
id: 81fa****a864
name: zh****ng
        provider: iam
        type: users
        regionId: global
        projectId:
        projectName:
        epld: 0
        epName: default
        checksum: 00ce****f053
        created: 2023-09-18T12:56:30Z
        updated: 2023-09-18T12:56:30Z
        provisioningState: Succeeded
        state: null
        tags: {}
        properties: {pwd_status=false, pwd_strength=high, group_list=[b04e****8dd2], role_list=[],
virtual_mfa_device=false, login_protect={enabled=false}, credentials=[], policy_list=[], access_mode=default,
enabled=true}
     }
  }]
  pageInfo: class PageInfo {
     currentCount: 1
     nextMarker: null
  }
```

#### 参考

更多信息请参考查看资源历史。

#### 修订记录

}

发布日期	文档版本	修订说明
2024-12-25	1.0	文档首次发布

## **3**通过 CES 实现不合规资源的告警通知

当资源配置不合规时,配置审计会将不合规资源自动投递到云监控服务(CES)。您可 以在云监控服务中查询告警记录,还可以基于云监控服务发送消息通知。

#### 应用场景

您在配置审计控制台通过预设策略"IAM用户的AccessKey在指定时间内轮换"创建一条合规规则。配置审计自动评估当前账号下所有IAM用户,其中部分IAM用户的合规结果为**不合规**,如下图所示。

< ∣ access-keys-rotate	d						
体信息 修正管理	标签						
评估结果 ( 号出 ~ )						◎ 已启用	不会報道課数 4
○ 合规评值编集: 不会规	× 添加等选条件				× Q 🛛	规则详情	
资源名称/贸源ID	合规评估结果	医腰	服务	资源类型	最后一次评估时间	规则名称	access-keys-rotated
Ju 0926901fe100l2101l8c	不合规		统一券份认证 IAM	用户	2024/12/24 16:45:51 GM	規則語介	IAM用户的访问密钥未在描述天散内轮转,视为"不合规" 预设管路
bac 0e0e4ea9cb564cfa914	不合规		统一券份认证 IAM	用户	2024/12/24 16:45:51 GM	216	소리
zhouji aa3fd56327be4d96aaa	不会规		统一券份认证 IAM	用户	2024/12/24 16:45:51 GM	创建时间	2024/12/24 16:45:23 GMT+08:00
Ha 973027/05cb8482890f1	不合规		统一册份认证 IAM	用户	2024/12/24 16:45:61 GM	触发器	@win.cl
忠祭数:4					50 × (1) >	Rayen	(Red)/v1
						周期频率	24小时
						<b>規則参数</b> 規則参数	maxAccessKeyAge: 90

#### 步骤一: 创建规则

- 1. 登录配置审计控制台。
- 2. 在左侧导航栏,选择资源合规。
- 3. 在规则页面,单击"添加规则"。
- 4. 在基础配置页面,选择预设策略中的"IAM用户的AccessKey在指定时间内轮换",单击"下一步"。
- 5. 在规则参数页面,选择评估全部区域的资源,AccessKey轮转时间使用默认值,单 击"下一步"。
- 6. 确认规则配置符合预期,单击"提交",完成规则创建。

在资源合规的规则页签,您可以查看该规则对IAM资源的检测结果。

#### 步骤二:设置消息通知主题

- 1. 登录消息通知服务控制台。
- 2. 在左侧导航栏,选择主题管理。
  - a. 在主题页面,右上角单击"创建主题"。
  - b. 设置合适的主体名称和显示名,单击"确定",完成主题创建。
- 3. 以短信方式为例,添加订阅。
  - a. 单击"添加订阅"。
  - b. 选择协议为"短信"。
  - c. 订阅终端中输入需要通知的有效手机号码。
  - d. 单击"确定"。
- 4. 在订阅页签,点击"请求订阅"。
- 5. 添加订阅的手机上,会收到确认短信,按照短信指示完成订阅确认。

主題 ③				◎ 演察度评价 🍈 使用指南 🛛 創建主職
(毎年 ∨)				
Q 选择属性筛选,或输入关键字搜索				<ul> <li>Image: Image: Ima</li></ul>
□ 主题名称/10 令	主题URN ⇔	创建时间 令	显示名 令	操作
5c1763140117	um.smn.c	2024/12/24 17:07:39 GMT+08:00		发布消息 基础订阅 图多 ~
总统数: 1				10 ~ (1) >

#### 步骤三: 设置云监控服务的告警通知

- 1. 登录云监控服务控制台,国内站用户选择北京四,国际站用户选择新加坡。
- 2. 在左侧导航栏,选择告警。
- 3. 在告警规则页面,单击"创建告警规则"。
  - a. 编辑告警规则名称。
  - b. 告警类型选择"事件"。
  - c. 事件类型选择"系统事件"。
  - d. 事件来源选择"配置审计"。
  - e. 触发规则选择"自定义创建"。
  - f. 打开发送通知,选择主题订阅,通知对象选择步骤二创建的SMN主题,其它 配置使用默认值。
  - g. 触发条件勾选"出现告警"。
  - h. 点击"立即创建",完成告警规则的创建。
- 告警规则创建完成后,如果再评估到不合规的资源,则会通过短信方式接受到不 合规的消息通知,并在告警记录中查询到相关告警。

告警记录 💿										@ I	職意度评价 🗊 打	創示説明
(9H)							最后更新时间	× 2024/12/17 19:12	:07 - 2024/12/24 19:12	07	资源精确匹置	3 💿
Q 默认按照1	古警规则名称搜索										Q	۲
#\$ ()	告警级别	产生时间	最后更新时间	告警持	告警类型	资源类型	告警资源	告警策略	告警规则名称/ID	通知类型	操作	
● 已触发	• 重要	2024/12/24 19:12:05 GMT	2024/12/24 1		事件	配置审计	zł a:	配要审计-配要不合规 立即触发	alarm-om7a al17350386756	通知组/通… ces-config	查看监控详情	屏蔽
● 已触发	• 重要	2024/12/24 19:12:05 GMT	2024/12/24 1		事件	配要审计	Hari 973	配置审计-配置不合规 立即触发	alarm-om7a al17350386756	通知组/通… ces-config	臺看這拉洋情	屏藏
● 已触发	• 重要	2024/12/24 19:12:05 GMT	2024/12/24 1		事件	配置审计	Ји 05	配置审计-配置不合规 立即触发	alarm-om7a al17350386756	通知追/通… ces-config	查看這拉洋情	屏藏
● 已粮发	• 重要	2024/12/24 19:12:05 GMT	2024/12/24 1	-	御仲	配置审计	bao 0e0	配置审计-配置不合规 立即触发	alarm-om7a al17350386756	通知组/通… ces-config	查看這拉洋情	屏幕

#### 相关文档

- 查看事件监控数据
- 创建事件监控的告警通知

### **4** 通过高级查询自定义查询资源并下载

本文为您介绍如何通过配置审计的高级查询功能,对当前资源数据执行基于属性的自定义查询,并下载查询结果。

#### 应用场景

Config提供高级查询能力,通过使用ResourceQL语法来自定义查询云资源。方便上云 企业根据资源属性灵活导出数据。

预设查询 自定义查询		
○ 选择属性筛选,或输入关键字搜索		
名称 ⇔	描述 🕀	操作
ECS Instance with EVS	查询ECS资源及其关联的EVS资源	使用查询
ECS Instance with EIP	查询ECS资源及其关联的弹性公网IP资源	使用查询
Resources Time	查询资源的创建时间和更新时间	使用查询
Count ECS by region_id	查询每个区域内弹性云服务器的数量	使用查询
Count resources more then 100 by region_id	查询每个区域内数量大于100的资源类型	使用查询
List OBS Bucket	列举对象存储桶	使用查询
Fuzzy Search resource	对象存储桶模糊查询	使用查询
List resources by tags	通过标签筛选资源	使用查询
List resources by ep_id	通过企业项目筛选资源	使用查询

#### 操作步骤

- 1. 登录配置审计控制台。
- 2. 在左侧导航栏,选择高级查询。
- 3. 点击自定义查询页签,单击右上角的"新建查询"。
- 4. 输入如下内容查询未使用的EVS磁盘,单击"运行"。 SELECT \* FROM tracked\_resources WHERE provider = 'evs' AND type = 'volumes' AND properties.status != 'in-use'
- 5. 单击"导出",选择CSV或JSON格式,将查询结果导出到本地。

1	SELECT	*											
2	FROM tra	acked_resour	es										
3	WHERE p	rovider = 'e	18'										
4	AND	type = 'volu	mes'										
5	AND	properties.	tatus != 'i	n-use'									
	运行 (	保存查询	历史执行	录》清晰	输入内容								
-		)											
查询	结果												
	Ru .		Tri Bulutti e non										
-	- me	日期只支持展开	재나당(四則)4,000	永登闻后来。									
	ev												
		provider	name	type	ep_id	project	tag	updated	created	checks	region_id	provisi	propert
J	SON		aug und		0	000122		2024.4	2021.1	61-00-	on parth 7	Sugges	
		842	evs-vol	volumes	v	000123	u	2021-1	2021-1	016206	cn-north-7	SUCCEB	宣旨许信

#### 相关文档

- 高级查询语法概览
- 高级查询支持的资源属性

### 5 使用 Config 查找未绑定指定标签的资源

本文为您介绍如何通过配置审计服务查询未绑定指定标签的资源。

#### 应用场景

企业上云后,云上创建的资源不断增加,有些大型企业资源数量达到十万、百万级 别,一个账号内存在大量资源,企业需要进行分类管理。华为云推荐您使用标签对资 源进行标记,进而实现资源的分组分类。通过标签对资源的业务归属、财务归属等资 源属性进行标记,例如:按所属部门、地域或项目等。

配置审计服务通过资源合规能力,可以帮助您识别未进行正确标签标记的资源。

○ 标签: tag × 添加筛选条件			×
策略名称	标签	资源类型	策略简介
○ 资源具有所有指定的标签键	tag	DDoS高防-实例 	指定标签列表,不具有所有指定标签 键的资源,视为"不合规"
○ 资源具有指定的标签	tag	DDoS高防-实例 	指定一个标签,不具有此标签的资 源,视为"不合规"
② 资源存在任一指定的标签	tag	DDoS高防-实例 	指定标签列表,不具有任一指定标签 的资源,视为"不合规"
资源具有指定前后缀的标签键	tag	DDoS高防-实例 	指定前缀和后缀,资源不具有任意匹 配前后缀的标签键,视为"不合规"
) 资源标签非空	tag	DDoS高防-实例	资源未配置标签,视为"不合规"

#### 操作步骤

- 1. 登录配置审计控制台。
- 2. 在左侧导航栏,选择资源合规。
- 3. 在规则页面,单击"添加规则"。
- 在基础配置页面,选择预设策略中的"资源具有指定的标签",单击"下一步"。
- 5. 在规则参数页面,选择服务为"虚拟私有云"、资源类型为"安全组"、区域为 "全部"。
- 6. 设置规则参数:标签键为department,标签值列表为["team1", "team2", "team3"]。
- 7. 确认规则配置符合预期,单击"提交",完成规则创建。

在资源合规的规则页签,您可以查看该规则对VPC安全组资源的检测结果。

<   required-tag-check	ĸ						立即评估 编编规则 <b></b>
<b>基本信息</b> 修正管理	标签						
<b>评估结果</b> 						◎ 已启用	不会现资源数 27
<ul> <li>合规评估结果:不合规</li> </ul>	× 添加筛选条件				× Q ()	规则详情	
资源名称/资源ID	合规评估结果	区域	服务	资源类型	最后一次评估时间	规则名称	required-tag-check
default 1b19b681-0c92-465b-9	不合规	华东二	虚拟私有云 VPC	安全组	2024/12/24 20:17:27 G	规则简介	指定一个标签,不具有此标签的资源,视为"不合规"
default 1aa14fc2-30f2-462f-b7f	不合规	华北北京一	虚拟私有云 VPC	安全组	2024/12/24 20:17:27 G	東南東亚	加速機構 全部
default 14bbf0ff-1b8e-401d-a3	不合规	华南-广州	遗拟私有云 VPC	安全组	2024/12/24 20:17:27 G	创建时间	2024/12/24 20:17:26 GMT+08:00
default 0e5#66a0-d651-4bf1-88	不会规	中国-香港	透拟私有云 VPC	安全组	2024/12/24 20:17:27 G	<b>触发器</b>	新要交車
default 2eb77327-c4ce-4285-b	不合规	西南-贵阳—	虚拟私有云 VPC	安全组	2024/12/24 20:17:27 G		
default 47c19488-9ce0-42e7-8	不合规	拉美-墨西哥城二	虚拟私有云 VPC	安全组	2024/12/24 20:17:27 G	<b>过滤器</b> 过滤器类型	指生资源
sg-3700 44576476-21bb-4206-8	不合规	拉美·圣保罗一	虚拟私有云 VPC	安全组	2024/12/24 20:17:27 G	1639 	通频粘有云 VPC
default 59a70e03-704f-4521-af	不合规	华东-上海—	透拟私有云 VPC	安全组	2024/12/24 20:17:27 G	20100-00	NEG.
default 623aa307-8116-4d23-a	不合规	拉美-墨西哥城一	透拟私有云 VPC	安全组	2024/12/24 20:17:27 G	<b>规则参数</b> 规则参数	specifiedTagKey : department
default 6c6ab21c-bfc0-4b67-9	不合规	华南-广州-发好用户环境	虚拟私有云 VPC	安全组	2024/12/24 20:17:27 G		specifiedTagValue : ["team1","team2","team3"]

#### 标签审计的预设策略列表

策略名称	策略描述
required-all-tags	指定标签列表,不具有所有指定标签键的资源,视为 "不合规"。
required-tag-exist	指定标签列表,不具有任一指定标签键的资源,视为 "不合规"。
resource-tag-key- prefix-suffix	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"。
resource-tag-not-empty	资源未配置标签,视为"不合规"。
required-tag-check	指定一个标签,不具有此标签的资源,视为"不合 规"。

### 6 通过 Config 实现资源的多维度合规审计

当企业进行云上资源合规落地时,通常会面临合规标准无法统一的问题,例如:

- 生产环境和测试环境的资源安全要求不同;
- 不同地区的法规不同,导致对资源的规范要求不同。

同时,企业内所有账号也需要配置统一的安全基准要求。配置审计通过丰富的托管规则,帮助企业在资源合规落地过程中针对不同场景,设置不同的合规策略。

#### 基于资源标签

**前提条件**:请确保您已为目标资源绑定标签。具体操作,请参见<mark>标签设计原则和命名</mark> 示例。

**具体场景:**根据开发环境对资源进行分类,可以实现对不同环境资源的不同审计。假 设您已为生产环境中的所有资源绑定标签Env:Prod,为测试环境中的所有资源绑定标 签Env:Test,标签值您可以根据实际情况自行定义,能区分不同环境中的资源即可。

#### 操作流程:

- 1. 登录配置审计控制台。
- 2. 在左侧导航栏,选择资源合规。
- 3. 在规则页面,单击"添加规则"。
- 4. 选择您需要的预设策略,如"ECS实例的镜像名称在指定的范围",单击"下一步"。
- 5. 在规则参数页面,保持默认的资源范围,区域选择"全部"。
- 6. 单击"过滤范围",选择标签,标签键和标签值填入 Env 和 Prod。

* <u>触发类型</u>	<ul> <li>配置支更</li> <li>周期执行</li> </ul>
* 过滤器类型	● 指定資源 指定資源失型下的所有资源均参与规则评估。 所有资源均参与规则评估。
指定资源范围	→ 19世 法服务器 ECS → ○ ( 云服务器 → ) ( 全部 → )
过滤范围	开启后您可通过资源DR成标签指定过滤范围。       资源D       KG       Env   Prod
规则参数	参数 描述 値 imageNames 使命名称列表,使命名称检查方式为部分匹配 ['prod']

- 7. 完成规则创建,则合规规则只会评估生产环境中的该类型资源。
- 8. 返回规则列表页面,查看新建合规规则的评估结果。

#### 基于资源区域

**具体场景:**因为不同地区有不同的法律法规要求,假设您不希望您海外的OBS桶内的 数据被公开访问,则可以按照如下操作步骤配置合规规则。

#### 操作流程:

- 1. 登录配置审计控制台。
- 2. 在左侧导航栏,选择资源合规。
- 3. 在规则页面,单击"添加规则"。
- 4. 选择预设策略"OBS桶禁止公开读",单击"下一步"。
- 5. 在规则参数页面,保持默认的资源范围,区域选择您期望检测的区域,如"亚太-新加坡"。

* 触发类型	● 配置変更   ◎ 周期执行	
* 过滤器类型	<ul> <li>● 指定資源</li> <li>指定資源类型下的所有资源均参与规则评估。</li> </ul>	源 的所有资源均参与规则评估。
指定资源范围	対象存储服务 OBS v 桶 v	亚太-新加坡 🗸
过滤范围	开启后您可通过资源ID或标签指定过滤范围。	

- 6. 完成规则创建,则合规规则只会评估"亚太-新加坡"的OBS桶。
- 7. 返回规则列表页面,查看新建合规规则的评估结果。

#### 统一下发到组织

**前提条件**:请确保您的账号已经加入组织,且为组织管理员或者Config服务的委托管 理员,请参考<mark>组织概述和添加、查看和取消委托管理员</mark>。

**具体场景**:多账号场景下,可以通过<mark>组织合规规则</mark>方式,将企业的合规要求部署到组 织内的所有成员账号。下发组织合规规则的账号一般为企业的安全管理员账号,不承 载具体的业务。

#### 操作流程:

- 1. 登录配置审计控制台。
- 2. 在左侧导航栏,选择资源合规。
- 3. 在组织规则页面,单击"添加规则"。
- 4. 选择您需要的预设策略,如"IAM用户开启MFA",单击"下一步"。
- 5. 在规则参数页面,保持默认的资源范围,单击"下一步",完成组织规则创建。
- 6. 返回组织规则列表页面,查看新建的组织合规规则的部署情况。

am-user-mia-enabled				SHARKEN ENGINE
部署账号 排除账号			規則详情	ion uses the analysis
〇、送採属性筛选、或输入关键字按束			规则额介	AM用户水开启MFA认证、视为"不合规"
账号ID ↔ 3(d2	部務状态 ⊕ ○ 戸部署	更加时间 ↔ 2024/12/25 17:00:50 GMT+08:00	策略类型	预设策略
e74e0	o 已部署	2024/12/25 17:00:50 GMT+08:00	区域	
总乐数:2		10 ~ (1) >	0330817175	

#### 统一查询组织成员的合规结果

前提条件:请确保您的账号已经加入组织,且为组织管理员或者Config服务的委托管理员,请参考组织概述和添加、查看和取消委托管理员。

**具体场景:**企业的安全管理员,能通过<mark>聚合器</mark>的能力,查询到组织内各个成员账号部 署的合规规则,并查询到各个成员账号的不合规资源情况。

#### 操作流程:

- 1. 登录配置审计控制台。
- 2. 在左侧导航栏,选择资源聚合器。
- 3. 在聚合器页面,单击"创建聚合器"。
- 勾选"允许数据复制",命名聚合器,并选择源类型为"添加组织",完成聚合器创建。
- 5. 在聚合器的规则页面,选择聚合器,则可以看到聚合到的各账号的规则情况。

配置审计 Config	规则		
总览 资源清单 资源合规	选择聚合器 org-aggregator > ② 规则名称: Org-iam-user-mfa-enabled > 3	添加筛选条件	
合规规则包 资源记录器	規则名称	合規评估结果	账号(D
高级查询	Org-iam-user-mfa-enabled	不合规 (4)	3fd2381
治源聚合器 へ	Org-iam-user-mfa-enabled	不合规 (27)	e74e04:
聚合器			
規则	总条数:2		

6. 单击规则名称,则可以看到该账号的这条规则所评估的资源的合规性情况。

Org-iam	Org-iam-user-mra-enabled								
评估结果	~				<b>聚合器信息</b> 聚合器名称	org-aggregator			
	刻汗估填果: 不合规	X 添加筛选条件				×Q	账号ID	3fd23	
资源名称	N/资源ID	合规评估结果	区域	服务	资源类型	最后一次评估时间			
ia 2		不合规	-	统一券份认证 IAM	用户	2024/12/25 17:01:04	<b>规则详情</b> 规则名称	Org-iam-user-mfa-enabled	
sh 35		不合规		统一身份认证 IAM	用户	2024/12/25 17:01:04	区域	-	
<b>cy</b> 7!		不合规		统一筹份认证 IAM	用户	2024/12/25 17:01:04	規則ID 規則篩介	6/bbc IAM用户未开启MFA认证,视为"不合规"	
hi bi	c	不合规		统一券份认证 IAM	用户	2024/12/25 17:01:04	更新时间	2024/12/25 17:01:03 GMT+08:00	

#### 常见问题

控制台为什么没有组织规则的页面?

账号是组织管理员,或加入组织并成为Config服务的委托管理员,才能看到该页面。

#### 组织规则下发后,状态为什么是部署异常?

是因为这些组织成员账号未开启资源记录器导致的部署异常。

Config服务的相关功能均依赖于资源记录器收集的资源数据,因此账号必须开启资源 记录器才可正常使用合规规则和合规规则包功能。

在组织合规规则和组织合规规则包场景下,除下发规则和合规规则包的组织管理员或 Config服务的委托管理员之外,所部署的组织成员账号也需要开启资源记录器,才能 正常下发合规规则和合规规则包。

## 7 通过 Config 实现资源自动化管理

本文为您介绍如何通过配置审计服务的资源评估和合规修正能力,自动化实现不合规 资源的发现和修正。通过该流程,可以确保云上任意用户,无论有意还是无意的行 为,造成了资源不合规,都可以在几分钟内被该流程自动修复,从而保证了云上的资 源安全。

#### 应用场景

**具体场景:**用户在云上的OBS桶,应该使用桶策略避免客户端误使用HTTP协议进行 OBS业务操作,详见确保您的数据在传输到OBS过程中不被窃取和篡改。

#### 操作流程

#### 创建合规规则:

- 1. 登录配置审计控制台。
- 2. 在左侧导航栏,选择资源合规。
- 3. 在规则页面,单击"添加规则"。
- 4. 选择预设策略"OBS桶策略授权行为使用SSL加密",单击"下一步"。
- 5. 在规则参数页面,保持默认的资源范围,区域选择"全部",完成规则创建。
- 6. 返回规则列表页面,查看新建合规规则的评估结果。

<   obs-bucket-ssl-	obs-bucket-ssi-requests-only						
基本信息 修正管理	标签						
评估结果 						◎ 已启用	不会授资源数 21
〇、数以按照名称搜索					Q ()	规则详情	
資源名称/资源ID	合规评估结果	医城	服务	资源类型	最后一次评估时间	规则名称	obs-bucket-ssl-requests-only
	合规	拉美-圣地亚哥	对象存储服务 OBS	柄	2024/12/26 15:08:53 G	规则简介	OBS播策略授权了无需SSL加密的行为,视为"不会规"
						策略类型	预设策略
0	合规	华隅。广州	对象存储服务 OBS	橋	2024/12/26 15:07:16 G	⊠tit	全部
3 3	會現	华北-北东四	对象存储服务 CBS	梢	2024/12/26 14:46:22 G	estate) (	2024/12/26 14:29:47 GMT+08:00

#### 配置修正函数:

以python方式为例,为您介绍如何通过FunctionGraph实现资源的自动修正。

- 1. 登录函数工作流控制台。
- 2. 在左侧导航栏,选择函数。
- 3. 在函数列表页面,单击"创建函数"。

4. 函数类型选择"事件函数",运行时选择"Python3.9",选择一个合适的委托, 至少包含如下权限:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
               "Action": [
                "obs:bucket:PutBucketPolicy",
               "obs:bucket:GetBucketPolicy",
                "rms:resources:get"
            ]
        }
    ]
}
```

#### 5. 完成函数创建后,为函数添加"huaweicloudsdk\_obs"和 "huaweicloudsdkconfig"两个依赖包。

代码依赖包 (共2/20个依赖包)				
添加依赖包 删除				
Q 选择属性筛选,或输入关键字搜索				
■ 依赖包名称	类型 ⊖	版本 🖯	运行时	
huaweicloudsdk_obs_py3.9	公共	1	Python3.9	
huaweicloudsdkconfig_python39	公共	1	Python3.9	

#### 6. 在 "index.py" 中贴入如下代码。

import json

```
from obs.client import ObsClient
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkconfig.v1.region.config_region import ConfigRegion
from huaweicloudsdkconfig.v1.config_client import ConfigClient
from huaweicloudsdkconfig.v1 import ShowResourceDetailRequest
def get_resource_region(context, domain_id, resource_id):
  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()
  resource = client.show resource detail(ShowResourceDetailRequest(resource id)).to json object()
  return resource.get("region_id")
def getBucketPolicy(obsClient, bucket_name):
  resp = obsClient.getBucketPolicy(bucket_name)
  if resp.status < 300:
     print("Get Bucket Policy Succeeded")
     return resp.body.policyJSON
  if resp.status == 404 and resp.errorCode == "NoSuchBucketPolicy":
     print("NoSuchBucketPolicy")
     return "{\"Statement\": []}'
  assert False, f"Get Bucket Policy Failed: {resp.errorCode} | {resp.errorMessage}"
def ensurePolicySSL(obsClient, bucket_name, policy):
  policy["Statement"] = policy["Statement"] + [{
     "Sid": "ensure_secure_transport",
     "Effect": "Deny"
     "Principal": {"ID": ["*"]},
"Action": ["*"],
```

```
"Resource": [bucket_name, bucket_name + "/*"],
    "Condition": {"Bool": {"g:SecureTransport": ["false"]}}
  }]
  resp = obsClient.setBucketPolicy(bucket_name, policy)
  if resp.status < 300:
    print("Set Bucket Policy Succeeded")
  else:
    print(policy)
    assert False, f"Set Bucket Policy Failed: {resp.errorCode} | {resp.errorMessage}"
def handler(event, context):
  domain_id = event.get("domain_id")
  bucket_name = event.get("bucket_name")
  print("domain_id", domain_id)
  print("bucket_name", bucket_name)
  region_id = get_resource_region(context, domain_id, bucket_name)
  print("region_id", region_id)
  server = f"https://obs.{region_id}.myhuaweicloud.com"
  obsClient = ObsClient(
    access_key_id=context.getSecurityAccessKey(),
    secret_access_key=context.getSecuritySecretKey(),
    server=server,
    security_token=context.getSecurityToken()
  )
  policy = getBucketPolicy(obsClient, bucket_name)
  policy = json.loads(policy)
  ensurePolicySSL(obsClient, bucket_name, policy)
  obsClient.close()
(可选)在函数的设置页面适当修改函数的"执行超时时间"和"内存",并启
用日志配置。强烈建议您执行该项操作,否则资源修正的行为有可能会失败,且
您无法通过日志记录定位函数执行的错误原因。
```

#### 配置合规修正:

7.

- 1. 登录配置审计控制台。
- 2. 在左侧导航栏,选择资源合规。
- 3. 在规则页面,单击规则名称。
- 4. 进入规则详情页面,选择"修正管理",单击"修正配置"。
- 5. 选择"手动修正"或"自动修正",重试时间和重试次数使用默认值。
- 6. 选择"FGS模版",选中前一步中所配置的函数。
- 7. 依赖于资源类型设置为"bucket\_name",参数中键和值分别输入domain\_id 和 账号ID的值。
- 8. 单击"保存",完成合规修正的配置。

修正操作详细信息 RFS模板 ● FGS模板			
<ul> <li>● 华北-北京四 ~</li> </ul>			
ensure_ssl ~ 请选择FGS模板资源	Q FGS模板列表 C		
<b>资源旧参数</b> 依赖于资源类型			
	」 「不合规资源的资源ID传递给修复操作		
参数 domain_id	0926901e	删除	
+ 添加 最多添加50个参数,您还可以添加49个	个参数。		

#### 资源的手动修正:

如果您在上一步的修正方法中选择"手动修正",则需要进行如下操作。

- 1. 重新进入修正配置的页面。
- 2. 在资源范围页面勾选您需要处理的资源:
  - 如果资源属于您认为需要处理的资源,则单击"执行修正"。
  - 如果资源属于您认为不需要处理的资源,则单击"加入修正例外"。
- 3. 登录对象存储服务控制台,进入您刚才执行修正的OBS桶的详情页。
- 4. 进入权限控制的桶策略页面,确认桶策略内容已经被更新。

桶策略							
植策略提供基于各种条件的集中访问	司控制,可以与ACL共同作用,	如果授权产生冲突,以桶策略大于桶AC	的优先级决定授权结果。了解更多				
Q 默认按照桶策略名称/效力/被	授权用户提索						
策略名称	效力	被授权用户	授权资源	授权操作	条件	操作	
✓ base_policy	❷ 允许	✓ 包含所有用户	✓ 包含当前碼、桶内所有対象	✓ 包含3个动作	● 无条件	编辑 删除	
ensure_secure_transport	t 😑 拒绝	✓ 包含所有用户	包含当前桶、桶内所有对象	✓ 包含1个动作	✓ 1个条件	编辑 删除	
		1.2	4	1.0	-g:SecureTransport(Bool fals	e)	

#### 常见问题

#### 手动修正和自动修正的区别?

如果配置为手动修正,则需要用户主动查询不合规资源,并执行修正;如果配置为自动修正,则Config服务会自动为该合规规则下的所有不合规资源执行修正行为。

强烈建议您在第一次配置修正时,选择手动修正。手动修正可以防止资源被修改导致 用户业务中断。

在您处理完所有存量的不合规资源后,再将修正配置修改为自动修正,此后所有新增 的不合规资源都会被自动修复,而且不需要人为干预。

#### 执行修正后,为什么资源未成功被修正?

这通常是因为您配置在函数工作流服务的代码存在问题,也可能是因为您赋予函数工作流的权限不足。请前往函数工作流的监控页面查询具体的失败日志。

#### 资源修正成功后,为什么资源在合规规则页面还是不合规?

资源修正完成后,资源的变更行为通常会在5分钟之内通知Config服务,规则会自动触发该资源的合规评估并生成最新的资源合规结果。