态势感知

用户指南

文档版本	54
发布日期	2022-11-24

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 权限管理 1
1.1 创建用户并授权使用 SA 1
1.2 SA 自定义策略 3
1.3 SA 权限及授权项 4
2 版本管理 6
2.1 选择计费模式 6
2.1.1 包周期计费 6
2.1.2 按需计费 6
2.1.3 按需转包周期 6
2.2 购买标准版 7
2.3 购买专业版 11
2.4 开通综合大屏 17
2.5 增加资产配额 19
2.6 续费 20
2.7 退订 21
2.8 态势感知升级至安全云脑 24
3 安全概览 26
3.1 总览 26
3.2 安全评分 31
4 资源管理 34
5 业务分析 37
6 综合大屏 40
6.1 综合态势感知 40
6.2 主机安全态势 45
7 威胁告警 51
7.1 威胁告警简介 51
7.2 查看告警列表 54
7.3 威胁分析 56
7.4 告警事件处理 56
7.4.1 DDoS 57
7.4.2 暴力破解 57

7.4.3 Web 攻击 59
7.4.4 后门木马 59
7.4.5 漏洞攻击 59
7.4.6 僵尸主机 60
7.4.7 命令与控制 61
7.4.8 异常行为 61
8 漏洞管理 63
8.1 漏洞管理简介 63
8.2 查看应急漏洞公告列表 65
8.3 查看主机漏洞扫描详情 66
8.4 查看网站漏洞扫描详情 68
9 基线检查 70
9.1 云服务基线简介 70
9.2 基线检查项目 70
9.3 配置基线检查功能所需的权限 105
9.4 设置基线检查计划 107
9.5 执行基线检查计划 109
9.6 执行手动检查 112
9.7 查看基线检查结果 113
9.8 处理基线检查结果 118
10 检测结果 122
10.1 查看全部检测结果 122
10.2 处理检测结果 126
10.3 导出检测结果 127
10.4 自定义结果列表 128
10.5 管理筛选条件 129
11 分析报告 132
11.1 创建安全报告 132
11.2 发送安全报告 135
11.3 查看报告详情 138
11.4 下载历史报告 139
11.5 查看安全报告 141
11.6 编辑安全报告 143
11.7 删除报告 144
12 日志管理 146
13 产品集成 148
13.1 管理产品集成 148
13.2 查看产品集成 150
13.3 查看探测状态 152
14 设置 155

14.1 告警设置 155
14.1.1 设置告警通知 155
14.1.2 设置告警监控 156
14.2 授权设置 159
14.2.1 主机授权 159
14.3 启动主机扫描任务 164
14.4 检测设置 165

1 权限管理

1.1 创建用户并授权使用 SA

如果您需要对您所拥有的态势感知（Situation Awareness，SA）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，IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的账号中，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SA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SA资源委托给更专业、高效的其他账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图1-1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的SA权限，并结合实际需求进行选择，SA支持的系统权限，请参见**SA系统权限**。若您需要对除SA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**。

如**表1-1**所示，包括了SA的所有系统权限。

表 1-1 SA 系统权限

策略名称	描述	类别	依赖关系
SA FullAccess	态势感知的所有权限。	系统策略	无
SA ReadOnlyAccess	态势感知只读权限，拥有该权限的用户仅能查看态势感知数据，不具备态势感知配置权限。	系统策略	无

说明

目前，“SA FullAccess”或“SA ReadOnlyAccess”权限需要配合“Tenant Guest”权限才能使用。具体说明如下：

- 配置SA所有权限：“SA FullAccess”和“Tenant Guest”权限。
  其中，如果需要使用SA的**资源管理**和**基线检查**功能需要配置以下权限：
  - **资源管理**：“SA FullAccess”和“Tenant Administrator”权限，详细操作请参见**配置相关功能所需的权限**。
  - **基线检查**：“SA FullAccess”、“Tenant Administrator”和IAM相关权限，详细操作请参见**配置相关功能所需的权限**。
- 配置SA只读权限：“SA ReadOnlyAccess”和“Tenant Guest”权限。

示例流程

图 1-1 给用户授予 SA 权限流程

1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予态势感知的权限“SA FullAccess”和“Tenant Guest”。
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：
   在服务列表中选择除态势感知外（假设当前策略仅包含“SA FullAccess”）的任一服务，若提示权限不足，表示“SA FullAccess”已生效。
4. 配置委托。
   其中，如果需要使用SA的**资源管理**和**基线检查**功能需要配置以下权限：
   - **资源管理**：“SA FullAccess”和“Tenant Administrator”权限，详细操作请参见**配置相关功能所需的权限**。

- **基线检查**：“SA FullAccess”、“Tenant Administrator”和IAM相关权限，详细操作请参见**配置相关功能所需的权限**。

1.2 SA 自定义策略

如果系统预置的SA权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**SA权限及授权项**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的SA自定义策略样例。

SA 自定义策略样例

- 示例1：授权用户获取告警列表、获取威胁分析结果

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "sa:threatevent:getList",
            "sa:threatevent:getAnalyze"
         ]
      }
   ]
}
```

- 示例2：拒绝用户修改告警配置信息

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循**Deny优先原则**。

  如果您给用户授予“SA FullAccess”的系统策略，但不希望用户拥有“SA FullAccess”中定义的修改告警配置的权限，您可以创建一条拒绝修改告警配置的自定义策略，然后同时将“SA FullAccess”和拒绝策略授予用户，根据Deny优先原则，则用户可以对SA执行除了修改告警配置外的所有操作。拒绝策略示例如下：

```
{
      "Version": "1.1",
      "Statement": [
            {
                  "Action": [
                        "sa:subscribe:operate"
                  ],
                  "Effect": "Deny"
            }
      ]
}
```

- 示例3：多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下：

```
{
   "Version": "1.1",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sa:cssb:operate",
        "sa:cssb:get"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "obs:bucket:GetReplicationConfiguration",
        "obs:bucket:PutReplicationConfiguration",
        "obs:bucket:DeleteReplicationConfiguration"
      ],
      "Resource": [
        "obs:*:*:bucket:*"
      ]
    }
  ]
}
```

1.3 SA 权限及授权项

如果您需要对您所拥有的态势感知（Situation Awareness，SA）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，IAM），如果账号已经能满足您的要求，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SA服务的其它功能。

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使用户组中的用户获得相应的权限，这一过程称为授权。授权后，用户就可以基于已有权限对云服务进行操作。

权限根据授权的精细程度，分为**角色**和**策略**。角色以服务为粒度，是IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。策略授权更加精细，可以精确到某个操作、资源和条件，能够满足企业对权限最小化的安全管控要求。

支持的授权项

策略包含系统策略和自定义策略，如果系统策略不满足授权要求，管理员可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制。

- 权限：允许或拒绝某项操作。
- 授权项：自定义策略中支持的Action，在自定义策略中的Action中写入授权项，可以实现授权项对应的权限功能。

表 1-2 支持的授权项

权限	授权项
获取告警列表	sa:threatevent:getList
获取威胁分析结果	sa:threatevent:getAnalyze
获取主机列表	sa:threatevent:getAsset
查看综合态势感知大屏	sa:threatevent:getDashboard
查看主机安全态势大屏	sa:threatevent:getHostscreen

权限	授权项
获取租户控制台信息	sa:threatevent:getSafety
获取态势总览信息	sa:threatevent:getOverview
更新告警设置	sa:subscribe:operate
获取告警设置信息	sa:subscribe:getList
获取全局态势信息	sa:subscribe:get
获取编排信息	sa:service:get
设置服务状态	sa:service:operateSwitch
更新白名单信息	sa:service:operateWhiteList
获取订阅主题信息	sa:service:operateSubscribe
获取基线检查信息	sa:cssb:get
设置基线检查	sa:cssb:operate

2 版本管理

2.1 选择计费模式

2.1.1 包周期计费

包年/包月的计费模式也称为包周期计费模式，是一种预付费方式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。

适用于包周期的资源

- SA资产配额，主要为主机配额。
- SA综合大屏功能，包括综合态势大屏和主机安全态势两个大屏。

若您需购买包年/包月的态势感知服务，可同时购买资产配额和综合大屏功能，配置费用包括两种资源的费用之和；也可先购买资产配额，再开通综合大屏功能，配置费用为分次计算，已购买资源不会重复计费，请放心购买。

您可以查看**态势感知价格详情**，快速了解态势感知的配置费用。

2.1.2 按需计费

按需计费是按小时付费，是一种后付费方式，可以随时开通/取消。系统会根据资源的实际使用情况（按SA服务的实际使用时长计费）每小时出账单，并从账户余额里扣款。

适用于按需的资源

SA资产配额，主要为主机配额。

您可以查看**态势感知价格详情**，快速了解态势感知的配置费用。

2.1.3 按需转包周期

- 按需计费：按需计费是后付费模式，按态势感知服务的实际使用时长计费，可以随时开通/取消。
- 包年/包月：包年/包月即包周期，是预付费模式，按订单的购买周期计费，适用于可预估资源使用周期的场景，价格比按需计费模式更优惠。

若您可预估使用态势感知服务的周期，并需要长期使用态势感知服务，可以将按需购买的态势感知资源转为包周期计费模式，节省开支。

说明

- 资产配额与综合大屏功能需分别转包周期。
- 当资产配额被全部退订/取消后，即当前为基础版时。您需单击“综合大屏”，进入大屏管理页面，在页面右上角再执行转包周期，将综合大屏功能从按需计费转为包周期。

前提条件

已购买按需计费的专业版服务，即已购买按需的资产配额或综合大屏。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理控制台。

步骤3 单击右上角“专业版”，显示版本管理窗口。

步骤4 针对按需购买的资产配额或综合大屏，单击“转包周期”，跳转到“按需转包年/包月”页面。

步骤5 确认资源信息，并选择购买时长。

步骤6 单击“去支付”，完成订单支付。

----结束

2.2 购买标准版

背景信息

态势感知 SA服务**即将下线**，态势感知 SA的能力将由**安全云脑 SecMaster**服务提供。为了避免影响您的业务，建议您使用安全云脑，购买安全云脑详细操作请参见**购买安全云脑**。

态势感知提供基础版、标准版、专业版供您选择。

- 用户可免费体验**基础版**。

  基础版仅提供检测部分威胁风险，呈现一定云上资产安全态势。
- 为及时和深入了解资产安全状况，确保云上资产安全，建议您升级为**标准版或专业版**。
  - **标准版**提供一定种类的威胁检测和分析服务，包括威胁分析、告警设置、主机漏洞、安全日志管理等功能。若需要使用标准版，你需根据全局资产数购买配额，一个资产配额支持全方位防护一台资产。
  - **专业版**提供更多种类的威胁检测和分析服务，包含威胁分析、告警设置、主机漏洞、网站漏洞、基线检查、安全日志管理及综合大屏等功能。若需使用**专业版**服务，您需根据全局资产数购买配额，一个资产配额支持全方位防护一台资产。

  - 更多基础版、标准版、专业版功能差异，请参见**服务版本差异**。
- **综合大屏**提供“综合态势感知大屏”和“主机安全态势大屏”两种大屏模式，集中展示云上综合安全态势和主机安全状况。**综合大屏**功能为专业版额外选购付费项目，您可以在购买资产配额后，参考**开通综合大屏**再购买。

须知

- 基础版不支持退订。
- 标准版**不支持**直接升级到专业版，且专业版也**不支持**直接变更到标准版。如需使用对应版本，需退订当前版本后再进行购买。
- 标准版仅支持通过包周期计费模式进行购买。
- 不支持部分配额购买标准版，部分配额购买专业版。
- 综合大屏为专业版额外选购付费项目，如需使用综合大屏，请先购买专业版。

前提条件

- 已获取管理控制台的登录账号与密码。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理控制台。

步骤3 在页面右上角单击“升级”。

步骤4 （可选）选择使用角色。

默认可选IT运维人员、安全运维人员、合规审计人员、CSO/CIO/CISO四类角色，不同角色推荐配置不同。

图 2-1 选择使用角色

步骤5 选择计费模式，“计费模式”选择“包周期”，按配置周期计费。

标准版仅支持“包周期”模式。

图 2-2 选择包周期计费

步骤6 选择态势感知版本，“态势感知版本”选择“标准版”。

图 2-3 选择版本

步骤7 配置资产配额，相关参数如**表1 配置参数说明**。

表 2-1 配置参数说明

参数	说明
主机配额	主机资产支持防护的最大主机数量。 请根据当前账户下所有主机资产总数设置配额数，可设置最大主机配额需等于或大于当前账户下主机总数量，且不支持减少。 主机配额最大限制如下： • 当前账户下主机总数量≤10台：主机配额最大限制为100台。 • 当前账户下主机总数量>10台：主机配额最大限制=当前账户下主机总数量x10台 示例：当前账户下主机总数量为20台，则主机配额最大限制为20x10=200台。 **说明** 为避免主机资产在防护份额外，不能及时感知攻击威胁，而造成数据泄露等安全风险。当主机资产数量增加后，请及时增加配额数。

步骤8 选择态势感知使用时长。

图 2-4 选择购买时长

- 配置资产配额的使用时长。

  计费模式选择“包周期”后，必须配置“购买时长”。

  - 可按月（选择1/2/3/4/5/6/7/8/9个月）或按年（选择1/2/3年）购买。
  - 在配置总价的基础上，购买1年享受8.3折优惠，购买2年享受7折优惠，购买3年享受5折优惠。
- 勾选“自动续费”。在账户余额充足前提下，当购买的版本即将到期时，自动续费，不影响使用。

表 2-2 自动续费周期说明

购买时长	自动续费周期
1/2/3/4/5/6/7/8/9个月	1个月
1年	1年

说明

- 若需对不同资产配置不同使用时长，请参考**增加资产配额**。
- 更多关于自动续费修改、取消等操作说明，请参见**自动续费规则说明**。

步骤9 配置完成后，单击“立即购买”。

步骤10 进入“订单详情”页面，确认订单无误并阅读《态势感知服务免责声明》后，勾选“我已阅读并同意《态势感知服务（SA）免责声明》”，单击“去支付”。

步骤11 在支付页面，选择付款方式完成付款。

步骤12 成功付款后，返回态势感知控制台页面，确认已生效和到期时间。

----结束

后续管理

图 2-5 版本管理窗口

- 若需变更资产配额，可单击“增加配额”，添加资产配额购买，详细说明请参见**增加资产配额**。
- 若购买的包周期版本即将到期或已经到期，可单击“续费”，延长当前包周期资源的使用期限，详细说明请参见**续费**。
- 若不再使用资产配额功能，可单击“退订”或“取消”，退订相应态势感知服务，详细说明请参见**退订**。

2.3 购买专业版

背景信息

态势感知 SA服务**即将下线**，态势感知 SA的能力将由**安全云脑 SecMaster**服务提供。为了避免影响您的业务，建议您使用安全云脑，购买安全云脑详细操作请参见**购买安全云脑**。

态势感知提供基础版、标准版、专业版供您选择。

- 用户可免费体验**基础版**。

  基础版仅提供检测部分威胁风险，呈现一定云上资产安全态势。
- 为及时和深入了解资产安全状况，确保云上资产安全，建议您升级为**标准版或专业版**。
  - **标准版**提供一定种类的威胁检测和分析服务，包括威胁分析、告警设置、主机漏洞、安全日志管理等功能。若需要使用标准版，你需根据全局资产数购买配额，一个资产配额支持全方位防护一台资产。
  - **专业版**提供更多种类的威胁检测和分析服务，包含威胁分析、告警设置、主机漏洞、网站漏洞、基线检查、安全日志管理及综合大屏等功能。若需使用**专业版**服务，您需根据全局资产数购买配额，一个资产配额支持全方位防护一台资产。
  - 更多基础版、标准版、专业版功能差异，请参见**服务版本差异**。
- **综合大屏**提供“综合态势感知大屏”和“主机安全态势大屏”两种大屏模式，集中展示云上综合安全态势和主机安全状况。**综合大屏**功能为专业版额外选购付费项目，您可以在购买资产配额后，参考**开通综合大屏**再购买。

须知

- 基础版不支持退订。
- 标准版**不支持**直接升级到专业版，且专业版也**不支持**直接变更到标准版。如需使用对应版本，需退订当前版本后再进行购买。
- 标准版仅支持通过包周期计费模式进行购买。
- 不支持部分配额购买标准版，部分配额购买专业版。
- 综合大屏为专业版额外选购付费项目，如需使用综合大屏，请先购买专业版。

前提条件

- 已获取管理控制台的登录账号与密码。

包周期方式

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理控制台。

步骤3 在页面右上角单击“升级”。

步骤4 （可选）选择使用角色。

默认可选IT运维人员、安全运维人员、合规审计人员、CSO/CIO/CISO四类角色，不同角色推荐配置不同。

图 2-6 选择使用角色

步骤5 选择计费模式，“计费模式”选择“包周期”，按配置周期计费。

图 2-7 选择包周期计费

步骤6 选择态势感知版本。

当前默认选择“专业版”，由基础版功能升级为专业版功能。

图 2-8 选择版本

步骤7 配置资产配额，相关参数如**表1 配置参数说明**。

表 2-3 配置参数说明

参数	说明
主机配额	主机资产支持防护的最大主机数量。 请根据当前账户下所有主机资产总数设置配额数，可设置最大主机配额需等于或大于当前账户下主机总数量，且不支持减少。 主机配额最大限制如下： ● 当前账户下主机总数量≤10台：主机配额最大限制为100台。 ● 当前账户下主机总数量>10台：主机配额最大限制=当前账户下主机总数量x10台 示例：当前账户下主机总数量为20台，则主机配额最大限制为20x10=200台。 **说明** 为避免主机资产在防护份额外，不能及时感知攻击威胁，而造成数据泄露等安全风险。当主机资产数量增加后，请及时增加配额数。

步骤8 （可选）开通综合大屏功能。

图 2-9 选择安全大屏

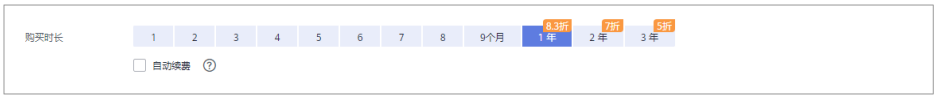
- **综合大屏**功能为增值付费项。
- 在勾选购买“安全大屏”时，可与资产配额一起购买，或在购买资产配额后再补充购买。

说明

“安全大屏”必须与资产配额搭配购买，不能单独购买，因在检测到资产的威胁攻击后，才能通过分析分类呈现安全态势大屏。

步骤9 选择态势感知使用时长。

图 2-10 选择购买时长



- 配置资产配额的使用时长。
  计费模式选择“包周期”后，必须配置“购买时长”。
  - 可按月（选择1/2/3/4/5/6/7/8/9个月）或按年（选择1/2/3年）购买。

  - 在配置总价的基础上，购买1年享受8.3折优惠，购买2年享受7折优惠，购买3年享受5折优惠。
- 勾选“自动续费”。在账户余额充足前提下，当购买的版本即将到期时，自动续费，不影响使用。

表 2-4 自动续费周期说明

购买时长	自动续费周期
1/2/3/4/5/6/7/8/9个月	1个月
1年	1年

说明

- 若需对不同资产配置不同使用时长，请参考**增加资产配额**。
- 更多关于自动续费修改、取消等操作说明，请参见**自动续费规则说明**。

步骤10 配置完成后，单击“立即购买”。

步骤11 进入“订单详情”页面，确认订单无误并阅读《态势感知服务免责声明》后，勾选“我已阅读并同意《态势感知服务（SA）免责声明》”，单击“去支付”。

步骤12 在支付页面，选择付款方式完成付款。

步骤13 成功付款后，返回态势感知控制台页面，确认已生效和到期时间。

----结束

按需方式

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理控制台。

步骤3 在页面右上角单击“升级”。

步骤4 （可选）选择使用角色。

默认可选IT运维人员、安全运维人员、合规审计人员、CSO/CIO/CISO四类角色，不同角色推荐配置不同。

图 2-11 选择使用角色

步骤5 选择计费模式，“计费模式”选择“按需”，按小时计费。

从开通开始到取消结束，按实际防护时长（小时）计费。

图 2-12 选择按需计费

步骤6 选择态势感知版本。

当前默认选择“专业版”，由基础版功能升级为专业版功能。

图 2-13 选择版本

步骤7 配置资产配额，相关参数如**表1 配置参数说明**。

表 2-5 配置参数说明

参数	说明
主机配额	主机资产支持防护的最大主机数量。 请根据当前账户下所有主机资产总数设置配额数，可设置最大主机配额需等于或大于当前账户下主机总数量，且不支持减少。 主机配额最大限制如下： • 当前账户下主机总数量≤10台：主机配额最大限制为100台。 • 当前账户下主机总数量>10台：主机配额最大限制=当前账户下主机总数量x10台 示例：当前账户下主机总数量为20台，则主机配额最大限制为20x10=200台。 **说明** 为避免主机资产在防护份额外，不能及时感知攻击威胁，而造成数据泄露等安全风险。当主机资产数量增加后，请及时增加配额数。

步骤8 （可选）开通综合大屏功能。

图 2-14 选择安全大屏

- **综合大屏**功能为增值付费项。
- 在勾选购买“安全大屏”时，可与资产配额一起购买，或在购买资产配额后再补充购买。

说明

“安全大屏”必须与资产配额搭配购买，不能单独购买，因在检测到资产的威胁攻击后，才能通过分析分类呈现安全态势大屏。

步骤9 配置完成后，单击“立即购买”。

步骤10 进入“订单详情”页面，确认订单无误并阅读《态势感知服务免责声明》后，勾选“我已阅读并同意《态势感知服务（SA）免责声明》”，单击“确认开通”。

步骤11 返回态势感知控制台页面，确认按需版本已生效。

----结束

后续管理

图 2-15 版本管理窗口

- 若需变更资产配额，可单击“增加配额”，添加资产配额购买，详细说明请参见**增加资产配额**。
- 若未同时开通综合大屏功能，可单击“立即开通”，开通大屏功能，详细说明请参见**开通综合大屏**。

- 若购买的按需资源后，需长期使用态势感知服务，可单击“转包周期”，将资源计费模式转为包年/包月，详细说明请参见**按需转包周期**。
- 若购买的包周期版本即将到期或已经到期，可单击“续费”，延长当前包周期资源的使用期限，详细说明请参见**续费**。
- 若不再使用资产配额或综合大屏功能，可单击“退订”或“取消”，退订相应态势感知服务，详细说明请参见**退订**。

2.4 开通综合大屏

综合大屏根据检测数据，资产安全数据可视化，集中呈现综合安全态势和主机全局安全。为充分呈现云上安全态势，建议您在购买态势感知资产配额后，再开通综合大屏功能。

包周期方式

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理控制台。

步骤3 单击“增加配额”，跳转到态势感知购买页面。

步骤4 查看当前配置。

图 2-16 查看当前配置

步骤5 选择计费模式，“计费模式”选择“包年/包月”，按配置周期计费。

图 2-17 选择包周期计费

步骤6 勾选“安全大屏”。

图 2-18 选择安全大屏

步骤7 选择“购买时长”。

图 2-19 选择购买时长

说明

综合大屏的“配置费用”根据大屏的使用时长计算。已有资产配额不会重复计费，请放心购买。

步骤8 配置完成后，单击“立即购买”。

步骤9 进入“订单确认”页面，确认订单无误并阅读《态势感知服务免责声明》后，勾选“我已阅读并同意《态势感知服务（SA）免责声明》”，单击“去支付”。

步骤10 在支付页面完成付款后，返回态势感知控制台页面，即可查看综合态势感知和主机安全态势两个大屏。

----结束

按需方式

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理控制台。

步骤3 单击“增加配额”，跳转到态势感知购买页面。

步骤4 查看当前配置。

图 2-20 查看当前配置

步骤5 选择计费模式，“计费模式”选择“按需计费”，按小时计费。

从开通开始到取消结束，按实际防护时长（小时）计费。

图 2-21 选择按需计费

步骤6 勾选“安全大屏”。

图 2-22 选择安全大屏

步骤7 配置完成后，单击“立即购买”。

步骤8 进入“订单确认”页面，确认订单无误并阅读《态势感知服务免责声明》后，勾选“我已阅读并同意《态势感知服务（SA）免责声明》”，单击“确认开通”。

步骤9 返回态势感知控制台页面，即可查看综合态势感知和主机安全态势两个大屏。

----结束

后续管理

- 若购买的按需资源后，需长期使用综合大屏功能，可在综合大屏管理页面，单击“转包周期”，将资源计费模式转为包年/包月，详细说明请参见**按需转包周期**。
- 若购买的包周期综合大屏即将到期或已经到期，可在综合大屏管理页面，单击“续费”，延长当前包周期资源的使用期限，详细说明请参见**续费**。
- 若不再使用综合大屏功能，可在综合大屏管理页面，单击“退订”或“取消”，退订相应态势感知服务，详细说明请参见**退订**。

2.5 增加资产配额

购买态势感知资产配额完成后，当用户资产数量增加，或需对不同资产有不同使用时长需求，可参考本小节扩充“主机配额”，并配置使用时长。

约束限制

- 主机配额是授权检测主机的数量。主机配额最大限制如下：

  表 2-6 主机配额最大限制

当前账户下主机总数量/台	主机最大配额/台
当前账户下主机总数量≤10	100
当前账户下主机总数量>10	当前账户下主机总数量x10 示例：已有20台主机，则主机最大配额为20x10=200。

- 在购买态势感知时，选择的最大配额需等于或大于当前账户下主机总数量，且不支持减少。若购买的最大配额小于主机数量，可能会造成如下影响：

  未授权检测的主机被攻击后，不能及时感知威胁，造成数据泄露等风险。

包周期方式

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理控制台。

步骤3 单击右上角“增加配额”，跳转到态势感知购买页面。

步骤4 查看当前配置。

步骤5 选择计费模式，“计费模式”选择“包周期”，按配置周期计费。

步骤6 配置“主机配额”，在原有配额数基础上，增加的资产配额数。

步骤7 选择“购买时长”。

说明

- 选择的“购买时长”为新增配额的使用时长，不影响已购买配额的使用时长。
- 增加配额的“配置费用”根据新增资产的配额数和使用时长计算。已有资产配额不会重复计费，请放心购买。
- 若需延长已购买配额的使用时间，请参见**续费**为目标配额延长使用时间。

步骤8 配置完成后，单击“立即购买”。

步骤9 进入“订单确认”页面，确认订单无误并阅读《态势感知服务免责声明》后，勾选“我已阅读并同意《态势感知服务（SA）免责声明》”，单击“去支付”。

步骤10 在支付页面完成付款后，返回态势感知控制台页面，即可对相应配额数的主机进行安全防护。

----结束

按需方式

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理控制台。

步骤3 单击“增加配额”，跳转到态势感知购买页面。

步骤4 查看当前配置。

步骤5 选择计费模式，“计费模式”选择“按需”，按小时计费。

从开通开始到取消结束，按实际防护时长（小时）计费。

步骤6 配置“主机配额”，在原有配额数基础上，增加的资产配额数。

步骤7 配置完成后，单击“立即购买”。

步骤8 进入“订单确认”页面，确认订单无误并阅读《态势感知服务免责声明》后，勾选“我已阅读并同意《态势感知服务（SA）免责声明》”，单击“确认开通”。

步骤9 返回态势感知控制台页面，即可对相应配额数的主机进行安全防护。

----结束

2.6 续费

态势感知续费是在原已购买的版本规格的基础上，延长使用时间。续费操作不可变更版本规格，即不能改变“主机配额”和“综合大屏”选择。

续费操作仅针对包周期版本规格。

- 包周期（包年/包月）模式为预付费方式。当购买的包周期版本到期时，用户需通过“续费”延长使用期。

- 按需计费为按小时计费，即开即用。在账户余额充足前提下，不涉及过期情况，即无需续费操作。

说明

资产配额与综合大屏功能需分别续费。

手动续费

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理控制台。

步骤3 单击右上角“标准版”或“专业版”，显示版本管理窗口。

步骤4 单击“续费”，系统跳转至费用中心“续费管理”页面。

步骤5 在态势感知专业版实例所在行，单击“续费”，跳转至“续费”页面。

步骤6 配置“选择续费时长”，如选择“一年”。

步骤7 单击“去支付”，跳转至支付页面，完成付款。

步骤8 返回续费管理页面，可查看态势感知已续费成功。

----结束

开通自动续费

在账户余额充足前提下，已配置“自动续费”后，包周期版本的资产配额和综合大屏将自动续费，延长使用周期。

自动续费的相关注意事项，请参见**自动续费规则说明**。

步骤1 登录管理控制台。

步骤2 单击“费用 > 续费管理”，跳转至费用中心“续费管理”页面。

步骤3 在“手动续费项”页签，选择态势感知专业版实例，单击“开通自动续费”，跳转至自动续费配置页面。

步骤4 选择配置“自动续费周期”和勾选“预设自动续费次数”。

步骤5 单击“开通”，完成自动续费配置。

步骤6 返回续费管理页面，在“自动续费项”页签，可查看态势感知已开通自动续费。

后续将根据配置，自动续费延长使用期。

----结束

2.7 退订

若用户不再使用态势感知防护功能或综合大屏，可执行退订或一键取消操作。

- 包周期（包年/包月）计费模式：预付费方式。新购5天内的资源，支持每年10次5天无理由“退订”；使用超过5天的资源，“退订”需要收取手续费。

- 按需计费模式：按小时计费方式。资源即开即停，支持一键“取消”释放资源。

说明

- 免费版不支持退订。
- 资产配额与综合大屏功能**需分别**退订/取消。
- 当资产配额被全部退订/取消后，即当前为基础版时。您需单击“综合大屏”，进入大屏管理页面，在页面右上角再执行退订或取消综合大屏功能。

更多费用和订单说明信息，请参见**费用中心**。

退订包周期计费

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理控制台。

步骤3 单击右上角“标准版”或“专业版”，显示版本管理窗口。

步骤4 针对包周期购买的资产配额或综合大屏，单击“退订”，进入“退订管理”列表页面。

图 2-23 退订包周期计费

步骤5 在需要退订的实例所在行，单击“操作”列中的“退订资源”，进入“退订资源”页面。

步骤6 确认待退订资源信息，选择退订原因，并勾选退订确认。

步骤7 单击“退订”，在退订管理页面确认退订。

退订成功后，返回版本管理窗口，包年/包月计费的资产配额已取消。

----结束

取消按需计费

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理控制台。

步骤3 单击右上角“专业版”，显示版本管理窗口。

步骤4 针对按需购买的版本或综合大屏，单击“取消”，一键释放按需计费的资产配额。

图 2-24 取消按需计费

返回版本管理窗口，按需计费的资产配额资源已取消。

----结束

退订综合大屏

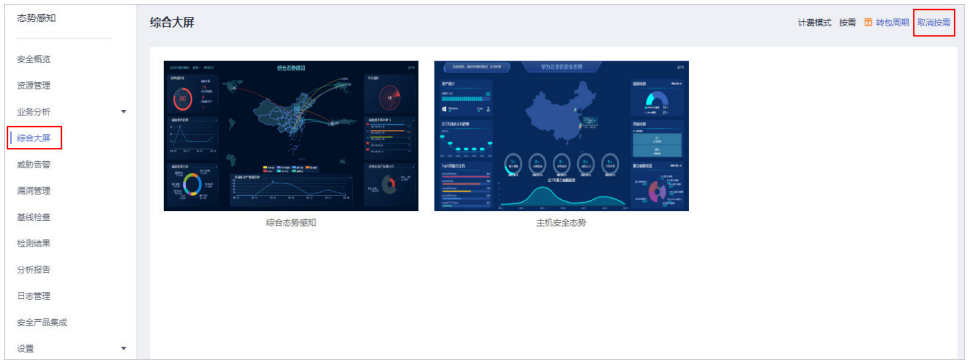
步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理控制台。

步骤3 在左侧导航栏中选择“综合大屏”，进入态势感知综合大屏页面。

步骤4 单击右上角“取消按需”或“取消包周期”，并在弹出的确认框中单击“是”，取消按需或包年/包月计费的综合大屏。

图 2-25 退订综合大屏



系统返回态势感知综合大屏页面，并显示为待开通状态，按需或包年/包月计费的综合大屏已取消。

----结束

2.8 态势感知升级至安全云脑

安全云脑（SecMaster）是华为云原生的新一代安全运营中心，集华为云多年安全经验，基于云原生安全，提供云上资产管理、安全态势管理、安全信息和事件管理、安全编排与自动响应等能力，可以鸟瞰整个云上安全，精简云安全配置、云防护策略的设置与维护，提前预防风险，同时，可以让威胁检测和响应更智能、更快速，帮助您实现一体化、自动化安全运营管理，满足您的安全需求。

安全云脑是态势感知的升级版本，后续功能变更、版本迭代也将在安全云脑中进行。因此，建议您升级至安全云脑。

升级说明

- 升级只支持从态势感知升级至安全云脑，不支持从安全云脑变更至态势感知。
- 升级时，需要将态势感知配额分配到不同区域，以及后续会关闭态势感知购买通道，请提前做好配合规划。
- 升级后，态势感知和安全云脑的生命周期共享，如果订单为按需类型，则仍需在原态势感知页面处理。
- 升级完成后，不支持在安全云脑中进行变更操作，如果需要执行版本升级或配额增加等操作，请在原态势感知中进行处理。

将态势感知升级至安全云脑

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，默认进入态势感知安全概览页面。

步骤3 在页面右上角，单击“升级到安全云脑”。

图 2-26 升级至安全云脑

步骤4 在升级至安全云脑页面中，配置参数信息。

- 版本关系：系统已自动同步SA的版本关系（版本、计费模式和安全大屏），无需手动配置。
- 配额分配：将态势感知全部额分配至安全云脑，在安全云脑配额中填写配额数。

步骤5 单击“立即升级”。

升级完成后，请在页面左上角单击  ，选择“安全与合规 > 安全云脑 SecMaster”，进入安全云脑管理页面，使用安全云脑管理云上资源，详细介绍和操作指导请参见**安全云脑介绍文档**。

----结束

3 安全概览

3.1 总览

SA的“安全概览”页面实时呈现云上整体安全评估状况，并联动其他云安全服务，集中展示云上安全。在“安全概览”查看安全概览信息和相关一键操作，实现云上安全态势一览和风险统一管控。

您可以在“安全概览”页面查看您的资产安全总览情况，并进行相关操作。“安全概览”分为以下几个板块：

- **安全评分**
- **安全监控**
- **安全趋势**
- **威胁检测**

安全评分

“安全评分”板块根据不同版本的威胁检测能力，评估整体资产安全健康得分，可快速了解未处理风险对资产的整体威胁状况，如**图3-1**。

图 3-1 安全评分

- 分值范围为0～100，分值越大表示风险越小，资产更安全，安全分值详细说明请参见**安全评分**。
- 分值环形图不同颜色表示不同威胁等级。例如，黄色对应“中危”。
- 单击“立即处理”，系统右侧弹出“安全风险处理”页面，您可根据该页面的提示，参考对应的帮助文档或直接对风险进行处理。

- 安全风险处理页面中包含所有需要您尽快处理的安全风险和威胁，分为“威胁告警”、“漏洞”、“合规检查”三大类别。
- “安全风险处理”页面中显示的数据为最近/最新检测后的数据结果，“检测结果”页面（单击“前往处理”，进入该页面）显示的是所有检测时间的各类数据详情，因此，安全风险处理页面的数据总数≤检测结果页面的数据总数。
- **处理安全风险**：
  i. 在“安全评分”栏中，单击“立即处理”，系统右侧弹出“安全风险处理”页面。
  ii. 在“安全风险处理”页面中，单击“前往处理”，进入检测结果页面。
  iii. 选择一个或多个“未处理”状态的结果，单击“忽略”或“标记为线下处理”，对不同检测结果批量执行相应的处理操作。
    - 忽略：如果确认该检测结果不会造成危害，在“忽略风险项”窗口记录“处理人”、“忽略理由”，可标记为“已忽略”状态。
    - 标记为线下处理：如果该检测结果已在线下处理，在“标记为线下处理”窗口记录“处理人”、“处理时间”和“处理结果”，可标记为“已线下处理”状态。

- 资产风险修复，并手动刷新告警事件状态后，安全评分实时更新。资产安全风险修复后，也可以直接单击“重新检测”，重新检测资产并进行评分。

  说明

  - 由于检测需要一定的时间，请您在单击“重新检测”按钮**5分钟**后，再刷新页面，查看最新检测的安全评分。
  - 资产安全风险修复后，为降低安全评分的风险等级，需手动忽略或处理告警事件，刷新告警列表中告警事件状态。

- 安全评分显示为历史扫描结果，**非实时**数据，如需获取最新数据及评分，可单击“重新检测”，获取最近的数据。

安全监控

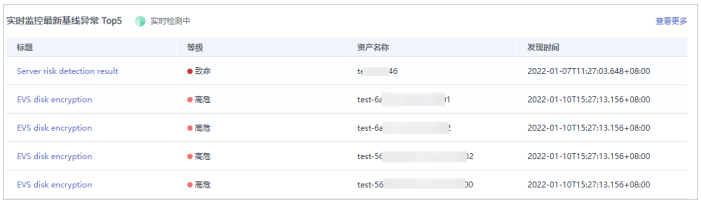
“安全监控”板块展示待处理**威胁告警**、待修复**漏洞**、**合规检查**问题的安全监控统计数据。

图 3-2 安全监控

表 3-1 安全监控参数说明

参数名称	参数说明
威胁告警	呈现最**近7天内**未处理威胁告警，可快速了解资产遭受的威胁告警类型和数量，呈现威胁告警的统计结果。 ● 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了入侵事件，建议您立即查看告警事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看告警事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该告警事件的详情。 ● 单击威胁告警模块，系统将列表实时呈现**近7天内**TOP5的威胁告警事件，可快速查看威胁告警详情，监控威胁告警状况，如图3-3所示。 – 列表呈现近7天TOP5的威胁告警事件的信息，包括威胁告警名称、告警等级、资产名称、告警发现时间。 – 若列表显示内容为空，表示近7天无威胁告警事件。 – 单击“查看更多”，可跳转到“检测结果”页面，查看更多的威胁告警信息，并可自定义过滤条件查询告警信息，查看威胁告警详细操作请参见**告警列表**。 **图 3-3** 查看实时威胁告警 

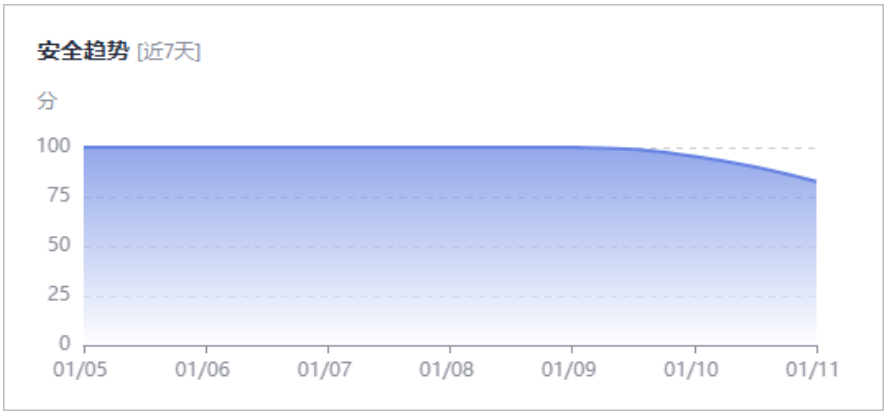
参数名称	参数说明
漏洞	展示您资产中TOP5漏洞类型，以及**近24小时内**还未修复的漏洞总数和不同漏洞风险等级对应的数量。 ● 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了漏洞事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常事件，建议您立即查看漏洞事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常事件，建议您及时查看该漏洞的详情。 ● 单击漏洞模块中的“漏洞类型Top5”栏，系统将列表呈现TOP5（根据某个漏洞影响的主机数量进行排序）的漏洞类型。 – 此处的TOP等级是根据某个漏洞影响的主机数量进行排序，受影响主机数量越多排名越靠前。 – 仅当主机中Agent版本为2.0时，才会在“漏洞类型Top5”中显示对应数据。如未显示数据或需要查看TOP5漏洞类型，请将主机将Agent1.0升级至Agent2.0。 **图 3-4** 漏洞类型  ● 单击漏洞模块中的“实时监控最新漏洞风险事件 Top5”栏，系统将列表实时呈现**近24小时内**TOP5的漏洞事件，可快速查看漏洞详情，如图3-5所示。 – 列表呈现当日最新TOP5漏洞事件详情，包括漏洞名称、漏洞等级、资产名称、漏洞发现时间。 – 若列表显示内容为空，表示当日无漏洞事件。 – 单击“查看更多”，可跳转到“检查结果”页面，查看更多的漏洞信息，并可自定义过滤条件查询漏洞信息，查看漏洞详细操作请参见**漏洞列表**。

参数名称	参数说明
	图 3-5 查看实时漏洞 
合规检查	展示您资产中**近30天内**存在的合规风险总数量和不同危险等级的合规检查风险对应的数量。 ● 此处严重等级含义如下： – 致命：即致命风险，表示您的资产中检测到了不合规的配置，建议您立即查看合规异常事件的详情并及时进行处理。 – 高危：即高危风险，表示资产中检测到了可疑的异常配置，建议您立即查看合规异常事件的详情并及时进行处理。 – 其他：即其他类型（中危、低危、提示）风险，表示服务器中检测到了有风险的异常配置，建议您及时查看该合规检查项目的详情。 ● 单击合规检查异常模块，系统将列表实时呈现**近30天内**TOP5的合规检查异常事件，可快速查看合规检查详情，如**图3-6**所示。 – 列表呈现最近一次合规检查中TOP的合规异常事件详情，包括合规检查项目名称、等级、资产名称、发现时间。 – 若列表显示内容为空，表示近30天无合规异常事件。 – 单击“查看更多”，可跳转到“检查结果”页面，查看更多的合规异常信息，并可自定义过滤条件查询合规检查信息，查看合规检查详细操作请参见**基线检查列表**。 **图 3-6** 查看合规异常事件 

安全趋势

“安全趋势”板块展示近7天内您的整体资产安全健康得分的趋势图。

图 3-7 安全趋势



威胁检测

“威胁检测”板块展示近7天内您的资产中检测到的告警数量及类型。

威胁检测服务（Managed Threat Detection，MTD）持续监控恶意活动和未经授权的行为，从而保护账户和工作负载。该服务通过集成AI智能引擎、威胁情报、规则基线等检测模型，识别各类云服务日志中的潜在威胁并输出分析结果，从而提升用户告警、事件检测准确性，提升运维运营效率。

开通威胁检测服务（MTD）后，才支持检测云服务日志数据中的访问行为，发现是否存在潜在威胁，对可能存在威胁的访问行为生成告警信息，输出告警结果。如果未开通，请单击“立即开通”，购买威胁检测服务。

图 3-8 开通威胁检测服务

3.2 安全评分

态势感知实时呈现您云上资产的整体安全评估状况，并根据不同版本的威胁检测能力，评估整体资产安全健康得分。

本章节将介绍在安全评分中，不同分值的含义以及扣分项的详细情况。

安全分值

SA根据不同版本的威胁检测能力，评估整体资产安全健康得分。

- 风险等级包括“无风险”、“提示”、“低危”、“中危”、“高危”和“致命”。

- 分值范围为0～100，分值越大表示风险越小，资产更安全。
- 分值从0开始，每隔20取值范围对应不同的风险等级，例如分值范围40~60对应风险等级为“中危”。
- 分值环形图不同色块表示不同威胁等级，例如黄色对应“中危”。
- 资产风险修复，并手动刷新告警事件状态后，安全评分实时更新。

说明

- 由于检测需要一定的时间，请您在单击“重新检测”按钮**5分钟**后，再刷新页面，查看最新检测的安全评分。
- 资产安全风险修复后，为降低安全评分的风险等级，需手动忽略或处理告警事件，刷新告警列表中告警事件状态。

表 3-2 安全分值表

风险等级	安全分值	分值说明
无风险	100分	恭喜您，您的资产当前安全状况良好。
提示	80≤分值<100	您的资产存在少量的安全隐患，建议您及时加固安全防护体系。
低危	60≤分值<80	您的资产存在较多的安全隐患，建议您及时加固安全防护体系。
中危	40≤分值<60	您的资产防御黑客入侵的能力较弱，建议您立即加固安全防护体系。
高危	20≤分值<40	您的资产存在较高的黑客入侵和病毒感染的风险，建议您立即处理。
致命	0≤分值<20	您的资产很可能遭受到黑客入侵和病毒感染的威胁，建议您立即处理。

安全评分扣分项

安全评分扣分项及其分值情况如表3-3所示。

表 3-3 安全评分扣分项

分类	扣分项	单项扣分项	处理建议	最高扣分上限
合规检查	存在未处理的致命不合规项	10	按照合规修复建议指导进行合规问题修复，修复后重新触发扫描任务，自动刷新评分。	20
	存在未处理的高危不合规项	5		
	存在未处理的中危不合规项	2		

分类	扣分项	单项扣分项	处理建议	最高扣分上限
	存在未处理的低危不合规项	0.1		
漏洞	存在未处理的致命漏洞	10	按照漏洞修复建议指导进行漏洞修复，修复后重新触发漏洞扫描任务，自动刷新评分。	20
	存在未处理的高危漏洞	5		
	存在未处理的中危漏洞	2		
	存在未处理的低危漏洞	0.1		
威胁告警	存在未处理的致命告警事件	10	按照威胁事件处置指导建议进行修复，修复后自动刷新评分。	30
	存在未处理的高危告警事件	5		
	存在未处理的中危告警事件	2		
	存在未处理的低危告警事件	0.1		

4 资源管理

态势感知提供资源管理功能。在“资源管理”页面，您可以查看当前账号中所有资源的安全状态统计信息，包括资源的名称、所属服务、所属区域、安全状况等，帮助您快速定位安全风险问题并提供解决方案。

目前，支持查看以下资源的安全状况：

弹性云服务器 ECS、虚拟私有云 VPC、对象存储服务 OBS、弹性公网IP EIP、云解析服务 DNS、弹性负载均衡 ELB、云数据库 RDS、裸金属服务器 BMS、云容器引擎 CCE、云容器实例 CCI、Web应用防火墙 WAF、SSL证书管理 SCM、云硬盘 EVS

前提条件

- 已购买态势感知**标准版**或**专业版**，且在有效使用期内。
- 操作账号权限检查。使用资源管理功能时，除了需要“SA FullAccess”、“SA ReadOnlyAccess”策略权限，还需要“Tenant Administrator”权限，请提前授予操作账号对应权限。

  “Tenant Administrator”权限配置详细操作请参见**如何配置资源管理功能所需的权限**。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“资源管理”，进入资源管理页面。

步骤4 查看全部资源安全状态，相关说明如**表4-1**所示。

图 4-1 资源管理

表 4-1 资源安全状态参数说明

参数名称	参数说明
名称	呈现资源的名称。
服务	呈现资源所属的服务。
区域	呈现资源所属的区域。
资源类型	呈现资源所属的类型。例如：云服务器、磁盘、实例等。
安全状况	呈现资源的安全风险等级。 ● 风险等级包括“致命”、“高危”、“中危”、“低危”、“提示”和“无风险”。 ● 呈现当前资源风险的最高等级。例如，ECS中有高危、低危和提示级别的风险，则此处取最高值，显示为高危。 ● 单击，可按风险等级排序资源列表。
IP地址	呈现资源的IP地址。
防护状态	呈现资源是否开启安全防护。如果未开启防护，可单击“去开启”进行设置。
威胁	呈现资源**近7天内**存在的威胁告警总数。 单击告警数量可跳转“检测结果”页面，查看更多的威胁告警信息，并可自定义过滤条件查询告警信息。
漏洞	呈现资源**近24小时内**未修复的漏洞总数。 ● 单击漏洞数量可跳转“检测结果”页面，查看更多的漏洞信息，并可自定义过滤条件查询漏洞信息。 ● “资源管理”页面中显示的数据为最近/最新检测后的数据结果，“检测结果”页面显示的是所有检测时间的各类数据详情，因此，资源管理页面的数据总数≤检测结果页面的数据总数。
基线	呈现资源**近30天内**存在的基线风险总数。 ● 单击基线检查异常数量可跳转“检测结果”页面，查看更多的基线异常信息，并可自定义过滤条件查询基线检查信息。 ● “资源管理”页面中显示的数据为最近/最新检测后的数据结果，“检测结果”页面显示的是所有检测时间的各类数据详情，因此，资源管理页面的数据总数≤检测结果页面的数据总数。
企业项目	呈现资源所属的企业项目。
标签	呈现资源已有的标签。 如果资源当天添加了标签，则在SA资源管理中第二天才会同步显示。

步骤5 根据资源信息，筛选查看相关资源安全状态。

单击“服务”、“区域”或“安全状况”后的选项，将呈现符合过滤条件的资源列表。

- **服务**：筛选资源所属的服务。选择服务后，还可以根据“资源类型”来查看选择指定资源类型的安全状态。
- **区域**：筛选资源所在的区域。

  可选择区域包括“华北-北京一”、“华北-北京四”、“华东-上海一”、“华东-上海二”、“华南-深圳”、“华南-广州”、“西南-贵阳一”或“中国-香港”。
- **安全状况**：筛选资源的安全风险等级。

  可选择风险等级包括“致命”、“高危”、“中危”、“低危”、“提示”或“无风险”。

步骤6 当资源列表较多时，可以通过搜索功能，快速查询指定资源。

在搜索框中输入资源的“弹性公网IP”、“名称”或“私有IP”，单击  ，即可查看目标资源的安全状态。

----结束

5 业务分析

态势感知提供安全业务的专项分析能力，实时为您全面展示云上资产的安全状态和存在的安全风险，并联动其他云安全服务，集中展示云上安全。

背景信息

- HSS专项分析

  主机安全服务（Host Security Service，HSS）是以工作负载为中心的安全产品，集成了主机安全、容器安全和网页防篡改，旨在解决混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。HSS通过对主机、容器进行系统完整性的保护、应用程序控制、行为监控和基于主机的入侵防御等，保护工作负载免受攻击。

  在SA中的HSS业务分析页面，您可以查看您所有资产的风险指数、风险趋势、TOP5事件类型以及您开通的主机安全和容器安全服务数量，帮助您实时了解主机和容器的安全状态和存在的安全风险。

- WAF专项分析

  Web应用防火墙（Web Application Firewall， WAF）对网站业务流量进行多维度检测和防护，结合深度机器学习智能识别恶意请求特征和防御未知威胁，全面避免网站被黑客恶意攻击和入侵。

  在SA中的WAF业务分析页面，您可以查看昨天、今天、3天、7天或者30天内所有防护网站或所有实例以及指定防护网站或实例的防护日志。包括请求与各攻击类型统计次数，QPS、响应码信息，以及事件分布、受攻击域名 Top10、攻击源IP Top10、受攻击URL Top10、攻击来源区域 Top10和业务异常监控 Top10等防护数据。

  安全总览页面统计数据每隔2分钟刷新一次。

- DBSS专项分析

  数据库安全服务（Database Security Service）是一个智能的数据库安全服务，基于机器学习机制和大数据分析技术，提供数据库审计，SQL注入攻击检测，风险操作识别等功能，保障云上数据库的安全。

  在SA中的DBSS业务分析页面，您可以查看最近30分钟、最近1小时、最近24小时、7天或者30天内数据库的总体审计情况、风险分布、会话统计以及SQL分布情况。

前提条件

已开通对应区域的对应服务。例如，需要查看“华北-北京四”区域中云主机的分析情况，则需要在“华北-北京四”区域开通企业主机安全服务。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 根据待分析选择对应的服务。

- HSS专项分析

  在左侧导航栏选择“业务分析 > HSS专项分析”，进入“HSS专项分析”页面。

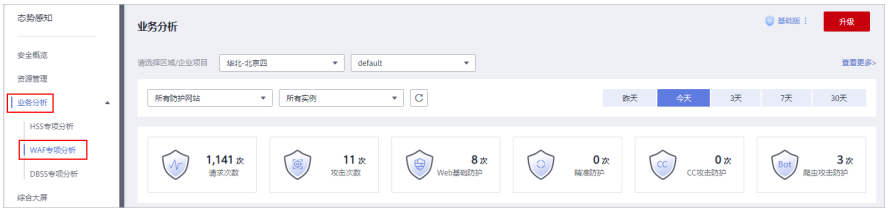
  图 5-1 HSS 专项分析

- WAF专项分析

  在左侧导航栏选择“业务分析 > WAF专项分析”，进入“WAF专项分析”页面。

  图 5-2 WAF 专项分析

- DBSS专项分析

  在左侧导航栏选择“业务分析 > DBSS专项分析”，进入“DBSS专项分析”页面。

  图 5-3 DBSS 专项分析

步骤4 查看分析情况。

- HSS安全总览

在SA中的HSS业务分析页面，您可以查看您所有资产的风险指数、风险趋势、TOP5事件类型以及您开通的主机安全和容器安全服务数量，帮助您实时了解主机和容器的安全状态和存在的安全风险。

具体分析情况请参见**HSS业务分析**。

- WAF安全总览

  在SA中的WAF业务分析页面，您可以查看昨天、今天、3天、7天或者30天内所有防护网站或所有实例以及指定防护网站或实例的防护日志。包括请求与各攻击类型统计次数，QPS、响应码信息，以及事件分布、受攻击域名 Top10、攻击源IP Top10、受攻击URL Top10、攻击来源区域 Top10和业务异常监控 Top10等防护数据。

  具体分析情况请参见**WAF业务分析**。

- DBSS安全总览

  在SA中的DBSS业务分析页面，您可以查看最近30分钟、最近1小时、最近24小时、7天或者30天内数据库的总体审计情况、风险分布、会话统计以及SQL分布情况。

  具体分析情况请参见**DBSS业务分析**。

----结束

6 综合大屏

6.1 综合态势感知

在现场讲解汇报、实时监控等场景下，为了获得更好的演示效果，通常需要将态势感知服务的分析结果展示在大型屏幕上。如果只是单纯将控制台界面放大显示，视觉效果并不是很理想。此时可以利用**综合大屏**，展示专为大型屏幕设计的服务界面，获得更清晰的态势信息和更好的视觉效果。

前提条件

已开通**安全大屏**增值项，可查看综合态势感知大屏相关信息。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“综合大屏”，进入“综合大屏”页面。

图 6-1 查看综合大屏信息

步骤4 单击“综合态势感知”图片，进入“综合态势感知”大屏信息页面，如图6-2。

页面中各个模块的功能介绍和使用方法详见下述内容。

图 6-2 综合态势感知大屏

----结束

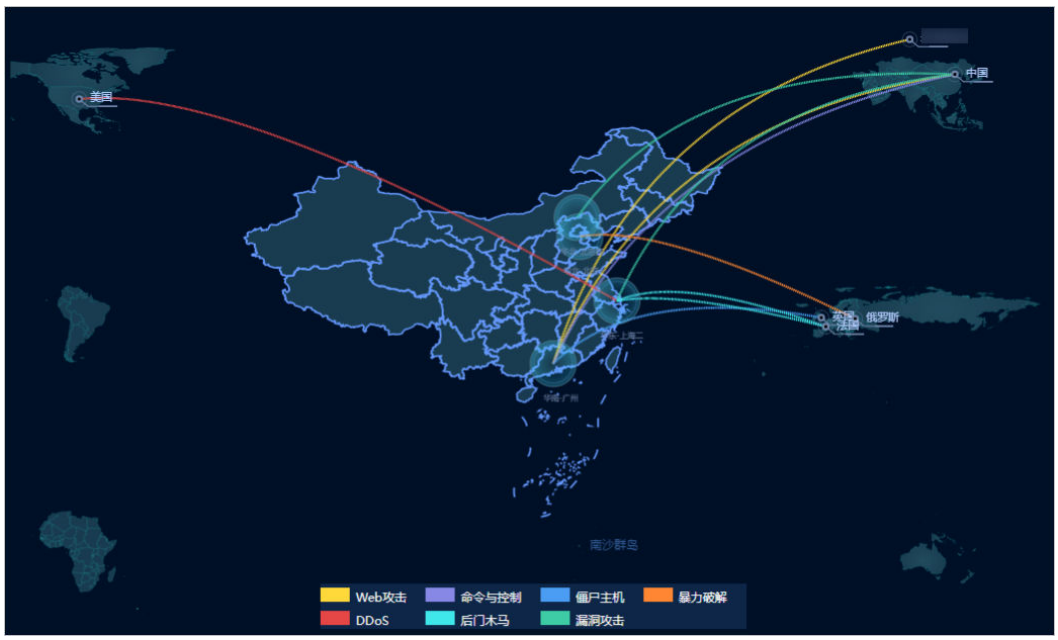
全网安全地图

如图6-3所示，全网安全地图以区域维度动态展示了客户所有资产**近7天内**受到的威胁情况。通过将攻击源和攻击目标具象化，用户可以直观了解资产的安全状况。图中每个圆圈代表一个华为云区域，每个华为云区域发生的告警来源通过攻击线在地图上表示出来，最多显示20条告警。

说明

- “综合态势感知”大屏全网安全示意地图，根据华为云部署区域概略展示，背景地图不能做高精确定位。
- “综合态势感知”大屏全网安全示意地图，仅用于演示与汇报，不是为了任何非法目的，也不具有任何恶意。

图 6-3 全网安全地图



全网威胁度

如图6-4所示，全网威胁度体现了**近7天内**资产的整体安全状况。图中体现的信息主要有威胁度、威胁总量和受威胁资产数。

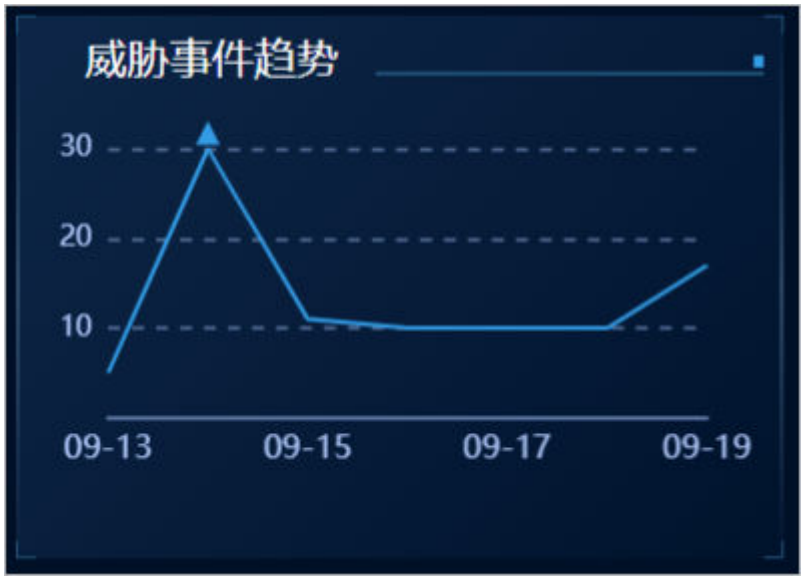
其中，威胁度的取值范围是0～100，数值越大表示威胁越高。由于不包含无风险的资产，所以受威胁资产数小于等于总资产数。

图 6-4 全网威胁度

威胁事件趋势

如图6-5所示，展示**近7天内**每日所受威胁的数量，威胁事件趋势的横坐标表示时间，纵坐标表示威胁事件的数量。将鼠标箭头置于某个日期上，可以看到该日发生的威胁事件总数。

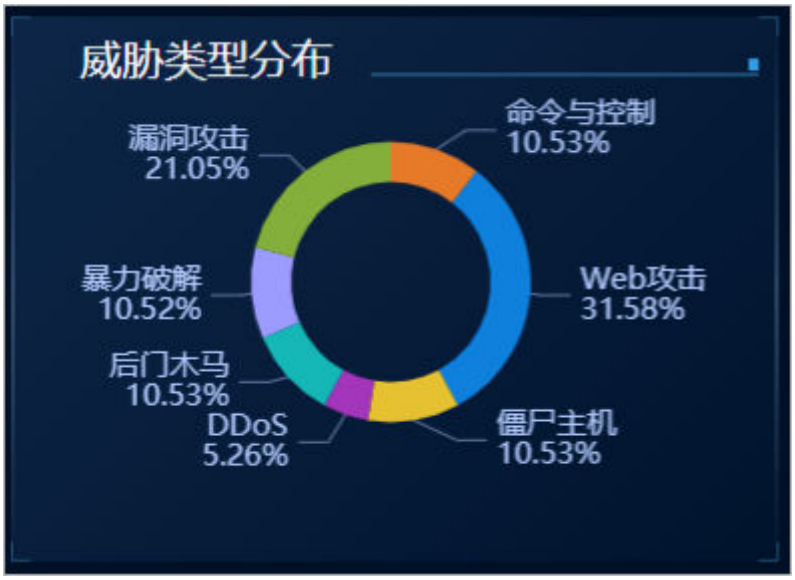
图 6-5 威胁事件趋势



威胁类型分布

如图6-6所示，威胁类型分布体现了**近7天内**受到威胁的类型及不同威胁类型所占的比例。

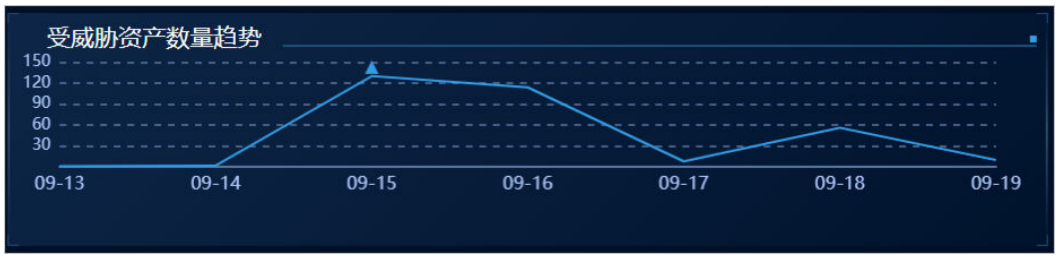
图 6-6 威胁类型分布



受威胁资产数量趋势

如图6-7所示，展示**近7天内**每日受到威胁的资产的数量，受威胁资产数量趋势的横坐标表示时间，纵坐标表示受威胁资产的数量。将鼠标箭头置于某个日期上，可以看到该日受威胁的资产总数。

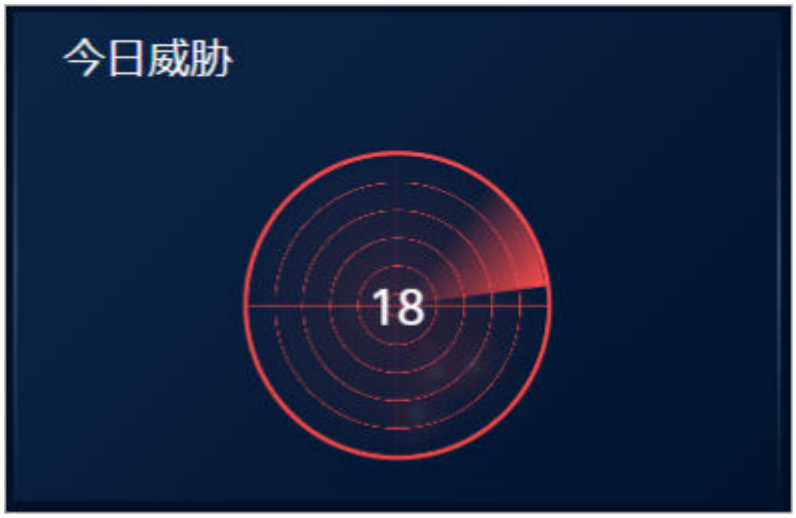
图 6-7 受威胁资产数量趋势



今日威胁雷达图

如图6-8所示，今日威胁雷达图体现了**今天**发现的威胁数量。

图 6-8 今日威胁雷达图



威胁源主机 TOP5

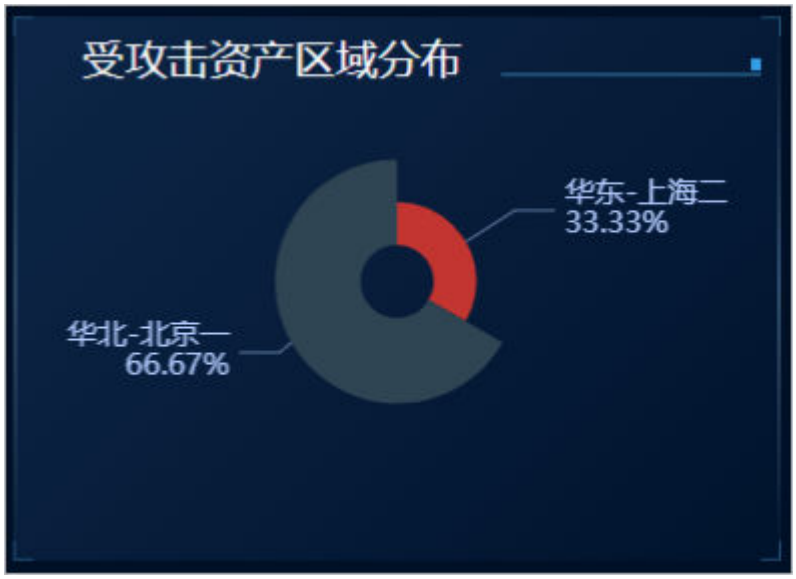
如图6-9所示，威胁源主机TOP5展示了**近7天内**产生威胁数最多的前5台主机的相关信息，包括主机的IP地址、所属国家/地区和攻击次数，并按照威胁数量从高到低的次序进行排列。

图 6-9 威胁源主机 TOP5

受攻击资产区域分布

如图6-10所示，受攻击资产区域分布以区域为维度，体现了**近7天内**受攻击资产的比例。

图 6-10 受攻击资产区域分布



6.2 主机安全态势

在现场讲解汇报、实时监控等场景下，为了获得更好的演示效果，通常需要将态势感知服务的分析结果展示在大型屏幕上。如果只是单纯将控制台界面放大显示，视觉效果并不是很理想。此时可以利用**综合大屏**，展示专为大型屏幕设计的服务界面，获得更清晰的态势信息和更好的视觉效果。

前提条件

已开通**安全大屏**增值项，可查看综合态势感知大屏相关信息。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“综合大屏”，进入“综合大屏”页面。

图 6-11 查看综合大屏信息

步骤4 单击“主机安全态势”图片，进入“华为云主机安全态势”信息页面，如图6-12。

界面中各个模块的功能介绍和使用方法详见下述内容。

图 6-12 主机安全态势大屏

----结束

风险主机地图

区域维度风险主机直观展示了**当天**不同华为云区域内是否有风险主机。没有风险主机的区域，指示灯为绿色，有威胁主机的区域，指示灯为红色。当用鼠标单击亮灯的区域时，则分别显示出该区域的主机总数、Windows系统主机台数、Linux系统主机台数和该区域的风险主机台数。通过将风险主机具象化，用户可以直观的了解资产的安全状况。

说明

- “华为云主机安全态势”大屏风险主机示意地图，根据华为云部署区域概略展示，背景地图不能做高精确定位。
- “华为云主机安全态势”大屏风险主机示意地图，仅用于演示与汇报，不是为了任何非法目的，也不具有任何恶意。

主机安全事件统计

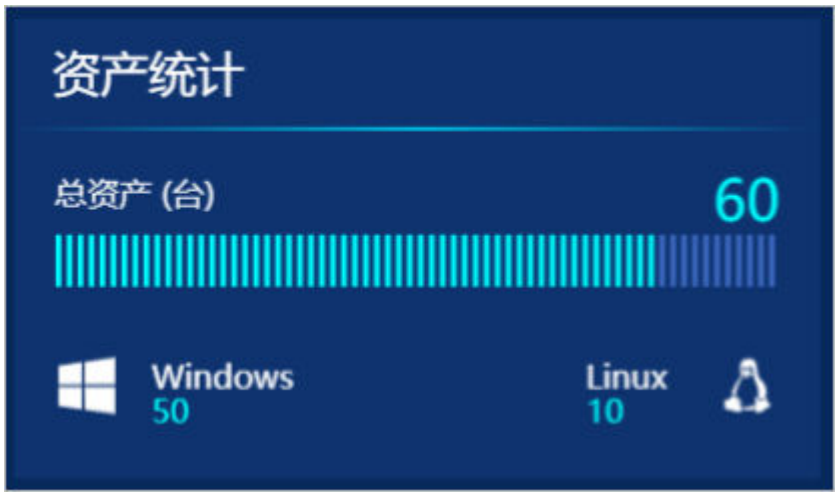
如图6-13所示，主机安全事件详情展示了**当天**威胁主机安全的5种告警类型，分别是暴力破解、异地登录、恶意程序、网站后门、文件变更。一个环形图表示一种类型，每个环形图中间的数字表示当天此种威胁出现的次数。环形图下方的风险主机台数体现了当天遭受此种威胁的主机数，亮蓝色的环形占总环形的比例表示风险主机占总资产的比例，以暴力破解环形图为例，当天一共有2台主机遭受了1次暴力破解。

图 6-13 主机安全事件详情

资产统计

如图6-14所示，资产统计展示了总资产的数量和类型，两类主机分为Windows系统主机和Linux系统主机。中间的条形图直观显示了这两种主机占总资产的比例，下方则显示了这两种主机的具体数量。

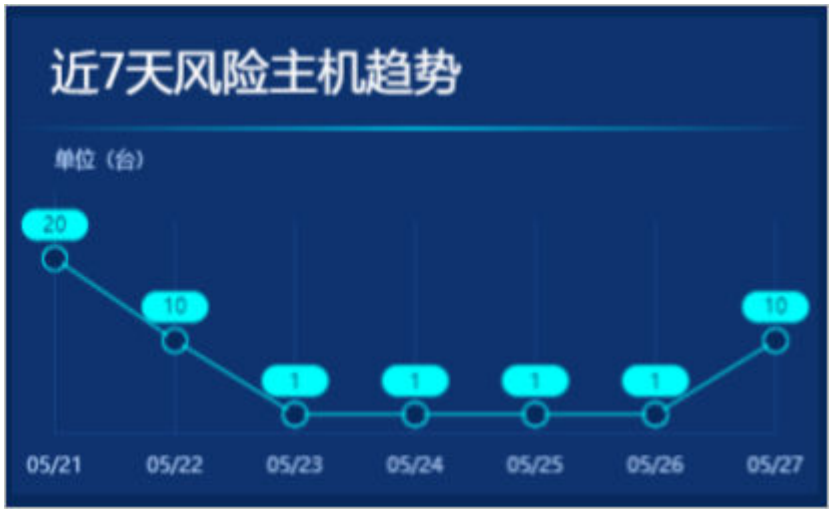
图 6-14 资产统计



近 7 天风险主机趋势

如图6-15所示，风险主机趋势的横坐标表示具体日期，纵坐标表示风险主机数量。从图中可看到**近7天内**每天的风险主机数量和风险主机趋势。

图 6-15 风险主机趋势



TOP5 风险云主机

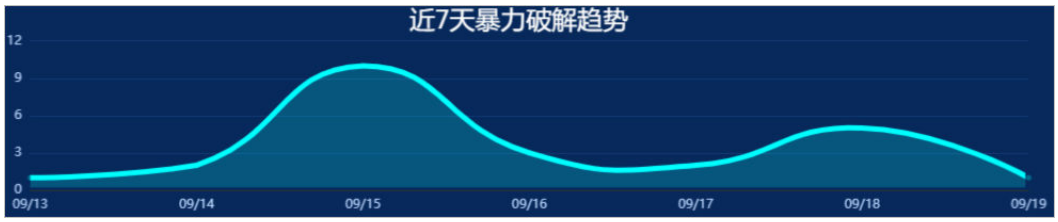
如图6-16所示，TOP5风险云主机按照安全风险等级由高到低展示了**当天**受威胁主机的相关信息，包括主机名称、主机系统及受到的攻击程度。TOP5风险云主机最多展示5条。安全风险等级由高到低分别是致命、高危、中危、低危和提示。

图 6-16 风险云主机

近 7 天暴力破解趋势

如图6-17所示，近7天暴力破解攻击趋势展示了**近7天内**每天的暴力破解次数，横坐标表示时间，纵坐标表示暴力破解的次数。将鼠标悬停于某日期范围内，可以看到该日暴力破解的次数。

图 6-17 近 7 天暴力破解攻击趋势



漏洞检测

如图6-18所示，漏洞检测的环形图展示了**当天**检测出的Window漏洞与Linux漏洞的比例。环形图下方显示两种漏洞的个数，右上角显示了检测出漏洞的风险主机的台数。

图 6-18 漏洞检测

基线检测

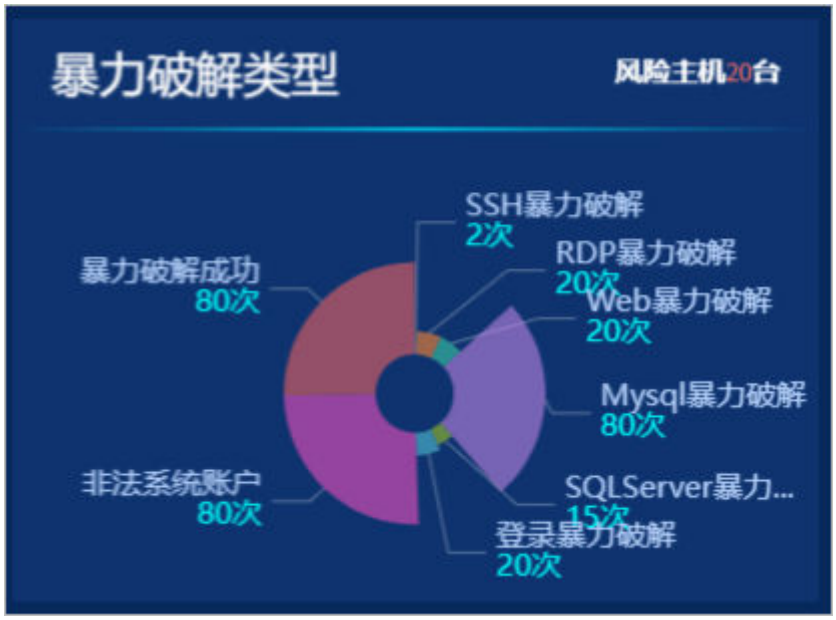
如图6-19所示，您可以通过主机基线模块查看口令复杂度和配置检测这两方面的风险及个数。

图 6-19 基线检测

暴力破解类型

如图6-20所示，暴力破解类型展示了**当天**暴力破解的类型及每种类型的攻击次数。暴力破解一共有5种类型，分别是SSH暴力破解、RDP暴力破解、WEB暴力破解、MsSQL暴力破解、SQLServer暴力破解。右上角展示了当天受到暴力破解威胁的全部风险主机的台数。

图 6-20 暴力破解类型



7 威胁告警

7.1 威胁告警简介

背景信息

态势感知威胁告警功能汇集了华为云多个安全服务的告警能力，按照告警类型和等级统一维度呈现，可以准确实时监控云上威胁攻击、检测您资产中的安全告警事件。

同时，通过威胁分析，从攻击源和受攻击资产两个维度，帮助您及时发现资产中的安全威胁、实时掌握您资产的安全态势。

态势感知威胁告警支持以下功能项：

- **告警列表**

  通过“实时监控”云上威胁告警事件，并接入AntiDDos、HSS、WAF等服务上报的告警事件，提供告警通知和监控，记录近180天告警事件详情。
- **威胁分析**

  从“攻击源”或“被攻击资产”查询威胁攻击，统计威胁攻击次数或资产被攻击次数。
- **告警通知**

  自定义威胁告警通知，设置每日定时告警通知和实时告警通知，通过接收消息通知及时了解威胁风险。
- **告警监控**

  自定义监控的威胁名单、告警类型、告警级别等，选择性呈现关注的威胁告警。

告警类型

目前SA支持检测8类威胁告警事件，共包括200+种子告警类型。

说明

SA**基础版**支持检测部分威胁攻击事件。为全面快速地了解并处理资产遭受的威胁，确保云上资产安全，建议您购买标准版或专业版。

DDoS 事件

“实时检测”华为云、非华为云及IDC的互联网主机的DDoS攻击。

共支持检测100+种子类型的DDoS威胁。

- 网络层攻击
  NTP Flood攻击、CC攻击等。
- 传输层攻击
  SYN Flood攻击、ACK Flood攻击等。
- 会话层攻击
  SSL连接攻击等。
- 应用层攻击
  HTTP Get Flood攻击、HTTP Post Flood攻击等。

暴力破解事件

“实时检测”入侵资产的行为和主机资产内部的风险，检测SSH、RDP、FTP、SQL Server、MySQL等账户是否遭受的口令破解攻击，以及检测资产账户是否被破解异常登录。

共支持检测22种子类型的暴力破解威胁。

- 支持检测的暴力破解威胁
  包括SSH暴力破解（2种）、RDP暴力破解、MSSQL暴力破解、MySQL暴力破解、FTP暴力破解、SMB暴力破解（3种）、HTTP暴力破解（4种）、Telnet暴力破解。
- 接入的HSS服务上报的告警事件
  包括SSH暴力破解、RDP暴力破解、FTP暴力破解、MySQL暴力破解、IRC暴力破解、Webmin暴力破解、其他端口被暴力破解、系统被成功爆破事件。

Web 攻击事件

“实时检测”Web恶意扫描器、IP、网马等威胁。

共支持检测38种子类型的Web攻击威胁。

- 支持检测的Web攻击威胁
  包括Webshell攻击（3种）、跨站脚本攻击、代码注入攻击（7种）、SQL注入攻击（9种）、命令注入攻击。
- 接入的HSS服务上报的告警事件
  包括Webshell攻击、Linux网页篡改、Windows网页篡改。
- 接入的WAF服务上报的告警事件
  包括跨站脚本攻击、命令注入攻击、SQL注入攻击、目录遍历攻击、本地文件包含、远程文件包含、远程代码执行、网站后门、网站信息泄露、漏洞攻击、IP信誉库、恶意爬虫、网页防篡改、网页防爬虫。

后门木马事件

“实时检测”资产系统是否存在后门木马风险，以及被后门木马程序入侵后的恶意请求行为。

共支持检测5种子类型的后门木马威胁。

- 检测主机资产上Web目录中的PHP、JSP等后门木马文件类型。
- 检测资产被植入木马特性

  检测内容包括资产系统存在win32/ramnit checkin木马、被入侵后执行wannacry勒索病毒相关的DNS解析请求、被入侵后尝试下载木马程序，被入侵后访问HFS下载服务器等。

僵尸主机事件

“实时检测”资产被入侵后对外发起攻击的威胁。共支持检测7种子类型的僵尸主机威胁。

- 对外发起SSH暴力破解
- 对外发起RDP暴力破解
- 对外发起Web暴力破解
- 对外发起MySQL暴力破解
- 对外发起SQLServer暴力破解
- 对外发起DDoS攻击
- 被入侵后安装挖矿程序

异常行为事件

“实时检测”资产系统异常变更和操作行为。共支持检测21种子类型的异常行为威胁。

共支持检测21种子类型的异常行为威胁。

- 支持检测的异常行为威胁

  包括文件系统被扫描、CMS V1.0漏洞、敏感文件被访问。
- 接入的HSS服务上报的告警事件

  包括系统成功登录审计事件、文件目录变更监测事件、混杂模式网卡、异常权限用户、反弹Shell、异常Shell、高危命令执行、异常自启动、文件提权、进程提权、Rootkit程序。
- 接入的WAF服务上报的告警事件

  包括自定义规则、白名单、黑名单、地理访问控制、扫描器爬虫、IP黑白名单、非法访问。
- 接入的MTD服务上报的告警事件

  包括暴力破解、恶意攻击、渗透、挖矿攻击等恶意活动和未经授权行为。

漏洞攻击事件

“实时检测”资产被尝试使用漏洞进行攻击。共支持检测2种子类型的漏洞攻击威胁。

- SMBv1漏洞攻击
- WebCMS漏洞攻击

命令控制事件

“实时检测”资产可能被命令与控制服务器（C&C，Command and Control Server）远程控制，访问与恶意软件或建立与恶意软件之间的链接。

共支持检测3种子类型的命令控制威胁。

- 监控主机存在访问DGA域名行为
- 监控主机存在访问恶意C&C域名行为
- 监控主机存在恶意C&C通道行为

7.2 查看告警列表

通过查看“告警列表”，您可以了解近180天的告警威胁的统计信息列表，列表内容包括告警事件的名称、类型、等级和发生时间等。并可通过自定义过滤条件，如告警名称、告警等级和发生时间等，快速查询到相应告警事件的统计信息。

此外，您还可以通过及时处理告警事件，标记告警事件处理状态，并支持一键导出近180天的告警事件。

约束限制

- 仅标准版和专业版支持忽略和标记告警事件，基础版不支持。
- 仅支持导出近180天的全部告警事件，暂不支持筛选导出告警事件信息。
- 按过滤场景筛选告警，最多可呈现10000条告警。

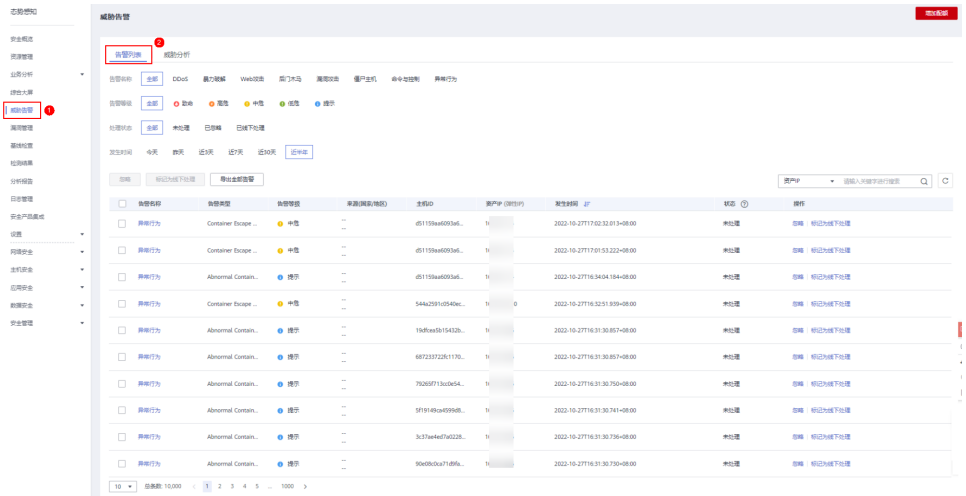
查看告警详情

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在态势感知管理页面选择“威胁告警 > 告警列表”，进入态势感知告警列表管理页面。

图 7-1 查看告警列表信息



步骤4 筛选“告警名称”、“告警等级”、“发生时间”和“处理状态”条件选项，在列表栏查看显示符合过滤条件的告警事件列表。

- 告警名称：告警事件所属的分类。
- 告警等级：告警事件对应的等级，包括“致命”、“高危”、“中危”、“低危”、“提示”。
- 处理状态：用户对告警事件的处理标记，可选择“未处理”、“已忽略”、“已线下处理”。
- 发生时间：告警事件发生的时间范围，可选择“今天”、“昨天”、“近3天”、“近7天”、“近30天”和“近半年”。

步骤5 当过滤后的告警事件较多时，可以利用搜索功能快速找到指定告警事件。

在下拉框中选择“资产IP”、“来源IP”、“主机ID”，在搜索框中输入相应IP或ID，单击，即可查看到指定资产相关的告警信息。

步骤6 查看告警事件详情。

单击列表中告警的“告警名称”，右侧滑出告警详情窗口，可查看与该告警相关的“基本信息”、“数据来源”、“攻击信息”、受影响的用户等信息，以及该告警的处理状态。

----结束

标记告警事件

当SA检测出告警事件后，您可手动标记已处理的告警事件。

步骤1 在“告警列表”页面，标记告警事件的处理状态。

- 忽略：如果确认该告警事件不会造成危害，可标记为“已忽略”状态。
- 标记为线下处理：如果该告警事件已在线下处理，在“标记为线下处理”窗口记录“处理人”、“处理时间”和“处理结果”，可标记为“已线下处理”状态。

步骤2 批量标记告警事件。

选择一个或多个“未处理”状态的告警，单击“忽略”或“标记为线下处理”，对不同告警事件批量执行相应的处理操作。

步骤3 单个标记告警事件。

在告警列表对应“操作”列，单击“忽略”或“标记为线下处理”，对单个告警事件执行相应处理操作。

步骤4 取消告警事件标记。

告警处理状态标记后，可在告警事件对应“操作”列，单击“取消忽略”或“取消标记”，恢复告警“未处理”状态，再修改告警状态。

----结束

导出告警事件

在“告警列表”页面，单击“导出全部告警”，一键导出列表中全部告警事件，并以excel文件形式保存在本地。导出完成后，即可离线查看告警事件列表。

图 7-2 导出告警事件

导出的excel文件中包含“事件标识”、“受影响资源”、“严重等级”和“发现时间”等信息。

说明

目前仅支持导出近180天的全部告警事件。

7.3 威胁分析

当告警列表中积累了较多威胁告警信息时，您可以使用“威胁分析”功能，从“攻击源”或“被攻击资产”的维度分析网络攻击情况。

前提条件

已购买态势感知标准版或专业版，且在有效使用期内。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在态势感知管理页面选择“威胁告警 > 威胁分析”，进入态势感知威胁分析管理页面。

步骤4 在下拉框中选择条件“攻击源”或“被攻击资产”、“发生时间”，并输入待查询的IP地址，单击“开始分析”。

说明

发生时间可选择“今天”、“昨天”、“近3天”、“近7天”、“近30天”、“近半年”。

步骤5 在列表栏查看符合过滤条件的威胁信息，可以直观看到该攻击源对哪些资产发起了何种类型的攻击，或被攻击资产遭到了哪些攻击。

----结束

7.4 告警事件处理

7.4.1 DDoS

告警类型说明

分布式拒绝服务（Distributed Denial of Service，简称DDoS）攻击是指攻击者使用网络上多个被攻陷的电脑作为攻击机器，向特定的目标发动DoS攻击。DoS（Denial of Service）攻击也称洪水攻击，是一种网络攻击手法，其目的在于使目标电脑的网络或系统资源耗尽，服务暂时中断或停止，导致合法用户不能够访问正常网络服务的行为。

DDoS威胁父类型约有100多种子类型，态势感知基础版、标准版和专业版支持全部DDoS的子类型威胁告警。

处理建议

当检测到应用系统受到DDoS类威胁时，代表应用系统受到DDoS类攻击，属于“提示”告警级别威胁，建议用户直接购买**DDoS高防服务**防护。

7.4.2 暴力破解

告警类型说明

暴力破解法（BruteForce）是一种密码分析方法，基本原理是在一定条件范围内对所有可能结果进行逐一验证，直到找出符合条件的结果为止。攻击者通常使用暴力破解的方式猜测远程登录的用户名和密码，一旦破解成功，即可实施攻击和控制。

态势感知支持检测22种子类型的暴力破解威胁，基础版不支持检测暴力破解类威胁，标准版支持检测8种子类型威胁，专业版支持检测全部子类型威胁（其中有8种类型需要购买**主机安全服务**）。

处理建议

当检测到暴力破解类威胁时，各子类型威胁处理建议参见**表7-1**。

表 7-1 部分暴力破解类威胁处理建议

威胁告警名称	告警等级	威胁说明	处理建议
SSH暴力破解	中危	检测到ECS实例被不断尝试SSH登录，代表有攻击者正在尝试对ECS实例做SSH暴力破解攻击尝试。	攻击发生主要原因是SSH端口开放到公网，因此建议按照如下方式处理： 1. 在安全组设置中限制外部SSH访问； 2. 在ECS操作系统中配置hosts.deny。
RDP暴力破解	中危	检测到ECS实例被不断尝试RDP登录，代表有攻击者正在尝试对ECS实例做RDP暴力破解攻击尝试。	攻击发生的主要原因是RDP端口开放到公网，因此建议按照如下方式处理： 1. 在安全组设置中限制外部RDP访问； 2. 在ECS操作系统中配置远程桌面访问控制，如配置Windows防火墙等。

威胁告警名称	告警等级	威胁说明	处理建议
Web暴力破解	中危	检测到Web服务（如登录页面等）被不断尝试登录，代表有攻击者正在尝试对Web应用登录页面等做暴力破解攻击尝试。	攻击发生的主要原因是将应用的后台管理页面（如phpMyAdmin、tomcat管理页面等）开放到公网；需要开放到公网访问的业务，登录页面未做登录校验。因此建议按照如下方式处理： 1. 在安全组设置中限制外部访问后台管理系统页面； 2. 在Web应用中设置防爆破逻辑，如设置登录短信验证码、图片验证码等；
MySQL爆破	中危	检测到ECS实例上的MySQL被不断尝试登录，代表有攻击者正在尝试对ECS实例做MySQL暴力破解攻击尝试。	攻击发生的主要原因是MySQL服务端口开放到公网，因此建议按照如下方式处理： 1. 在安全组中限制外部访问MySQL实例； 2. 配置OS上的防火墙策略，限制外部访问； 3. 解除安装MySQL实例的ECS与EIP的绑定关系。
MS SQL爆破	中危	检测到ECS实例上的MS SQLServer被不断尝试登录，代表有攻击者正在尝试对ECS实例做MS SQLServer暴力破解攻击尝试。	攻击发生的主要原因是MS SQLServer服务端口开放到公网，因此建议按照如下方式处理： 1. 在安全组设置中限制外部访问MS SQLServer实例； 2. 配置OS上的防火墙策略，限制外部访问； 3. 解除安装MS SQLServer实例的ECS与EIP的绑定关系。
系统爆破检测事件	中危	检测到ECS实例被暴力破解攻击，不断被尝试登录。	建议登录企业主机安全管理控制台处理。
非法系统账户	中危	检测到ECS实例被暴力破解攻击，不断被非法系统账户尝试登录。	建议登录企业主机安全管理控制台处理。
系统被成功爆破事件	高危	检测到用户ECS实例被爆破成功。	建议登录企业主机安全管理控制台处理。

7.4.3 Web 攻击

告警类型说明

Web攻击（WebAttack）是针对用户上网行为或网站服务器等设备进行攻击的行为。常见的Web攻击方式包括SQL注入攻击、跨站脚本攻击、跨站请求伪造攻击等。

态势感知支持检测38种子类型的Web攻击威胁，基础版不支持检测Web攻击类威胁，标准版支持检测19种子类型威胁，专业版支持检测全部子类型威胁（其中有14种类型需要购买**Web应用防火墙服务**，3种类型需购买**主机安全服务**）。

处理建议

当检测到Web攻击类威胁时，代表有攻击者正在尝试对Web应用漏洞做攻击尝试，属于“中危”及以下告警级别威胁。因此建议按照如下方式处理：

1. 检查Web应用逻辑是否有相应漏洞；
2. 购买Web应用防火墙服务防护。

7.4.4 后门木马

告警类型说明

后门木马又称特洛伊木马（Trojan Horse），是一种后门程序。后门木马具有很高的伪装性，通常表现为一个正常的应用程序或文件，以获得广泛的传播和目标用户的信任。当目标用户执行后门木马程序后，攻击者即可对用户的主机进行破坏或盗取敏感数据，如各种账户、密码、保密文件等。在黑客进行的各种攻击行为中，后门木马基本上都起到了先导作用，为进一步的攻击打下基础。

态势感知支持检测5种子类型的后门木马威胁，基础版不支持检测后门木马类威胁，标准版支持检测1种子类型威胁，专业版支持检测全部子类型威胁。

处理建议

当检测到后门木马类威胁时，ECS实例存在木马程序网络请求，代表ECS实例已经存在被植入木马的特征，如尝试做wannacry勒索病毒相关DNS解析请求、尝试下载exe类木马程序等，属于“高危”告警级别威胁。因此建议按照如下方式处理：

1. 关闭被攻击ECS实例；
2. 检查实例所在子网的其他主机是否被入侵；
3. 购买企业主机安全服务防护。

7.4.5 漏洞攻击

告警类型说明

漏洞是指计算机系统安全方面的缺陷，可导致系统或应用数据遭受保密性、完整性、可用性等方面的威胁。攻击者利用漏洞获取计算机权限、盗取敏感数据、破坏软硬件系统等行为均可称为漏洞攻击。

态势感知支持检测2种子类型的漏洞攻击威胁，基础版不支持检测漏洞攻击类威胁，标准版不支持检测漏洞攻击，专业版支持检测全部子类型威胁。

处理建议

当检测到漏洞攻击类威胁时，各子类型威胁处理建议参见表7-2。

表 7-2 漏洞攻击类威胁处理建议

威胁告警名称	告警等级	威胁说明	处理建议
MySQL漏洞攻击	低危	检测到ECS实例被尝试利用MySQL漏洞攻击，代表ECS实例被尝试使用MySQL漏洞进行攻击。	攻击发生主要原因是ECS实例在公网上开放了MySQL服务，因此建议按照如下方式处理： 1. 配置安全组规则，限制MySQL服务公网访问； 2. 解绑ELB，关闭MySQL服务公网访问入口。
Redis漏洞攻击	低危	检测到ECS实例被尝试利用Redis漏洞攻击，代表ECS实例被尝试使用Redis漏洞进行攻击。	攻击发生主要原因是ECS实例在公网上开放了Redis服务，因此建议按照如下方式处理： 1. 配置安全组规则，限制Redis服务公网访问； 2. 解绑ELB，关闭Redis服务公网访问入口。

7.4.6 僵尸主机

告警类型说明

僵尸主机亦称傀儡机，是由攻击者通过木马蠕虫感染的主机，大量僵尸主机可以组成僵尸网络（Botnet）。攻击者通过控制信道向僵尸网络内的大量僵尸主机下达指令，令其发送伪造包或垃圾数据包，使攻击目标瘫痪并“拒绝服务”，这就是常见的DDoS攻击。此外，随着虚拟货币（如比特币）价值的持续增长，以及挖矿成本的逐渐增高，攻击者也开始利用僵尸主机进行挖矿和牟利。

态势感知支持检测7种子类型的僵尸主机威胁，基础版不支持检测僵尸主机类威胁，标准版支持检测5种子类型威胁，专业版支持检测全部子类型威胁。

处理建议

当检测到僵尸主机类威胁时，检测到ECS实例存在挖矿特性行为（如访问矿池地址等）、对外发起DDoS攻击或暴力破解攻击，代表ECS实例可能已经被植入挖矿木马或后门程序，可能变成僵尸网络，属于“高危”告警级别威胁。因此建议按照如下方式处理：

1. 对ECS实例做病毒木马查杀，查杀失败则关闭该实例；
2. 检查实例所在子网的其他主机是否被入侵；
3. 购买企业主机安全服务防护。

7.4.7 命令与控制

告警类型说明

域名生成算法（Domain Generation Algorithm，DGA）是一种利用随机字符生成命令与控制（Command and Control，C&C）域名的技术，常被用于逃避域名黑名单功能的检测。攻击者利用DGA产生恶意域名后，选择部分域名进行注册并指向C&C服务器。当受害者运行恶意程序后，主机将通过恶意域名连接至C&C服务器，攻击者即可远程操控主机。

态势感知支持检测3种子类型的命令与控制类威胁，基础版和标准版不支持检测命令与控制类威胁，专业版支持检测全部子类型威胁。

处理建议

当检测到命令与控制类威胁时，ECS实例存在访问DGA域名、访问远程C&C服务器或建立了连接C&C的通道，一种恶意软件访问或连接行为，代表ECS实例可能正在被C&C远程控制，可能变成僵尸网络，属于“高危”告警级别威胁。因此建议按照如下方式处理：

1. 对ECS实例做病毒木马查杀，查杀失败则关闭该实例；
2. 检查实例所在子网的其他主机是否被入侵；
3. 购买企业主机安全服务防护。

7.4.8 异常行为

告警类型说明

异常行为（Abnormal Behavior）主要指在主机中发生了一些不应当出现的事件。例如，某用户在非正常时间成功登录了系统，一些文件目录发生了计划外的变更，进程出现了非正常的行为等。这些异常的行为事件很多是有恶意程序在背后作乱。所以在发生这类异常行为时，应当引起重视。态势感知中的异常行为数据主要来源于主机安全服务和Web应用防火墙服务。

态势感知支持检测21种子类型的异常行为威胁，基础版不支持检测异常行为类威胁，标准版支持检测7种子类型威胁，专业版支持检测全部子类型威胁（其中有7种类型需要购买**Web应用防火墙**，11种类型需要购买**主机安全服务**）。

处理建议

当检测到异常行为类威胁时，各子类型威胁处理建议参见**表7-3**。

表 7-3 部分异常行为类威胁处理建议

威胁告警名称	告警等级	威胁说明	处理建议
文件目录变更监测事件	提示	检测到ECS实例的关键文件被更改。	建议登录企业主机安全管理控制台处理。
系统成功登录审计事件	提示	检测到ECS实例已异常成功登录。	建议登录企业主机安全管理控制台处理。

威胁告警名称	告警等级	威胁说明	处理建议
进程异常行为	低危	检测到ECS实例存在进程异常行为，疑似恶意程序。	建议登录企业主机安全管理控制台处理。

8 漏洞管理

8.1 漏洞管理简介

背景介绍

态势感知通过集成华为云安全公告、漏洞扫描数据，以及实施扫描任务，集中呈现云上资产漏洞风险，以及实时通报突发安全漏洞预警，帮助用户及时发现资产安全短板，修复危险漏洞。

态势感知支持以下类型的漏洞：

- **应急漏洞公告**

  接入华为云安全公告数据信息，呈现业界近期广泛披露的热点安全漏洞。
- **主机漏洞**

  包括Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞。
- **网站漏洞**

  包括Web常规漏洞、端口漏洞、弱密码、CVE漏洞、网页内容合规（图片、文字）、网站挂马、链接健康等共8大类漏洞的检测。

应急漏洞公告

态势感知通过采集华为云安全公告讯息，及时呈现业界近期广泛披露的安全漏洞，并支持一键获取安全漏洞详情、影响范围和处置建议等信息，提供对资产风险的消减建议。应急漏洞功能支持以下特性：

- 支持追溯已披露的安全漏洞至2014年4月。
- 支持每5分钟抓取一次安全公告讯息，更新应急漏洞公告。
- 支持按披露时间排序应急漏洞公告列表。
- 支持按关键字查找应急漏洞公告。
- 支持导出应急漏洞公告列表。

主机漏洞

态势感知通过**授权主机**，并**一键扫描主机漏洞**，呈现主机漏洞扫描检测信息，支持查看漏洞详情，并提供相应漏洞修复建议。

主机漏洞共支持3大类漏洞项的检测，详情请参见**表8-1**说明。

表 8-1 主机漏洞检测项说明

检测项	说明
Linux软件漏洞检测	通过与漏洞库进行比对，检测系统和软件（例如：SSH、OpenSSL、Apache、MySQL等）是否存在的漏洞，呈现漏洞结果，并提供修复建议。
Windows系统漏洞检测	通过订阅微软官方更新，判断服务器上的补丁是否已经更新，并推送微软官方补丁，呈现漏洞结果，并提供修复建议。
Web-CMS漏洞检测	通过对Web目录和文件进行检测，识别出Web-CMS漏洞，呈现漏洞结果。

网站漏洞

态势感知通过接入漏洞管理服务的扫描结果数据，集中呈现网站存在的漏洞，提供详细的漏洞分析结果，并针对不同类型的漏洞提供专业可靠的修复建议。

网站漏洞共支持8大类漏洞项的检测，详情扫描内容参见**表8-2**。

表 8-2 网站漏洞检测项说明

检测项	说明
Web常规漏洞扫描	默认必选扫描项。扫描常规的30+种Web漏洞，包括XSS、SQL等网站漏洞。
端口扫描	（可选）扫描服务器端口的开放状态，检测出容易被黑客发现的“入侵通道”。
弱密码扫描	（可选）扫描网站的弱密码漏洞。 • 全方位的OS连接，涵盖90%的中间件，支持标准Web业务弱密码检测、操作系统、数据库等弱口令检测。 • 丰富的弱密码匹配库，模拟黑客对各场景进行弱口令探测。
CVE漏洞扫描	（可选）接入公共暴露漏洞库（Common Vulnerabilities and Exposures，CVE），根据漏洞库快速更新漏洞规则，扫描CVE最新漏洞。
网页内容合规检测（文字）	（可选）检测网站文字的合规性。
网页内容合规检测（图片）	（可选）检测网站图片的合规性。
网站挂马检测	（可选）检测网站的挂马漏洞风险。

检测项	说明
链接健康检测	（可选）检测网站的链接地址健康性，避免死链、暗链、恶意链接。

8.2 查看应急漏洞公告列表

当业界有新安全漏洞披露时，您可以使用“应急漏洞公告”功能，获取业界近期披露的热点安全漏洞信息，助您及时确认资产是否有受到威胁，消减资产风险。

应急漏洞功能支持以下特性：

- 支持每5分钟抓取一次安全公告讯息，更新应急漏洞公告。
- 支持按披露时间排序应急漏洞公告。
- 支持按关键字查找应急漏洞公告。
- 支持导出全部应急漏洞公告列表。

约束限制

- 仅支持追溯已披露的安全漏洞公告至2014年4月。
- 仅支持导出应急漏洞公告列表，暂不支持导出公告详细信息。

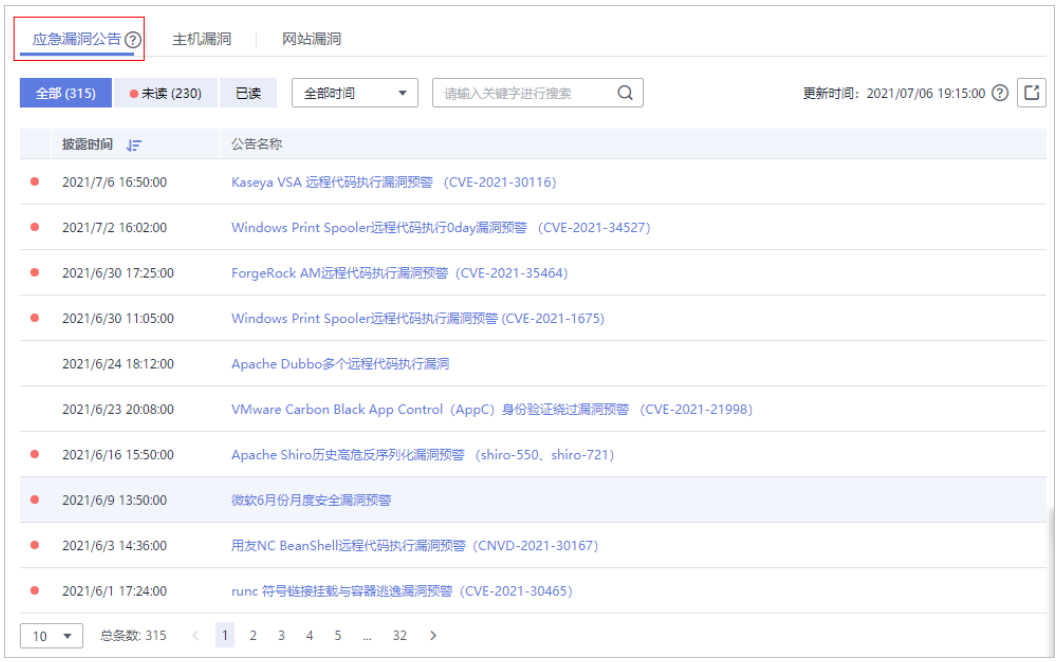
查看应急漏洞公告

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在态势感知管理页面选择“漏洞管理 > 应急漏洞公告”，进入“应急漏洞公告”汇聚页面。

图 8-1 应急漏洞公告



步骤4 查看应急漏洞公告列表刷新时间。

查看右上角“更新时间”，即可获知列表刷新时间。

步骤5 查看应急漏洞公告详细信息。

单击应急漏洞公告名称，“一键跳转”到安全公告的漏洞详情页面，可查看安全漏洞披露历程，威胁级别、影响范围、处置办法等信息。

步骤6 按时间查看应急漏洞公告。

在下拉框筛选“全部时间”、“近7天”、“近3天”或“近24小时”条件选项，在列表栏查看显示符合过滤条件的应急漏洞公告。

步骤7 搜索历史应急漏洞公告。

通过在搜索框输入关键字，可搜索到相关应急漏洞公告，在列表栏查看显示符合过滤条件的应急漏洞公告。

----结束

导出应急漏洞公告

在“应急漏洞公告”页面，单击右上角导出标识，“一键导出”当前列表中安全公告，并以Excel文件形式保存在本地。导出完成后，即可离线查看应急漏洞公告列表。

导出的Excel文件中包含“公告名称”、“披露时间”、“链接”等信息。

8.3 查看主机漏洞扫描详情

执行完主机漏洞扫描任务后，可在主机漏洞页面查看扫描结果。

约束限制

受漏洞管理服务（CodeArts Inspector）调整影响，仅付费续存期用户可继续正常使用主机漏洞功能。

新用户以及付费版本到期的用户，请先开启HSS产品集成（详情请参见**启用产品集成**），通过查看全部检查结果，获取主机扫描结果。

前提条件

- 已购买态势感知标准版或专业版，且在有效使用期内。
- 已完成主机漏洞扫描任务。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在态势感知管理页面选择“漏洞管理 > 主机漏洞”，进入“主机漏洞”页面。主机漏洞参数说明如**表8-3**。

说明

在列表的右上角，用户可以根据漏洞IP、漏洞等级或者漏洞名称进行筛选查看目标类漏洞详情。

图 8-2 主机漏洞

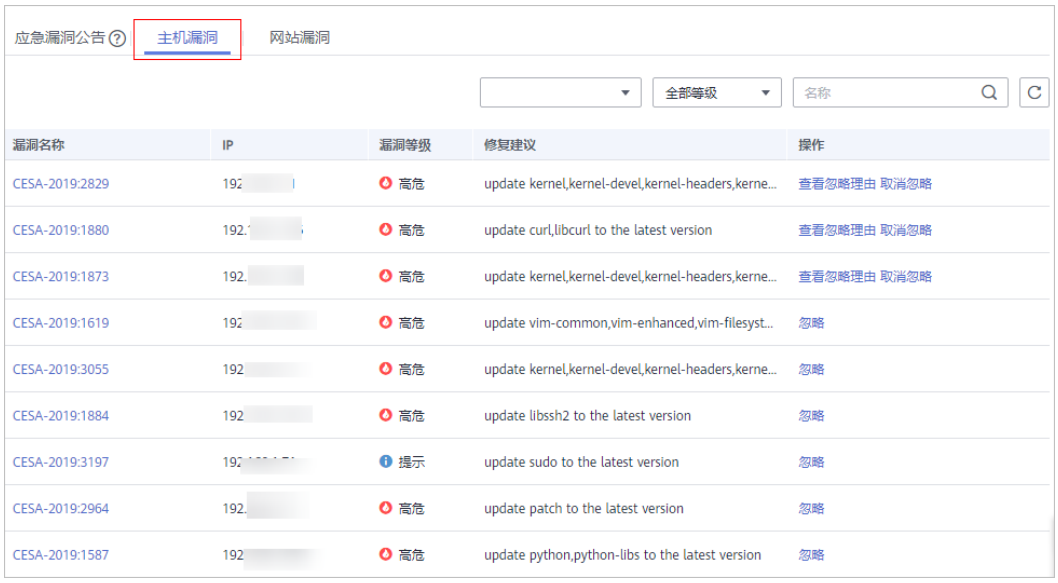


表 8-3 主机漏洞参数说明

参数名称	参数说明
漏洞名称	扫描出的漏洞名称。 单击漏洞名称，可查看该漏洞的简介、相关漏洞库信息。
IP	主机的IP地址。

参数名称	参数说明
漏洞等级	按照漏洞的危险程度分为：“高危”、“中危”、“低危”、“提示”。
修复建议	根据修复建议，快速对漏洞做出响应处理。
操作	• 如果某一项漏洞您已经完成了修复，可以在目标漏洞的“操作”列，单击“忽略”。 • 如果希望重新关注已经忽略的漏洞，可以在目标漏洞的“操作”列，单击“查看忽略理由”了解当时的处理原因，确认需要恢复风险项后，单击“取消忽略”，恢复风险项检测。

----结束

8.4 查看网站漏洞扫描详情

执行完网站漏洞扫描任务后，可在网站漏洞页面查看扫描结果。

约束限制

- 受漏洞管理服务（CodeArts Inspector）调整影响，仅付费续存期用户可继续正常使用主机漏洞功能。

  新用户以及付费版本到期的用户，请先开启CodeArts Inspector产品集成（详情请参见**启用产品集成**），通过查看全部检查结果，获取网站扫描结果。

前提条件

- 已购买态势感知专业版，且在有效使用期内。
- 已完成网站扫描任务。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在态势感知管理页面选择“漏洞管理 > 网站漏洞”，进入“网站漏洞”页面。

图 8-3 查看网站漏洞信息

步骤4 查看漏洞分布比例及漏洞等级分布比例，如图8-4。

图 8-4 网站漏洞

步骤5 查看漏洞详情列表，网站漏洞参数说明如表8-4。

图 8-5 网站漏洞详情列表

表 8-4 网站漏洞参数说明

参数名称	参数说明
漏洞名称/漏洞ID	扫描出的漏洞名称。 单击漏洞名称，可查看该漏洞的简介、相关漏洞库信息。
目标网址	网站的IP地址。
发现时间	任务扫描出漏洞的时间。
漏洞等级	按照漏洞的危险程度分为：“高危”、“中危”、“低危”、“提示”。
检测项目	漏洞类型。
状态	• “未修复” • “已修复” • “已忽略”
操作	• 如果确认该风险类型不存在风险，在目标风险类型所在行的“操作”列，单击“忽略”，忽略此风险项。 • 如果想对已忽略的风险项恢复为风险类型，在目标风险类型所在行的“操作”列，单击“取消忽略”，恢复检测此风险。

----结束

9 基线检查

9.1 云服务基线简介

态势感知提供云服务基线检查功能。支持检测云服务关键配置项，通过执行扫描任务，检查云服务基线配置风险状态，分类呈现云服务配置检测结果，告警提示存在安全隐患的配置，并提供相应配置加固建议和帮助指导。

针对华为云服务关键配置项，您可以从“安全上云合规检查1.0”、“等保2.0三级要求”、“护网检查”三大风险类别，了解云服务风险配置的所在范围和风险配置数目。

约束与限制

- SA**基础版**暂不支持使用基线检查功能。**标准版**暂不支持云服务基线查看详情功能。为及时了解云服务配置状态，以及确保云服务的配置的合理性，建议您**购买专业版**。
- 操作账号权限检查。使用基线检查功能时，除了需要“SA FullAccess”、“SA ReadOnlyAccess”策略权限，还需要“Tenant Administrator”权限和IAM相关权限，请提前授予操作账号对应权限。

  “Tenant Administrator”权限和IAM相关权限配置详细操作请参见**配置基线检查功能所需的权限**。
- 基线检查功能为Region级别功能，具体上线region请以SA控制台显示为准。

9.2 基线检查项目

态势感知支持检测云服务关键配置项，通过执行扫描任务，检查云服务基线配置风险状态，分类呈现云服务配置检测结果，告警提示存在安全隐患的配置，并提供相应配置加固建议和帮助指导。

如需查看每个检查项目的详情，如检查状态、风险等级、检查内容等信息，请在检查项目详情页面进行查看，具体操作请参见**查看基线检查项目详情**。

本章节将介绍SA云服务基线检查支持的检查项目。

表 9-1 基线检查项目

检查规范	检查类别		包含的检查项数量
安全上云合规检查1.0	身份与访问管理		12
	检测		7
	基础设施防护		24
	数据防护		22
	事件响应		13
护网检查	安全套件覆盖		12
	账号加固		5
	主机加固		4
	Sudo漏洞		1
	访问控制		1
	敏感信息排查		5
等保2.0三级要求	安全通用要求	安全物理环境	22
		安全通信网络	8
		安全区域边界	20
		安全计算环境	34
		安全管理中心	12
		安全管理制度	7
		安全管理机构	14
		安全管理人员	12
		安全建设管理	34
		安全运维管理	48
	云计算安全扩展要求	安全物理环境	1
		安全通信网络	5
		安全区域边界	8
		安全计算环境	19
		安全管理中心	4
		安全建设管理	8
		安全运维管理	1
	安全运维管理		1

检查规范	检查类别	包含的检查项数量
	安全运维管理	1

安全上云合规检查—身份与访问管理

表 9-2 身份与访问管理风险项检查项目

检查项目	检查内容
IAM用户启用检查	启用统一身份认证（Identity and Access Management，IAM）服务后，系统默认用户组admin中的IAM用户，可以使用华为云所有服务。 检查所有IAM用户列表，是否已启用至少两个IAM用户，以及IAM用户所属的用户组是否都为admin用户组。
IAM用户开启登录保护检查	在IAM的安全设置中启用登录保护后，登录时还需要通过虚拟MFA或短信或邮件验证，再次确认登录者身份，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，保护您安全使用云产品。 检查在IAM的安全设置中是否开启登录保护。
IAM用户开启操作保护检查	在IAM的安全设置中开启操作保护后，主账户及子用户在控制台进行敏感操作（如：删除弹性云服务器、解绑弹性IP等）时，将通过虚拟MFA、手机短信或邮件再次确认操作者身份，进一步提高账号安全性，有效保护您安全使用云产品。 检查IAM用户是否开启操作保护。
管理员账号AK/SK启用检查	访问密钥（AK/SK，Access Key ID/Secret Access Key）是账号的长期身份凭证。 由于管理员具有IAM用户管理权限，且具有大范围的操作权限。为了避免因AK/SK泄露带来的安全隐患，建议管理员账号不启用AK/SK身份凭证。 检查管理员账户是否启用访问密钥。
IAM用户密码配置检查	IAM用户的密码策略建议设置强密码策略。建议满足以下要求：包含以下字符中的3种：大写字母、小写字母、数字和特殊字符；密码最小长度为8；新密码不能与最近的历史密码相同（重复次数设置为3） 检查IAM用户的密码策略是否符合要求。

检查项目	检查内容
IAM登录验证策略（账号锁定策略）检查	拥有安全管理员权限（Security Administrator权限）的用户可以设置登录验证策略来提高用户信息和系统的安全性。 IAM允许用户设置账号锁定策略，即如果在限定时间长度内达到登录失败次数后，用户会被锁定一段时间，锁定时间结束后，才能重新登录。 建议设置为在60分钟内登录失败5次，用户被锁定。 检查账号锁定策略是否设置为在60分钟内登录失败5次，用户被锁定。
IAM登录验证策略（账号锁定时限）检查	拥有安全管理员权限（Security Administrator权限）的用户可以设置登录验证策略来提高用户信息和系统的安全性。 用户可设置账号锁定策略，即如果在限定时间长度内达到登录失败次数后，用户会被锁定一段时间，锁定时间结束后，才能重新登录。 IAM应允许用户设置账号锁定时间，且在此期间用户将无法输入密码。账号锁定时限建议设置为15分钟。 检查账号锁定时限是否设置为15分钟。
IAM密码策略（防止密码重复使用）检查	IAM允许用户设置密码策略。 启用防止密码重复使用规则后，新密码不能与最近使用的密码相同。 检查IAM密码策略是否启用密码重复使用规则，且重复次数小于五次。
会话超时策略检查	IAM允许用户设置会话到期时间。如果用户超过设置的时长未操作界面，会话将会失效，需要重新登录。 检查会话时限是否设置为15分钟。
账号停用策略检查	IAM用户可以通过使用用户名和密码登录华为云控制台。如果用户在90天或更长时间内未登录控制台，建议禁用该用户的控制台访问权限。 检查账号停用策略是否启用，且有效期设置为90天。
IAM用户密码强度检查	IAM用户的登录密码建议设置为安全程度强的密码。 IAM用户设置的登录密码分为弱、中、强三个级别。安全性高的密码可以使账号更安全，建议您定期更换密码以保护账号安全。 检查IAM用户的密码强度是否为最高级别。
CBH实例登录开启多因子认证检查	通过Web浏览器或SSH客户端登录CBH实例时应开启用户的多因子认证，进一步提高堡垒机账号安全性。多因子认证方式有：手机短信、手机令牌、USBKey、动态令牌。 检查CBH实例是否已开启多因子认证。

安全上云合规检查—检测

表 9-3 检测风险项检查项目

检查项目	检查内容
ELB健康状态检查	弹性负载均衡（Elastic Load Balance，ELB）定期向后端服务器发送请求健康检查，通过健康检查来判断后端服务器是否可用。 如果判断出后端服务器健康检查异常，ELB会将异常后端服务器的流量分发到正常后端服务器。 当异常后端服务器恢复正常运行后，ELB会自动恢复其承载业务流量能力。 检查所有ELB实例是否开启健康检查功能，以及检查后端服务器状态是否正常。
CTS启用检查	云审计服务（Cloud Trace Service，CTS）可以将当前账户下所有的操作记录在追踪器中，通过查询和审计操作记录，实现安全分析、资源变更、合规审计、问题定位等。 检查是否已经开通CTS，以及检查是否有一个追踪器的状态为正常。
OBS桶日志记录启用检查	对象存储服务（Object Storage Service，OBS）的桶日志记录，指用户开启一个桶的日志记录功能后，OBS会自动对这个桶的访问请求记录日志，并生成日志文件写入用户指定的桶（即目标桶）中。通过访问日志记录，桶的拥有者可以深入分析访问该桶的用户请求性质、类型或趋势。 检查所有OBS桶，是否开启日志记录功能。
数据库安全审计启用检查（云上RDS场景）	数据库安全审计提供旁路模式审计功能，通过实时记录用户访问数据库行为，形成细粒度的审计报告，对风险行为和攻击行为进行实时告警，对数据库的内部违规和不正当操作进行定位追责。 检查是否已启用数据库安全审计。
云监控服务启用检查	云监控（Cloud Eye）服务为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。使您全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。 检查是否已启用云监控服务。
云监控服务中的主机监控检查	主机监控针对主机提供多层次指标监控，包括基础监控、操作系统监控和进程监控。 基础监控为用户提供免安装的基础指标监控服务；操作系监控和进程监控通过在主机中安装开源插件，为用户主机提供系统级、主动式、细颗粒度的监控服务。 检查主机监控中的弹性云服务器是否已安装监控插件。

检查项目	检查内容
云监控服务中站点监控检查	站点监控用于模拟真实用户对远端服务器的访问，从而探测远端服务器的可用性、连通性等问题。 检查是否配置站点监控。

安全上云合规检查—基础设施防护

表 9-4 基础设施防护风险项检查项目

检查项目	检查内容
安全组入方向规则控制检查	安全组入方向规则应满足最小化访问控制原则。 一般，在非业务需要的情况下，以下情况视为未按最小化访问控制（风险由高到低）：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24。
高危端口、远程管理端口暴露检查	安全组是一个逻辑上的分组，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。安全组创建后，可以在安全组中设置出方向、入方向规则，这些规则会对安全组内部的云服务器出入方向网络流量进行访问控制，当云服务器加入该安全组后，即受到这些访问规则的保护。 安全组入方向规则中不应对外开放或未最小化开放高危端口、远程管理端口。 高危端口如下：20，21，135，137，138，139，445，389，593，1025 未最小化开放指的是：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24 检查安全组入方向规则中是否存在对外开放或未最小化开放高危端口、远程管理端口。
绑定EIP的ECS配置密钥对登录检查	当存在ECS对外暴露EIP的情况下，为安全起见，弹性云服务器登录时应使用密钥方式进行身份验证。
日志指标过滤和告警事件（VPC更改）检查	日志审计模块是信息安全审计功能的核心必备组件，是企事业单位信息系统安全风险管控的重要组成部分。云审计服务（Cloud Trace Service，以下简称CTS），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。 检查CTS中是否存在因VPC更改而产生的日志和告警事件。

检查项目	检查内容
日志指标过滤和告警事件（网络网关更改）检查	日志审计模块是信息安全审计功能的核心必备组件，是企事业单位信息系统安全风险管控的重要组成部分。云审计服务（Cloud Trace Service，以下简称CTS），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。 检查CTS中是否存在因网络网关更改而产生的日志和告警事件。
日志指标过滤和告警事件（安全组更改）检查	日志审计模块是信息安全审计功能的核心必备组件，是企事业单位信息系统安全风险管控的重要组成部分。云审计服务（Cloud Trace Service，以下简称CTS），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。 检查CTS中是否存在因安全组更改而产生的日志和告警事件。
日志指标过滤和告警事件（子网更改）检查	日志审计模块是信息安全审计功能的核心必备组件，是企事业单位信息系统安全风险管控的重要组成部分。云审计服务（Cloud Trace Service，以下简称CTS），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。 检查CTS中是否存在因子网更改而产生的日志和告警事件。
日志指标过滤和告警事件（VPN更改）检查	日志审计模块是信息安全审计功能的核心必备组件，是企事业单位信息系统安全风险管控的重要组成部分。云审计服务（Cloud Trace Service，以下简称CTS），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。 检查CTS中是否存在因VPN更改而产生的日志和告警事件。
ELB实例（共享型）启用访问控制检查	共享型负载均衡器用户可以通过添加白名单和黑名单的方式控制访问负载均衡监听器的IP。通过白名单能够设置允许特定IP访问，而其它IP不许访问。通过黑名单能够设置允许特定的IP不能访问，而其它IP允许访问。 检查弹性负载均衡（Elastic Load Balance，ELB）实例，是否开启访问控制策略。
网络ACL规则配置检查	网络ACL是对子网的访问控制策略系统，根据与子网关联的入站/出站规则，判断数据包是否被允许流入/流出关联子网。同一个VPC内的子网间设置网络ACL，可以增加额外的安全防护层，实现更精细、更复杂的安全访问控制。 检查是否配置网络ACL规则。

检查项目	检查内容
用于VPC对等连接路由表检查	对等连接是指两个VPC之间的网络连接，因此用于对等连接的路由表应满足最小访问权限。 本端路由的目的地址最好限定在最小子网网段内，对端路由的目的地址最好限定在最小子网网段内。 检查用于对等连接的路由表是否满足最小访问权限。
VPC规划检查	如果在当前区域下有多套业务部署，且希望不同业务之间进行网络隔离时，则可为每个业务在当前区域建立相应的VPC。 两个VPC之间可以采用对等连接进行互连。 VPC具有区域属性，默认情况下，不同区域的VPC之间内网不互通，同区域的不同VPC内网不互通，同一个VPC下的不同可用区之间内网互通。 检查VPC规范是否合理。
WAF启用（云模式/独享模式/ELB模式）检查	启用Web应用防火墙（Web Application Firewall，WAF）服务后，网站所有的公网流量都会先经过Web应用防火墙，恶意攻击流量在Web应用防火墙上被检测过滤，而正常流量返回给源站IP，从而确保源站IP安全、稳定、可用。 检查是否已启用WAF。
WAF回源配置检查（未配置ELB）	使用Web应用防火墙（Web Application Firewall，WAF）服务后，需配置源站服务器只允许来自WAF的访问请求访问源站，既可保障访问不受影响，又能防止源站IP暴露。 未使用弹性负载均衡（Elastic Load Balance，ELB）情况下，检查在ECS关联的安全组源地址中，是否添加WAF回源IP。
WAF防护策略配置（地理位置访问控制）检查	WAF的防护策略应配置地理位置访问控制，可针对指定国家、地区的来源IP自定义访问控制。配置后，可以进一步减小业务网站的攻击面（检测版和专业版暂不支持该功能）。
Web基础防护配置检查	Web基础防护支持“拦截”（发现攻击行为后立即阻断并记录）和“仅记录”（发现攻击行为后只记录不阻断攻击）模式，检测版仅支持“仅记录”模式。 WAF中所有待防护的域名应开启Web基础防护并设置为拦截模式，开启后，默认防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击。 检查是否已开启Web基础防护并设置为拦截模式。

检查项目	检查内容
CodeArts Inspector启用检查	漏洞管理服务（ CodeArts Inspector ）是针对网站进行漏洞扫描的一种安全检测服务，可以帮助快速检测出网站存在的漏洞，提供详细的漏洞分析报告，并针对不同类型的漏洞提供专业可靠的修复建议。 检查是否已启用CodeArts Inspector服务。
Anti-DDoS流量清洗启用检查	DDoS原生基础防护（ Anti-DDoS流量清洗 ）服务为华为云内公网IP资源，提供网络层和应用层的DDoS攻击防护，并提供攻击拦截实时告警，有效提升用户带宽利用率，保障业务稳定可靠。 检查是否已启用Anti-DDoS流量清洗服务。
DDoS高防启用检查	DDoS高防（ Advanced Anti-DDoS，AAD ）是企业重要业务连续性的有力保障。DDoS高防通过高防IP代理源站IP对外提供服务，将恶意攻击流量引流到高防IP清洗，确保重要业务不被攻击中断。 检查是否已启用DDoS高防。
云堡垒机启用检查	云堡垒机（ Cloud Bastion Host，CBH ）是华为云的一款4A统一安全管控平台，为企业提供集中的账号、授权、认证和审计管理服务。启用后，可实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计，不仅能保障系统运行安全，且满足相关合规性规范。 检查是否已启用云堡垒机服务。
主机安全防护启用检查	企业主机安全服务（ Host Security Service，HSS ）是提升主机整体安全性的服务。可以全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。 主机实例应安装HSS且开启防护，版本要求至少为企业版（旗舰版、网页防篡改版更优）。 检查主机是否开启主机安全防护。
HSS网页防篡改启用与防护目录配置检查	网页防篡改可实时监控网站目录，并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。 有网站或者关键系统防篡改需求，以及有应用安全防护需求的主机，应开启HSS中的网络防篡改防护并配置好防护目录。 检查主机是否开启网络防篡改防护且已配置好防护目录。
主机紧急修复漏洞检查	企业主机安全服务（ Host Security Service，HSS ）提供漏洞管理功能，检测Linux软件漏洞、Windows系统漏洞和Web-CMS漏洞。 检查HSS中是否存在紧急修复漏洞。

检查项目	检查内容
CDN访问控制配置检查	当客户CDN需要对访问者身份进行识别和过滤，限制部分用户访问，提高CDN的安全性，应配置防盗链与IP黑名单。 检查CDN是否配置访问控制规则。

安全上云合规检查—数据防护

表 9-5 数据防护风险项检查项目

检查项目	检查内容
ELB证书有效性检查	弹性负载均衡（Elastic Load Balance，ELB）支持两种类型的证书，服务器证书和CA证书。配置HTTPS监听器时，需要为监听器绑定服务器证书，如果开启双向认证功能，还需要绑定CA证书。 检查所有ELB中的证书是否有效可用。如果SSL证书过期且未及时更新，用户访问网站时会显示“网站的安全证书已过期”的告警信息。
CDN证书有效性检查	通过配置加速域名的HTTPS证书，并将其部署在全网CDN节点，实现HTTPS安全加速。 检查CDN中证书是否均在有效期内，如果SSL证书过期且未及时更新，用户访问网站时会显示“网站的安全证书已过期”的告警信息。
SSL证书有效性检查	SSL证书管理（SSL Certificate Manager，SCM）是一个SSL（Secure Socket Layer）证书管理平台。SSL证书部署到服务器后，服务器端的访问将启用HTTPS协议。SSL证书超出有效期，将无法正常使用SSL证书。 检查所有SSL证书（检查已签发状态SSL证书，如果SSL证书未签发则默认为检查合格）状态是否在有效期内。
RDS数据库绑定EIP时的安全设置检查	当云数据库RDS（Relational Database Service，简称RDS）配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，需要最小化控制访问源以及开启SSL通道、更改默认数据库端口。 检查当RDS数据库配置公网连接时，是否限制访问源以及开启SSL、更改默认端口。
DDS数据库绑定EIP时安全设置检查	当文档数据库服务（Document Database Service）配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，需要最小化控制访问源以及开启SSL通道、更改默认数据库端口。 检查当DDS数据库配置公网连接时，是否限制访问源以及开启SSL、更改默认端口。

检查项目	检查内容
DCS数据库绑定EIP时的安全设置检查	当分布式缓存服务（Distributed Cache Service，简称DCS）配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，需要最小化控制访问源以及开启SSL通道、更改默认数据库端口。 检查当DCS数据库配置公网连接时，是否限制访问源以及开启SSL、更改默认端口。
云数据库GaussDB绑定EIP时的安全设置检查	当云数据库GaussDB配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，需要最小化控制访问源以及开启SSL通道、更改默认数据库端口。 检查当云数据库GaussDB配置公网连接时，是否限制访问源以及开启SSL、更改默认端口。
RDS数据库绑定EIP检查	当云数据库RDS（Relational Database Service，简称RDS）配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，不建议数据库开通公网连接方式。 检查当RDS数据库配置，是否开通公网连接方式。
DDS数据库绑定EIP检查	当文档数据库服务（Document Database Service）配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，不建议数据库开通公网连接方式。 检查当DDS数据库配置，是否开通公网连接方式。
DCS数据库绑定EIP检查	当分布式缓存服务（Distributed Cache Service，简称DCS）配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，不建议数据库开通公网连接方式。 检查当DCS数据库配置，是否开通公网连接方式。
云数据库GaussDB绑定EIP检查	当云数据库GaussDB配置公网连接时，业务数据会在公网上进行传输，数据容易泄露，因此，不建议数据库开通公网连接方式。 检查当云数据库GaussDB配置，是否开通公网连接方式。
RDS数据库实例安全组规则检查	检查关系型数据库（Relational Database Service，RDS）实例所关联的安全组规则是否存在不安全规则，即检查安全组规则的允许范围是否超过使用范围。当源地址为0.0.0.0/0或空时，代表未设置IP访问的限制，数据库将会有高安全风险。不安全规则示例：方向为入方向，协议为任一类别协议，源地址为0.0.0.0/0（所有地址），端口为1~65535或者数据库业务端口，如3306。
GaussDB数据库实例安全组规则检查	安全组入方向规则应满足最小化访问控制原则。 一般地，在非业务需要的情况下，以下情况视为未按最小化访问控制（风险由高到低）： IPv4：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24 IPv6：源地址为::/0

检查项目	检查内容
OBS桶服务端加密检查	OBS服务端加密是在上传对象到桶时，将数据在服务端加密成密文后存储。再次下载加密对象时，存储的密文会先在服务端解密为明文，再反馈给用户。将数据加密后存储到OBS桶中，提高数据的安全性。 检查所有OBS桶是否开启服务端加密。
OBS桶的ACL权限检查	OBS桶ACL是基于账号或用户组的桶级访问控制，桶的拥有者可以通过桶ACL授予指定账号或用户组特定的访问权限。 匿名用户指未注册华为云的普通访客。如果OBS桶的ACL赋予了匿名用户桶的访问权限或ACL访问权限，表示所有人无需经过任何身份验证即可访问OBS桶。 检查所有OBS桶，是否给匿名用户赋予桶访问权限或者ACL访问权限。
MySQL数据库实例root用户远程登录控制检查	MySQL数据库实例的root应做好远程登录的控制，限制仅应用端、DAS管理网段等业务需要方可登录，防止root账号被暴力破解。
RDS数据库实例安全组入方向规则检查	安全组入方向规则应满足最小化访问控制原则。 一般，在非业务需要的情况下，以下情况视为未按最小化访问控制（风险由高到低）： IPv4：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24 IPv6：源地址为::/0 检查云数据库（Relational Database Service，RDS）实例所关联的安全组入方向规则是否按最小化访问控制。
DCS数据库实例安全组入方向规则检查	安全组入方向规则应满足最小化访问控制原则。 一般，在非业务需要的情况下，以下情况视为未按最小化访问控制（风险由高到低）： IPv4：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24 IPv6：源地址为::/0 检查分布式缓存服务（Distributed Cache Service，DCS）实例所关联的安全组入方向规则是否按最小化访问控制。
DDS数据库实例安全组入方向规则检查	安全组入方向规则应满足最小化访问控制原则。 一般，在非业务需要的情况下，以下情况视为未按最小化访问控制（风险由高到低）： IPv4：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24 IPv6：源地址为::/0 检查文档数据库服务（Document Database Service，DDS）实例所关联的安全组入方向规则是否按最小化访问控制。

检查项目	检查内容
RDS数据库实例安全组端口开放检查	检查云数据库（Relational Database Service，RDS）实例所关联的安全组规则是否存在不安全规则，即检查安全组规则的允许范围是否超过使用范围。 不安全规则示例：方向为入方向，端口为1~65535或者非数据库业务端口，如3306。 检查RDS实例是否开放非必要的端口。
DCS数据库实例安全组端口开放检查	检查分布式缓存服务（Distributed Cache Service，DCS）实例所关联的安全组规则是否存在不安全规则，即检查安全组规则的允许范围是否超过使用范围。 不安全规则示例：方向为入方向，端口为1~65535或者非数据库业务端口，如6379。 检查DCS实例是否开放非必要的端口。
DDS数据库实例安全组端口开放检查	检查文档数据库服务（Document Database Service，DDS）实例所关联的安全组规则是否存在不安全规则，即检查安全组规则的允许范围是否超过使用范围。 不安全规则示例：方向为入方向，端口为1~65535或者非数据库业务端口，如8635。 检查DDS实例是否开放非必要的端口。

安全上云合规检查—事件响应

表 9-6 事件响应风险项检查项目

检查项目	检查内容
云硬盘备份开启检查	云备份（Cloud Backup and Recovery）可以为云硬盘（Elastic Volume Service，EVS）提供简单易用的备份服务，当发生病毒入侵、人为误删除、软硬件故障等事件时，可将数据恢复到任意备份点。 检查所有是否开启云硬盘备份。
OBS桶跨区域复制检查	OBS跨区域复制能够提供跨区域数据容灾的能力，通过创建跨区域复制规则，在同一个账号下，将一个桶（源桶）中的数据自动、异步地复制到不同区域的另外一个桶（目标桶）中，满足用户数据复制到异地进行备份的需求。 检查所有OBS桶是否开启跨区域复制。
云审计服务关键操作通知启用检查	云审计服务在记录某些特定关键操作时，支持对这些关键操作通过消息通知服务实时向相关订阅者发送通知，该功能由云审计服务触发，消息通知服务（SMN）完成通知发送。

检查项目	检查内容
云日志服务LTS的日志转储（OBS/DIS）检查	主机和云服务的日志数据上报至云日志服务后，默认存储时间为7天。超出存储时间的日志数据将会被自动删除，对于需要长期存储的日志数据（日志持久化），云日志服务提供转储功能，可以将日志转储至其他云服务中进行长期保存。 检查LTS是否已配置日志转储（OBS/DIS）。
ECS/BMS实例的云服务器备份检查	云备份（Cloud Backup and Recovery, CBR）为云内的弹性云服务器（Elastic Cloud Server, ECS）、云耀云服务器（Hyper Elastic Cloud Server，HECS）、裸金属服务器（Bare Metal Server, BMS）（下文统称为服务器）提供简单易用的备份服务，当发生病毒入侵、人为误删除、软硬件故障等事件时，可将数据恢复到任意备份点。 检查ECS/BMS实例是否已开启云服务器备份。
RDS数据库实例备份检查	RDS数据库实例应开启自动备份功能，以保证数据可靠性。 检查RDS数据库实例是否已开启自动备份功能。
GaussDB数据库实例备份检查	GaussDB数据库实例应开启自动备份功能，以保证数据可靠性。 检查GaussDB数据库实例是否已开启自动备份功能。
WAF全量日志功能开启检查	启用WAF全量日志功能后，可以将攻击日志、访问日志记录到华为云的云日志服务（Log Tank Service，简称LTS）中，通过LTS记录的WAF日志数据，快速高效地进行实时决策分析、设备运维管理以及业务趋势分析。 检查WAF是否已启用全量日志功能。
WAF防护事件告警通知开启检查	通过对攻击日志进行通知设置，WAF可将仅记录和拦截的攻击日志通过用户设置的接收通知方式（例如邮件或短信）发送给用户，以便在发生攻击时运维人员进行及时响应，告警频率、事件类型可以根据业务场景进行调整。 检查WAF防护事件是否已开启告警通知。
数据库安全审计日志备份检查	数据库安全审计支持将数据库的审计日志备份到OBS桶，实现高可用容灾，以便可以根据需要备份或恢复数据库审计日志。 检查数据库安全审计是否已配置日志备份。
数据库安全审计告警通知设置检查	通过设置告警通知，当数据库发生设置的告警事件时，您可以收到DBSS发送的告警通知，及时了解数据库的安全风险。 检查数据库安全审计是否设置告警通知。
云硬盘可用备份检查	云备份（Cloud Backup and Recovery）可以为云硬盘（Elastic Volume Service, EVS）提供简单易用的备份服务，当发生病毒入侵、人为误删除、软硬件故障等事件时，可将数据恢复到任意备份点。 检查云硬盘中是否有可用备份，以便用于恢复。

检查项目	检查内容
RDS数据库实例备份检查	云数据库（Relational Database Service，RDS）支持数据库实例的备份和恢复，以保证数据可靠性。RDS数据库实例默认开启数据自动备份策略，备份周期默认每天备份数据一次。 检查所有RDS实例，是否开启自动备份功能。
DDS数据库开启自动备份	文档数据库服务（Document Database Service，DDS）支持数据库实例的备份和恢复，以保证数据可靠性。DDS数据库实例开启数据自动备份策略后，备份周期默认每天备份数据一次。 检查所有DDS实例是否开启自动备份功能。

护网检查—安全套件覆盖

表 9-7 安全套件覆盖风险项检查项目

检查项目	检查内容
主机防护状态检查	企业主机安全服务（Host Security Service，HSS）是提升主机整体安全性的服务，通过主机管理、风险预防、入侵检测、高级防御、安全运营、网页防篡改功能，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。 检查主机是否已开启防护。
主机Agent状态检查	企业主机安全服务（Host Security Service，HSS）是一个用于全面保障主机整体安全的服务，能帮助您高效管理主机的安全状态，并构建服务器安全体系，降低当前服务器面临的主要安全风险。 在主机中安装Agent后，您的主机才能收到HSS的保护。 检查主机Agent是否为在线状态。
主机安全检测状态检查	企业主机安全服务（Host Security Service，HSS）将实时检测主机中的风险和异常操作，在每日凌晨将对主机执行全面扫描。执行配置检测后，您可以根据检测结果中的相关信息，修复主机中含有风险的配置项或忽略可信任的配置项。 检查主机的检测结果是否存在异常。
WAF（云模式）基础防护配置检查	Web基础防护开启后，默认防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击。 检查WAF在云模式下是否已开启Web基础防护。

检查项目	检查内容
WAF（云模式）防护策略配置检查	Web基础防护支持“拦截”（发现攻击行为后立即阻断并记录）和“仅记录”（发现攻击行为后只记录不阻断攻击）模式，检测版仅支持“仅记录”模式。 WAF中所有待防护的域名应开启Web基础防护并设置为拦截模式，开启后，默认防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击。 检查WAF在云模式下是否已开启Web基础防护并设置为拦截模式。
WAF（独享模式）基础防护配置检查	Web基础防护开启后，默认防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击。 检查WAF在独享模式下是否已开启Web基础防护。
WAF（独享模式）防护策略配置检查	Web基础防护支持“拦截”（发现攻击行为后立即阻断并记录）和“仅记录”（发现攻击行为后只记录不阻断攻击）模式，检测版仅支持“仅记录”模式。 WAF中所有待防护的域名应开启Web基础防护并设置为拦截模式，开启后，默认防范SQL注入、XSS跨站脚本、远程溢出攻击、文件包含、Bash漏洞攻击、远程命令执行、目录遍历、敏感文件访问、命令/代码注入等常规的Web攻击。 检查WAF在独享模式下是否已开启Web基础防护并设置为拦截模式。
网站高危漏洞检查	漏洞管理服务（CodeArts Inspector）可以帮助您快速检测出您的网站存在的漏洞，提供详细的漏洞分析报告，并针对不同类型的漏洞提供专业可靠的修复建议。 检查网站中是否存在高危漏洞。
网站中危漏洞检查	漏洞管理服务（CodeArts Inspector）可以帮助您快速检测出您的网站存在的漏洞，提供详细的漏洞分析报告，并针对不同类型的漏洞提供专业可靠的修复建议。 检查网站中是否存在中危漏洞。
扫描时间检查	漏洞管理服务（CodeArts Inspector）可以帮助您快速检测出您的网站存在的漏洞，提供详细的漏洞分析报告，并针对不同类型的漏洞提供专业可靠的修复建议。 检查扫描时间是否已超过一周。
SA专业版购买检查	态势感知提供基础版、标准版和专业版三个版本，不同版本有不同功能使用范围。 专业版可以呈现全局安全态势。通过动态安全检测和威胁分析，并提供安全加固建议。 检查是否已购买SA专业版。

检查项目	检查内容
主机Agent版本检查	在主机中安装Agent后，您的主机将受到HSS云端防护中心全方位的安全保障，在安全控制台可视化界面上，您可以统一查看并管理同一区域内所有主机的防护状态和主机安全风险。 企业主机安全服务有基础版、企业版、旗舰版和网页防篡改版四个版本。 基础版一般只用于测试、个人用户防护主机账户安全。建议您选择企业版及以上版本。 检查所有主机Agent是否为企业版及以上版本。

护网检查—账号加固

表 9-8 账号加固风险项检查项目

检查项目	检查内容
管理员账号AK/SK启用检查	访问密钥（AK/SK，Access Key ID/Secret Access Key）是账号的长期身份凭证。 由于管理员具有IAM用户管理权限，且具有大范围的操作权限。为了避免因AK/SK泄露带来的安全隐患，建议管理员账号不启用AK/SK身份凭证。 检查管理员账户是否启用访问密钥。
主机弱密码检查	HSS提供基线检查功能，主动检测主机中口令复杂度策略，给出修改建议，帮助用户提升口令安全性检测账户口令是否属于常用的弱口令，针对弱口令提示用户修改，防止账户口令被轻易猜解。 检查主机是否存在弱口令。
委托账号检查	通过创建委托，可以将资源共享给其他账号，或委托更专业的人或团队来代为管理资源。被委托方使用自己的账号登录后，切换到委托方账号，即可管理委托方委托的资源，避免委托方共享自己的安全凭证（密码/密钥）给他人，确保账号安全。 在云服务环境中，如果创建委托给个人账号，可能会导致不可信，因此不建议委托给个人账号。 检查是否存在个人委托账号。
全局服务中的委托权限配置检查	检查全局服务中的委托权限是否存在Security Administrator, Tenant Administrator。
项目服务中的委托权限配置检查	检查项目服务中的委托权限是否存在Security Administrator, Tenant Administrator。

护网检查—主机加固

表 9-9 主机加固风险项检查项目

检查项目	检查内容
主机高危端口暴露检查	HSS提供资产管理功能，主动检测主机中的开放端口，及时发现主机中含有风险的各项资产。 如果检测到开放了危险端口或者开放了不必要的端口，需要排查这些端口是否是正常业务使用，如果不是正常业务端口，建议关闭端口。对于危险端口建议进一步检查程序文件，如果存在风险建议删除或者隔离源文件。 检查所有主机是否在对外开放或未最小化开放的高危端口。
CCE集群Kubernetes版本检查	云容器引擎（Cloud Container Engine，简称CCE）提供高度可扩展的、高性能的企业级Kubernetes集群，支持运行Docker容器。借助云容器引擎，您可以在华为云上轻松部署、管理和扩展容器化应用程序。 当CCE集群Kubernetes版本低于1.15，有安全漏洞风险，建议您进行升级。 检查CCE集群Kubernetes版本是否在1.15以下。
VPC配置（对等连接）检查	对等连接是指两个VPC之间的网络连接。您可以使用私有IP地址在两个VPC之间进行通信，就像两个VPC在同一个网络中一样。您可以在自己的VPC之间创建对等连接，也可以在自己的VPC与同一区域内其他的VPC之间创建对等连接。 检查VPC是否已经创建对等连接，如果已创建，则检查是否开放或未最小化高危端口。
VPC配置（VPN网关）检查	VPN网关是虚拟私有云中建立的出口网关设备，通过VPN网关可建立虚拟私有云和企业数据中心或其它区域VPC之间的安全可靠的加密通信。 检查VPC是否已经创建了VPN网关。

护网检查—Sudo 漏洞

表 9-10 Sudo 漏洞风险项检查项目

检查项目	检查内容
检查主机是否存在Sudo漏洞	HSS提供漏洞管理功能，检测Linux软件漏洞，通过与漏洞库进行比对，检测出系统和官方软件（非绿色版、非自行编译安装版；例如：SSH、OpenSSL、Apache、MySQL等）存在的漏洞，帮助用户识别出存在的风险。 检查所有主机是否存在Sudo漏洞。

护网检查—访问控制

表 9-11 访问控制风险项检查项目

检查项目	检查内容
安全组入方向规则控制检查	安全组入方向规则应满足最小化访问控制原则。 一般，在非业务需要的情况下，以下情况视为未按最小化访问控制（风险由高到低）：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24。 IPv4：源地址为0.0.0.0/0；公网地址的掩码小于32；内网地址的掩码小于24。 IPv6：源地址为::/0。

护网检查—敏感信息排查

表 9-12 敏感信息排查风险项检查项目

检查项目	检查内容
OBS桶的ACL权限检查	OBS桶ACL是基于账号或用户组的桶级访问控制，桶的拥有者可以通过桶ACL授予指定账号或用户组特定的访问权限。 匿名用户指未注册华为云的普通访客。如果OBS桶的ACL赋予了匿名用户桶的访问权限或ACL访问权限，表示所有人无需经过任何身份验证即可访问OBS桶。 检查所有OBS桶，是否给匿名用户赋予桶访问权限或者ACL访问权限。
OBS桶日志记录启用检查	对象存储服务（Object Storage Service，OBS）的桶日志记录，指用户开启一个桶的日志记录功能后，OBS会自动对这个桶的访问请求记录日志，并生成日志文件写入用户指定的桶（即目标桶）中。通过访问日志记录，桶的拥有者可以深入分析访问该桶的用户请求性质、类型或趋势。 检查所有OBS桶，是否开启日志记录功能。
数据库中敏感信息检查	数据安全中心服务（Data Security Center，DSC）根据敏感数据发现策略来识别数据库中的敏感数据，基于多种预置脱敏算法+用户自定义脱敏算法，实现全栈敏感数据防护。 检查数据库中是否存在敏感信息。
OBS中敏感信息检查	数据安全中心服务（Data Security Center，DSC）根据敏感数据发现策略来识别数据库中的敏感数据，基于多种预置脱敏算法+用户自定义脱敏算法，实现全栈敏感数据防护。 检查OBS中是否存在敏感信息。

检查项目	检查内容
ES中敏感信息检查	数据安全中心服务（Data Security Center，DSC）根据敏感数据发现策略来识别数据库中的敏感数据，基于多种预置脱敏算法+用户自定义脱敏算法，实现全栈敏感数据防护。 检查ES中是否存在敏感信息。

等保 2.0 三级要求—安全物理环境

表 9-13 安全物理环境风险项检查项目

检查子项目	检查项目
物理位置选择	机房场地应选择在具有防震、防风和防雨等能力的建筑内。
	机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
防盗窃和防破坏	应将设备或主要部件进行固定，并设置明显的不易除去的标识。
	应将通信线缆铺设在隐蔽安全处。
	应设置机房防盗报警系统或设置有专人值守的视频监控系统。
防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。
	应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
防火	机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。
	机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。
	应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。
防水和防潮	应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。
	应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。
	应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
防静电	应采用防静电地板或地面并采用必要的接地防静电措施。

检查子项目	检查项目
	应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
电力供应	应在机房供电线路上配置稳压器和过电压防护设备。
	应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。
	应设置冗余或并行的电力电缆线路为计算机系统供电。
电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。
	应对关键设备实施电磁屏蔽。

等保 2.0 三级要求—安全通信网络

表 9-14 安全通信网络风险项检查项目

检查子项目	检查项目
网络架构	应保证网络设备的业务处理能力满足业务高峰期需要。
	应保证网络各个部分的带宽满足业务高峰期需要。
	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。
	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。
	应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。
通信传输	应采用密码技术保证通信过程中数据的完整性。
	应采用密码技术保证通信过程中数据的保密性。
可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

等保 2.0 三级要求—安全区域边界

表 9-15 安全区域边界风险项检查项目

检查子项目	检查项目
边界防护	应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
	应能够对非授权设备私自联到内部网络的行为进行限制或检查。
	应能够对内部用户非授权联到外部网络的行为进行限制或检查。
	应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
访问控制	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。
	应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。
	应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。
	应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。
	应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
入侵防范	应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。
	应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。
	应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。
	当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。
恶意代码和垃圾邮件防范	应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。
	应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。
安全审计	应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。
	审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

检查子项目	检查项目
	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。
	应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。

等保 2.0 三级要求—安全计算环境

表 9-16 安全计算环境风险项检查项目

检查子项目	检查项目
身份鉴别	应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。
	应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。
	当进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。
	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。
访问控制	应对登录的用户分配账户和权限。
	应重命名或删除默认账户，修改默认账户的默认口令。
	应及时删除或停用多余的、过期的账户，避免共享账户的存在。
	应授予管理用户所需的最小权限，实现管理用户的权限分离。
	应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。
	访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级。
	应对主体、客体设置安全标记，并依据安全标记和强制访问控制规则确定主体对客体的访问。
安全审计	应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

检查子项目	检查项目
	审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。
	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。
	应对审计进程进行保护，防止未经授权的中断。
入侵防范	应遵循最小安装的原则，仅安装需要的组件和应用程序。
	应关闭不需要的系统服务、默认共享和高危端口。
	应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。
	应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。
	应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。
	应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
恶意代码和垃圾邮件防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的所有执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，并进行动态关联感知。
数据完整性	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。
	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。
数据保密性	应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
	应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
数据备份恢复	应提供重要数据的本地数据备份与恢复功能。
	应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。
	应提供重要数据处理系统的热冗余，保证系统的高可用性。

检查子项目	检查项目
剩余信息保护	应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。
	应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
个人信息保护	应仅采集和保存业务必需的用户个人信息。
	应禁止未授权访问和非法使用用户个人信息。

等保 2.0 三级要求—安全管理中心

表 9-17 安全管理中心风险项检查项目

检查子项目	检查项目
系统管理	应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。
	应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
审计管理	应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计。
	应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
安全管理	应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计。
	应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
集中管控	应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控。
	应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理。
	应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。
	应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。
	应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。

检查子项目	检查项目
	应能对网络中发生的各类安全事件进行识别、报警和分析。

等保 2.0 三级要求—安全管理制度

表 9-18 安全管理制度风险项检查项目

检查子项目	检查项目
安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
管理制度	应对安全管理活动中的各类管理内容建立安全管理制度。
	应对管理人员或操作人员执行的日常管理操作建立操作规程。
	应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
制定和发布	应指定或授权专门的部门或人员负责安全管理制度的制定。
	安全管理制度应通过正式、有效的方式发布，并进行版本控制。
评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

等保 2.0 三级要求—安全管理机构

表 9-19 安全管理机构风险项检查项目

检查子项目	检查项目
岗位设置	应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权。
	应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责。
	应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
人员配备	应配备一定数量的系统管理员、审计管理员和安全管理员等。
	应配备专职安全管理员，不可兼任。

检查子项目	检查项目
授权和审批	应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等。
	应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度。
	应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。
沟通和合作	应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。
	应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通。
	应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
审核和检查	应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。
	应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。
	应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

等保 2.0 三级要求—安全管理人员

表 9-20 安全管理人员风险项检查项目

检查子项目	检查项目
人员录用	应指定或授权专门的部门或人员负责人员录用。
	应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核。
	应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
人员离岗	应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。
	应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
安全意识教育和培训	应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

检查子项目	检查项目
	应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训。
	应定期对不同岗位的人员进行技能考核。
外部人员访问管理	应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。
	应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。
	外部人员离场后应及时清除其所有的访问权限。
	获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

等保 2.0 三级要求—安全建设管理

表 9-21 安全建设管理风险项检查项目

检查子项目	检查项目
定级和备案	应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由。
	应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定。
	应保证定级结果经过相关部门的批准。
	应将备案材料报主管部门和相应公安机关备案。
安全方案设计	应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。
	应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件。
	应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
产品采购和使用	应确保网络安全产品采购和使用符合国家的有关规定。
	应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求。
	应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。
自行软件开发	应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制。

检查子项目	检查项目
	应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。
	应制定代码编写安全规范，要求开发人员参照规范编写代码。
	应具备软件设计的相关文档和使用指南，并对文档使用进行控制。
	应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。
	应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制。
	应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。
外包软件开发	应在软件交付前检测其中可能存在的恶意代码。
	应保证开发单位提供软件设计文档和使用指南。
	应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
工程实施	应指定或授权专门的部门或人员负责工程实施过程的管理。
	应制定安全工程实施方案控制工程实施过程。
	应通过第三方工程监理控制项目的实施过程。
测试验收	应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告。
	应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。
系统交付	应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。
	应对负责运行维护的技术人员进行相应的技能培训。
	应提供建设过程文档和运行维护文档。
等级测评	应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改。
	应在发生重大变更或级别发生变化时进行等级测评。
	应确保测评机构的选择符合国家有关规定。
服务供应商选择	应确保服务供应商的选择符合国家的有关规定。
	应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。

检查子项目	检查项目
	应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

等保 2.0 三级要求—安全运维管理

表 9-22 安全运维管理风险项检查项目

检查子项目	检查项目
环境管理	应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理。
	应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定。
	应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
资产管理	应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容。
	应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。
	应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。
介质管理	应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。
	应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
设备维护管理	应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理。
	应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。
	信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密。
	含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
漏洞和风险管理	应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。

检查子项目	检查项目
	应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。
网络和系统安全管理	应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限。
	应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。
	应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。
	应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等。
	应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
	应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为。
	应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库。
	应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。
	应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。
	应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。
恶意代码防范管理	应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。
	应定期验证防范恶意代码攻击的技术措施的有效性。
配置管理	应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。
	应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。
密码管理	应遵循密码相关国家标准和行业标准。
	应使用国家密码管理主管部门认证核准的密码技术和产品。
变更管理	应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。

检查子项目	检查项目
	应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程。
	应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。
备份与恢复管理	应识别需要定期备份的重要业务信息、系统数据及软件系统等。
	应规定备份信息的备份方式、备份频度、存储介质、保存期等。
	应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
安全事件处置	应及时向安全管理部门报告所发现的安全弱点和可疑事件。
	应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等。
	应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。
	对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。
应急预案管理	应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容。
	应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容。
	应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。
	应定期对原有的应急预案重新评估，修订完善。
外包运维管理	应确保外包运维服务商的选择符合国家的有关规定。
	应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容。
	应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明。
	应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对IT基础设施中断服务的应急保障要求等。

等保 2.0 三级要求—安全物理环境

表 9-23 安全物理环境风险项检查项目

检查子项目	检查项目
基础设施位置	应保证云计算基础设施位于中国境内。

等保 2.0 三级要求—安全通信网络

表 9-24 安全通信网络风险项检查项目

检查子项目	检查项目
网络架构	应保证云计算平台不承载高于其安全保护等级的业务应用系统。
	应实现不同云服务客户虚拟网络之间的隔离。
	应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。
	应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略。
	应提供开放接口或开放安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。

等保 2.0 三级要求—安全区域边界

表 9-25 安全区域边界风险项检查项目

检查子项目	检查项目
访问控制	应在虚拟化网络边界部署访问控制机制，并设置访问控制规则。
	应在不同等级的网络区域边界部署访问控制机制，设备访问控制规则
入侵防范	应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
	应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等。
	应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量。
	应在检测到网络攻击行为、异常流量情况时进行告警。

检查子项目	检查项目
安全审计	应对云服务提供商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启。
	应保证云服务提供商对云服务客户系统和数据的操作可被云服务客户审计。

等保 2.0 三级要求—安全计算环境

表 9-26 安全计算环境风险项检查项目

检查子项目	检查项目
身份鉴别	当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制。
访问控制	应保证当虚拟机迁移时，访问控制策略随其迁移。
	应允许云服务客户设置不同虚拟机之间的访问控制策略。
入侵防范	应能检测虚拟机之间的资源隔离失效，并进行告警。
	应能检测到非授权新建虚拟机或者重新启用虚拟机，并进行告警。
	应能检测恶意代码感染及在虚拟机间蔓延情况，并进行告警。
镜像和快照保护	应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务。
	应提供虚拟机镜像、快照完整性检验功能，防止虚拟机镜像被恶意篡改。
	应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问。
数据完整性和保密性	应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定。
	应确保只有在云服务客户授权下，云服务提供商或第三方才具有云服务客户数据的管理权限。
	应确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。
	应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。
数据备份恢复	云服务客户应在本地保存其业务数据的备份。
	应提供查询云服务客户数据及备份存储位置的能力。

检查子项目	检查项目
	云服务提供商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致。
	应为云服务客户将业务系统及数据迁移到其体云计算平台和本地系统提供技术手段，并协助完成迁移过程。
剩余信息保护	应保证虚拟机所使用的内存和存储空间回收时得到完全清除。
	云服务客户删除业务应用数据时，云计算平台将云存储中所有副本删除。

等保 2.0 三级要求—安全管理中心

表 9-27 安全管理中心风险项检查项目

检查子项目	检查项目
集中管控	应能对物理资源和虚拟资源按照策略做统一管理调度与分配。
	应保证云计算平台管理流量与云服务客户业务流量分离。
	应根据云服务提供商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计。
	应根据云服务提供商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

等保 2.0 三级要求—安全建设管理

表 9-28 安全建设管理风险项检查项目

检查子项目	检查项目
云服务提供商选择	应选择安全合规的云服务提供商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力。
	应在服务水平协议中规定云服务的各项服务内容和具体技术指标。
	应在服务水平协议规定云服务提供商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。
	应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除。

检查子项目	检查项目
	应与选定的云服务提供商签署保密协议，要求其不得泄漏云服务客户数据。
供应链管理	应确保供应商的选择符合国家有关规定。
	应将供应链安全事件信息或安全威胁信息及时传达到云服务客户。
	应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

等保 2.0 三级要求—安全运维管理

表 9-29 安全运维管理风险项检查项目

检查子项目	检查项目
云计算环境管理	云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

等保 2.0 三级要求—安全运维管理

表 9-30 安全运维管理风险项检查项目

检查子项目	检查项目
配置管理	应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

等保 2.0 三级要求—安全运维管理

表 9-31 安全运维管理风险项检查项目

检查子项目	检查项目
感知节点管理	应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理。

9.3 配置基线检查功能所需的权限

当您需要使用SA的**基线检查**功能时，需要给操作账号配置“Tenant Administrator”权限和IAM相关权限。

本章节将介绍如何配置SA相关功能所需的权限。

前提条件

已获取管理员账号及密码。

配置基线检查功能所需的权限

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“管理与监管 > 统一身份认证服务”，进入统一身份认证服务管理控制台。

步骤3 添加IAM相关权限。

1. 在左侧导航栏选择“权限管理 > 权限”，并在权限页面右上角单击“创建自定义策略”。
2. 配置策略。
   a. 策略名称：自定义。
   b. 作用范围：选择“全局级范围”。
   c. 策略配置方式：选择“JSON视图”。
   d. 策略内容：请直接复制粘贴以下内容。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:users:getUser",
                "iam:securitypolicies:getLoginPolicy",
                "iam:credentials:listCredentials",
                "iam:users:getUserLoginProtect",
                "iam:agencies:listAgencies",
                "iam:securitypolicies:getProtectPolicy",
                "iam:users:listUsers",
                "iam:securitypolicies:getPasswordPolicy",
                "iam:groups:listGroups",
                "iam:permissions:listRolesForAgencyOnProject",
                "iam:users:listUsersForGroup",
                "iam:projects:listProjectsForUser",
                "iam:permissions:listRolesForAgencyOnDomain"
            ]
        }
    ]
}
```

3. 单击“确定”。

步骤4 在左侧导航栏选择“委托”，进入委托页面。

步骤5 在委托列表中选择“ssa_admin_trust”，进入委托详情页面。

步骤6 选择“授权记录”页签，并在页面中单击“授权”。

步骤7 在权限配置栏目搜索并选择“Tenant Administrator”和步骤3创建的权限。

图 9-1 基线检查权限策略

步骤8 单击页面下方“下一步”，设置最小授权范围。

步骤9 单击页面下方的“确定”，完成配置。

----结束

9.4 设置基线检查计划

态势感知支持根据基线检查计划检查您的服务器基线配置是否存在风险。

本文档介绍了如何新增、编辑、删除基线检查计划。

背景信息

开通基线检查服务后，态势感知将使用默认检查计划对所有资产进行检查。默认检查计划的自动检查时间、检查对象如下：

- 自动检查时间：每隔3天检查一次，每次在00:00~06:00进行检查。
- 检查对象：您账号下当前区域的所有资产。

约束限制

创建检查计划是同一个检查规范只能属于一个检查计划。

前提条件

已购买态势感知**标准版**或**专业版**。

创建检查计划

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 进入基线检查计划配置页面。

- 方法一：
  a. 在左侧导航栏选择“基线检查”，进入基线检查页面。
  b. 单击页面右上角的“设置检查计划”，进入检测设置页面。

图 9-2 进入基线检查计划配置页面

- 方法二：
  在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。

图 9-3 检测设置页面

步骤4 在检测设置页面中，选择待创建计划所在的区域，并单击“创建计划”，系统右侧弹出新建检查计划的页面。

图 9-4 创建检查计划

步骤5 配置检查计划。

1. 填写基本信息，具体参数配置如**表9-32**所示。

表 9-32 检查计划基本信息

参数名称	参数说明
计划名称	自定义检查计划的名称。
检查时间	选择检测周期和检查触发时间。 – 检测周期：每隔1天、3天、7天、15天、30天检查一次 – 检查触发时间：00:00~06:00、06:00~12:00、12:00~18:00、18:00~24:00

2. 选择检查规范。

   选择需要检测的基线检查项目。更多关于基线检查项目详细描述请参见**云服务基线简介**。

3. 单击“确定”。

   检查计划创建完成。

   SA会在指定的时间执行云服务基线扫描，扫描结果可以在“基线检查”中查看。

----结束

相关操作

基线检查计划创建后，您可以查看检查计划、对检查计划进行编辑或删除。

- 查看已有检查计划
  a. 登录管理控制台。
  b. 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。
  c. 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。
  d. 在检测设置页面中，查看已有的基线检查计划。
- 编辑检查计划
  a. 在目标计划所在框的右上角单击“编辑”，系统右侧弹出编辑检查计划页面。
  b. 编辑需要修改的计划参数。
  c. 单击“确定”。
- 删除检查计划
  a. 在目标计划所在框的右上角单击“删除”。
  b. 在弹出的对话框中，单击“是”。

9.5 执行基线检查计划

基线检查项目分为“自动检查”和“手动检查”项目两种，本章节介绍自动检查项目执行检查的操作。

为了解最新的云服务基线配置状态，您需要执行扫描任务，扫描结束后才能获取云服务基线的风险配置。

基线检查功能支持定期自动检查和立即检查。

- 定期自动检查：根据SA为您提供的默认基线检查计划或您自定义的基线检查计划，定时自动执行基线检查。默认检查计划每隔3天在0点的时候自动执行基线检查。
- 立即检查：如果您新增或修改了自定义的基线检查计划，您可以在基线检查页面选择该基线检查计划，立即执行基线检查，实时查看服务器中是否存在对应的基线风险。

约束限制

- “立即检查”任务在10分钟内仅能执行一次。
- 手动立即执行“定期自动检查任务”在10分钟内仅能执行一次。

前提条件

已配置自定义的基线检查计划。

立即检查所有检查规范

SA可根据您设置的检查规范，立即执行已配置的检查规范。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“基线检查”，并在基线检查页面右上角单击“设置检查规范”，系统弹出选择检查规范窗口。

图 9-5 基线检查页面

步骤4 在弹出的选择规范窗口中，选择检查规范，并单击“确定”。

图 9-6 选择检查规范

步骤5 在页面右上角单击“立即检查”，立即执行扫描任务。

刷新页面，查看“最近检查时间”，即可确认是否为最新的扫描结果。

系统将立即执行已配置的检查规范。

----结束

立即执行某个检查计划

本部分将介绍如何立即执行某个检查计划，配置后，系统将立即执行已选择的基线检查计划。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。

步骤4 在检测设置页面，选择检查计划所在的区域。

步骤5 在待执行立即手动检查的检查计划所在栏的上方单击“立即检查”。

图 9-7 执行某个检查计划

系统将立即执行已选择的基线检查计划。

----结束

9.6 执行手动检查

基线检查项目分为“自动检查”和“手动检查”项目两种，本章节介绍手动检查项目执行检查的操作。

基线检查的“等保2.0三级要求”中所有的检查项目、“安全上云合规检查1.0”和“护网检查”中的一些检查项目为手动检查项，需要您在线下执行检查后，再在控制台上反馈检查结果，以便计算检查项合格率。

前提条件

- 已购买态势感知**专业版**，且在有效使用期内。
- 已在线下完成检查。

约束与限制

反馈结果有效期为7天，7天后请重新手动检查。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤4 选择待查看检查结果所在的区域。

步骤5 在待反馈结果检查项目所在行的“操作”列，单击“反馈结果”。

图 9-8 反馈结果入口

步骤6 在弹出提示框中，选择反馈结果，并单击“确定”。

图 9-9 反馈结果

说明

反馈结果有效期为7天，7天后请重新手动检查。

----结束

9.7 查看基线检查结果

本章节介绍如何查看基线检查详情、结果，您可以了解基线检查项影响的资产、基线项目详情等信息。

前提条件

- 已购买态势感知**专业版**，且在有效使用期内。
- 已扫描云服务基线。

查看检查结果总数据

查看某区域中所有检查项的检查结果。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤4 选择待查看检查结果所在的区域，系统将展示当前区域的所有检查结果相关数据。

步骤5 查看当前区域检测到的基线检查结果汇总数据。

图 9-10 检查结果总数据

- 检查规范数：最近一次执行基线检查的检查规范数/检查规范总数。
- 检查项：最近一次执行基线检查中所有的检查项数目。
- 检查项合格率：最近一次执行基线检查的基线合格率。

  整体合格率=合格检查项数量/检查项总数。合格率的统计范围为全部规范的全部检查项目。

  检查项结果分为合格、不合格、检查失败和待检查几种。
- 风险资源分布：最近一次执行基线检查的风险资源分布情况以及风险资源的数量。

风险等级分为：致命、高危、中危、低危、提示几个级别。

----结束

查看基线检查规范列表

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤4 选择待查看检查结果的区域，并选择“检查规范”页签。

步骤5 在基线检查规范中，选择“全部规范”，系统将显示当前区域所有检查规范及其详细信息，如图9-11所示。

图 9-11 全部检查规范

基线检查规范页面会展示所有基线检查规范的列表，包括检查项、检查状态、检查分类、风险资源、描述，以及最近检查时间等信息。

说明

您也可在基线检查规范列表中，选择某个基线检查规范，查看该规范对应的基线检查项目列表。

----结束

查看某个基线检查项目详情

说明

SA**基础版**和**标准版**暂不支持云服务基线查看详情功能。如需查看“风险资源列表”，“修复方式”等详情信息，建议您**购买专业版**。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤4 选择待查看检查项目的区域，并选择“检查规范”页签。

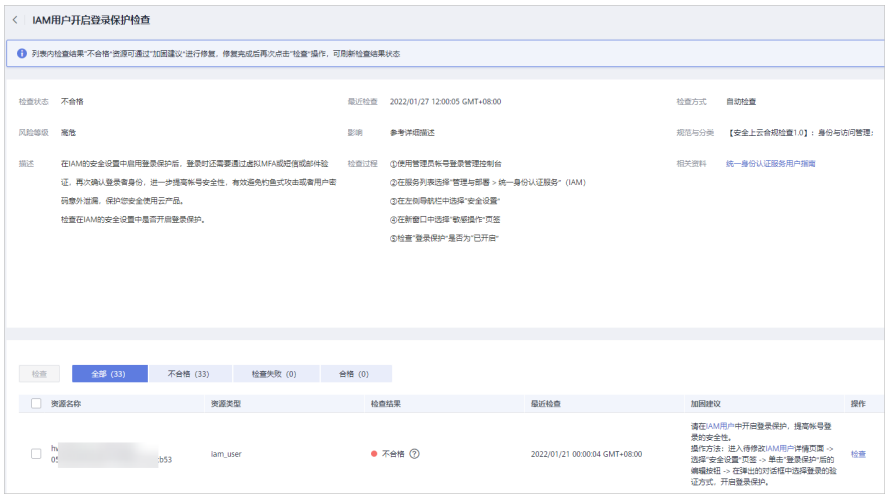
步骤5 在基线检查规范列表中，在待查看检查项目所在行的“操作”列，单击“查看详情”，系统进入检查项目详情页面。

图 9-12 检查项目详情

步骤6 在检查项目详情页面，查看检查项目的详细信息。

查看该风险检查项的详细描述、检查提示和检查结果等。

图 9-13 检查项目详情页面



----结束

查看检查资源列表

资料列表只展示已检查的资源。

步骤1 登录管理控制台。

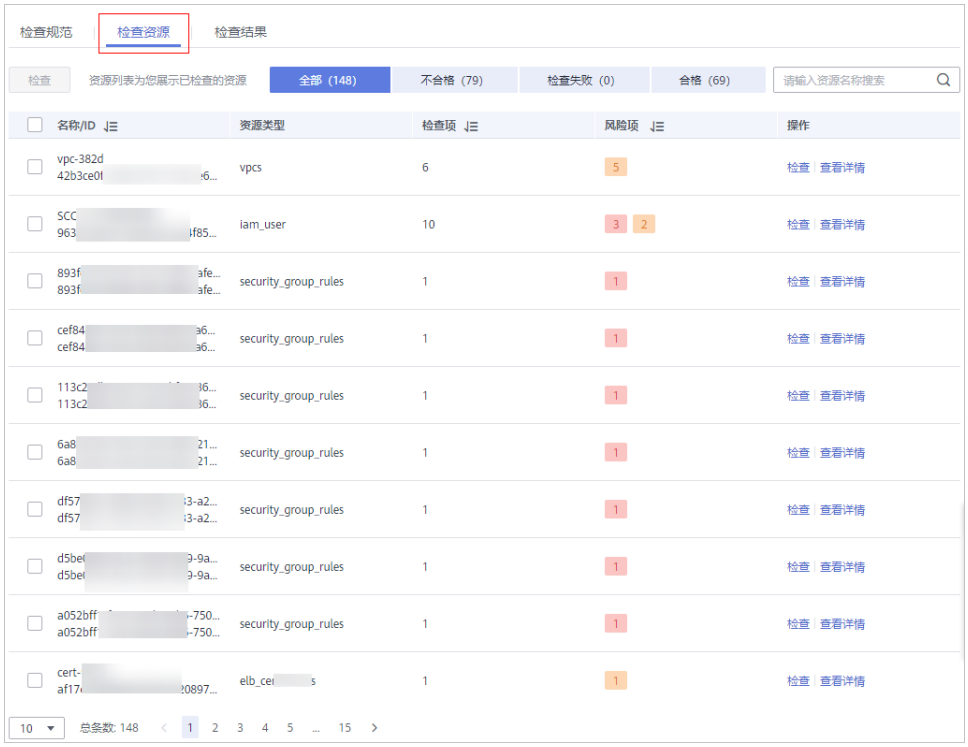
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤4 选择待查看检查结果的区域。

步骤5 选择“检查资源”页签，系统将显示当前区域所有检查资源以及其详细信息，如图9-14所示。

图 9-14 全部检查资源



检查资源页面会展示所有检查资源的列表，包括资源名称、资源类型、检查项，以及风险项等信息。

----结束

查看某个资源的检查详情

说明

SA**基础版**和**标准版**暂不支持云服务基线查看详情功能。如需查看“风险资源列表”，“修复方式”等详情信息，建议您**购买专业版**。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤4 选择待查看检查项目的区域，并选择“检查资源”页签。

步骤5 在检查资源列表中，在待查看资源所在行的“操作”列，单击“查看详情”，系统进入资源详情页面。

图 9-15 检查资源详情

步骤6 在资源详情页面，查看资源的详细信息。

查看该资源的检查项、检查状态、检查方式、最近检查时间等。

图 9-16 检查资源详情页面

----结束

查看检查结果列表

说明

SA**基础版**和**标准版**暂不支持云服务基线查看检查结果功能。为及时了解云服务配置状态，以及确保云服务的配置的合理性，建议您**购买专业版**。

步骤1 登录管理控制台。

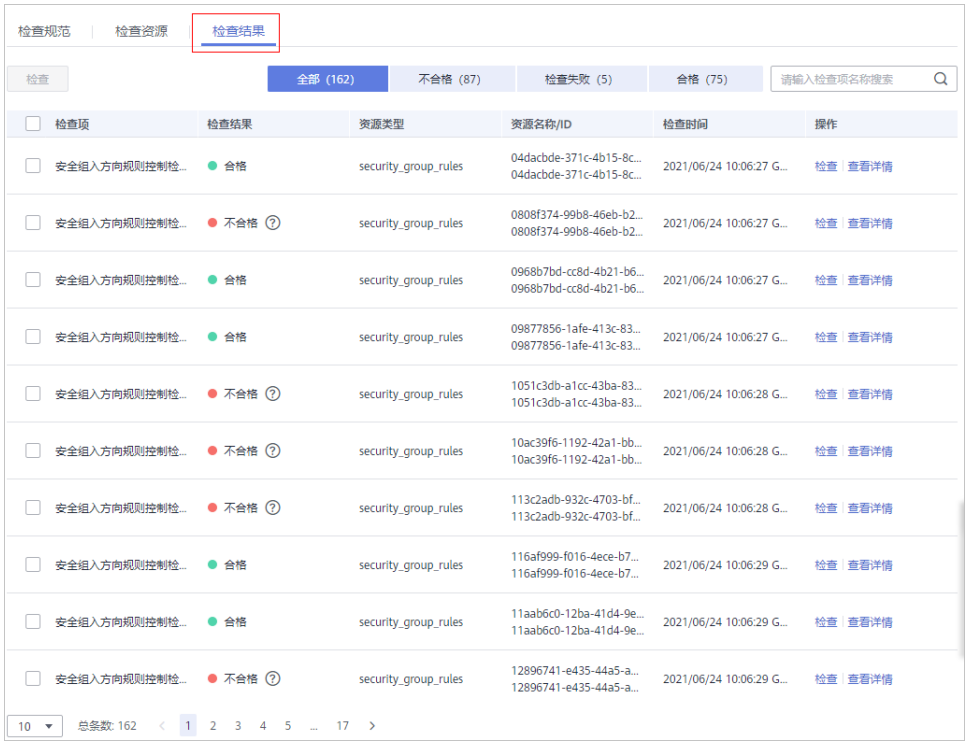
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤4 选择待查看检查结果的区域。

步骤5 选择“检查结果”页签，系统将显示当前区域所有检查结果以及其详细信息，如图9-17所示。

图 9-17 全部检查结果



检查结果页面会展示所有检查结果的列表，包括检查项、检查结果、资源类型、资源名称，以及最近检查时间等信息。

----结束

9.8 处理基线检查结果

本章节介绍如何根据修复建议处理风险配置，以及如何反馈检查结果。

前提条件

- 已购买态势感知**专业版**，且在有效使用期内。
- 已扫描云服务基线。

修复风险项

以修复“IAM用户开启登录保护检查”的子检查项为例。

步骤1 登录管理控制台。

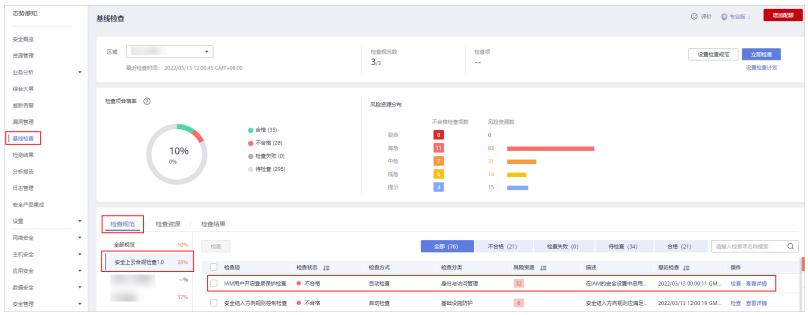
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤4 选择待查看检查结果的区域。

步骤5 在“检查规范”页签中，选择“安全上云合规检查1.0”，查看子检查项风险状态。

图 9-18 子检查项风险状态



- 检查状态图标呈绿色，则表示配置合格，不存在风险配置；
- 检查状态图标呈红色，则表示配置不合格，资产存在一定风险。

步骤6 在“IAM用户开启登录保护检查”所在行的“操作”列，单击“查看详情”，系统进入检查项目详情页面。

步骤7 查看风险详细信息，并根据“检查结果”和“帮助指导”，修复风险点。

表 9-33 子检查项信息说明

参数名称	参数说明
检查状态	呈现当前检查项的检查状态。 ● 合格，提示当前子检查项配置合理，全部合格。 ● 不合格，提示当前子检查项配置可能不合理，并列表呈现检查结果。
最近检查	最近一次执行当前检查项的时间。
检查方式	当前检查项的检查方式。
风险等级	当前检查项出现问题所属的级别。
影响	当前检查项如果有问题将会带来的安全影响。
规范与分类	当前检查项所属的规范以及分类。
描述	当前检查项的具体检查内容。
检查过程	当前检查项的具体检查过程。
相关资料	子检查项涉及云服务配置手册指导。 单击引导链接，可直接跳转至详细手册指导页面。
检查资源	执行当前检查项所属的资源。 检查结果呈现检查合格和不合格两种。 ● 合格，提示当前子检查项配置合理，全部合格。 ● 不合格，提示当前子检查项配置可能不合理，并列表呈现检查结果，单击“操作”列引导，可直接跳转至配置项管理页面，进行安全风险修复。

步骤8 修复所有存在风险的配置后，可单击“检查”，确认风险项是否已修复。

----结束

反馈结果

态势感知的基线检查项目中的手动检查项，您在线下执行检查后，需要在控制台上反馈检查结果，以便计算检查项合格率。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤4 选择待查看检查结果所在的区域。

步骤5 在待反馈结果检查项目所在行的“操作”列，单击“反馈结果”。

图 9-19 反馈结果入口

步骤6 在弹出提示框中，选择反馈结果，并单击“确定”。

图 9-20 反馈结果

说明

反馈结果有效期为7天，7天后请重新手动检查。

----结束

忽略检查项

如果您对某个检查项有其他检查要求（例如，SA的“会话超时策略检查”检查项中检查会话时限是否设置为15分钟，而您的需求为会话时限是否设置为20分钟）或不需要对某检查项进行检查，可以执行忽略操作。

忽略后，再次检查时，将不再对已忽略检查项进行检查，且“检查项合格率”中，也将不再纳入计算中。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“基线检查”，进入基线检查页面。

步骤4 选择待查看检查结果所在的区域。

步骤5 在“检查规范”页签中，在待忽略子检查项的“操作”列单击“忽略”。

下图以忽略“SA专业版购买检查”的子检查项为例：

图 9-21 忽略检查项

如果您想批量忽略检查项，可以勾选所有需要忽略的检查项，然后在列表左上角，单击“忽略”。

步骤6 在弹出的确认框中，单击“确定”。

图 9-22 确认忽略

说明

- 忽略后，再次执行检查时，将不再对已忽略检查项进行检查，且“检查项合格率”中，也将不再纳入计算中。
- 忽略后，如需再次检查该检查项目，在待取消忽略子检查项的“操作”列单击“取消忽略”，并在弹出的确认框单击“确定”。

----结束

10 检测结果

10.1 查看全部检测结果

您可以在“全部结果”页面，获取安全状态的全视图，助您及时确定检测结果的优先级，统筹分析安全趋势。

“全部结果”支持以下特性：

- 支持呈现威胁告警、漏洞、风险、合规检查、违法违规、时讯舆情等领域信息。
- 支持实时接收安全产品检测数据，实时更新结果列表。
- 支持按时间范围、过滤场景等筛选结果。默认呈现近7天内检测结果。
- 支持查看检测结果详情，以及JSON格式的结果详情。
- 支持自定义结果列表呈现的属性。
- 支持标识检测结果的处理状态。
- 支持威胁情报溯源。

约束限制

- 按过滤场景筛选检测结果，最多可呈现10000条结果。
- 仅可呈现近180天的检测结果。

前提条件

- 已接收到安全产品的检测结果。

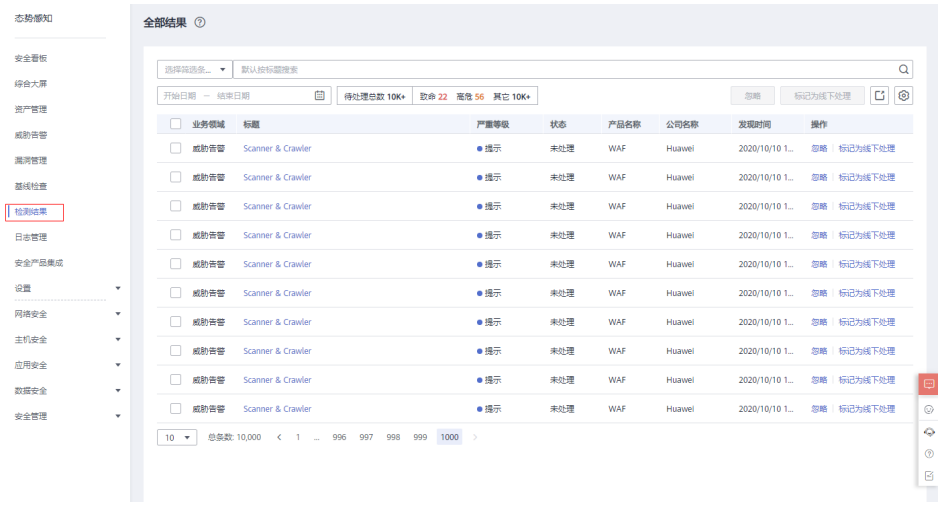
操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“检查结果”，进入全部结果管理页面。

图 10-1 查看全部结果列表



步骤4 筛选查看检测结果。

- 在场景列框选择过滤场景，单击，即可查看到目标场景下检测结果。
- 当过滤后的结果仍较多时，可补充过滤条件和选择时间范围，快速查找结果。
  - 在筛选框补充过滤条件，添加一项或多项过滤条件，并配置相应条件属性，单击，快速查找指定条件属性的结果。
  - 在时间过滤框中，选择检测结果发现的时间范围，单击“确认”，快速查找指定时间范围内的结果。

步骤5 查看检测结果列表。

筛选后的列表，可查看满足条件的检测结果列表，以及结果统计信息。

步骤6 查看检测结果详情。

1. 单击列表中结果的“标题”，右侧滑出结果详情窗口。

图 10-2 检测结果详情

2. 查看与该结果相关的“基本信息”、“描述”、“资源信息”、“攻击信息”、受影响的用户等信息，更多参数说明请参考**表10-1**。

表 10-1 检测结果详情参数说明

参数	参数说明
基本信息	检测结果的基本信息，包括标题、级别、状态、时间、业务领域、公司名称、产品名称、类别等信息。
描述	检测结果的简要介绍。
资源信息	受影响的资源信息，包括资源名称、资源ID、资源类型、资源区域等信息。
租户信息	受影响的用户信息，包括租户ID、项目名称、项目ID、用户所在区域等信息。
攻击源信息	攻击来源信息，包括攻击源IP、查看威胁情报溯源、攻击源端口、经度等信息。
攻击目标信息	攻击目标信息，包括攻击目标IP、攻击目标端口等信息。
相关检测结果	相关联检测结果的信息，包括相关联资源名称、结果来源等信息。
漏洞信息	漏洞结果信息，包括漏洞ID、CVSS分数、CVSS版本、提供方等信息。
漏洞影响范围	漏洞影响范围信息，包括影响版本、安全版本等信息。
合规检查信息	合规检查基本信息，包括检查项、检查结果等信息。
涉及CVE	漏洞结果CVE编号。
参考链接/链接	结果相关参考链接。
修复建议/处置建议	结果修复或处置建议说明。

3. 单击“查看JSON”，查看JSON格式检测结果详情。

----结束

查看威胁情报溯源

本部分介绍如何查看威胁情报溯源。

前提条件

已启用产品集成，具体操作请参见启用产品集成。

操作步骤

步骤1 进入目标检测结果的详情页面，在“攻击源信息”中，单击“威胁情报溯源”。

图 10-3 威胁情报溯源

步骤2 选择威胁情报分析平台。

图 10-4 分析平台

步骤3 在弹出的确认框中，确认授权并单击“同意并立即前往”，系统进入安天威胁分析平台。

首次登录需注册。

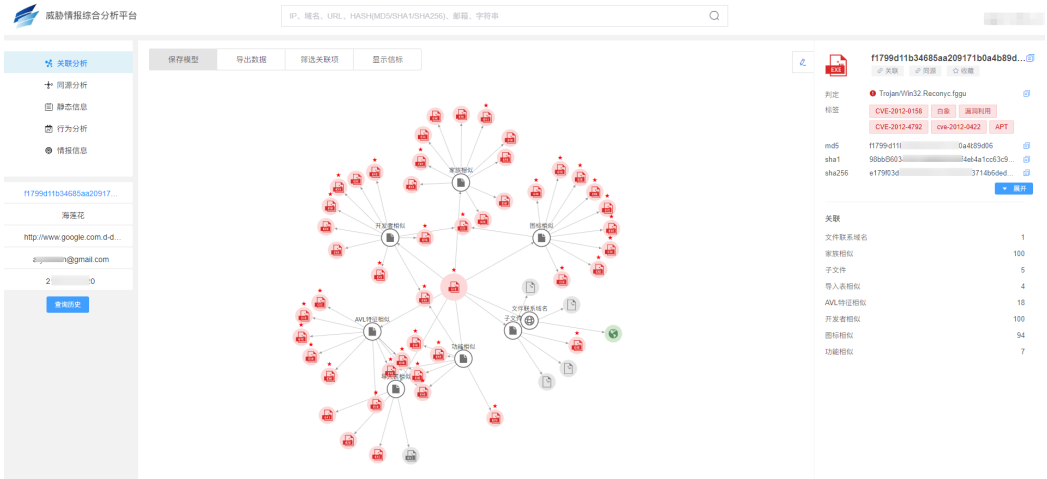
说明

安天分析平台在用户注册后，享受免费试用24小时。试用结束后，需要用户线下购买安天分析能力服务，安天平台人工审核通过后，可继续享用该服务。

步骤4 查看威胁分析数据。

安天威胁分析示例如图10-5所示。

图 10-5 威胁分析数据



----结束

10.2 处理检测结果

当接收到检测结果后，您可标记结果处理状态。

- 忽略：如果确认该检测结果不会造成危害，在“忽略风险项”窗口记录“处理人”、“忽略理由”，可标记为“已忽略”状态。
- 标记为线下处理：如果该检测结果已在线下处理，在“标记为线下处理”窗口记录“处理人”、“处理时间”和“处理结果”，可标记为“已线下处理”状态。

说明

由于SA中的检测结果汇聚了企业主机安全（Host Security Service，HSS）、DDoS高防（Advanced Anti-DDoS，AAD）、Web应用防火墙（Web Application Firewall，WAF）等安全防护服务上报的告警数据，因此，处理检测结果时须注意以下顺序：

1. 需先在SA检测结果详情页面查看来源。
2. 前往来源服务进行优先处理。
3. 处理后再到SA中来标记结果处理状态。

例如，告警显示来源产品名称为HSS，则需在HSS控制台上进行处理后，再在SA中进行标记处理。

前提条件

已接收到安全产品的检测结果。

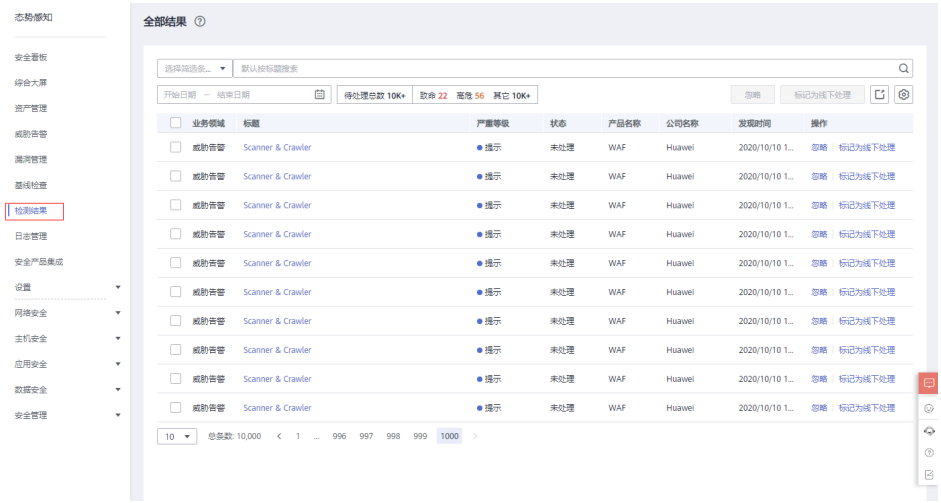
操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“检测结果”，进入全部结果管理页面。

图 10-6 处理检测结果



步骤4 筛选检测结果。

步骤5 批量标记检测结果。

选择一个或多个“未处理”状态的结果，单击“忽略”或“标记为线下处理”，对不同检测结果批量执行相应的处理操作。

步骤6 单个标记检测结果。

- 在结果列表对应“操作”列，单击“忽略”或“标记为线下处理”，对单个检测结果执行相应处理操作。
- 在结果详情窗口，右下角单击“忽略”或“标记为线下处理”，对单个检测结果执行相应处理操作。

----结束

10.3 导出检测结果

态势感知支持一键导出检测结果。

导出的excel文件中包含“产品名称”、“公司名称”、“受影响资源”、“业务领域”、“标题”、“发生时间”、“发生次数”、“置信度”、“重要性”和“状态”等信息。

约束限制

- 按过滤场景筛选检测结果，最多可导出10000条结果。
- 仅可导出近180天的检测结果。

前提条件

- 已接收到安全产品的检测结果。

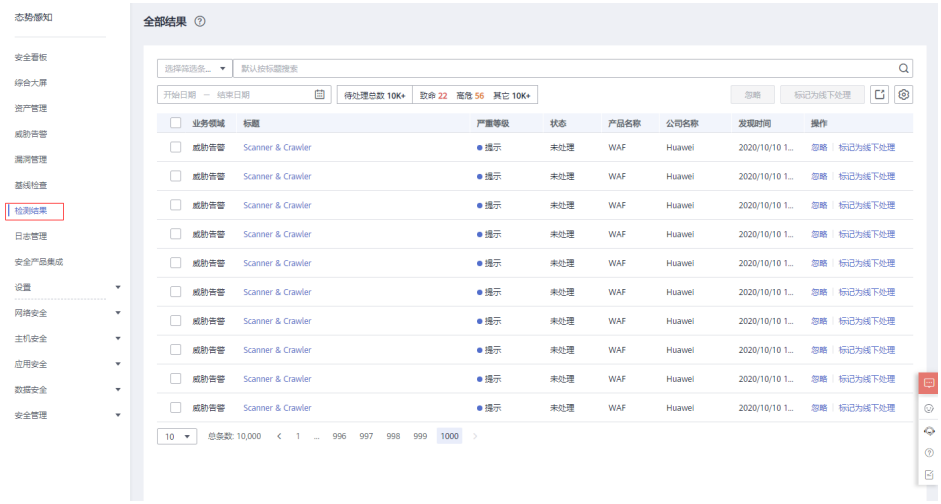
操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“检测结果”，进入全部结果管理页面。

图 10-7 导出检测结果



步骤4 筛选检测结果。

步骤5 单击，一键导出筛选的检测结果列表，并以.csv格式文件保存在本地。

导出完成后，即可离线查看结果。

----结束

10.4 自定义结果列表

态势感知支持自定义检测结果列表。

前提条件

- 已接收到安全产品的检测结果。

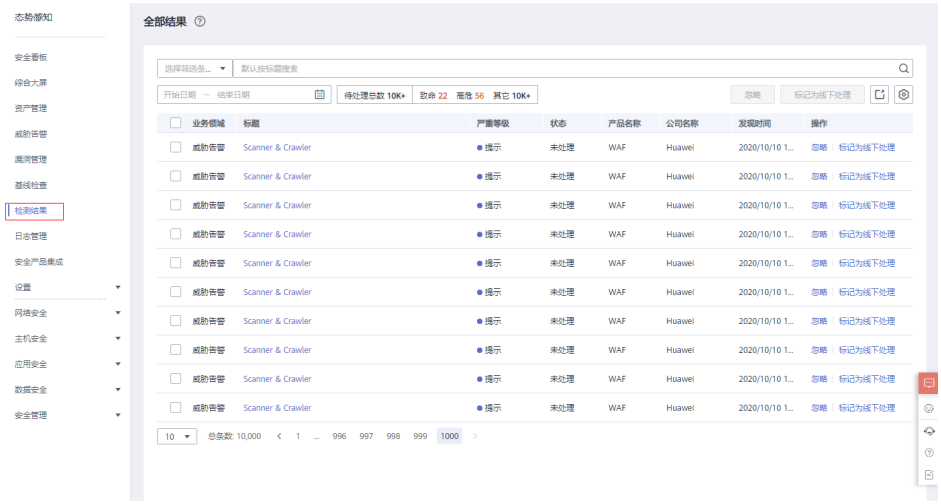
操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“检测结果”，进入全部结果管理页面。

图 10-8 自定义结果列表



步骤4 单击，展开结果列表属性框。

步骤5 勾选结果属性。

步骤6 刷新结果列表，即可在列表查看目标属性。

----结束

10.5 管理筛选条件

筛选条件用于筛选符合场景中过滤条件的结果，呈现匹配的结果列表。例如筛选条件添加产品名称和资源类型两个条件，属性分别为“企业主机安全”和“云服务器”，则匹配的结果必须同时符合这两个条件属性。

目前可添加的条件及属性如下：

- 标题：检测结果的标题内容，可输入关键字。默认按标题搜索。
- 严重等级：检测结果的风险等级，包括“致命”、“高危”、“中危”、“低危”、“提示”。
- 业务领域：检测结果所属业务领域，包括“威胁告警”、“漏洞”、“合规检查”、“违法违规”、“风险”、“舆情”、“安全公告”。
- 状态：用户对检测结果的处理状态，包括“未处理”、“已忽略”、“已线下处理”。
- 资源名称：检测结果来源资源的名称，需输入资源名称。
- 资源类型：检测结果来源资源的类型，包括“云服务器”、“虚拟私有云”、“安全组”、“弹性公网IP”、“磁盘”、“其他”。
- 公司名称：检测结果来源产品所属公司，需输入公司名全称。
- 产品名称：检测结果来源安全产品，需输入产品名全称。

约束限制

- 一个筛选条件仅能包含一组“标题”关键字。
- 一个筛选条件仅能包含一个“资源名称”。
- 一个筛选条件仅能包含一个“公司名称”。
- 一个筛选条件仅能包含一个“产品名称”。

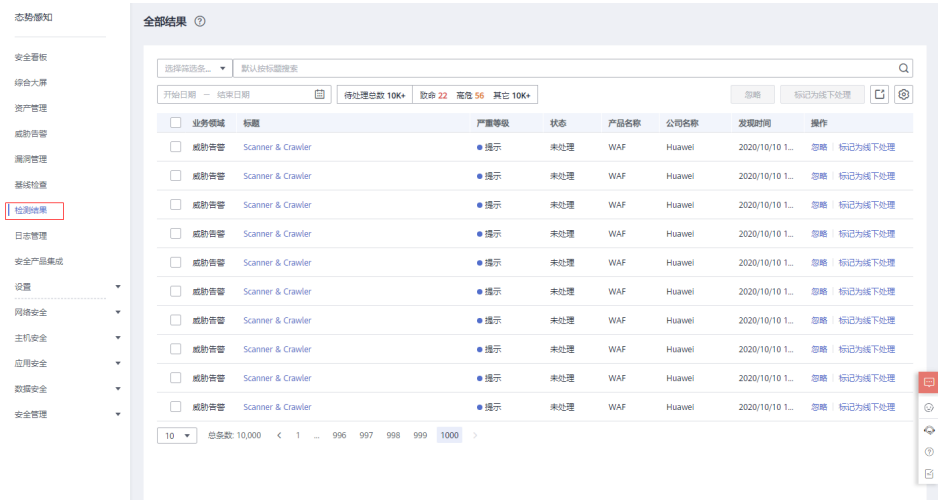
创建筛选条件

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“检测结果”，进入全部结果管理页面。

图 10-9 检测结果



步骤4 添加筛选条件。

- 在筛选框添加过滤条件，添加一项或多项过滤条件，并配置相应条件属性。
- 在时间筛选框中，选择时间范围。

步骤5 单击筛选框后“保存”，弹出筛选条件保存窗口。

图 10-10 保存筛选条件

步骤6 配置筛选条件信息。

- 设置“场景名称”，自定义筛选条件名称。
- （可选）勾选“设为默认筛选条件”。

步骤7 单击“确定”，返回全部结果列表页面，即可在场景列框查看新建的筛选条件。

----结束

修改筛选条件

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“检查结果”，进入全部结果管理页面。

步骤4 在筛选条件列框，选择筛选条件。

步骤5 在筛选框后单击“编辑”，弹出编辑窗口。

图 10-11 编辑筛选条件

步骤6 修改筛选条件名称。

步骤7 单击“确认”，返回全部结果列表页面，即可查看已修改的筛选条件。

----结束

删除筛选条件

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知管理页面。

步骤3 在左侧导航栏选择“检查结果”，进入全部结果管理页面。

步骤4 在筛选条件列框，选择筛选条件。

步骤5 在筛选框后单击“编辑”，弹出编辑窗口。

图 10-12 删除筛选条件

步骤6 单击“删除”，返回全部结果列表页面，即完成筛选条件的删除。

----结束

11 分析报告

11.1 创建安全报告

本小节主要介绍如何新建安全报告，以及通过复制已创建的报告快速创建报告。

约束限制

- 目前分析报告功能处于公测（beta）阶段，如有问题，请联系华为云技术支持进行处理。

- 仅**专业版**支持使用分析报告功能。
- 默认创建定期周报和月报各一个，可免费生成2期报告。**专业版**最多可创建12个安全报告，可多次生成报告。
- 支持创建周报、月报、自定义报告。
  - 周期报告：默认周报和月报，统计上一周或上一月安全信息。
  - 单次报告：可自定义季度报、月报、周报、日报等，分别按季度、月、周、日等周期统计安全信息。

前提条件

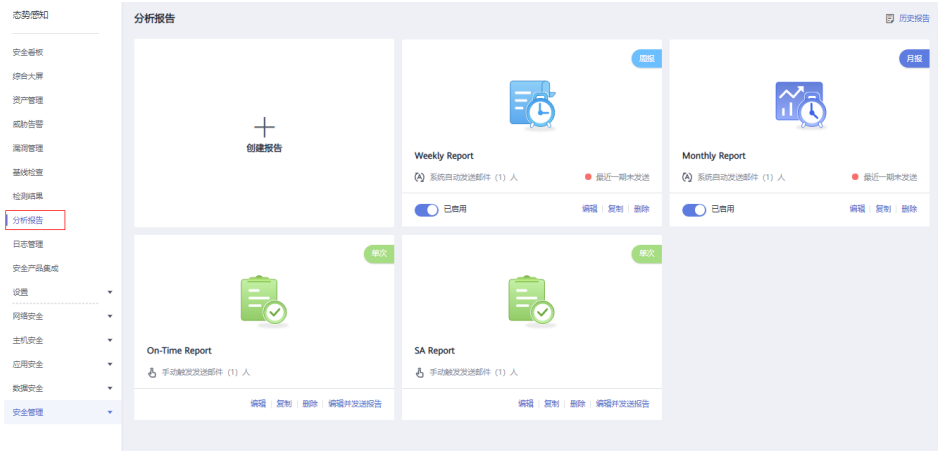
已购买态势感知专业版，且在有效使用期内。

新建安全报告

步骤1 登录管理控制台。

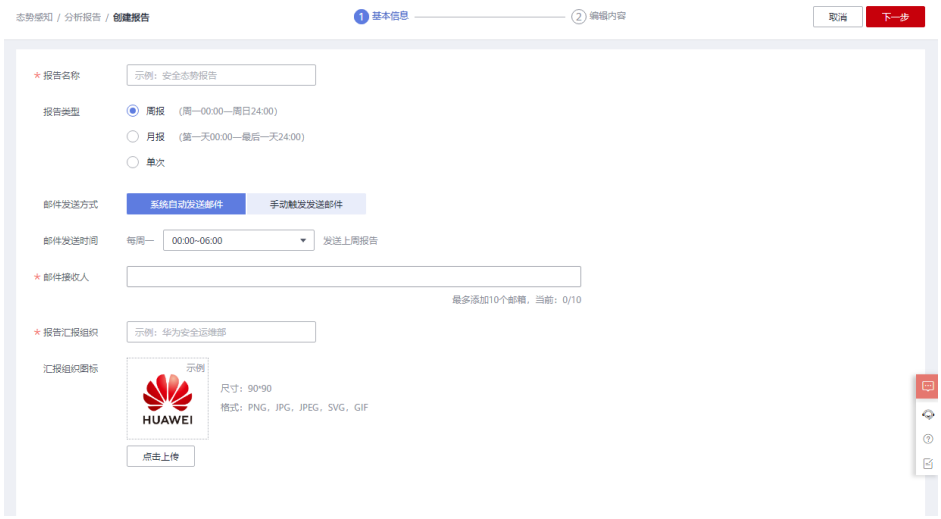
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知 > 分析报告”，进入安全报告管理页面。

图 11-1 新建安全报告



步骤3 单击“创建报告”，跳转到报告基本信息配置页面。

图 11-2 配置报告基本信息



步骤4 配置报告基本信息。

表 11-1 报告基本信息参数说明

参数	说明
报告名称	自定义报告名称，例如安全态势报告。
报告类型	选择报告类型，可勾选“周报”、“月报”、“单次”。 • 周报：默认统计上一周安全信息，上周一00:00到上周日24:00。 • 月报：默认统计上一月安全信息，上月第一天00:00到上月最后一天24:00。 • 单次：自定义选择时间范围，可统计一年、一季度、一月、一周、一天等安全信息。

参数	说明
邮件发送方式	选择自动或手动发送邮件。 ● 自动发送：定期自动发送安全报告，适用于“周报”和“月报”类型的报告。 ● 手动触发：手动触发发送安全报告，适用于需编辑报告小节内容的报告。
邮件发送时间	针对自动发送方式，需选择发送时间。 ● 默认可选择四个发送时间段。 ● “周报”默认为每周一发送上一周周报。 ● “月报”默认为每月一号发送上一月月报。
邮件接收人	添加邮箱地址，例如test@example.com。 ● 最多可添加10个邮箱。
报告汇报组织	自定义汇报组织，例如安全运维部。
汇报组织图标	单击“上传”，上传组织图标。图标要求如下： ● 尺寸90×90 ● 格式PNG、JPG、JPEG、SVG、GIF

步骤5 单击右上角“下一步”，进入报告内容配置页面。

自定义报告内容。

1. 勾选报告内容模块，可选择报告说明、报告总结、安全评分、资产风险、威胁告警、基线风险、资产漏洞、后续规划等模块。
2. 勾选“报告说明”、“自定义小结”、“后续规划”等模块后，需编辑小结内容。

步骤6 预览报告内容。

1. 单击右上角“预览”，预览自定义报告内容。
2. 单击右上角“关闭预览”，返回报告内容配置页面。

步骤7 单击右上角“保存”，返回安全报告管理页面，即可查看创建的安全报告。

----结束

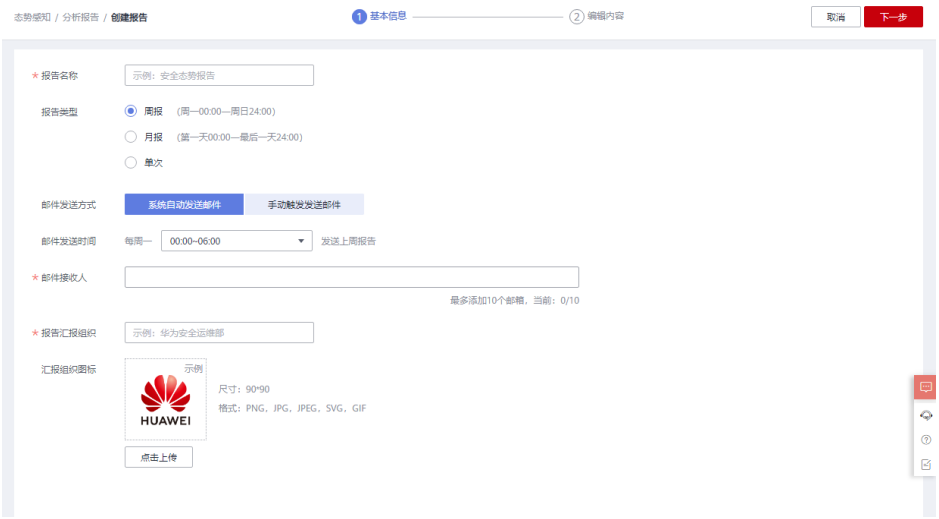
复制安全报告

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知 > 分析报告”，进入安全报告管理页面。

步骤3 在已创建的安全报告模块，单击“复制”，跳转到报告基本信息配置页面。

图 11-3 配置报告基本信息



步骤4 修改报告基本信息。

步骤5 单击右上角“下一步”，进入报告内容配置页面，修改报告内容。

1. 勾选报告内容模块。
2. 重新编辑小结内容。

步骤6 单击右上角“预览”，预览自定义报告内容

步骤7 单击右上角“保存”，返回安全报告管理页面，即可查看新创建的安全报告。

----结束

11.2 发送安全报告

态势感知通过自动或手动方式发送报告到接收人邮箱，接收人收到报告邮件后，通过报告“查阅/地址”可跳转到报告详情页面，查看或下载报告。

首次发送报告后，邮箱将收到“确认订阅”的邮件。确认订阅后，再次发送报告才会收到报告查阅地址。

本小节主要介绍如何发送安全报告，包括自动发送报告、手动发送报告，以及如何发送历史报告。

约束限制

- 目前分析报告功能处于公测（beta）阶段，如有问题，请联系华为云技术支持进行处理。

- 安全报告发送的约束限制如表11-2所示。

表 11-2 安全报告限制说明

报告类型	触发方式	是否支持多次编辑并发送
单次报告	手动	支持
周期报告	手动、自动 自动发送时，必须编辑接收人邮箱地址、汇报组织、组织图标等信息后，才能开启自动发送。	仅支持编辑并发送一次
历史报告	手动	不可编辑，支持多次发送
所有报告一次最多可发送到10个邮箱。		

前提条件

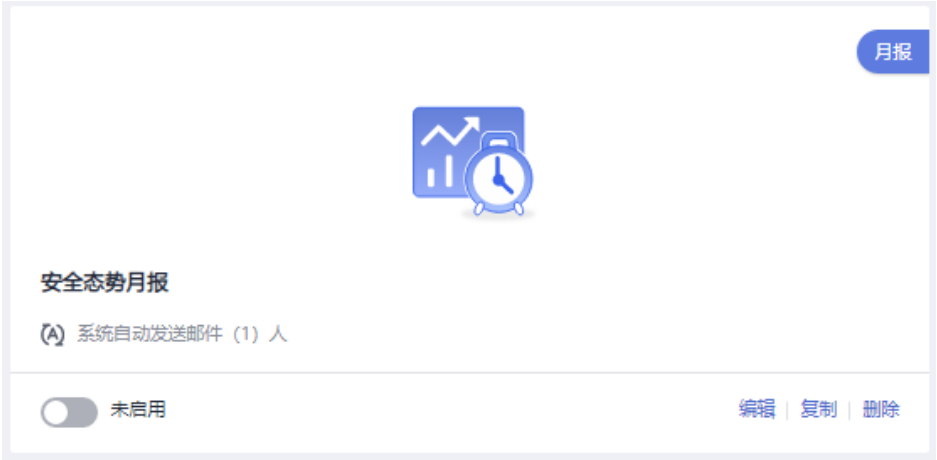
- 已购买态势感知专业版，且在有效使用期内。

自动发送报告

定期发送的“周报”和“月报”创建完成后，默认状态为“已启用”。态势感知会在设置的时间内，将安全报告自动推送到邮箱。

若后续不再需要推送该报告，可单击  ，切换报告状态为“未启用”，关闭该报告的发送。

图 11-4 关闭报告



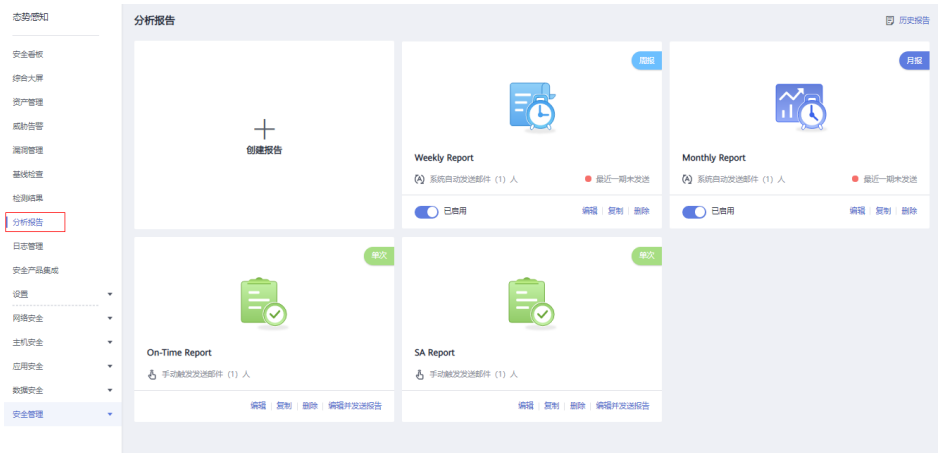
手动发送报告

手动触发发送的报告，在创建报告后，需编辑相关信息并

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知 > 分析报告”，进入安全报告管理页面。

图 11-5 手动发送报告



步骤3 选择目标报告，单击“编辑并发送报告”，跳转到报告内容配置页面。

步骤4 编辑报告内容。

1. 勾选报告内容模块。
2. 重新编辑小结内容。

步骤5 单击右上角“预览”，预览自定义报告内容

步骤6 单击右上角“保存并发送邮件”，返回安全报告管理页面，即可历史报告中查看发送记录。

----结束

发送历史报告

安全报告发送后，可在历史报告栏查看并发送历史报告。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知 > 分析报告”，进入安全报告管理页面。

步骤3 单击右上角“历史报告”，展开历史报告列表。

图 11-6 发送历史报告

步骤4 选择目标历史报告，在对应“操作”列单击“发送邮件”，立即发送邮件。

说明

也可单击目标报告图标，进入报告详情页面，选择报告统计时间，再单击右上角“发送邮件”，立即发送邮件。

----结束

11.3 查看报告详情

本小节主要介绍发送报告后，如何查看历史报告详情。

约束限制

- 目前分析报告功能处于公测（beta）阶段，如有问题，请联系华为云技术支持进行处理。

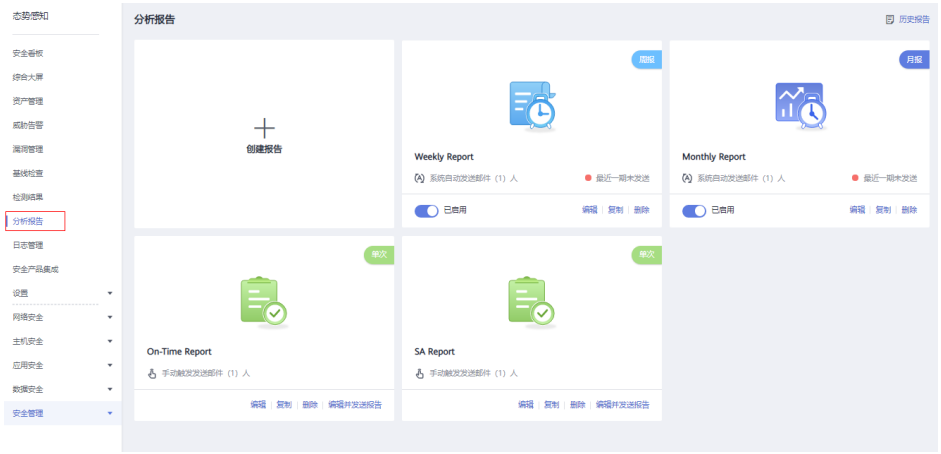
- 成功发送一期报告后，才能查看历史报告详情。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知 > 分析报告”，进入安全报告管理页面。

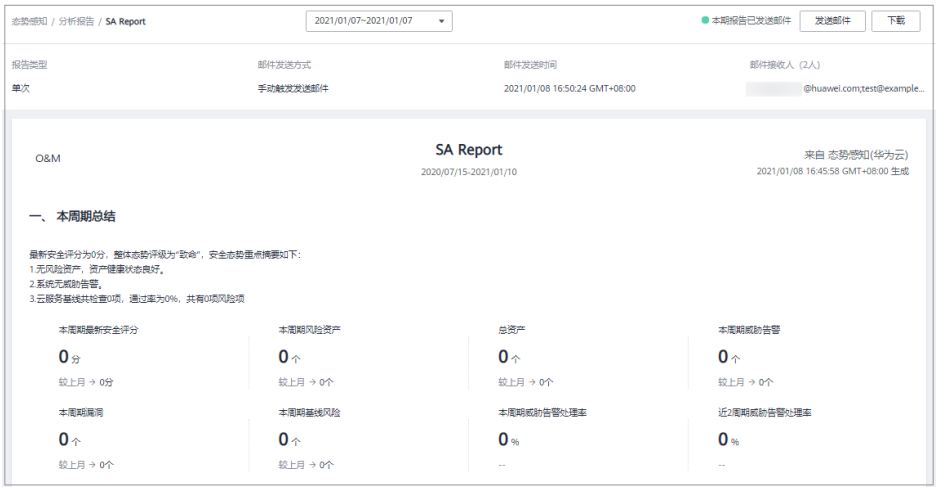
图 11-7 查看报告列表



步骤3 选择目标报告，单击报告图标，跳转到最新一期报告详情页面。

查看最新一期发送的报告基本信息、报告内容、报告发送信息、报告发送状态等。

图 11-8 查看报告详情



步骤4 在“统计时间”框中，选择报告统计时间，可切换到其他历史报告详情页面，查看相应历史报告详情。

----结束

11.4 下载历史报告

报告发送后，态势感知支持下载的历史报告到本地。

本小节主要介绍如何下载历史报告。

约束限制

- 目前分析报告功能处于公测（beta）阶段，如有问题，请联系华为云技术支持进行处理。

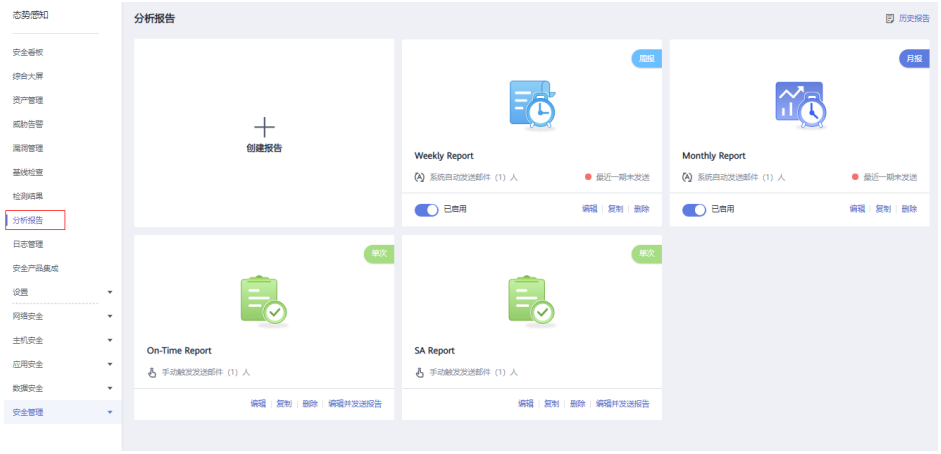
- 默认支持下载pdf格式的报告。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知 > 分析报告”，进入安全报告管理页面。

图 11-9 下载历史报告

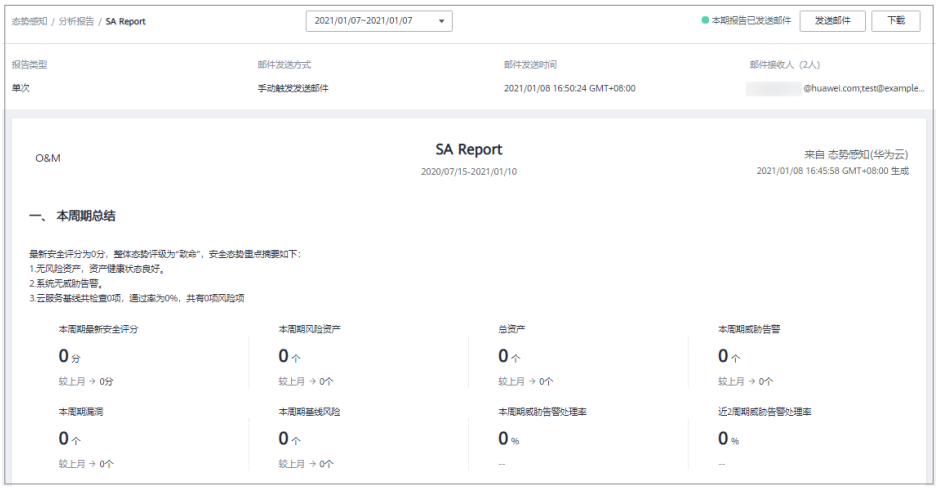


步骤3 单击右上角“历史报告”，展开历史报告列表。

图 11-10 历史报告列表

步骤4 选择目标历史报告，在对应“操作”列单击“下载”，跳转到报告详情页面。

图 11-11 报告详情页面



步骤5 查看历史报告，单击右上角“下载”，将报告下载到本地。

说明

也可单击目标报告图标，进入报告详情页面，选择报告统计时间，再单击右上角“下载”，下载报告。

----结束

11.5 查看安全报告

本小节主要介绍态势感知生成的月报样例以及月报显示的信息。

前提条件

- 目前分析报告功能处于公测（beta）阶段，如有问题，请联系华为云技术支持进行处理。

- 已下载安全月报。

安全月报样例

态势感知安全月报将显示当月的安全评分、整体态势、威胁告警等相关信息，具体信息如下图所示。

图 11-12 月报样例 1-本月总结

图 11-13 月报样例 2-安全评分

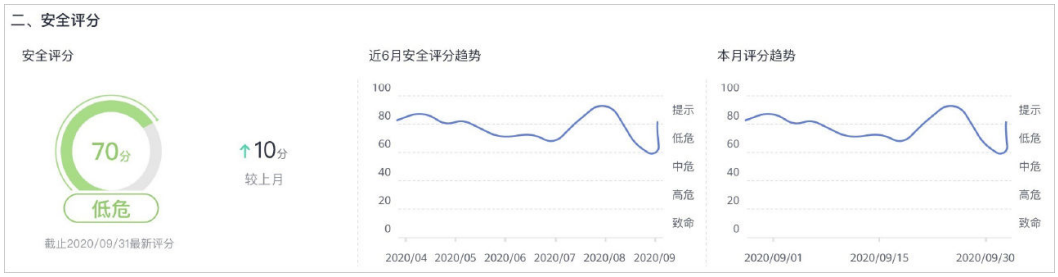


图 11-14 月报样例 3-资产风险

图 11-15 月报样例 4-威胁告警

图 11-16 月报样例 5-基线风险

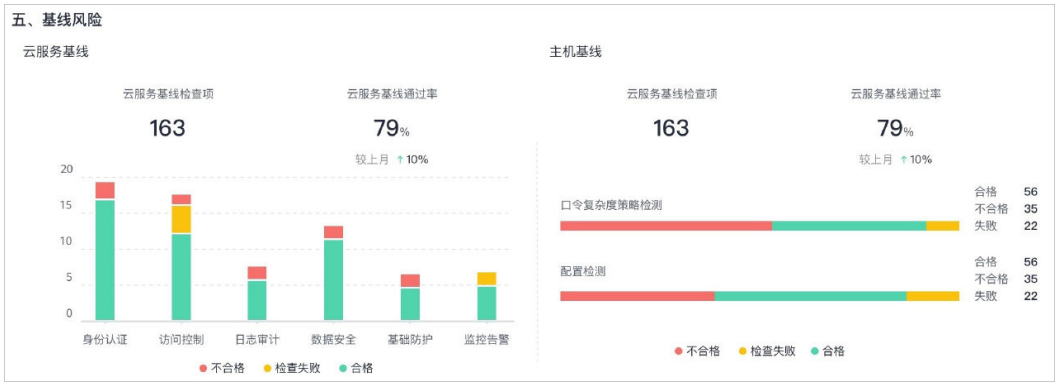
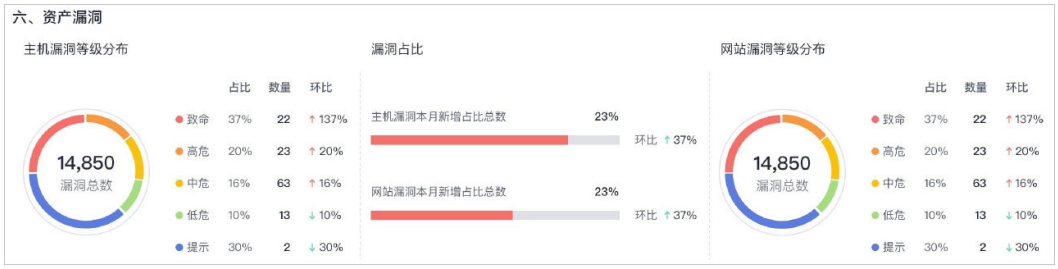


图 11-17 月报样例 6-资产漏洞



11.6 编辑安全报告

本小节主要介绍创建报告后，如何修改报告基本信息和报告内容。

约束限制

- 目前分析报告功能处于公测（beta）阶段，如有问题，请联系华为云技术支持进行处理。

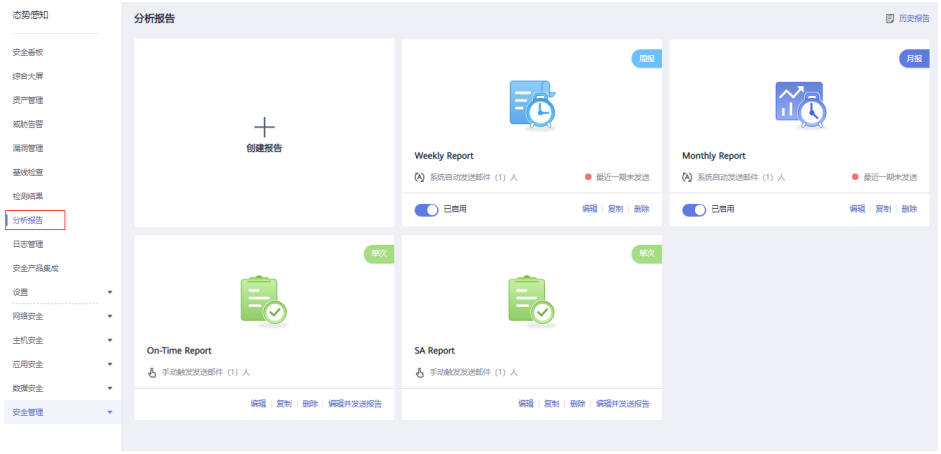
- 报告类型不支持修改。
- 周期报告可修改报告名称、发送方式、发送时间、接收人、汇报组织、组织图标等信息。
- 单次报告可修改报告名称、接收人、汇报组织、组织图标等信息。

操作步骤

步骤1 登录管理控制台。

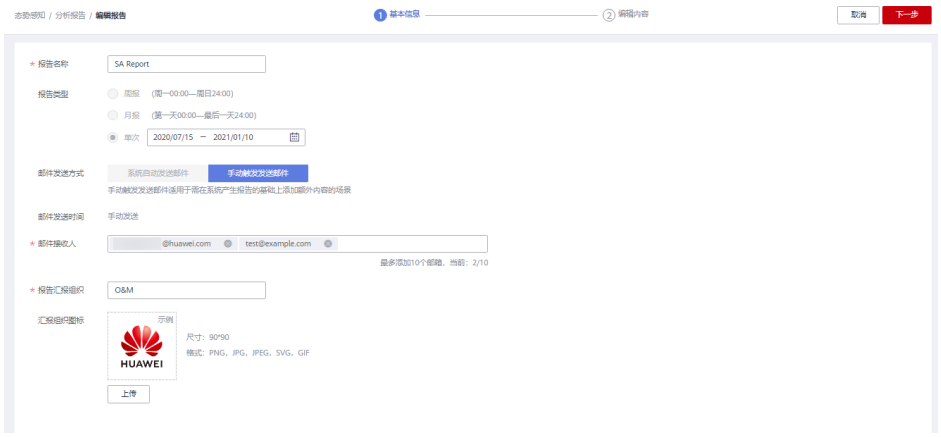
步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知 > 分析报告”，进入安全报告管理页面。

图 11-18 编辑安全报告



步骤3 选择目标报告，单击“编辑”，跳转到报告基本信息配置页面。

图 11-19 修改报告基本信息



步骤4 （可选）编辑报告基本信息。

步骤5 单击“下一步”，跳转到报告内容配置页面。

步骤6 （可选）勾选报告模块，自定义小结。

步骤7 单击右上角“保存”，返回安全报告管理页面。

----结束

11.7 删除报告

本小节主要介绍如何删除报告。

须知

删除报告后，相应历史报告数据及记录也将被删除且不可找回，请谨慎操作。

约束与限制

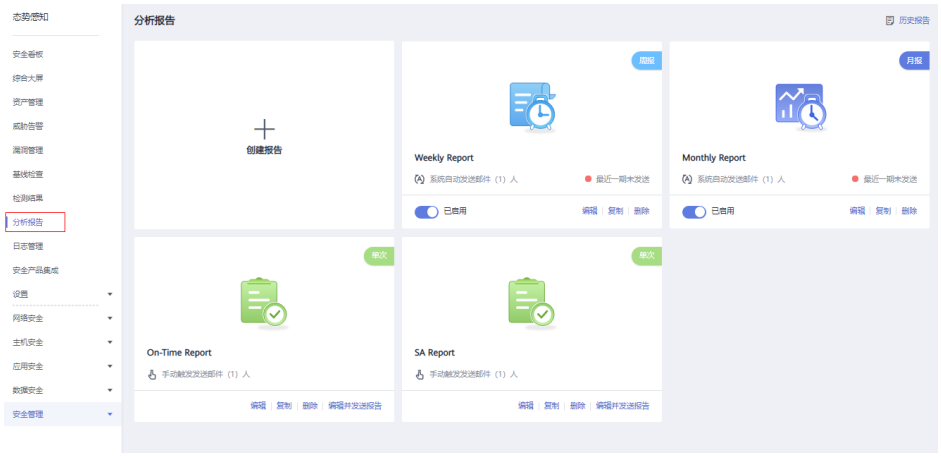
- 目前分析报告功能处于公测（beta）阶段，如有问题，请联系华为云技术支持进行处理。

操作报告

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知 > 分析报告”，进入安全报告管理页面。

图 11-20 删除安全报告



步骤3 选择目标报告，单击“删除”，弹出删除报告确认窗口。

图 11-21 删除报告确认

步骤4 单击“是”，返回安全报告管理页面。

----结束

12 日志管理

通过授权对象存储服务（Object Storage Service，OBS）存储态势感知日志，帮助用户轻松应对安全日志存储、导出场景，以及满足日志存储180天及集中审计的要求。

为应对SA日志的容灾恢复，将存储到OBS桶的日志，通过数据接入服务（Data Ingestion Service）传输到线下SIEM系统，恢复和离线管理SA日志数据。同时，可将线下SIEM系统日志数据，通过DIS重新传输上云进行分析和存储。

说明

- DIS支持通过以下几种方式上传和下载数据：Kafka Adapter、DIS Agent、DIS Flume Plugin、DIS Flink Connector、DIS Spark Streaming、DIS Logstash Plugin等，详细说明请参见**使用DIS**。
- 存储至OBS功能为Region级别功能。
- OBS独立收费，具体收费情况请以OBS服务为准。

前提条件

- 已购买专业版态势感知，且在有效使用期内。
- 操作账号权限检查。使用资源管理功能时，除了需要“SA FullAccess”、“SA ReadOnlyAccess”策略权限，还需要“Tenant Administrator”权限，请提前授予操作账号对应权限。

  “Tenant Administrator”权限配置详细操作请参见**如何配置日志管理功能所需的权限**。

创建日志存储至 OBS 桶

为满足安全审计日志存储180天要求，可将日志存储至OBS桶。OBS支持长久存储日志数据，并支持在OBS控制台下载日志文件。

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知 > 日志管理”，进入日志管理页面。

步骤3 在“存储至OBS桶”栏中，单击  ，开启存储，如**图12-1**所示。

图 12-1 存储至 OBS 桶

步骤4 配置存储日志相关参数，具体参数说明如表12-1所示。

表 12-1 配置存储日志参数说明

参数名称	参数说明
桶名称	选择已创建的OBS桶。 如果没有可选择的OBS桶，单击“您没有可用的OBS桶，请前往创建”，进入对象存储服务管理控制台，创建OBS桶。 **说明** • 目前仅支持选择当前账号所在的区域中已有的OBS桶。 • 目前仅支持存储类别为“标准存储”和“低频访问存储”的OBS桶。
对象名称	自定义对象名称。
存储路径	根据桶名称和对象名称生成的存储路径。

步骤5 单击“确定”，完成配置。

配置成功后，日志将在大约10分钟后存储至OBS桶。

----结束

其他操作

若不再需要将日志存储至OBS，可在“存储至OBS桶”栏中，单击  ，关闭日志存储至OBS桶。取消后，显示如图12-2所示。取消后，已上传存储到OBS桶的日志数据不会被删除。

图 12-2 取消存储

13 产品集成

13.1 管理产品集成

态势感知通过集成安全防护产品，接入各安全产品检测数据，集中管理风险检测结果。

目前默认支持以下产品/服务的集成管理：

- 企业主机安全（HSS）
- Anti-DDoS流量清洗（Anti-DDOS）
- Web应用防火墙（WAF）
- 云堡垒机（CBH）
- 容器安全服务（CGS）
- 漏洞管理服务（CodeArts Inspector）
- 安天威胁情报综合分析平台（TID）

说明

若需启用其他产品集成，请在“安全产品集成”页面，单击右上角“我要推荐”，反馈相关产品信息。

本小节主要介绍如何管理安全产品集成，包括启用和取消产品集成。

约束限制

- 需按区域分别启用或取消产品集成。
- 启用产品集成需账户具有“Tenant Administrator”角色。

启用产品集成

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

图 13-1 产品集成

步骤3 选择“区域”。

选择产品所在的区域，可选择“华北-北京一”、“华北-北京四”、“华东-上海二”、“华东-上海一”、“华南-深圳”、“华南-广州”或“西南-贵阳一”。

步骤4 查询目标产品。

选择“未集成”筛选条件，查找符合条件的产品。更多查询方式请参见**查看产品集成列表**。

步骤5 开启接收检测结果。

在目标产品列框，单击“开启集成”，开启接收来自该产品的检测数据。

启用产品集成后，约5分钟后即可接收到产品上报的数据。

说明

为确保产品检测数据的正常接收，请确保已开启各产品相应防护功能。

----结束

取消产品集成

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

图 13-2 产品集成

步骤3 选择“区域”。

选择产品所在的区域，可选择“华北-北京一”、“华北-北京四”、“华东-上海二”、“华东-上海一”、“华南-深圳”、“华南-广州”或“西南-贵阳一”。

步骤4 查询目标产品。

选择“已集成”筛选条件，查找符合条件的产品。更多查询方式请参见**查看产品集成列表**。

步骤5 取消接收检测结果。

在目标产品列框，单击“关闭集成”，取消接收来自该产品的检测数据。

----结束

13.2 查看产品集成

启用产品集成，并接入安全产品数据后，您可以管理集成列表，并可查看从产品接收的统计结果数量。

查看产品集成列表

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

图 13-3 产品集成

步骤3 选择“区域”。

选择产品所在的区域，可选择“华北-北京一”、“华北-北京四”、“华东-上海二”、“华东-上海一”、“华南-深圳”、“华南-广州”或“西南-贵阳一”。

步骤4 选择“集成类型”和“探测状态”。

集成类型分为“检测结果类产品集成”、“调查分析类产品集成”。

探测状态分为“探测正常”、“探测异常”、“从未探测”、“停止探测”。

步骤5 选择“产品名称”、“产品类型”或“公司名称”筛选条件。

步骤6 在搜索框输入关键字，单击，即可查看到满足条件的产品。

----结束

查看产品集成结果

步骤1 登录管理控制台。

步骤2 在页面左上角单击，选择“安全与合规 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

图 13-4 产品集成

步骤3 选择“区域”。

选择产品所在的区域，可选择“华北-北京一”、“华北-北京四”、“华东-上海二”、“华东-上海一”、“华南-深圳”、“华南-广州”或“西南-贵阳一”。

步骤4 查询目标产品。

选择“已集成”、集成类型和探测状态，查找符合条件的产品。更多查询方式请参见**查看产品集成列表**。

步骤5 查看接收结果数量。

- 在目标产品列框，可查看从该产品的接收的全部和近一小时接收的结果数量。
- 单击“查看”，可跳转到“全部结果”管理页面，呈现该产品的检测结果列表。更多检测结果说明，请参见**查看全部检测结果**。

图 13-5 查看产品上报数据

----结束

13.3 查看探测状态

“探测状态”是指安全产品数据上报到SA的状态。通过查看探测状态，您可以判断是否正常上报当前产品数据。

表 13-1 探测状态说明

状态	说明
探测正常	表示一个小时内，数据接口被调用次数大于等于8次，接口连通性正常，“探测状态”检测正常，正常上报当前产品数据。 启用产品集成后一个小时内，默认探测状态为正常。
探测异常	表示一个小时内，数据接口被调用次数大于0次小于8次，接口连通性异常，“探测状态”检测异常，不能正常上报当前产品数据。
停止探测	表示已停止上报当前产品数据。
从未探测	表示从未上报当前产品数据。

说明

探测正常状态判断原则：启用产品集成上报数据后，产品可每5分钟调用一次探测接口确认连通性。通过记录产品调用数据接口次数，判断探测健康状态。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知 > 安全产品集成”，进入产品集成管理页面。

图 13-6 产品集成页面

步骤3 选择“区域”。

选择产品所在的区域，可选择“华北-北京一”、“华北-北京四”、“华东-上海二”、“华东-上海一”、“华南-深圳”、“华南-广州”或“西南-贵阳一”。

步骤4 在探测状态中，选择目标状态，即可呈现该状态的全部产品。

步骤5 在产品介绍栏，即可查看从该产品接收的数据量，以及该产品探测状态。

图 13-7 查看产品上报数据

----结束

14 设置

14.1 告警设置

14.1.1 设置告警通知

开启通知告警功能后，如果用户的资产受到了威胁，态势感知将会定时向用户发送提示消息（短信或Email）。

前提条件

已购买态势感知**标准版**或**专业版**，且在有效使用期内。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知页面。

步骤3 在左侧导航栏选择“设置 > 通知设置”，并在设置页面，选择“告警设置 > 通知告警”，进入告警通知设置页面。

图 14-1 告警通知设置页面

步骤4 选择重点关注的通知项目和告警等级。

- 每日告警通知

  每日告警通知会在每天10:00向您发送告警通知消息。

  选择关注的威胁告警和告警等级。只有当“通知项目”和“告警等级”同时有选项被选中时，每日告警通知才能够生效。

- 实时告警通知

  实时告警通知会在威胁告警发生后的整点时刻向您发送告警提示消息。

  选择重点关注的威胁告警和告警等级。只有当“通知项目”和“告警等级”同时有选项被选中时，实时告警通知才能够生效。

  为了避免过多信息打扰您的日常工作，除了全天通知，您还可以选择仅在特定时段发送实时告警通知。在通知时间栏选择“24小时”或指定时间段。

步骤5 选择消息通知主题。

- 通过下拉框选择已有的主题，或者单击“查看消息通知主题”创建新的主题，具体操作请参见**创建主题**。
- 每个消息通知主题可添加多个订阅，并可选择多种订阅终端（例如短信、邮件等），详细订阅说明请参见**添加订阅**。

  说明

  在选择主题前，请确保您主题中订阅状态为“已确认”，即当前订阅终端可用，否则可能不能收到告警通知。

更多关于主题和订阅的信息，请参见《消息通知服务用户指南》。

步骤6 单击“应用”，生效告警通知。

当关注的威胁攻击事件发生后，将收到来自手机短信、邮箱邮件的告警通知。

----结束

14.1.2 设置告警监控

用户可通过告警监控设置想要监控的告警信息，设置后态势感知将仅检测并推送关注的告警信息。

- 目前支持从“告警监控名单”、“告警监控类型和级别”及“监控的告警源”三个维度来设置监控信息。
  - “告警监控名单”支持的格式为IP、IP:端口、IP/掩码或IP-IP，两条信息之间以换行符相隔、不可重复，最多可包含50条。
  - “告警监控类型和级别”支持设置DDoS、暴力破解、Web攻击、后门木马、漏洞攻击、命令与控制、异常行为、僵尸主机八大类告警类型，以及选择设置致命、高危、中危、低危、提示全部类型告警等级。
  - “监控的告警源”支持设置接入的告警源，包括IDS、IPS、DDoS、HSS、WAF等。
- 设置告警监控后，“威胁告警”列表仅呈现同时满足设置条件的告警信息，重点监控关注的威胁告警。告警监控设置仅对新上报的告警生效，不影响历史告警列表的呈现。
- 默认不设置，态势感知将监控对资产所有的端口及IP的攻击，呈现所有资产威胁告警信息。

约束限制

- 需至少选择一类告警类型，每类告警类型下需至少选择一个告警等级，否则告警监控应用无效。
- 需至少选择一种告警源，否则告警监控应用无效。

前提条件

已购买态势感知**专业版**，且在有效使用期内。

操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知页面。

步骤3 在左侧导航栏选择“设置 > 通知设置”，并在设置页面，选择“告警设置 > 告警监控设置”，进入告警监控设置页面。

图 14-2 告警监控设置页面

步骤4 设置告警监控名单。

在“告警监控名单”区域下，单击“设置名单”，弹出“告警监控名单”窗口，导入或手动设置监控名单。

设置告警监控来源名单的方法如下：

1. 导入监控名单。

   单击“添加文件”，选择需要导入的监控名单文件，文件支持txt格式，导入后监控名单会自动呈现在输入框内。

2. 在输入框中输入符合格式的监控名单。

   如图14-3，若设置了22和3389 端口以及IP10.1.1.1，态势感知将只展现来自于这些IP/端口的告警信息。

3. 同步安全组策略。

   单击“同步安全组策略”，可直接将安全组同步到监控名单，同步后监控名单会自动呈现在输入框内。

4. 单击“确定”，完成监控名单的设置。

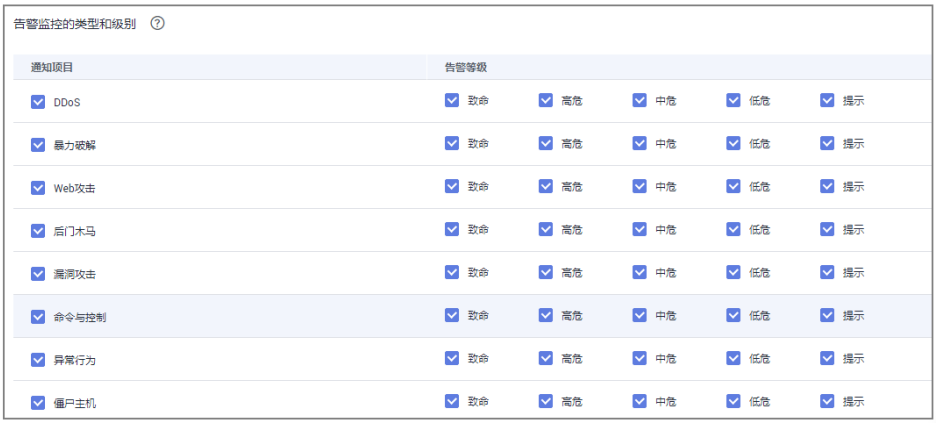
图 14-3 告警监控名单

步骤5 设置告警监控的类型和级别。

在“告警监控的类型和级别”区域下，勾选需监控告警类型的“通知项目”和“告警等级”。未勾选的“通知项目”和“告警等级”，相关告警类型将不会被监控。

设置成功后将仅监控关注类型和等级的告警信息。

图 14-4 选择通知项目和告警等级

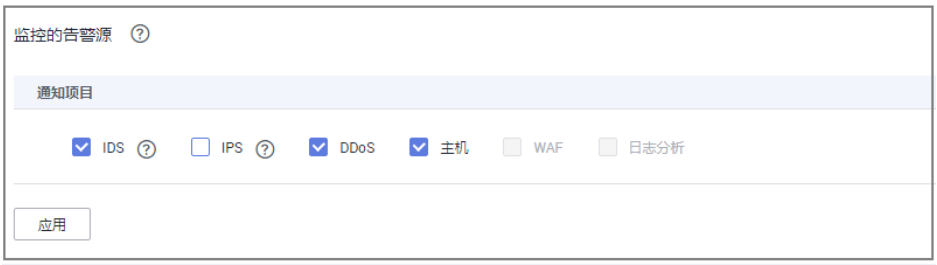


步骤6 设置监控的告警源。

在“监控的告警源”区域下，勾选需监控的告警源的“通知项目”。

设置成功后将仅监控关注来源的告警信息。

图 14-5 选择通知项目



步骤7 单击“应用”，3~5分钟后告警监控配置将生效。

----结束

14.2 授权设置

14.2.1 主机授权

只有经过授权的主机，态势感知才能对其执行漏洞扫描。请在添加主机后，使用此功能对Linux或Windows主机进行授权。

目前Linux主机授权可通过“SSH账号登录”和“授权脚本执行”两种方式，而Windows主机授权通过关联“Windows账号登录”方式。

前提条件

- 已在“漏洞扫描服务 > 资产列表”中完成“添加主机”操作。

操作步骤

步骤1 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知页面。

步骤2 在左侧导航栏选择“设置 > 通知设置”，并在设置页面选择“授权设置 > 主机授权”，进入主机授权设置页面。

图 14-6 主机授权设置页面

步骤3 单击待配置主机“操作”列的“配置授权信息”。

如果需要同时为多个主机授权，请勾选各个主机前的勾选框，单击主机列表上方的“批量配置授权信息”。

步骤4 对Linux和Windows操作系统，分别选择相应授权方式进行主机授权。

- **Linux操作系统：SSH账号登录**
- **Linux操作系统：授权脚本执行**
- **Windows操作系统：Windows账号登录**

步骤5 单击“确定”，完成主机授权。

授权成功后，可在主机授权列表，查看对应主机的已授权信息。

说明

脚本执行授权成功后，在主机授权列表页面，暂时不能显示已授权信息，仅能通过脚本运行结果验证授权成功与否。

----结束

Linux 操作系统：SSH 账号登录

步骤1 在弹出的“配置授权信息”窗口中，选择“方法一：SSH账号登录”。

图 14-7 选择 SSH 账号

步骤2 在下拉框中选择已有的SSH账号。

步骤3 单击“确定”，完成Linux主机授权。

授权成功后，可在主机授权列表，查看对应主机的已授权信息。

说明

- 若无可用SSH账号，需首先创建SSH账号。
  单击“创建SSH账号”，账置SSH账号信息，具体参数说明参考表14-1。设置完成后，单击“确认”，即可使用该账号对主机授权。
- 若需要修改已有SSH账号，单击“编辑”，修改账号信息。
- 若需要删除已有SSH账号，单击“删除”，删除账号。

图 14-8 账建 SSH 账号信息

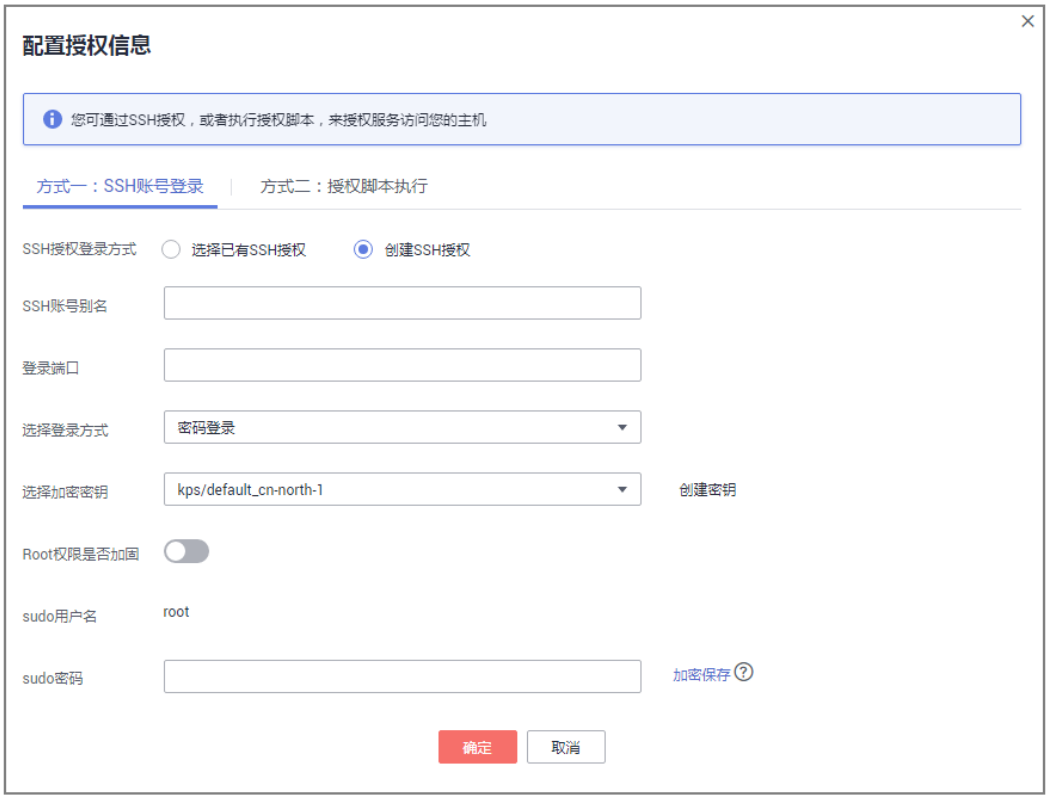


表 14-1 参数说明

参数名称	参数说明
SSH账号别名	自定义SSH账号名称。
登录端口	SSH账号登录的端口号。
选择登录方式	选择登录方式。可选择：“密码登录”或“密钥登录”。 选择“密钥登录”时，需要“创建私钥”。
选择加密密钥	选择已有的加密密钥，或者单击“创建密钥”，创建新的密钥，具体方法请参考创建密钥。
Root权限是否加固	打开该权限后，不可以用root账号直接登录，而是只能通过普通用户登录，然后才能切换到root用户。
sudo用户名	默认为root。

参数名称	参数说明
sudo密码	设置sudo用户对应的密码，单击“加密保存”，对密码进行加密保存。

----结束

Linux 操作系统：授权脚本执行

步骤1 在弹出的“配置授权信息”窗口中，选择“方法二：授权脚本执行”。

步骤2 单击右侧的“复制”，复制开通授权的命令。

步骤3 使用远程管理工具（例如：“Xshell”、“SecureCRT”、“PuTTY”），通过弹性IP地址登录到待开通授权的弹性云服务器。

也可使用弹性云服务器的“远程登录”功能，登录弹性云服务器。

步骤4 执行复制的命令（这里用“SecureCRT”工具登录）。

提示“Install Success”时则执行成功，完成Linux主机授权。

说明

脚本执行授权成功后，在主机授权列表页面，暂时不能显示已授权信息，仅能通过脚本运行结果验证授权成功与否。

```
# curl -O -s http://XX.XX.XX.XX/southchina-vss-hostscan/vss_hostscan_427c_install.sh && bash
vss_hostscan_427c_install.sh --start
[INFO] Uninstall Success
[INFO] Create vss_hostscan_55e9 account
[INFO] Grant sudo privileges for vss_hostscan_55e9
[INFO] Inject SSH Public Key
[INFO] Install Success
```

----结束

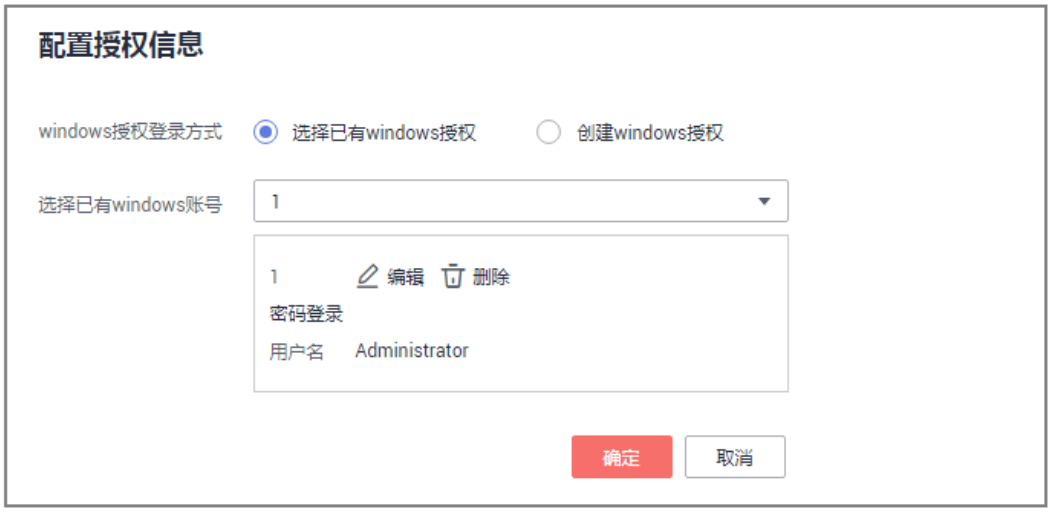
Windows 操作系统：Windows 账号登录

步骤1 在弹出的对话框中，选择已有Windows账号。

步骤2 单击“确定”，完成Windows主机授权。

授权成功后，可在主机授权列表，查看对应主机的已授权信息。

图 14-9 配置授权信息



说明

- 若无可用Windows账号，需首先创建Windows账号。
  单击“创建Windows账号”，配置Windows账号信息，具体参数说明参考**表14-2**。设置完成后，单击“确认”，账可使用该账号对主机授权。
- 如果需要修改已有Windows账号，单击“编辑”，修改号信息。
- 如果需要删除已有Windows账号，单击“删除”，删除账号。

图 14-10 创建 Windows 账号

表 14-2 参数说明

参数名称	参数说明
Windows账号别称	自定义Windows账号名称。
选择加密密钥	选择已有的加密密钥，或者单击“创建密钥”，创建新的密钥，具体方法请参考**创建密钥**。
用户名	默认为Administrator。
密码	Windows系统登录密码。
账号域	查看该Windows系统的账号域并填写到此处，该参数也可以为空，不填写。

----结束

14.3 启动主机扫描任务

在对主机授权后，可以参考此章节启动主机漏洞扫描和主机基线扫描任务。

前提条件

- 已购买态势感知**专业版**，且在有效使用期内。
- 已在“漏洞管理服务 > 资产列表”中完成“添加主机”操作。
- 已在“态势感知 > 设置 > 通知设置 > 授权设置 > 主机授权”中对主机完成授权。

  说明

  为了确保扫描成功，在开启主机扫描前，请先完成以下操作。

  1. 完成**主机授权**。
  2. 如果主机所在的安全组设置了对漏洞管理服务（CodeArts Inspector）的访问限制，请参见**如何解决主机不能访问**添加策略允许CodeArts Inspector的IP网段访问您的主机。
  3. 如果用户同时使用了**主机安全服务**，参见**配置SSH登录IP白名单**将您的主机IP配置为白名单。否则，主机IP会被当成不信任IP被**主机安全服务**拦截，造成扫描任务失败。

背景信息

在使用态势感知的**主机漏洞扫描**功能时，请参考如下使用流程：

1. 添加主机：请在“漏洞管理服务 > 资产列表”中完成。
2. 主机授权：请在“态势感知 > 设置 > 通知设置 > 授权设置 > 主机授权”中完成。
3. **启动扫描任务**：请在“态势感知 > 设置 > 通知设置 > 扫描任务”中执行。请参考本章节执行。
4. 查看主机漏洞扫描结果：请在“态势感知 > 漏洞管理 > 主机漏洞”中查看。
5. 查看主机基线数据：请在“态势感知 > 检测结果”中查看。

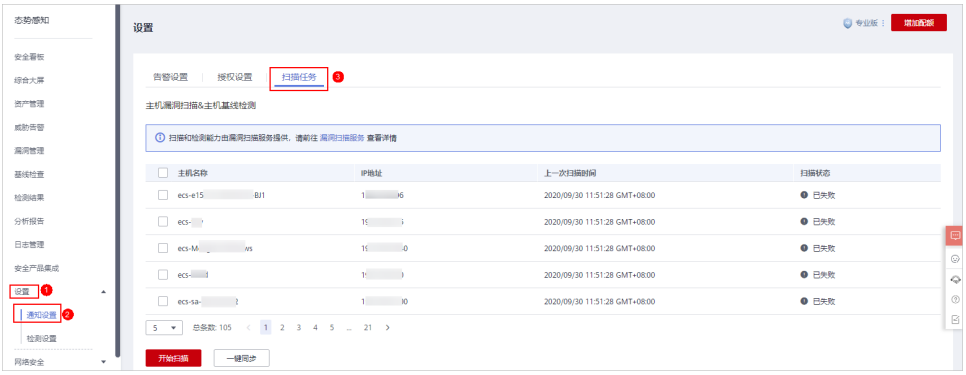
操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知页面。

步骤3 在左侧导航栏选择“设置 > 通知设置”，并在设置页面选择“扫描任务”页签，进入扫描任务设置页面。

图 14-11 扫描任务设置页面



步骤4 在“主机漏洞扫描&主机基线扫描”栏下，单击“一键同步”，同步当前账号下的弹性服务器IP信息，刷新“IP地址”列表。

步骤5 在“主机漏洞扫描&主机基线扫描”栏下，选择需要执行扫描的主机，单击“开始扫描”，启动扫描任务。

“扫描状态”为“已完成”时，可在“态势感知 > 漏洞管理 > 主机漏洞”和“态势感知 > 检测结果”查看详细扫描结果。

----结束

14.4 检测设置

使用云服务基线相关功能时，需要先参考本章节设置检查计划。

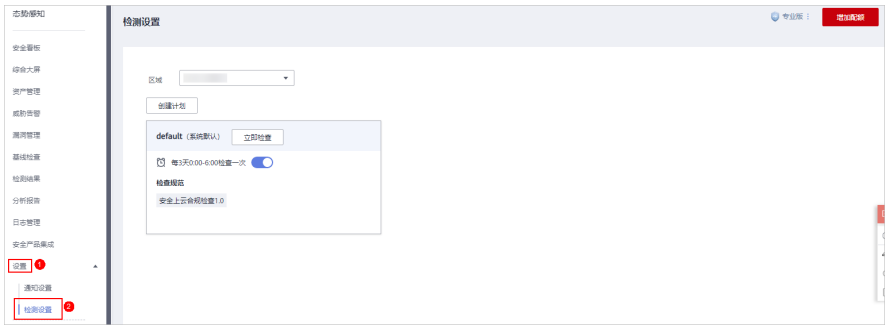
操作步骤

步骤1 登录管理控制台。

步骤2 在页面左上角单击 ☰，选择“安全与合规 > 态势感知”，进入态势感知页面。

步骤3 在左侧导航栏选择“设置 > 检测设置”，进入检测设置页面。

图 14-12 检测设置



步骤4 在检测设置页面中，选择待创建计划所在的区域，并单击“创建计划”，系统右侧弹出新建检查计划页面。

图 14-13 创建检查计划

步骤5 配置检查计划。

1. 填写基本信息，具体参数配置如**表14-3**所示。

表 14-3 检查计划基本信息

参数名称	参数说明
计划名称	自定义检查计划的名称。
检查时间	选择检测周期和检查触发时间。 – 检测周期：每隔1天、3天、7天、15天、30天检查一次 – 检查触发时间：00:00~06:00、06:00~12:00、12:00~18:00、18:00~24:00

2. 选择检查规范。

   选择需要检测的基线检查项目。更多关于基线检查项目详细描述请参见**云服务基线简介**。

3. 单击“确定”。

步骤6 检查计划创建完成。

SA会在指定的时间执行云服务基线扫描，扫描结果可以在“安全与合规 > 态势感知 > 基线检查”中查看。

----结束

