

管理检测与响应

用户指南

文档版本 47
发布日期 2024-03-30



版权所有 © 华为云计算技术有限公司 2024。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。

目录

1 购买管理检测与响应	1
1.1 购买企业版.....	1
1.2 购买等保建设助手.....	2
1.3 购买 DDoS 攻击缓解助手.....	5
1.4 购买专项版.....	7
1.5 购买密评建设助手.....	9
2 下载管理检测与响应报告	12
3 验收管理检测与响应	13
4 评价管理检测与响应	15
5 查看服务单信息	16
6 权限管理	18
6.1 创建用户并授权使用 MDR.....	18
7 云审计服务	20
7.1 云审计服务支持的 MDR 操作列表.....	20
7.2 查看云审计日志.....	20

1 购买管理检测与响应

1.1 购买企业版

企业版管理检测与响应结合企业业务场景，通过云服务方式，提供华为云安全标准化的运维运营服务。帮助企业与机构实现对安全风险与安全事件的有效监控，并及时采取有效措施持续降低安全风险并消除安全事件带来的损失。


在购买时，您只需要选择“资源数”和“公司名称”。购买服务成功后，华为云安全专家团队将快速响应并结合您业务实际情况，提供华为云安全标准化的运维运营服务。

购买须知

- 购买实例的账号需具有“SES Administrator”和“BSS Administrator”角色。
 - SES Administrator：管理检测与响应服务的管理员权限。
 - BSS Administrator：对账号中心、费用中心、资源中心中的所有菜单项执行任意操作。项目级策略，在同项目中勾选。
- 企业版价格与项目实际情况、IT系统所在地息息相关，费用仅做参考。
- 购买前，请拨打950808或直接联系您的客户经理，确定项目报价后再下单。
- 该订单服务周期为1年，订单下单后1年将自动失效；订单失效后将不再提供相关服务。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 管理检测与响应服务”。

步骤3 在“企业版”下方，单击“立即购买”，进入“购买MDR服务”界面。

图 1-1 选择企业版



企业版

结合企业业务场景，通过云服务方式，提供华为云安全标准化的运维运营服务。

立即购买

步骤4 设置“资源数”、“公司名称”并勾选“我已正确设置服务单消息通知接收人”。

资源数：需要进行检测的服务器数量和网站数量。从购买日起，服务有效期为1年。

图 1-2 设置信息

服务版本 企业版 等保建设助手 密评建设助手

服务类型

企业版	
服务内容	
网站安全体检	主机安全体检
安全加固指导	安全监测服务
应急响应服务	安全配置服务
安全防护服务开通与部署	定期策略更新与维护
安全漏洞预警服务	主动安全预警服务
安全设备维护服务	漏洞管理服务

资源数

服务周期 1年

公司名称

我确认 我已正确设置服务单消息通知接收人。
您可以前往 [消息中心](#) 配置消息接收人。服务单进账消息会通知到消息中心“服务单提醒”项所配置的接收人。如果您不进行设置将会默认通知到您注册账号的联系方式。

步骤5 在页面右下方，单击“下一步”。

步骤6 确认订单无误并阅读《管理检测与响应免责声明》和《隐私政策声明》后，勾选“我已阅读并同意《管理检测与响应免责声明》和《隐私政策声明》”，单击“去支付”。

步骤7 在“支付”页面，请选择付款方式进行付款。

步骤8 付款成功后，单击“返回管理检测与响应控制台”，返回到“我的服务单”界面。

说明

购买成功后，管理检测与响应将在1个工作日内联系您，与您沟通并结合您业务实际情况，提供华为云安全标准化的运维运营服务。

---结束

1.2 购买等保建设助手

等保建设助手为您提供等保定级和差距评估咨询，根据系统情况提供定级参考意见和相关技术建议书以及等保条款分析情况汇总，根据等保差距要求，服务类型以远程或现场方式提供安全加固建议。


购买时，您需要选择服务类型的数量，以及您的信息。在成功购买服务后，管理检测与响应团队将根据您IT系统的实际情况提供定级意见、差距分析以及安全加固建议。

购买须知

- 购买实例的账号需具有“SES Administrator”和“BSS Administrator”角色。
 - SES Administrator：管理检测与响应服务的管理员权限。
 - BSS Administrator：对账号中心、费用中心、资源中心中的所有菜单项执行任意操作。项目级策略，在同项目中勾选。
- 等保建设助手价格与项目实际情况、IT系统所在地息息相关，MDR管理控制台上提供的费用仅做参考。
- 购买前，请拨打950808或直接联系您的客户经理，确定项目报价后再下单。
- 该订单服务周期为1年，订单下单后1年将自动失效；订单失效后将不再提供相关服务。

立即购买

步骤1 [登录管理控制台](#)。

步骤2 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 管理检测与响应服务”。

步骤3 在“等保建设助手”下方，单击“立即购买”，进入“购买MDR服务”页面。

图 1-3 选择等保建设助手



等保建设助手

提供等保定级和差距评估咨询，根据系统情况提供定级参考意见和相关技术建议书以及等保条款分析情况汇总

[立即购买](#)

步骤4 选择服务类型“基础版”或“高级版”，并设置购买数量，如[图1-19](#)所示。

图 1-4 购买等保建设助手

服务版本

企业版
等保建设助手
密评建设助手

服务类型

基础版

服务内容

提供等保定级和差距评估咨询，根据系统情况提供定级参考意见和相关技术建议书以及等保条款分析情况汇总，等保安全加固方案：根据等级保护差距要求，远程方式提供安全加固建议

高级版

服务内容

提供等保定级和差距评估咨询，现场方式进行系统情况提供定级参考意见和相关技术建议书以及分析情况汇总，等保安全加固方案：根据等级保护差距要求，现场方式提供安全加固建议

基础版数量

-
0
+

服务周期

1次

⚠ 购买前，请拨打950808按1转1或直接联系您的客户经理，确定项目报价后再下单，谢谢！
 因等保建设助手价格与项目实际情况、IT系统所在地息息相关，费用仅供参考。
 该订单服务周期为1年，订单下单后1年将自动失效；订单失效后将不再提供相关服务。
 非公有云场景购买前，请联系等保售前经理，确定项目范围后再下单，谢谢！

公司名称

机构所在省市

--请选择--

--请选择--

行业属性

--请选择--

步骤5 设置用户相关信息，如图1-20所示，各参数说明如表1-4所示。

图 1-5 设置用户信息

公司名称

机构所在省市

--请选择--

--请选择--

行业属性

--请选择--

联系人姓名

联系人电话

+86 (中国)

联系人邮箱 (可选)

⚠ 您填写完整的联系人信息，用于接收项目进展和验收通知；如果您后续需要导出所填写的个人信息，您可以提工单申请导出，谢谢！

表 1-1 用户信息参数说明

参数	说明	配置样例
公司名称	输入公司的名称。	-
机构所在省市	选择公司所在的省市。	北京市
行业属性	选择行业的类型。	银行

参数	说明	配置样例
联系人姓名	输入真实的联系人姓名。	-
联系人电话	输入真实的联系人的联系电话。	-
联系人邮箱	输入真实的联系人的邮箱。	-

步骤6 在页面右下方，单击“下一步”。

步骤7 确认订单无误并阅读《管理检测与响应免责声明》和《隐私政策声明》后，勾选“我已阅读并同意《管理检测与响应免责声明》和《隐私政策声明》”，单击“去支付”。

步骤8 在“支付”页面，请选择付款方式进行付款。

步骤9 付款成功后，单击“返回管理检测与响应控制台”，返回到“我的服务单”界面。

📖 说明

购买成功后，管理检测与响应将在1个工作日内联系您，与您沟通确定等保需求。

----结束

1.3 购买 DDoS 攻击缓解助手

DDoS攻击缓解助手面向有DDoS攻击风险的客户，提供专家建议和DDoS服务规格、配置以及防御策略的参考方案。


购买时，您需要选择服务类型的数量，以及您信息。在成功购买服务后，管理检测与响应团队将根据您IT系统的实际情况提供定级意见、差距分析以及安全加固建议。

购买须知

- 购买实例的账号需具有“SES Administrator”和“BSS Administrator”角色。
 - SES Administrator：管理检测与响应服务的管理员权限。
 - BSS Administrator：对账号中心、费用中心、资源中心中的所有菜单项执行任意操作。项目级策略，在同项目中勾选。
- DDoS攻击缓解助手价格与项目实际情况、IT系统所在地息息相关，MDR管理控制台上提供的费用仅做参考。
- 购买前，请拨打950808或直接联系您的客户经理，确定项目报价后再下单。
- 该订单服务周期为1年，订单下单后1年将自动失效；订单失效后将不再提供相关服务。

立即购买

步骤1 [登录管理控制台](#)。

步骤2 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 管理检测与响应服务”。

步骤3 在“DDoS攻击缓解助手”下方，单击“立即购买”，进入“购买MDR服务”页面。

步骤4 选择服务类型“标准助手”、“专业助手”或“值守助手”，并设置购买数量，如图1-6所示。

图 1-6 购买 DDOS 攻击缓解助手

服务版本：企业版 | 等保建设助手 | **DDoS攻击缓解助手** | 密评建设助手

服务类型：
标准助手
 服务内容：针对客户业务系统，以及风险等级（如历史攻击情况、勒索细节等信息）给出专项配置调优。所需增加的DDoS防护服务费用不在防DDoS缓解助手专业版内。
专业助手
 服务内容：DDoS防护服务配置开通 客户根据“DDoS防护服务推荐”方案完成服务选购后，帮助客户完成DDoS防护方案的配置。确保DDoS防护方案有效执行。根据客户的业务场景和风险评估，给出DDoS防护的产品套餐方案，例如如何选择华为云DDoS高防包，防护IP个数、保底带宽选择等。

标准助手数量：- 0 +

服务周期：**1次**

❗ 购买前，请拨打950808按1转1或直接联系您的客户经理，确定项目报价后再下单，谢谢！因等保建设助手价格与项目实际情况、IT系统所在地息息相关，费用仅作参考。

❗ 该订单服务周期为1年，订单下单后1年将自动失效；订单失效后将不再提供相关服务。

❗ 非公有云场景购买前，请联系等保售前经理，确定项目范围后再下单，谢谢！

步骤5 设置用户相关信息，各参数说明如表1-2所示。

图 1-7 设置用户信息

* 公司名称

* 机构所在省市

* 行业属性

* 联系人姓名

* 联系人电话

联系人邮箱

❗ 您填写完整的联系人信息，用于接收项目进展和验收通知；如果您后续需要导出所填写的个人信息，您可以提工单申请导出。谢谢！

表 1-2 用户信息参数说明

参数	说明	配置样例
公司名称	输入公司的名称。	-

参数	说明	配置样例
机构所在省市	选择公司所在的省市。	北京市
行业属性	选择行业的类型。	银行
联系人姓名	输入真实的联系人姓名。	-
联系人电话	输入真实的联系人的联系电话。	-
联系人邮箱	输入真实的联系人的邮箱。	-

步骤6 在页面右下方，单击“下一步”。

步骤7 确认订单无误并阅读《管理检测与响应免责声明》和《隐私政策声明》后，勾选“我已阅读并同意《管理检测与响应免责声明》和《隐私政策声明》”，单击“去支付”。

步骤8 在“支付”页面，请选择付款方式进行付款。

步骤9 付款成功后，单击“返回管理检测与响应控制台”，返回到“我的服务单”界面。

说明

购买成功后，管理检测与响应将在1个工作日内联系您，与您沟通确定等保需求。

----结束

1.4 购买专项版

专项版服务内容包括业务信息收集、安全保障方案制定、安全自查与整改、安全防护加固、安全团队建设、现场+远程监控及响应、安全服务保障总结。


购买时，您需要选择服务类型的数量，以及您的信息。在成功购买服务后，管理检测与响应团队将根据您IT系统的实际情况提供定级意见、差距分析以及安全加固建议。

购买须知

- 购买实例的账号需具有“SES Administrator”和“BSS Administrator”角色。
 - SES Administrator：管理检测与响应服务的管理员权限。
 - BSS Administrator：对账号中心、费用中心、资源中心中的所有菜单项执行任意操作。项目级策略，在同项目中勾选。
- 专项版价格与项目实际情况、IT系统所在地息息相关，MDR管理控制台上提供的费用仅做参考。
- 购买前，请拨打950808或直接联系您的客户经理，确定项目报价后再下单。
- 该订单服务周期为1年，订单下单后1年将自动失效；订单失效后将不再提供相关服务。

立即购买

步骤1 [登录管理控制台](#)。

步骤2 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 管理检测与响应服务”。

步骤3 在“专项版”下方，单击“立即购买”，进入“购买MDR服务”页面。

步骤4 选择服务类型“云会议安全保障”或“特技安全保障”，并设置购买数量，如图1-8所示。

图 1-8 购买专项版



步骤5 设置用户相关信息，参数说明如表1-3所示。

表 1-3 用户信息参数说明

参数	说明	配置样例
公司名称	输入用户公司的名称。	-
我确认	用户已正确设置服务单消息通知接收人。	-

步骤6 在页面右下方，单击“下一步”。

步骤7 确认订单无误并阅读《管理检测与响应免责声明》和《隐私政策声明》后，勾选“我已阅读并同意《管理检测与响应免责声明》和《隐私政策声明》”，单击“去支付”。

步骤8 在“支付”页面，请选择付款方式进行付款。

步骤9 付款成功后，单击“返回管理检测与响应控制台”，返回到“我的服务单”界面。

说明

购买成功后，管理检测与响应将在1个工作日内联系您，与您沟通确定需求。

----结束

1.5 购买密评建设助手

密评建设助手提供“密评”合规、国密改造、密码安全评估咨询服务，根据密码应用情况提供密码合规参考意见、相关技术建议书以及密评条款分析情况汇总。


在购买时，您需要选择服务类型的数量，以及您的信息。在成功购买服务后，管理检测与响应团队将为客户量身定制等保合规整改方案，指导客户进行安全服务的选型和部署，对您的网络、主机、数据库、安全管理制度等进行整改，优选具有资质的权威等保测评机构，提供专业的测评服务。

购买须知

- 购买实例的账号需具有“SES Administrator”和“BSS Administrator”角色。
 - SES Administrator：管理检测与响应服务的管理员权限。
 - BSS Administrator：对账号中心、费用中心、资源中心中的所有菜单项执行任意操作。项目级策略，在同项目中勾选。
- 密评建设助手价格与项目实际情况、IT系统所在地息息相关，费用仅做参考。
- 购买前，请拨打950808或直接联系您的客户经理，确定项目报价后再下单。
- 该订单服务周期为1年，订单下单后1年将自动失效；订单失效后将不再提供相关服务。

立即购买

步骤1 [登录管理控制台](#)。

步骤2 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 管理检测与响应服务”。

步骤3 在“密评建设助手”下方，单击“立即购买”，进入“购买MDR服务”界面。

图 1-9 选择密评建设助手



密评建设助手

提供“密评”合规、国密改造、密码安全评估咨询服务，根据密码应用情况提供密码合规参考意见、相关技术建议书以及密评条款分析情况汇总

立即购买

步骤4 选择服务类型“标准版”，并设置数量，如[图1-10](#)所示。

图 1-10 购买密评建设助手



服务版本：企业版、等保建设助手、**密评建设助手**

服务类型：**标准版**
服务内容：提供“密评”合规、国密改造、密码安全评估咨询服务，根据密码应用情况提供密码合规参考意见、相关技术建议书以及密评条款分析情况汇总

数量：- 0 +

计费模式：**一次性付款**

⚠️ 购买前，请拨打950808按1转1或直接联系您的客户经理，确定项目报价后再下单，谢谢！该订单服务周期为1年，订单下单后1年将自动失效；订单失效后将不再提供相关服务。

步骤5 设置用户相关信息，各参数说明如表1-4所示。

表 1-4 用户信息参数说明

参数	说明	配置样例
公司名称	输入公司的名称。	-
机构所在省市	选择公司所在的省市。	北京市
行业属性	选择行业的类型。	银行
系统类型	选择系统类型。 <ul style="list-style-type: none"> 公有云租户系统 线下IDC系统 	公有云租户系统
待测评系统等级	选择待测评系统等级。 <ul style="list-style-type: none"> 二级 三级 	二级
联系人姓名	输入真实的联系人姓名。	-
联系人电话	输入真实的联系人的联系电话。	-
被测评信息系统名称	输入被测评信息系统名称。	-
系统部署的服务器台数	输入系统部署的服务器台数。	-
联系人邮箱	输入真实的联系人的邮箱。	-

- 步骤6** 在页面右下方，单击“下一步”。
- 步骤7** 确认订单无误并阅读《管理检测与响应免责声明》和《隐私政策声明》后，勾选“我已阅读并同意《管理检测与响应免责声明》和《隐私政策声明》”，单击“去支付”。
- 步骤8** 在“支付”页面，请选择付款方式进行付款。
- 步骤9** 付款成功后，单击“返回管理检测与响应控制台”，返回到“我的服务单”界面。

 **说明**

购买成功后，管理检测与响应将在1个工作日内联系您，与您沟通确定等保需求。

---**结束**

2 下载管理检测与响应报告

操作场景


检测完成后，系统自动生成管理检测与响应服务报告，您会收到邮件和短信通知信息。您可在收到通知信息后下载管理检测与响应服务报告。

前提条件

服务完成，且服务单的状态为“待用户验收”或“已完成”。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 管理检测与响应服务”。

步骤3 在左侧菜单单击“服务列表”进入“支持与服务”。

步骤4 单击左侧菜单栏的“专业服务”，选择“专业服务 > 我的服务单”，在目标服务单“操作”列单击“验收”。

步骤5 在“服务单完成信息”区域，单击“下载”获取详细的管理检测与响应服务的报告。

同时也可在“处理日志”区域，单击“下载”查看服务单的过程交付件和管理检测与响应服务报告。

---结束

3 验收管理检测与响应

操作场景

服务完成后，您会收到短信通知信息。您可在收到短信通知起的10日内，对本次管理检测与响应服务进行验收。如果超出该时间范围，系统将对本次管理检测与响应服务进行自动验收。


须知

单击“立即验收”后，MDR服务默认此服务单已交付完成，验收后此服务单将不再提供服务。

前提条件

服务完成，且服务单的状态为“待用户验收”。

操作步骤

- 步骤1** [登录管理控制台](#)。
- 步骤2** 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 管理检测与响应服务”。
- 步骤3** 在左侧菜单单击“服务列表”进入“支持与服务”。
- 步骤4** 单击左侧菜单栏的“专业服务”，选择“专业服务 > 我的服务单”，在目标服务单“操作”列单击“验收”。
- 步骤5** 在“服务单完成信息”区域了解服务单的完成情况。
您可以单击“下载”获取详细的服务报告。
- 步骤6** 验收服务单。
 - 如果服务单满足交付要求，请单击“立即验收”。

须知

单击“立即验收”后，MDR服务默认此服务单已交付完成，验收后此服务单将不再提供服务。

- 如果服务单不满足交付要求，请单击“验收延期”，并填写延期原因。

📖 说明

- 您需要在收到验收请求后于10个自然日内完成验收。如您在此期间未验收，系统将自动进行验收。
- 延期验收，每延期一次，验收时长将增加10个工作日，最多可延期三次。

----结束

4 评价管理检测与响应

操作场景


管理检测与响应完成后，您会收到短信通知信息。您可在收到短信通知后，对本次管理检测与响应服务进行评价，并反馈建议或意见。

前提条件

- 管理检测与响应完成且服务单状态为“已完成”。
- 已验收管理检测与响应。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 管理检测与响应服务”。

步骤3 在左侧菜单单击“服务列表”进入“支持与服务”。

步骤4 单击左侧菜单栏的“专业服务”，选择“专业服务 > 我的服务单”，在目标服务单“操作”列单击“评价”。

步骤5 在“服务评价”区域对本次管理检测与响应服务进行维度评价。

服务维度包括：方案完善度、实施专业性、响应及时性。

须知

您提交评价意见后，该服务单的服务评价功能失效，您不能再次提交评价意见。

----结束

5 查看服务单信息

操作场景


该任务指导您在服务单列表查看服务单基础信息和处理进展。

前提条件

您已购买管理检测与响应并成功生成服务单。

操作步骤

步骤1 [登录管理控制台](#)。

步骤2 在页面上方选择“区域”后，单击 ，选择“安全与合规 > 管理检测与响应服务”。

步骤3 在左侧菜单单击“服务列表”进入“支持与服务”。

步骤4 单击左侧菜单栏的“专业服务”，选择“专业服务 > 我的服务单”，在目标服务单“操作”列单击“查看”，服务单状态说明如表5-1所示。

表 5-1 服务单状态参数说明

参数名称	说明
待处理	用户购买企业版管理检测与响应，服务单付款成功，服务单状态为“待处理”。
处理中	<ul style="list-style-type: none">用户购买企业版管理检测与响应，通过沟通联系并审核资质后，服务单状态为“处理中”。用户购买等保建设助手，服务单付款成功，服务单状态为“处理中”。
服务取消	华为云终止本次管理检测与响应，系统将服务单状态更新为“服务取消”。
待用户验收	管理检测与响应报告由管理检测与响应审核通过后，系统将服务单状态更新为“待用户验收”。


参数名称	说明
已完成	服务完成后，用户对本次管理检测与响应进行验收后，系统将服务单状态更新为“已完成”。

说明

服务单列表展示了您名下的所有服务单，以上服务单的状态说明为管理检测与响应服务单的状态说明。

步骤5 详情页面包含以下内容：

- 基础信息：服务单的产品信息、联系人信息、服务内容等。

您可以单击，修改联系人电话和邮箱。

- 服务单完成信息：服务总结、服务报告。
- 服务评价：方案完善度、实施专业性、响应及时性。
- 处理日志：服务单的历史处理进展。

对于服务单的过程交付件，您可以单击“下载”来获取。

说明

“服务单完成信息”和“服务评价”区域在管理检测与响应完成后，您进行验收时呈现。

----结束

6 权限管理

6.1 创建用户并授权使用 MDR

如果您需要对您所拥有的MDR进行精细的权限管理，您可以使用[统一身份认证服务](#)（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用MDR资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将MDR资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足用户的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用MDR服务的其它功能。

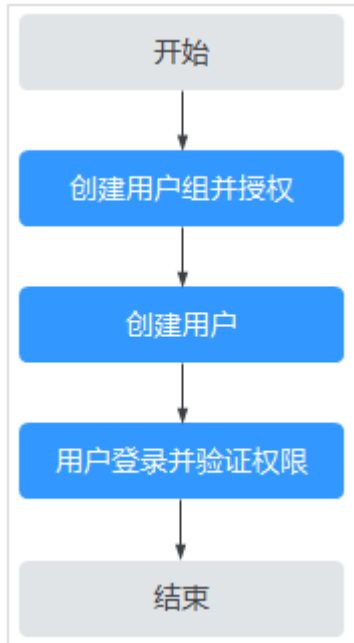
本章节为您介绍对您授权的方法。

前提条件

给用户组授权之前，请您了解用户组可以添加的MDR权限，并结合实际需求进行选择，MDR支持的系统权限，请参见：[MDR系统权限](#)。若您需要对除MDR之外的其它服务授权，IAM支持服务的所有权限请参见[系统权限](#)。

示例流程

图 6-1 给用户授予权限流程



1. **创建用户组并授权**
在IAM控制台创建用户组，并授予管理检测与响应权限“SES Administrator”。
2. **创建用户并加入用户组**
在IAM控制台创建用户，并将其加入1中创建的用户组。
3. **用户登录并验证权限**
新创建的用户登录控制台，切换至授权区域，验证权限：
验证方式（参考）：在“服务列表”中选择除管理检测与响应外（假设当前权限仅包含“SES Administrator”角色）的任一服务，若提示权限不足，表示“SES Administrator”已生效。

7 云审计服务

7.1 云审计服务支持的 MDR 操作列表

云审计服务（Cloud Trace Service, CTS）记录管理检测与响应相关的操作事件，方便您日后的查询、审计和回溯，详情请参见[云审计服务用户指南](#)。

云审计服务支持的MDR操作列表如[表7-1](#)所示。

表 7-1 云审计服务支持的 MDR 操作列表


操作名称	资源类型	事件名称
管理检测与响应-创建订单	PSDM	createMdrOrder
管理检测与响应-租户申请交付	PSDM	mdrCustomerApplication
租户侧上传附件	PSDM	customerUploadAccessory
租户侧下载指定模板文件	PSDM	customerDownloadTemplate
服务单附件下载	PSDM	downLoadAccessories
服务单验收通过	PSDM	professionalTicketsAcceptanceSuccess
服务单验收延期	PSDM	professionalTicketsAcceptanceExtend
服务单评价	PSDM	professionalTicketsEvaluate

7.2 查看云审计日志

开启了云审计服务后，系统开始记录管理检测与响应资源的操作。云审计服务管理控制台保存最近7天的操作记录。

查看 MDR 的云审计日志

步骤1 登录管理控制台。

步骤2 单击页面左上方的 ，选择“管理与部署 > 云审计服务”，进入云审计服务信息页面。

步骤3 单击左侧导航树的“事件列表”，进入事件列表信息页面。

步骤4 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：

- “事件类型”、“事件来源”、“资源类型”和“筛选类型”。

在下拉框中选择查询条件。

- “事件类型”选择“管理事件”。
- “事件来源”选择“PSDM”。
- “筛选类型”选择“事件名称”时，还需选择某个具体的事件名称；选择“资源ID”时，还需选择或者手动输入某个具体的资源ID；选择“资源名称”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”：可在页面右上角选择查询最近1小时、最近1天、最近1周及自定义时间段的操作事件。

步骤5 单击“查询”，查看对应的操作事件。


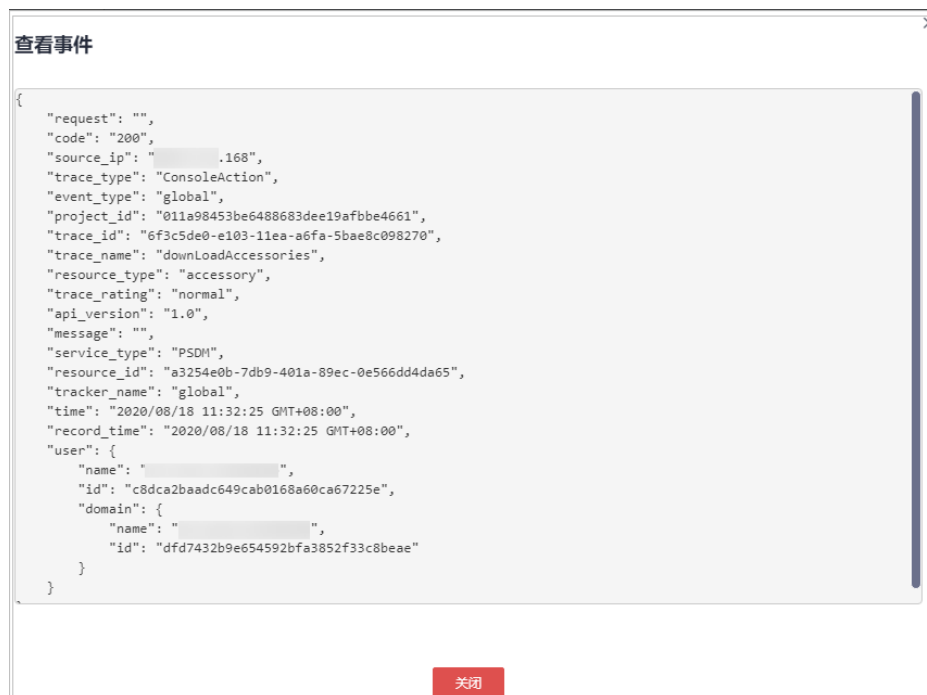
步骤6 在需要查看的记录左侧，单击  展开该记录的详细信息，展开记录如**图7-1**所示。

图 7-1 展开记录

事件名称	资源类型	事件来源	资源ID	资源名称	事件级别	操作用户	操作时间	操作
downloadA...	accessory	PSDM	a3254e0b-7db9-4...	--	normal		2020/08/18 11:32:25 GMT+08:00	查看事件
request								
code	200							
source_ip	.168							
trace_type	ConsoleAction							
event_type	global							
project_id	011a98453be6488683dee19afbbe4661							
trace_id	6f3c5de0-e103-11ea-a6fa-5bae8c098270							
trace_name	downloadAccessories							
resource_type	accessory							
trace_rating	normal							
api_version	1.0							

步骤7 在需要查看的记录右侧，单击“查看事件”，弹出一个窗口，如**图7-2**所示，显示了该操作事件结构的详细信息。

图 7-2 查看事件



----结束