

数据安全中心

最佳实践

文档版本 06
发布日期 2025-01-02



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



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

目录

1 如何防止个人敏感数据在开发测试中被泄露?	1
2 OBS 数据安全防护最佳实践.....	7
3 API 数据安全防护最佳实践.....	11
3.1 系统功能配置及使用场景举例.....	11
3.1.1 系统快速使用指南.....	11
3.1.2 应用代理连接配置.....	14
3.1.3 白名单配置.....	17
3.1.4 黑名单配置.....	19
3.1.5 脱敏规则配置.....	21
3.1.6 水印规则配置.....	24

1 如何防止个人敏感数据在开发测试中被泄露？

敏感数据是指那些如果被未经授权的人访问、泄露或滥用，可能会对个人或组织造成严重风险的信息。

- 对个人而言，身份证号码、家庭住址、工作单位、银行卡号等隐私信息都是敏感数据。
- 对企业或组织而言，客户资料、财务信息、技术资料、重大决策等公司核心信息都是敏感数据。

华为云数据安全中心（Data Security Center，简称DSC）提供静态数据脱敏功能：可以按照脱敏规则一次性完成大批量数据的变形转换处理，静态脱敏通常用在将生产环境中的敏感数据交付至开发、测试或者外发环境的情况使用，适用于开发测试、数据分享、数据研究等场景。


常见数据泄露原因

- 内部数据泄漏
 - 笔记本电脑和移动设备的丢失或失窃
 - 敏感数据越权访问和存储
 - 员工外发、打印和复制敏感数据
 - 意外传输敏感数据
- 外部攻击导致的数据泄漏
 - 基础措施不可控，避免数据存储系统存在漏洞
 - 配置不当导致的外部攻击
 - 敏感数据越权访问和存储

步骤一：购买数据安全中心专业版

步骤1 [登录管理控制台](#)。

步骤2 单击左上角的，选择区域或项目。

步骤3 在左侧导航树中，单击，选择“安全与合规 > 数据安全中心”。

步骤4 首次购买DSC，在界面左侧，单击“立即购买”。

步骤5 在“购买数据安全中心”页面，选择“当前区域”。

图 1-1 选择区域和版本规格



说明

如果您需要切换区域，请在“区域”下拉框里选择区域。同一个区域只支持购买一个DSC版本。

步骤6 选择“数据库扩展包”和“OBS扩展包”的数量。

图 1-2 选择扩展包



- 1个数据库扩展包包含1个可添加数据库（支持RDS、DWS、ECS自建数据库、DLI、Elasticsearch、ECS自建大数据等）资产。
- 1个OBS扩展包包含1T体量，即1024GB。

步骤7 选择“购买时长”。单击时间轴的点，选择购买时长，可以选择1个月~3年的时长。

说明

勾选“自动续费”后，当服务期满时，系统会自动按照购买周期进行续费。

步骤8 在页面的右下角，单击“立即购买”。

如果您对价格有疑问，可以单击页面左下角的“了解计费详情”，了解产品价格。

步骤9 确认订单无误后，阅读并勾选“我已阅读并同意《数据安全中心免责声明》”，单击“去支付”。

步骤10 进入“付款”页面，请选择付款方式进行付款。

----结束

步骤二：识别敏感数据

步骤1 登录[管理控制台](#)。

步骤2 在左侧导航树中，单击，选择“安全 > 数据安全中心”。

步骤3 在左侧导航树中，选择“敏感数据识别 > 识别任务”，进入“识别任务”页面。

步骤4 单击“新建任务”，在弹出的“新建任务”对话框中，配置任务基本信息。

表 1-1 新建任务参数说明

参数	说明	取值样例
任务名称	您可以自定义敏感数据识别任务名称。 任务名称需要满足以下要求： <ul style="list-style-type: none"> • 4~255个字符。 • 字符可由中文、英文字母、数字、下划线或中划线组成。 • 开头需为中文或者字母。 • 任务名称不能与已有的任务名称重复。 	test
数据类型	选择识别的数据类型，可多选。 <ul style="list-style-type: none"> • OBS：授权DSC访问您的华为云OBS资产后，DSC将对华为云OBS里的资产进行敏感数据识别，添加OBS资产的相关操作请参见添加OBS资产。 • 数据库：DSC将对已授权的数据库资产进行敏感数据识别，授权数据库资产的相关操作请参见授权数据库资产。 • 大数据：DSC将对已授权的大数据资产进行敏感数据识别，授权大数据源资产请参见授权大数据资产。 • MRS：DSC将对已授权的MRS资产进行敏感数据识别，授权MRS资产请参见授权大数据资产。 • LTS：DSC将对已授权的LTS资产进行敏感数据识别，添加日志流请参见添加日志流。 	数据库 > gbx-jiami
识别模板	选择内置模板或者自定义模板，DSC将根据您选择的模板对数据进行分级分类展示。添加模板请参见 新增识别模板 。	华为云数据安全分类分级模板

参数	说明	取值样例
识别周期	设置数据识别任务的执行策略： <ul style="list-style-type: none"> ● 单次：根据设置的执行计划，在设定的时间执行一次该识别任务。 ● 每天：选择该选项，即在每天的固定时间执行该识别任务。 ● 每周：选择该选项，即在设定的每周这一时间点执行该识别任务。 ● 每月：选择该选项，即在设定的每月这一时间点执行该识别任务。 	单次
执行计划	“识别周期”为“单次”时，显示该选项： <ul style="list-style-type: none"> ● 立即执行：选择该选项，单击“确定”，系统立即执行数据识别任务。 ● 定时启动：在指定时间执行一次该识别任务。 	立即执行

步骤5 单击“确定”，返回敏感数据任务列表。

步骤6 任务状态为“识别完成”后，在该任务的操作列，单击“识别结果”，查看数据识别结果。

Birthday和PhoneNumbers列被识别为敏感数据风险。

步骤7 单击“查看分类分级结果详情”，查看结果详情。

图 1-3 分类分级结果详情



执行**步骤三：数据静态脱敏**对数据库“gbx-jiami”中的表“info1”的Birthday和PhoneNumbers列进行脱敏。

----结束

步骤三：数据静态脱敏

DSC支持对数据库、ES、MRS以及Hive等数据类型的脱敏任务，本节以创建数据库静态脱敏任务为例进行演示，如需了解其他脱敏相关的方法请参见：[创建数据库静态脱敏任务](#)。

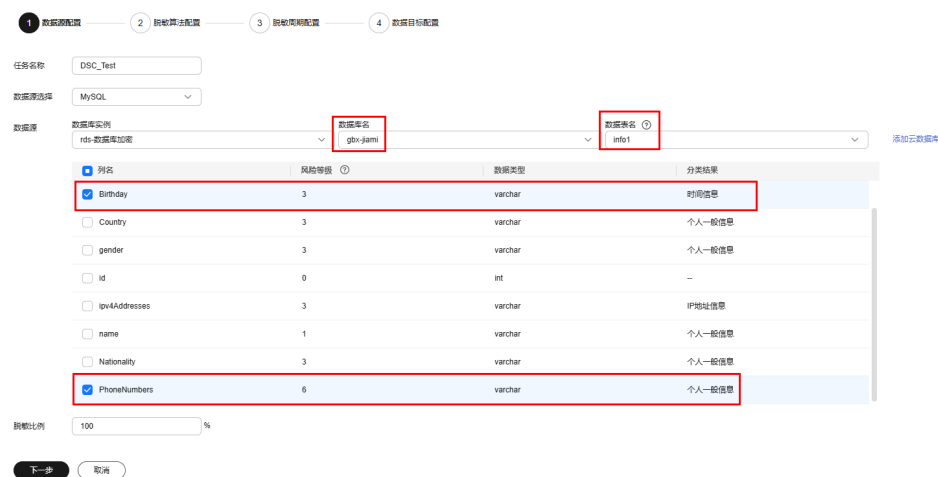
步骤1 在左侧导航树中，选择“数据资产保护 > 数据静态脱敏”，进入“数据脱敏”页面。

步骤2 将“数据库脱敏”设置为 ，开启数据库脱敏。

步骤3 单击“新建任务”，进行“数据源配置”。

如果您想脱敏后生成一张完整的表，此处勾选所有数据类型。

图 1-4 数据源配置



步骤4 单击“下一步”，进行“脱敏算法配置”。

图 1-5 脱敏算法配置




步骤5 单击“下一步”，进入“脱敏周期”页面，配置脱敏周期。

步骤6 单击“下一步”，进行“数据目标配置”，配置脱敏后生成的表的存放位置。

图 1-6 数据目标配置

数据源配置 — 脱敏算法配置 — 脱敏周期配置 — 4 数据目标配置

数据库实例	数据库名	数据表名
mysql_db	demo	请输入表名
数据源列名	风险等级	数据目标列名
Birthday	3	Birthday
PhoneNumbers	6	PhoneNumbers

步骤7 单击“完成”，返回到数据库脱敏任务列表，单击 ，启用脱敏任务，并在任务所在行的“操作”列，单击“立即运行”，执行脱敏任务。

当“状态”为“已完成”时，表示脱敏成功。

----结束

2 OBS 数据安全防护最佳实践

本文介绍如何使用数据安全中心（DSC），对OBS中存储的敏感数据进行识别、分类分级和保护。

背景信息

敏感数据主要包括个人隐私信息、密码、密钥、敏感图片等高价值数据，这些数据通常会以不同的格式存储在您的OBS桶中，一旦发生泄漏，会给企业带来重大的经济和名誉损失。

DSC在您完成数据源识别授权后，从您存储在OBS的海量数据中快速发现和定位敏感数据，对敏感数据分类分级并统一展示，同时追踪敏感数据的使用情况，并根据预先定义的安全策略，对数据进行保护和审计，以便您随时了解OBS数据资产的安全状态。

应用场景

- 敏感数据识别
OBS中存储了大量的数据与文件，但无法准确获知这些OBS数据中是否包含敏感信息以及敏感数据所在的位置。
您可以使用DSC内置算法规则，或根据其行业特点自定义规则，对其存储在OBS中的数据进行整体扫描、分类、分级，并根据结果做进一步的安全防护，如利用OBS的访问控制和加密功能等。
- 异常检测和审计
DSC可检测敏感数据相关的访问、操作、管理等异常，并提供告警提示信息，用户可以对异常事件进行确认和处理。通常情况下，以下行为均被视为异常事件：
 - 非法用户在未经授权的情况下对敏感数据进行了访问、下载。
 - 合法用户对敏感数据进行了访问、下载、修改、权限更改、权限删除。
 - 合法用户对敏感数据的桶进行权限更改、权限删除。
 - 访问敏感数据的用户登录终端异常等情况。

操作步骤

- 步骤1 [购买数据安全中心服务](#)。
- 步骤2 登录[管理控制台](#)。



- 步骤3** 在左侧导航树中，单击 ，选择“安全 > 数据安全中心”，进入“资产地图”界面。
- 步骤4** 在“资产地图”左上角单击云资产授权“修改”，进入“云资产委托授权”页面。
- 步骤5** 在OBS资产所在行的“操作”列，单击  开启授权。
- 步骤6** 添加OBS资产，具体的操作请参见[添加OBS资产](#)。
- 步骤7** 在左侧导航树中，选择“敏感数据识别 > 识别任务”，单击“新建任务”，配置敏感数据的扫描任务。
- “数据类型”选择[步骤6](#)中添加的OBS资产，其他配置请参见[创建敏感数据识别任务](#)。

表 2-1 新建任务参数说明

参数	说明	取值样例
任务名称	<p>您可以自定义敏感数据识别任务名称。</p> <p>任务名称需要满足以下要求：</p> <ul style="list-style-type: none"> 4~255个字符。 字符可由中文、英文字母、数字、下划线或中划线组成。 开头需为中文或者字母。 任务名称不能与已有的任务名称重复。 	Test_OBS
数据类型	<p>选择识别的数据类型，可多选。</p> <ul style="list-style-type: none"> OBS：授权DSC访问您的华为云OBS资产后，DSC将对华为云OBS里的资产进行敏感数据识别，添加OBS资产的相关操作请参见添加OBS资产。 数据库：DSC将对已授权的数据库资产进行敏感数据识别，授权数据库资产的相关操作请参见授权数据库资产。 大数据：DSC将对已授权的大数据资产进行敏感数据识别，授权大数据源资产请参见授权大数据资产。 MRS：DSC将对已授权的MRS资产进行敏感数据识别，授权MRS资产请参见授权大数据资产。 LTS：DSC将对已授权的LTS资产进行敏感数据识别，添加日志流请参见添加日志流。 	OBS
识别模板	<p>选择内置模板或者自定义模板，DSC将根据您选择的模板对数据进行分级分类展示。添加模板请参见新增识别模板。</p>	华为云数据安全分类分级模板

参数	说明	取值样例
识别周期	设置数据识别任务的执行策略： <ul style="list-style-type: none"> ● 单次：根据设置的执行计划，在设定的时间执行一次该识别任务。 ● 每天：选择该选项，即在每天的固定时间执行该识别任务。 ● 每周：选择该选项，即在设定的每周这一时间点执行该识别任务。 ● 每月：选择该选项，即在设定的每月这一时间点执行该识别任务。 	单次
执行计划	“识别周期”为“单次”时，显示该选项： <ul style="list-style-type: none"> ● 立即执行：选择该选项，单击“确定”，系统立即执行数据识别任务。 ● 定时启动：在指定时间执行一次该识别任务。 	立即执行

步骤8 在左侧导航树中选择“敏感数据识别 > 识别任务”，进入识别任务页面。

步骤9 单击目标任务“操作”列的“识别结果”查看识别结果。

在页面左上角，识别任务名称选择Test_OBS、资产类型选择OBS、资产名称选择全部资产，筛选OBS敏感数据识别结果。

步骤10 在目标扫描对象所在行的“操作”列，单击“查看分类分级结果详情”，进入“分类分级结果详情”弹框，如图2-1所示。

图 2-1 分类分级结果详情

分类分级结果详情
×

识别对象详情

对象名称 111多项命中res.txt 对象路径/采集时间 空目录/OBS识别/111多项命中res.txt

资产名称 [redacted] 资产类型 OBS

分级结果 L4

结果详情 样例数据

添加规则

匹配规则	命中数	分级结果	分类结果	分类分...	操作
国籍	5	L2	个人一般信息	华为云数据...	替换 移除
生日	5	L2	个人一般信息	华为云数据...	替换 移除
时间	4	L1	时间信息	华为云数据...	替换 移除
企业类型	2	L1	公开披露信息	华为云数据...	替换 移除
OS类型	1	L1	系统网络信息	华为云数据...	替换 移除
婚姻状况	1	L4	个人私密信息	华为云数据...	替换 移除
加密私钥	1	L4	密钥凭证信息	华为云数据...	替换 移除
邮箱	1	L3	个人一般信息	华为云数据...	替换 移除
SSL Certifi...	1	L3	密钥凭证信息	华为云数据...	替换 移除
RSA私钥	1	L4	密钥凭证信息	华为云数据...	替换 移除

总条数: 14 10 < 1 2 >

1. 在异常告警列表中，根据风险等级查看异常情况，排查是否存在高风险事件。具体操作请参见[OBS使用审计](#)。
2. 在OBS控制台，针对存在风险的桶或文件，修改读写权限。具体操作请参见[桶策略](#)。

----结束

3 API 数据安全防护最佳实践

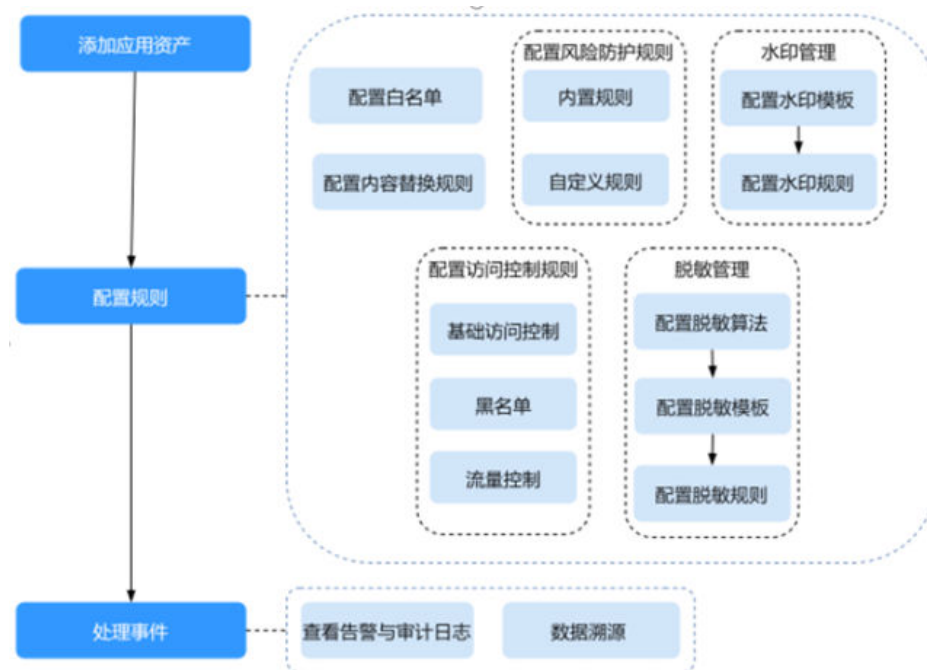
3.1 系统功能配置及使用场景举例

3.1.1 系统快速使用指南

本文介绍API数据安全防护的功能使用流程，帮助您快速了解和使用API数据安全防护。

API数据安全防护的使用流程图和流程介绍如下图3-1所示。

图 3-1 使用流程



步骤一：添加应用资产

在使用各功能之前，您需要将需要防护的应用添加到系统中。

- 步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2 在左侧导航栏，选择“资产中心 > 应用服务”。
- 步骤3 单击“添加”。
- 步骤4 在“添加应用资产”对话框中，设置资产信息。

图 3-2 添加应用资产

添加应用资产

智能填写: 172.16.43.51:8182 识别

* 应用名称: demo

* 服务:

访问地址: 172.16.43.51:46586

协议: http

WebSocket:

服务名: http://172.16.43.51:46586

* 访问路径: /
访问路径需以"/"开始和结尾, 例: "/api/"

* 源站协议: http https

* 源站地址: IP 域名

172.16.43.51:8182

IPv4地址示例: 172.16.43.51:8080
IPv6地址示例: [fe80::fb0a:24d9:d772:1cca]:8080

源站路径: 请输入
源站路径需以"/"开始和结尾, 例: "/api/"

* 负载均衡策略: 轮询 IP Hash 随机 最小连接

取消 确定

表 3-1 添加应用资产

参数	说明
智能填写	将应用服务器原始URL复制到此处，单击“识别”，可智能识别并填写各项参数。
应用名称	自定义设置应用服务的名称。
服务-访问地址	填写客户端用户最终访问的地址，与应用协议绑定。 <ul style="list-style-type: none"> ● 如果填写域名（例如example.com），无需填写端口。配置后访客通过该域名代理访问应用资产。 ● 如果填写域名，需要修改域名和IP的映射关系，使该域名解析到API数据安全防护的IP。正常情况下修改DNS中域名与IP的映射关系；没有DNS时或者测试时，可以通过修改客户端的hosts文件，使域名解析到API数据安全防护的IP。 ● 如果填写IP，则填写API数据安全防护的IP与代理端口，端口可配置为1~65535范围内的空闲端口。配置后，访客通过该IP + 端口号即可代理访问应用资产。
服务-协议	<ul style="list-style-type: none"> ● 选择API数据安全防护服务器的代理协议。 ● 如果选择https，需要在证书选择下拉框中选择证书。
证书选择	如果“应用协议”选择“https”，需要在“应用证书”下拉框中选择证书。在此之前，需要在证书管理页面上传或制作证书。具体操作请参见 证书管理 。
访问路径	代理路径，客户端访问地址url的前缀。
源站协议	选择源站协议，即应用原地址所用协议。
源站地址	选择源站地址的类型，包括ip与域名。 <ul style="list-style-type: none"> ● 如果源站地址为ip，则输入应用服务器原始IP地址，即服务端原本的地址（例如图中的172.16.35.53+端口号）。 ● 如果源站地址为域名，则输入应用服务器原始域名。
DNS服务器	如果源站地址选择域名，则需要输入代理服务器DNS地址。
服务端IP	如果源站地址选择域名，不输入DNS地址也可以输入服务端IP。
源站路径	源站url的前缀。
负载均衡策略	选择代理访问的负载均衡策略，当源站地址有多个时将采用配置的负载均衡策略进行访问。
启用状态	选择是否启用该应用代理服务。

步骤5 单击“确定”。

步骤6 添加完成后，访客通过配置的应用域名/IP（例如example.com）可对应用进行代理访问。

图 3-3 应用资产列表

应用名称	代理协议	访问地址	源协议	源应用域名/IP	授权状态	操作
demo	http	172.16.43.57:8182/	http	172.16.194.36:5000	<input checked="" type="checkbox"/>	编辑 删除

----结束

步骤二：配置规则

您可以直接配置审计与防护策略，也可以根据审计日志的风险点设置审计与防护策略。策略配置完成后，开启对应策略，将对应用数据资产开启针对性的防护与审计。

- 配置白名单，请参见[创建白名单](#)。
- 配置访问控制规则，请参见[访问控制](#)。
- 配置风险防护规则，请参见[添加自定义规则](#)和[启用内置规则](#)。
- 配置内容替换规则，请参见[添加内容替换规则](#)。
- 配置脱敏规则，请参见[添加脱敏规则](#)。
- 配置水印规则，请参见[添加水印规则](#)。
- 在告警或检索页面配置策略，请参见[告警页面配置策略](#)和[检索页面配置策略](#)。

步骤三：处理事件

- 配置完成后，系统根据审计策略审计资产，自动生成审计日志和告警信息，具体操作，请参见[查看审计日志信息](#)和[查看告警信息](#)。
- 您可以使用水印溯源功能追溯数据外泄事件，从而定位到相关责任人进行追责，具体操作，请参见[执行水印溯源](#)。

3.1.2 应用代理连接配置

API数据安全防护支持反向代理部署方式。客户端的访问请求转发到API数据安全防护，由API数据安全防护解析请求后，转发到应用服务器，应用服务器返回的数据同样经过API数据安全防护后返回给客户端PC。本举例为用户展示API数据安全防护代理连接的操作过程。

组网需求

API数据安全防护的组网配置情况如下[图3-4](#)所示。

图 3-4 反向代理组网

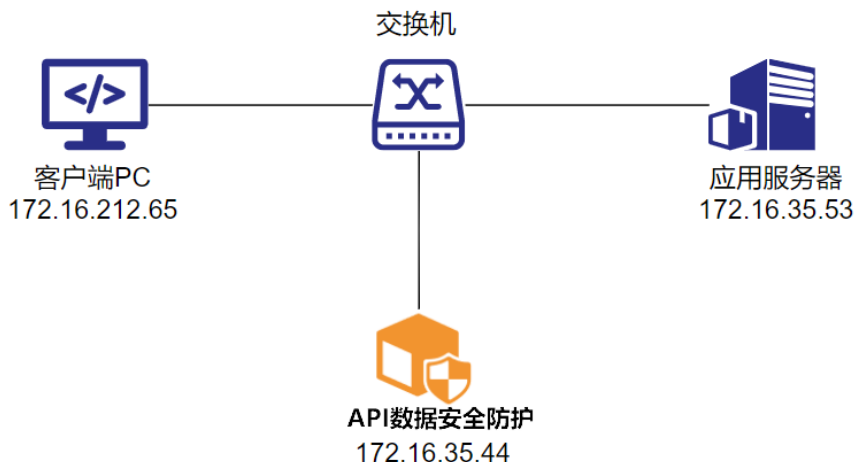


表 3-2 组网说明

设备	说明
客户端PC	IP地址： 172.16.212.65
API数据安全防护	IP地址： 172.16.35.44
应用服务器	IP地址： 172.16.35.53

直接访问应用

在进行代理连接前，直接在浏览器输入应用原始URL进行访问（http://172.16.35.53:8182），示例如图3-5所示。

图 3-5 直接访问应用



操作步骤

步骤1 使用系统管理员sysadmin账号登录API数据安全防护系统web控制台。

步骤2 在左侧导航栏，选择“资产中心 > 应用服务”，进入“应用服务”页面。

步骤3 单击右上角的“添加”，在弹出的对话框中输入相关信息，参数配置如表3-3所示。

图 3-6 添加应用资产

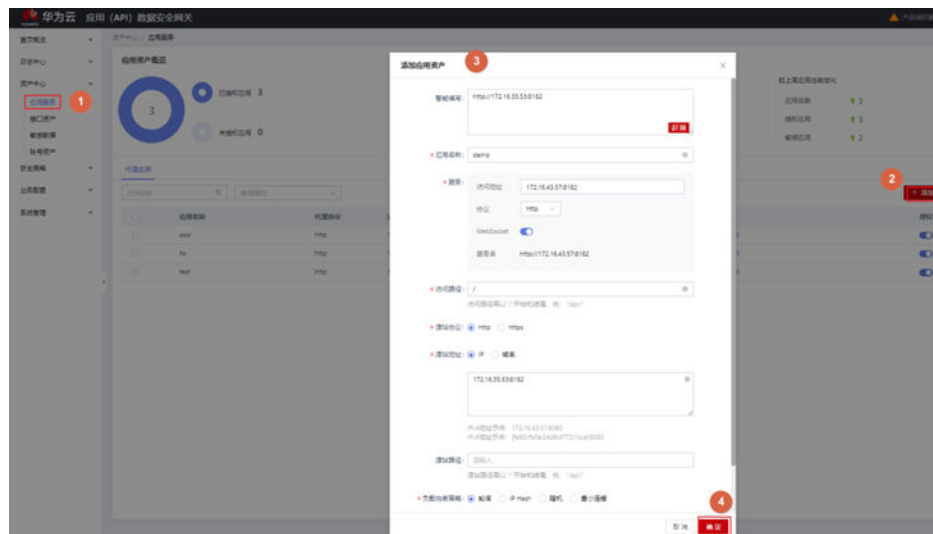


表 3-3 参数说明

参数	说明
智能填写	将应用服务器原始URL复制到此处，单击识别，可智能识别并填写各项参数。
应用名称	自定义设置应用服务的名称。
服务-访问地址	填写客户端用户最终访问的地址，与应用协议绑定。 <ul style="list-style-type: none"> ● 如果填写域名（例如example.com），无需填写端口。配置后访客通过该域名代理访问应用资产。 ● 如果填写域名，需要修改域名和IP的映射关系，使该域名解析到API数据安全防护的IP。正常情况下修改DNS中域名与IP的映射关系；没有DNS时或者测试时，可以通过修改客户端的hosts文件，使域名解析到API数据安全防护的IP。 ● 如果填写IP，则填写API数据安全防护的IP与代理端口，端口可配置为1~65535范围内的空闲端口。配置后，访客通过该IP + 端口号即可代理访问应用资产。
服务-协议	<ul style="list-style-type: none"> ● 选择API数据安全防护服务器的代理协议。 ● 如果选择https，需要在证书选择下拉框中选择证书。
证书选择	如果应用协议选择https，需要在应用证书下拉框中选择证书。在此之前，需要在证书管理页面上传证书。具体操作，请参见 证书管理 。
访问路径	代理路径，客户端访问地址url的前缀。
源站协议	选择源站协议，即应用原地址所用协议。

参数	说明
源站地址	选择源站地址的类型，包括ip与域名。 <ul style="list-style-type: none"> 如果源站地址为ip，则输入应用服务器原始IP地址，即服务端原本的地址（例如图中的172.16.35.53+端口号）。 如果源站地址为域名，则输入应用服务器原始域名。
DNS服务器	如果源站地址选择域名，则需要输入代理服务器DNS地址。
服务端IP	如果源站地址选择域名，不输入DNS地址也可以输入服务端IP。
源站路径	源站url的前缀。
负载均衡策略	选择代理访问的负载均衡策略，当源站地址有多个时将采用配置的负载均衡策略进行访问。
启用状态	选择是否启用该应用代理服务。
高级配置	如果源站应用系统有高级认证，可在此处配置应用请求头中的host、Referer、origin、编码（Content-Encoding）参数，并可配置最大请求体来限制发送。

步骤4 配置完成后，单击“确定”，保存应用资产。

----结束

验证代理配置效果

在浏览器地址栏中输入添加应用时配置的应用域名/IP（例如example.com），如下图3-7所示，表示成功通过代理访问应用。

图 3-7 代理访问应用



3.1.3 白名单配置

API数据安全防护支持配置白名单策略。命中白名单策略的访问会被放行，访问的风险等级被标记为可信。

组网需求

API数据安全防护的组网配置情况如下图3-8所示。

图 3-8 反向代理组网

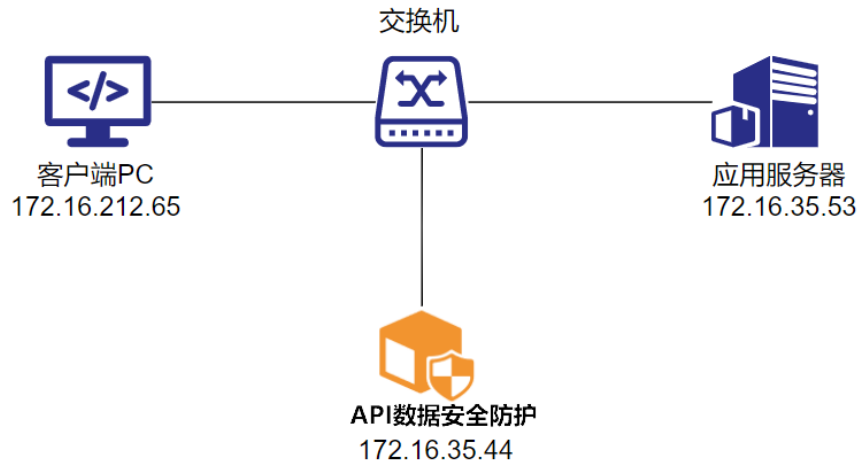


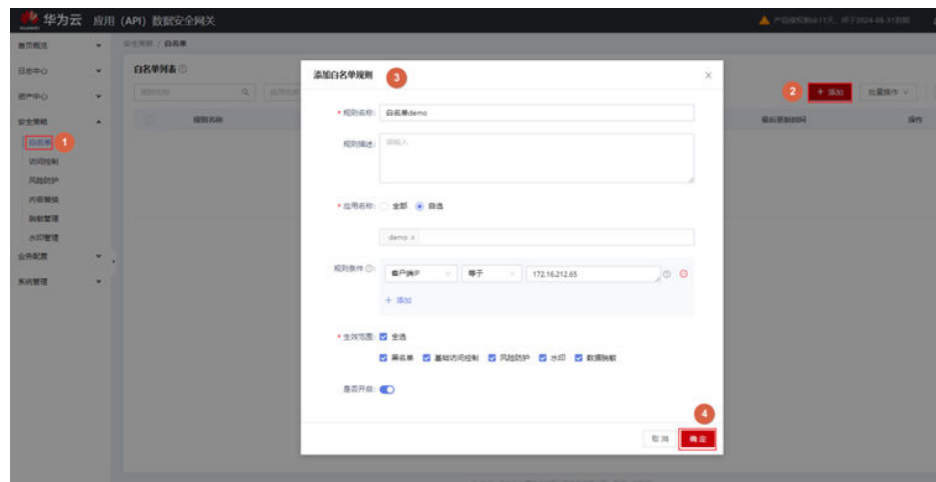
表 3-4 组网说明

设备	说明
客户端PC	IP地址: 172.16.212.65
API数据安全防护	IP地址: 172.16.35.44
应用服务器	IP地址: 172.16.35.53

配置白名单

配置白名单之前，确保您已添加应用资产，具体操作请参见[添加代理应用](#)；确保未开启与白名单冲突的规则。配置白名单流程如下[图3-9](#)所示。

图 3-9 配置白名单



步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

- 步骤2 在左侧导航栏，选择“安全策略 > 白名单”。
- 步骤3 单击右上角的“添加”。
- 步骤4 在添加白名单规则对话框中，配置白名单，如图3-9所示。
- 步骤5 配置完成后，单击“确定”，保存白名单。

----结束

验证白名单配置效果

- 步骤1 以客户端IP“172.16.212.65”在浏览器地址栏中输入应用的代理连接IP+端口（172.16.35.44:8182），通过代理连接IP+端口访问应用资产。
- 步骤2 使用系统管理员sysadmin账号登录API数据安全防护系统web控制台。
- 步骤3 在左侧导航栏选择“日志中心 > 检索”。
- 步骤4 检索列表中出现相应的访问放行记录，访问的风险等级被标记为可信，表示白名单配置生效。

----结束

3.1.4 黑名单配置

API数据安全防护支持配置黑名单策略。命中黑名单策略的访问会被阻断；命中黑名单策略的审计日志，其风险等级会标记为非法。

组网需求

API数据安全防护的组网配置情况如下图3-10所示。

图 3-10 反向代理组网

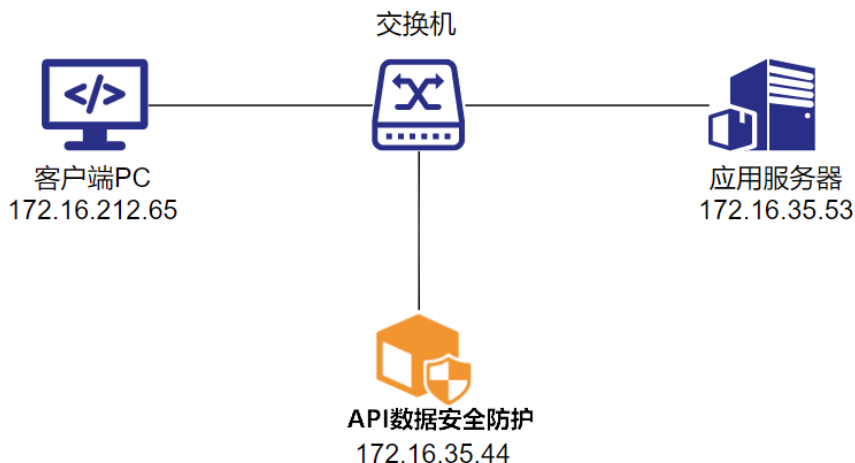


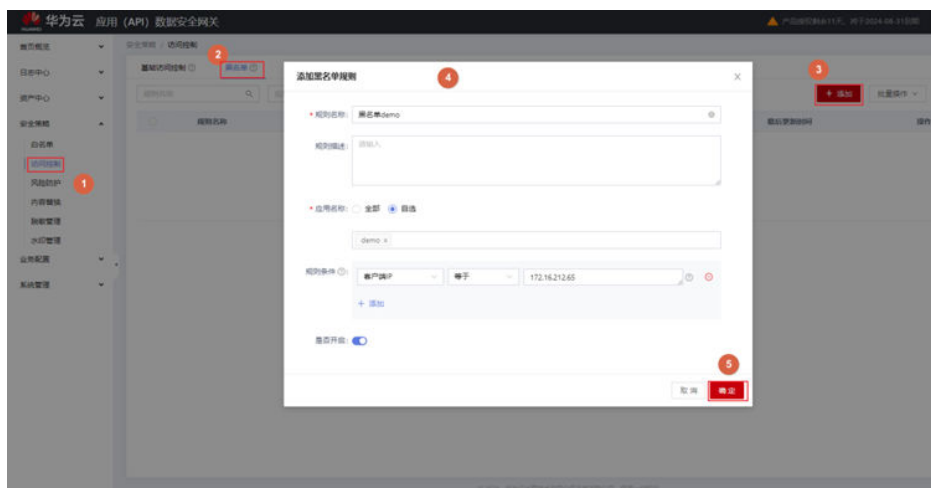
表 3-5 组网说明

设备	说明
客户端PC	IP地址：172.16.212.65
API数据安全防护	IP地址：172.16.35.44
应用服务器	IP地址：172.16.35.53

配置黑名单

配置黑名单之前，确保您已添加应用资产，具体操作请参见[添加代理应用](#)；确保未开启与黑名单冲突的规则。配置黑名单流程如下[图3-11](#)所示。

图 3-11 配置黑名单



步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“安全策略 > 访问控制”。

步骤3 单击“黑名单”页签，单击右上角的“添加”。

步骤4 在添加白名单规则对话框中，配置黑名单，如[图3-11](#)所示。

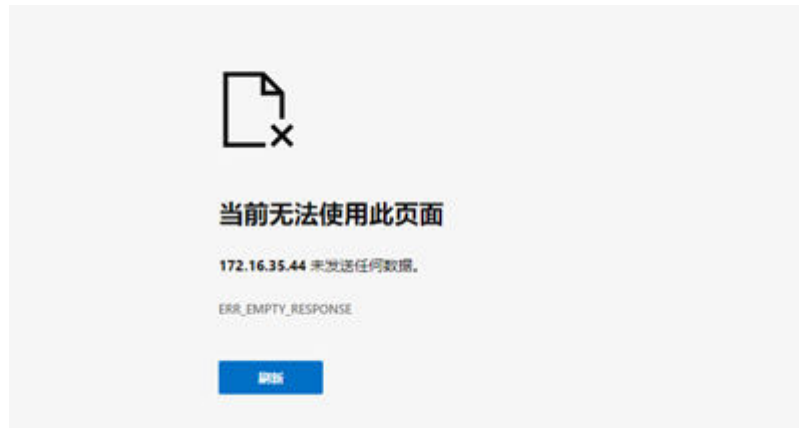
步骤5 配置完成后，单击“确定”，保存黑名单。

----结束

验证黑名单配置效果

步骤1 以客户端IP“172.16.212.65”在浏览器地址栏中输入应用的代理连接IP+端口（172.16.35.44:8182），通过代理连接IP+端口访问应用资产。如果访问被阻断，表示黑名单配置生效。示例如下图所示。

图 3-12 访问被阻断



步骤2 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤3 在“日志中心 > 告警页面”找到目标请求记录，单击“详情”。

步骤4 请求匹配到所配置的黑名单规则，访问的风险等级被标记为非法，表示黑名单配置生效。

----结束

3.1.5 脱敏规则配置

API数据安全防护支持通过配置脱敏规则，对接口中的敏感数据进行脱敏。本举例为用户展示API数据安全防护通过配置脱敏规则对访问采取脱敏响应的操作过程。

组网需求

API数据安全防护的组网配置情况如[图3-13](#)所示。

图 3-13 反向代理组网

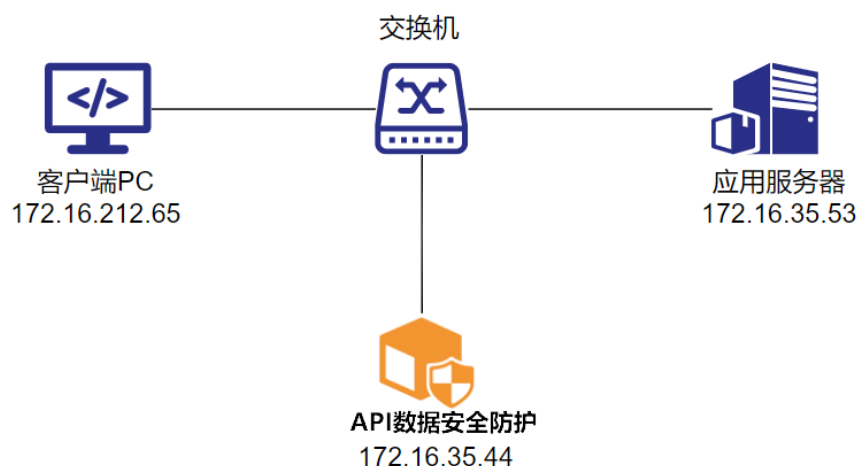


表 3-6 组网说明

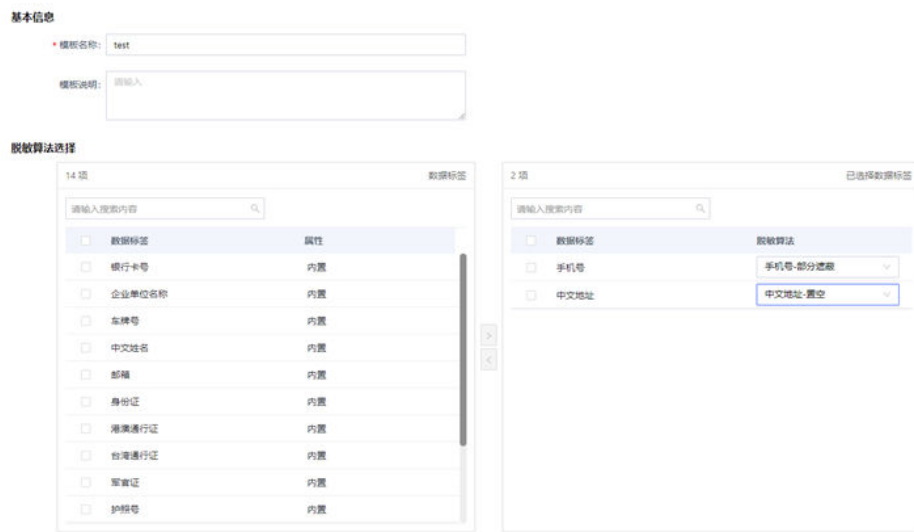
设备	说明
客户端PC	IP地址：172.16.212.65
API数据安全防护	IP地址：172.16.35.44
应用服务器	IP地址：172.16.35.53

(可选) 配置脱敏模板

在配置自定义脱敏规则前，可配置脱敏模板，便于在配置脱敏规则时直接引用。

- 步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2 在左侧导航栏，选择“安全策略 > 脱敏管理”，并单击“脱敏模板”页签。
- 步骤3 在页面右上角，单击“添加模板”。
- 步骤4 在行业模板页面配置脱敏模板具体信息，如[图3-14](#)所示。

图 3-14 配置脱敏模板流程



- 步骤5 脱敏模板配置完成后，单击“保存”。

----结束

配置脱敏规则

配置脱敏规则之前，确保您已添加应用资产，具体操作请参见[应用服务](#)；确保未开启与脱敏规则冲突的规则。

- 步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。
- 步骤2 在左侧导航栏，选择“安全策略 > 脱敏管理”，单击“脱敏规则”页签。
- 步骤3 单击页面右上角的“添加”。

步骤4 在添加脱敏规则对话框中，配置脱敏规则。本示例按模板进行脱敏，如下图3-15所示。

图 3-15 配置脱敏规则

步骤5 配置完成后，单击“确定”。

----结束

验证脱敏规则配置效果

步骤1 在客户端浏览器地址栏中输入应用的代理连接IP+端口（172.16.35.44:8182），通过代理连接IP+端口访问应用资产。响应的敏感数据被脱敏，表示脱敏规则配置生效。示例如下图3-16所示。

图 3-16 验证脱敏效果



步骤2 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤3 在“日志中心 > 检索”页面，中找到目标请求记录，单击“详情”。请求匹配到所配置的脱敏规则，表示脱敏规则配置生效。

----结束

3.1.6 水印规则配置

本举例为用户展示API数据安全防护配置水印规则，为页面添加文字水印的操作过程。

组网需求

API数据安全防护的组网配置情况如下[图3-17](#)所示。

图 3-17 反向代理组网

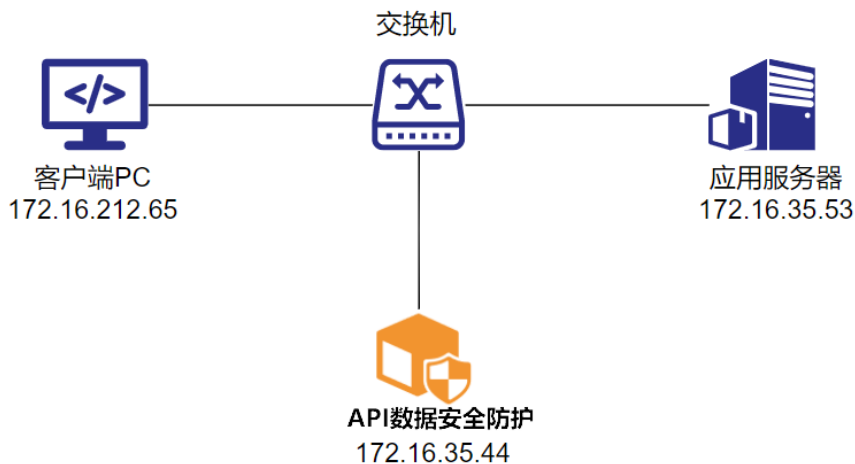


表 3-7 组网说明

设备	说明
客户端PC	IP地址：172.16.212.65

设备	说明
API数据安全防护	IP地址：172.16.35.44
应用服务器	IP地址：172.16.35.53

配置水印模板

在配置自定义水印规则前，需要配置水印模板，便于在配置水印规则时引用。

步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“安全策略 > 水印管理”，单击“水印模板”页签。

步骤3 在页面右上角，单击“添加”。

步骤4 在“添加水印模板”页面配置水印模板具体信息，如[图3-18](#)所示。

图 3-18 配置水印模板

[返回](#)

* 名称:

描述:

* 水印类型: 网页水印 数据水印 文档水印 文档暗水印 点阵水印

水印内容: 时间 IP 用户名 应用名称 自定义内容

字体大小: 14 (12-32)

显示方式: 平铺 固定

间距:

倾斜角度:

字体颜色:

不透明度: 20%

步骤5 水印模板配置完成后，单击“保存”。

----结束

配置水印规则

配置水印规则之前，确保您已添加应用资产，具体操作请参见[应用服务](#)，确保未开启与水印规则冲突的规则。

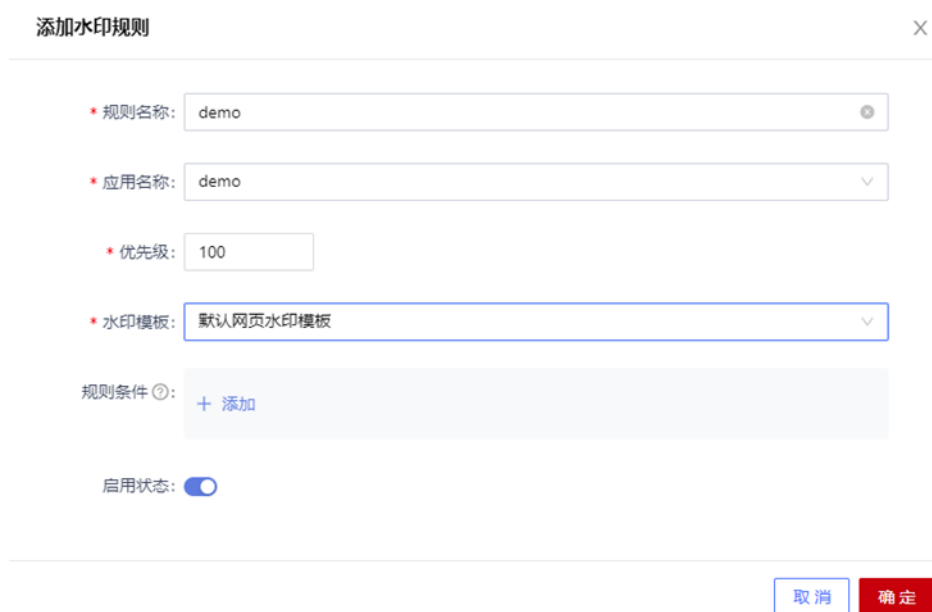
步骤1 使用系统管理员sysadmin账号[登录API数据安全防护系统web控制台](#)。

步骤2 在左侧导航栏，选择“安全策略 > 水印管理”，单击“水印规则”页签。

步骤3 单击页面右上角的“添加”。

步骤4 配置水印规则，示例如下[图3-19](#)所示。

图 3-19 配置水印规则



添加水印规则

* 规则名称: demo

* 应用名称: demo

* 优先级: 100

* 水印模板: 默认网页水印模板

规则条件: + 添加

启用状态:

取消 确定

步骤5 配置完成后，单击“确定”。

----结束

验证水印规则配置效果

在客户端浏览器地址栏中输入应用的代理连接IP+端口（172.16.35.44:8182），通过代理连接IP+端口访问应用资产。响应页面出现文字水印，表示水印规则配置生效。示例如[图3-20](#)所示。

图 3-20 页面水印



登录API数据安全防护Web控制台，在“日志中心 > 检索页面”，找到目标请求记录，单击“详情”。请求匹配到所配置的水印规则，表示水印规则配置生效。