ALIBABA CLOUD

阿里云

安全管家

用户指南

文档版本：20220420

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.Mssp服务关联角色

本文为您介绍安全管家服务关联角色（AliyunServiceRoleForMssp）的应用场景以及如何删除服务关联角色。

背景信息

安全管家服务关联角色AliyunServiceRoleForMssp是安全管家在日常运营的情况下，为了帮助用户完成安全加固服务和安全评估服务，需要获取其他云服务的访问权限而提供的RAM角色，无需您主动创建或做任何修改。更多服务关联角色的信息请参见服务关联角色。

AliyunServiceRoleForMssp应用场景

安全管家需要访问您的云服务器ECS、云安全中心、对象存储OSS、云数据库RDS、漏洞扫描、企业级分布式应用服务EDAS、负载均衡、访问控制的资源进行安全加固和安全评估，用以完成安全管家的运营服务。

AliyunServiceRoleForMssp介绍

角色名称：AliyunServiceRoleForMssp

角色权限策略：AliyunServiceRolePolicyForMssp

权限说明：

> **说明**
>
> 以下权限说明为系统默认提供的策略，不支持修改。

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeInvocationResults",
        "ecs:DescribeCloudAssistantStatus",
        "ecs:RunCommand",
        "ecs:RebootInstance",
        "ecs:DescribeInstances",
        "ecs:DescribeSnapshots",
        "ecs:InstallCloudAssistant",
        "ecs:DescribeRegions",
        "ecs:AssumeRole",
        "ecs:CreateSecurityGroup",
        "ecs:AuthorizeSecurityGroup",
        "ecs:AuthorizeSecurityGroupEgress",
        "ecs:RevokeSecurityGroup",
        "ecs:RevokeSecurityGroupEgress",
        "ecs:DeleteSecurityGroup",
        "ecs:DescribeSecurityGroupAttribute",
        "ecs:DescribeSecurityGroups",
        "ecs:DescribeSecurityGroupReferences",
        "ecs:DescribeDisks",
        "ecs:CreateSnapshot",
```

```
        "ecs:DeleteSnapshot",
        "ecs:ModifyOperateVul",
        "ecs:DescribeVpcs",
        "ecs:JoinSecurityGroup",
        "ecs:LeaveSecurityGroup"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "yundun-waf:CreateProtectionModuleRule",
        "yundun-waf:ModifyProtectionModuleRule",
        "yundun-waf:ModifyProtectionRuleStatus",
        "yundun-waf:DeleteProtectionModuleRule",
        "yundun-waf:Describe*",
        "yundun-waf:Get*",
        "yundun-waf:List*",
        "yundun-waf:Query*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "eip:DescribeEipAddresses",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "rds:DescribeDBInstances",
        "rds:DescribeDBInstanceAttribute",
        "rds:DescribeDBInstanceNetInfo",
        "rds:ModifySecurityIps",
        "rds:DescribeDBInstanceIPArrayList"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "oss:ListBuckets",
        "oss:getBucketInfo",
        "oss:setBucketAcl",
        "oss:getBucketAcl",
        "oss:getBucketTagging",
        "oss:SetBucketTagging"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "slb:ListResourceGroups",
        "slb:DescribeHealthStatus"
```

```
        "slb:DescribeHealthStatus",
        "slb:DescribeLoadBalancers",
        "slb:DescribeLoadBalancerAttribute",
        "slb:SetLoadBalancerStatus",
        "slb:CreateAccessControlList",
        "slb:DeleteAccessControlList",
        "slb:DescribeAccessControlLists",
        "slb:DescribeAccessControlListAttribute",
        "slb:AddAccessControlListEntry",
        "slb:RemoveAccessControlListEntry",
        "slb:DeleteLoadBalancerListener",
        "slb:StartLoadBalancerListener",
        "slb:StopLoadBalancerListener",
        "slb:DescribeLoadBalancerTCPListenerAttribute",
        "slb:DescribeLoadBalancerUDPListenerAttribute",
        "slb:DescribeLoadBalancerHTTPListenerAttribute",
        "slb:DescribeLoadBalancerHTTPSListenerAttribute",
        "slb:SetLoadBalancerUDPListenerAttribute",
        "slb:SetLoadBalancerTCPListenerAttribute",
        "slb:SetLoadBalancerHTTPListenerAttribute",
        "slb:SetLoadBalancerHTTPSListenerAttribute"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "yundun-sas:ModifyCreateVulWhitelist",
        "yundun-sas:ModifyOperateVul"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "avds:AddAssets",
        "avds:DeleteAssets",
        "avds:DescribeAssets",
        "avds:CreateScan",
        "avds:DescribeAllVulnerabilities",
        "avds:GenerateVulReport",
        "avds:DescribeScanSessions",
        "avds:DescribeVulnerability"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "edas:ListVpc",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": [
            "mssp.aliyuncs.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "yundun-cloudfirewall:Get*",
        "yundun-cloudfirewall:Describe*",
        "yundun-cloudfirewall:Query*",
        "yundun-cloudfirewall:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "yundun-high:Get*",
        "yundun-high:Describe*",
        "yundun-high:Query*",
        "yundun-high:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "log:GetConfig",
        "log:GetIndex",
        "log:GetCursor",
        "log:GetCursorTime",
        "log:GetLogStore",
        "log:GetProject",
        "log:GetSavedSearch",
        "log:ListSavedsearch",
        "log:GetSlsService",
        "log:GetAlert",
        "log:ListAlert",
        "log:GetLogs",
        "log:GetHistograms",
        "log:GetLogging",
        "log:GetLogStoreLogs",
        "log:GetProjectLogs",
        "log:ListLogStores",
        "log:ListProject",
        "log:ListConfig",
        "log:ListDomains"
      ],
      "Resource": [
        "acs:log:*:*:project/sas-log-*/logstore/*",
```

```
        "acs:log:*:*:project/waf-project-*/logstore/*",
        "acs:log:*:*:project/cloudfirewall-project-*/logstore/*",
        "acs:log:*:*:project/ddoscoo-project-*/logstore/*",
        "acs:log:*:*:project/aegis-log-*/logstore/*",
        "acs:log:*:*:project/*/logstore/actintrail_*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "yundun-aegis:Get*",
        "yundun-aegis:Describe*",
        "yundun-aegis:Query*",
        "yundun-aegis:List*",
        "yundun-sas:Get*",
        "yundun-sas:Describe*",
        "yundun-sas:Query*",
        "yundun-sas:ModifyStartVulScan",
        "yundun-aegis:ModifyStartVulScan",
        "yundun-sas:List*"
      ],
      "Resource": "*"
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "mssp.aliyuncs.com"
        }
      }
    }
  ]
}
```

删除服务关联角色

在安全管家的服务有效期之内要协助您完成云上的安全运营工作，暂不支持删除服务关联角色，在服务到期之后您可以自行删除。

删除服务关联角色具体操作请参见删除服务关联角色。

2.服务流程

介绍安全管家服务流程。

安全管家服务流程：

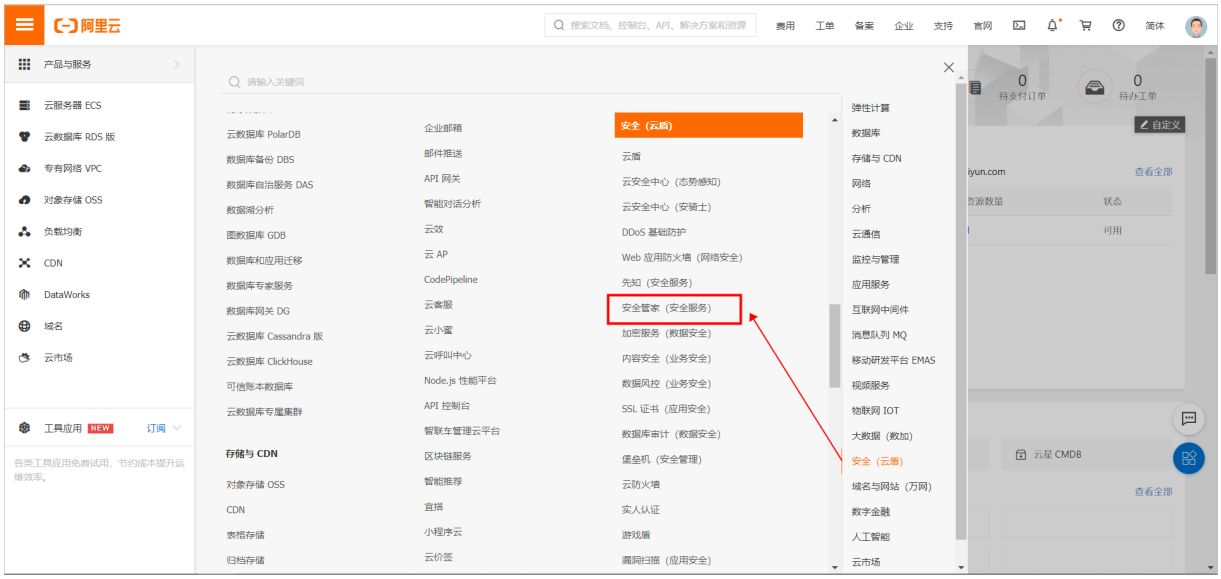
3.安全管家控制台使用手册

本文档用于介绍安全管家控制台的使用方法。

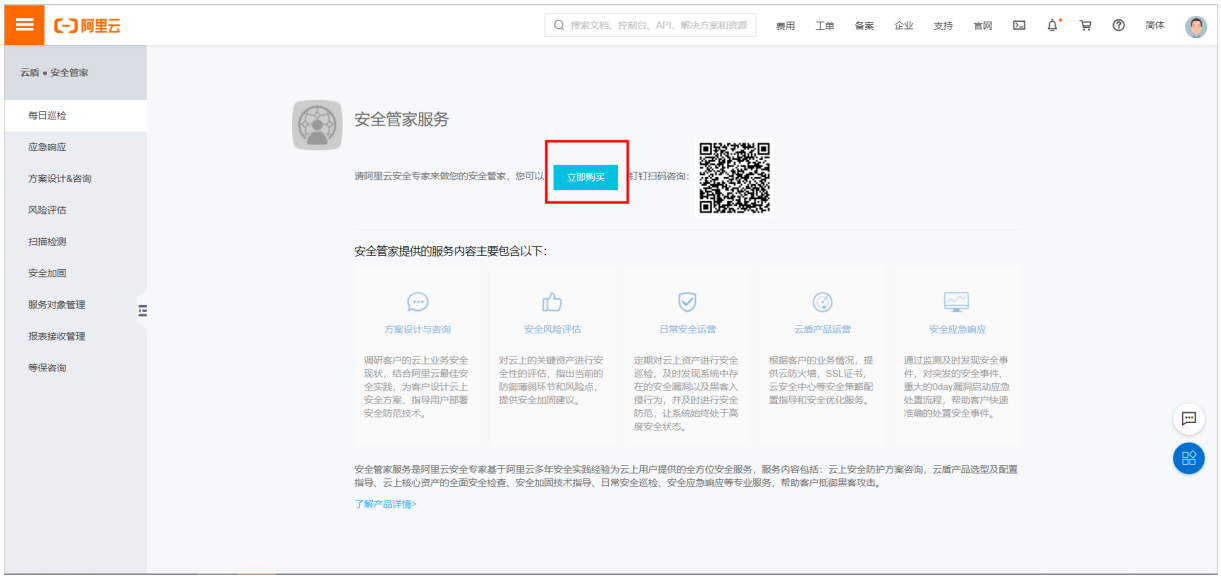
登录安全管家控制台

方法一：在购买成功的页面单击**管理控制台**按钮，快速打开控制台。

方法二：在阿里云控制台中，通过搜索找到并单击**安全管家**进入管家控制台首页。



方法三：未购买务情况下登录安全管家服务控制台时，通过控制台首页上的**立即购买**前往下单。



方法四：通过产品官网详情页面单击**管理控制台**进入。

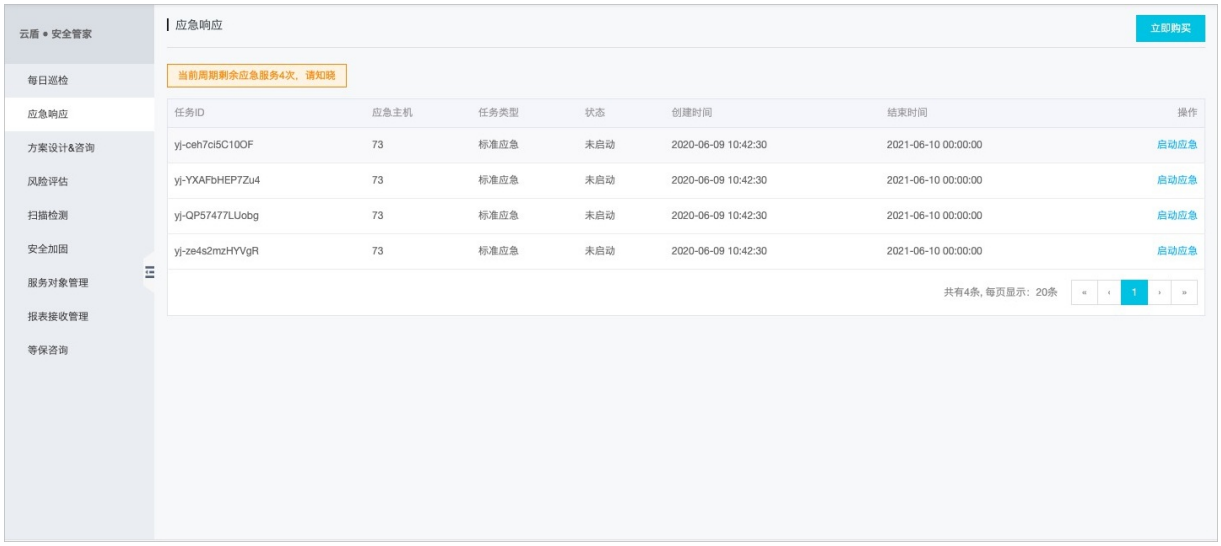
每日巡检

进入控制台后，显示管家每日巡检的日报页面。

- 显示当天和近七天的日报，可通过单击操作列的**下载日报**来获取日报的详细内容。
- 正常情况下，当天的日报会在当日下午6点之前发出，如果提示**下载失败**，请稍后重试。
- 新用户下单之后，日报需在下单后的第二个工作日提供。

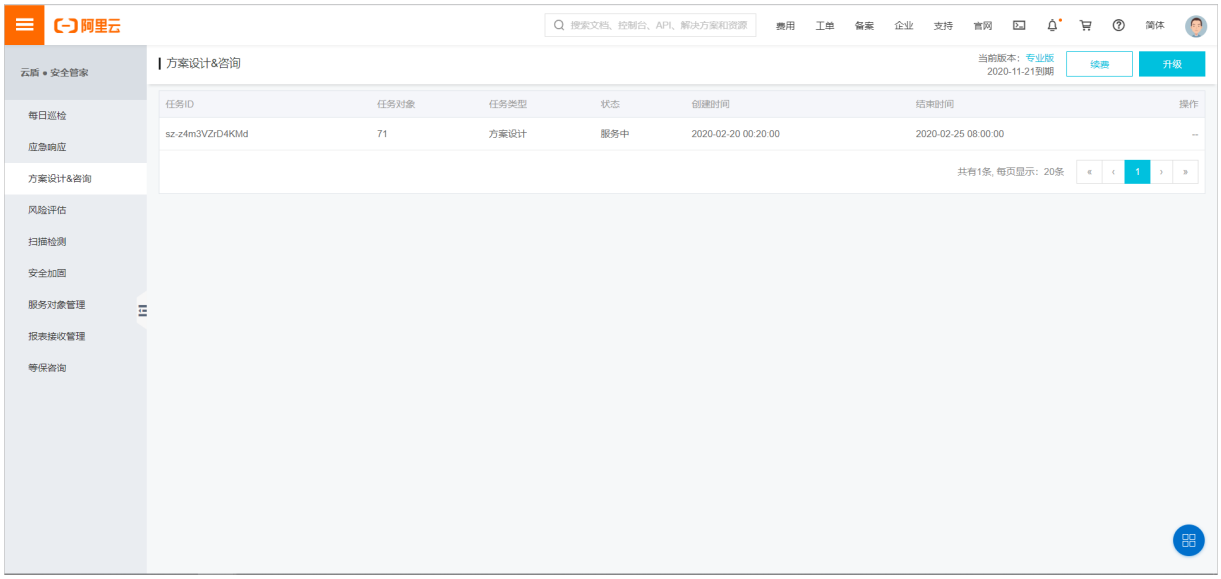
应急响应

根据安全管家的服务内容，每年提供4次安全事件的应急响应服务，当出现安全事件的时候客户可以主动单击**启动应急**来启动应急响应服务，如果时间紧急的情况下交付人员会在和客户确认情况之后直接启动应急响应，缩短处理时间降低对业务的影响。



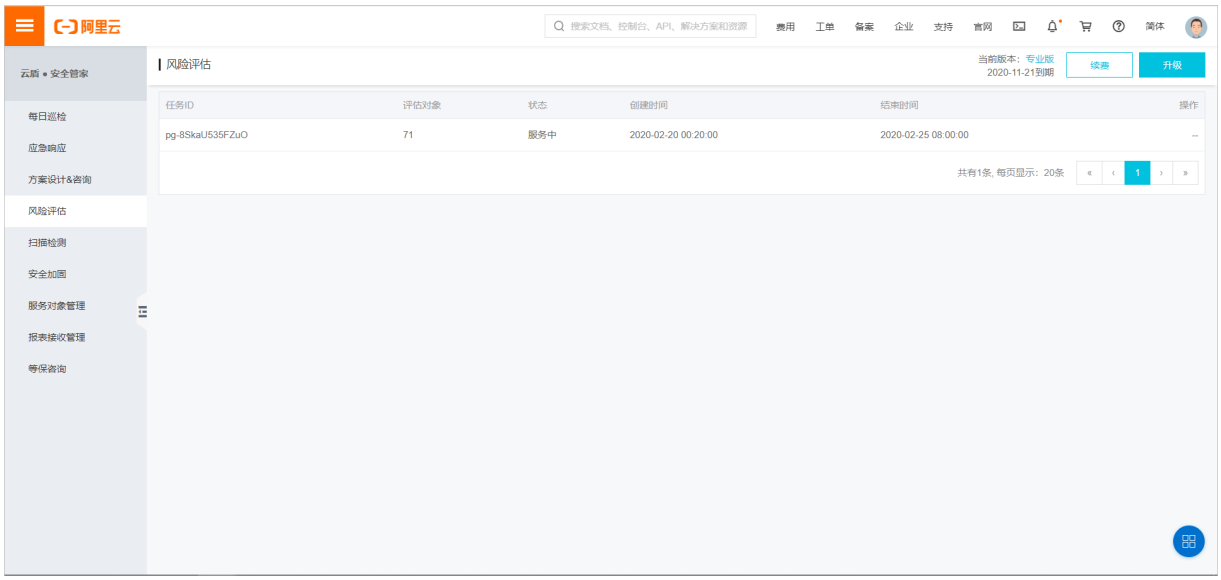
方案设计&咨询

根据安全管家的服务内容，每年提供1次安全运营方案设计服务和服务周期内的不限次数的咨询服务，已购买管家服务后方案设计&咨询模块中的状态会调整为在服务中，运营方案可通过钉钉服务群发送给客户。



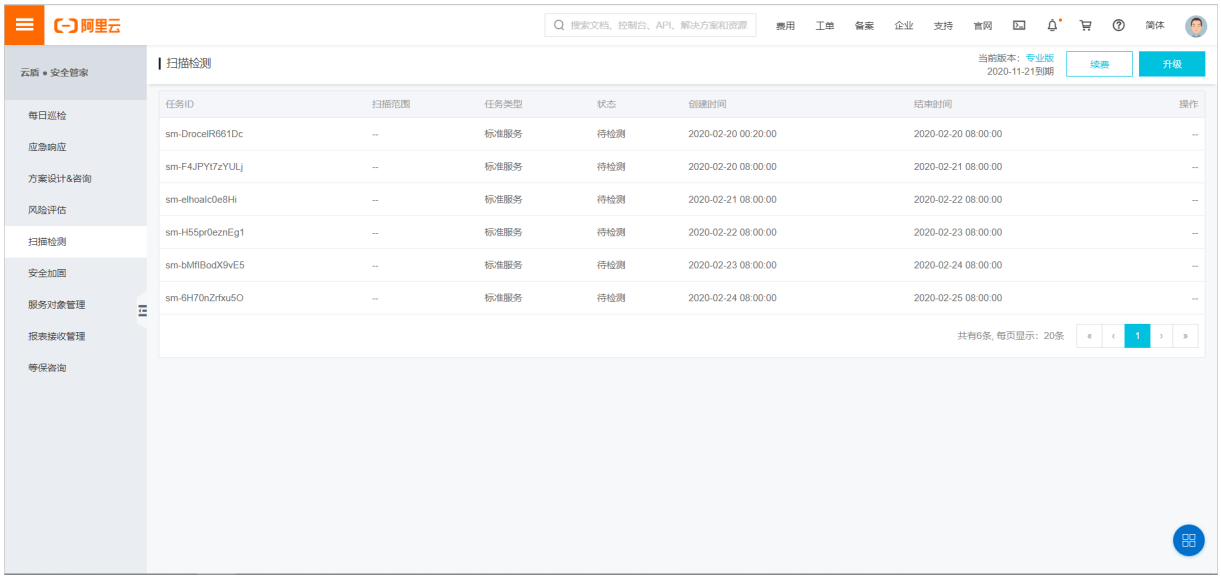
风险评估

根据安全管家的服务内容，每年提供1次云上整体的风险评估服务，目前安全管家能力提升中，如果需要增加风险评估次数可以与负责钉钉服务群的交付人员说明。已购买管家服务后风险评估模块中的状态会调整为在服务中，服务的交付报告将通过钉钉服务群发送给客户。



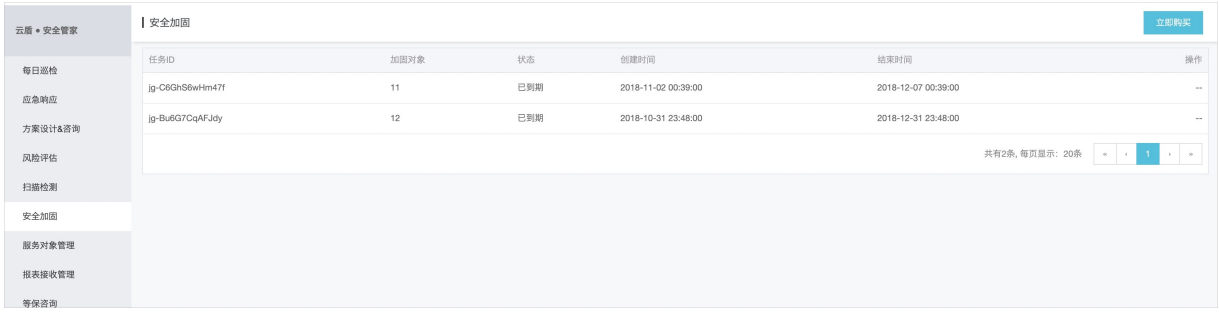
扫描检测

根据安全管家的服务内容，每季度为客户提供1次漏洞扫描检测服务，具体的扫描时间及扫描范围服务同学会通过钉钉服务群与客户沟通确认，最终的交付结果将通过钉钉服务群发送给客户。



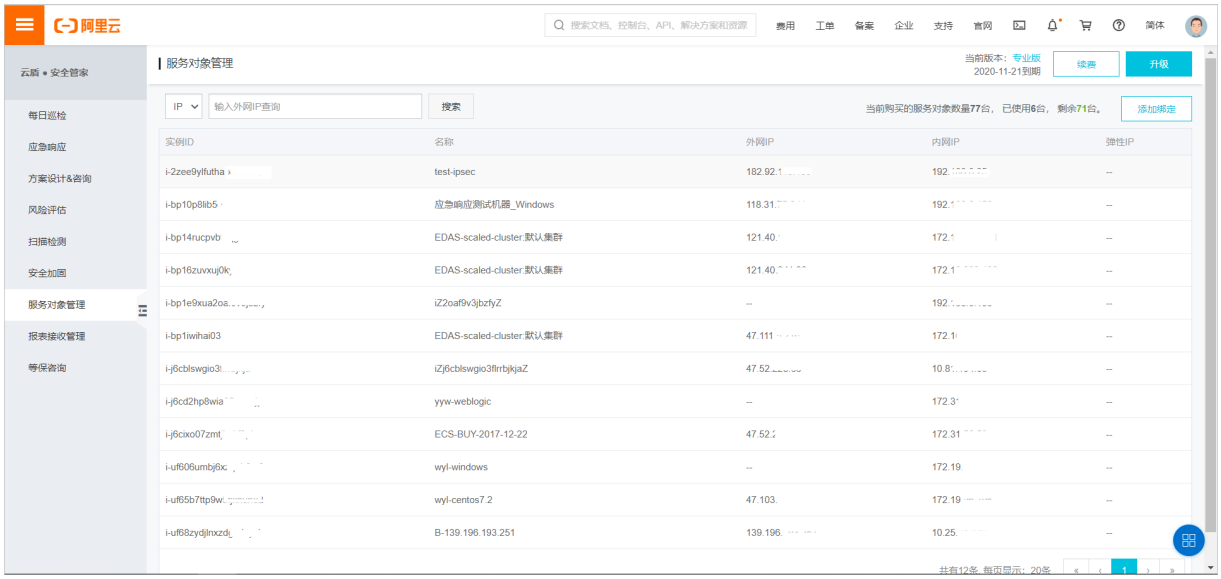
安全加固

根据安全管家的服务内容，每年提供1次安全加固服务，目前安全管家能力提升中，如果需要增加安全加固次数可以与交付人员说明。服务默认下单后开始状态为服务中，服务的交付报告将通过钉钉服务群发送给客户。

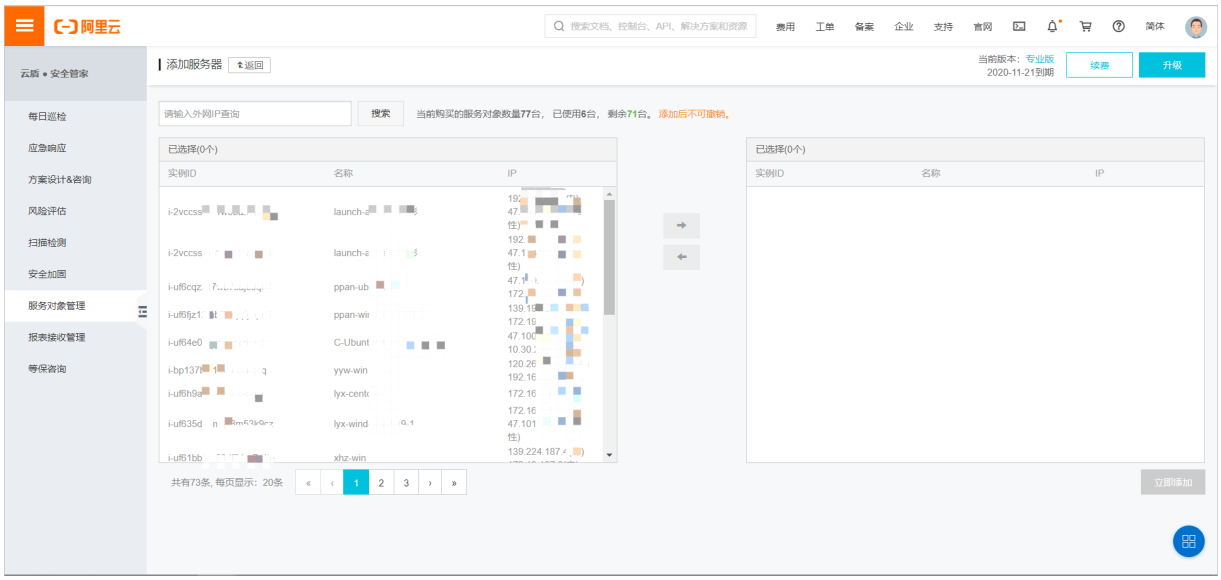


服务对象管理

用户可将所有的需要防护的资产实例信息添加进来，便于查看被服务信息。为了防止购买与绑定存在时间差或者意外遗忘等情况，安全管家会默认服务于客户已购买的设备实例。

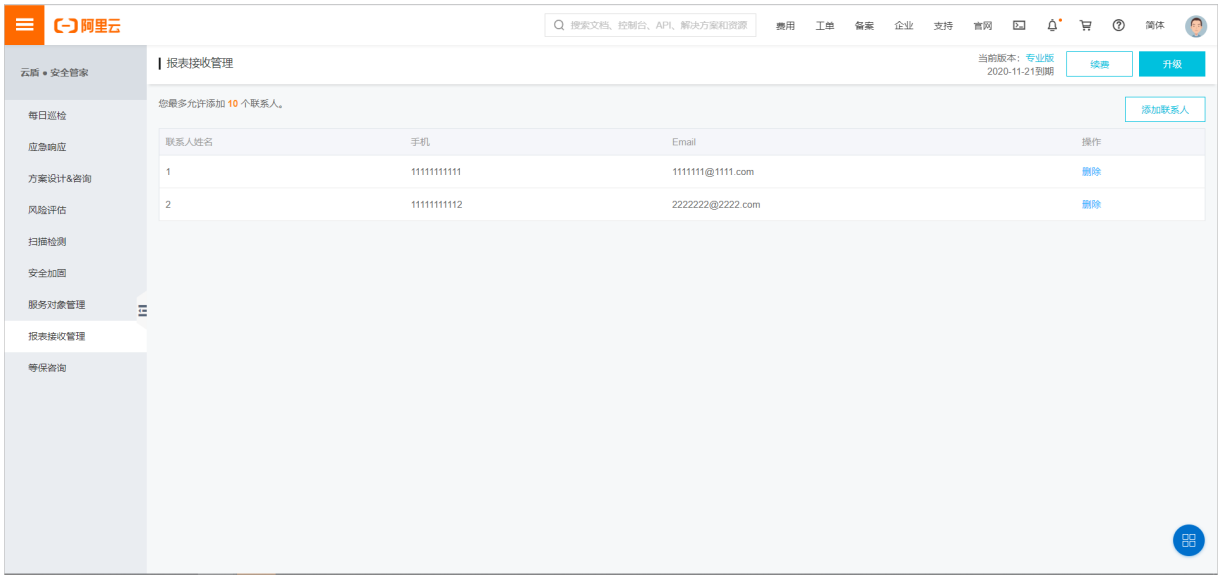


用户可通过单击**添加绑定**按钮添加购买的实例。



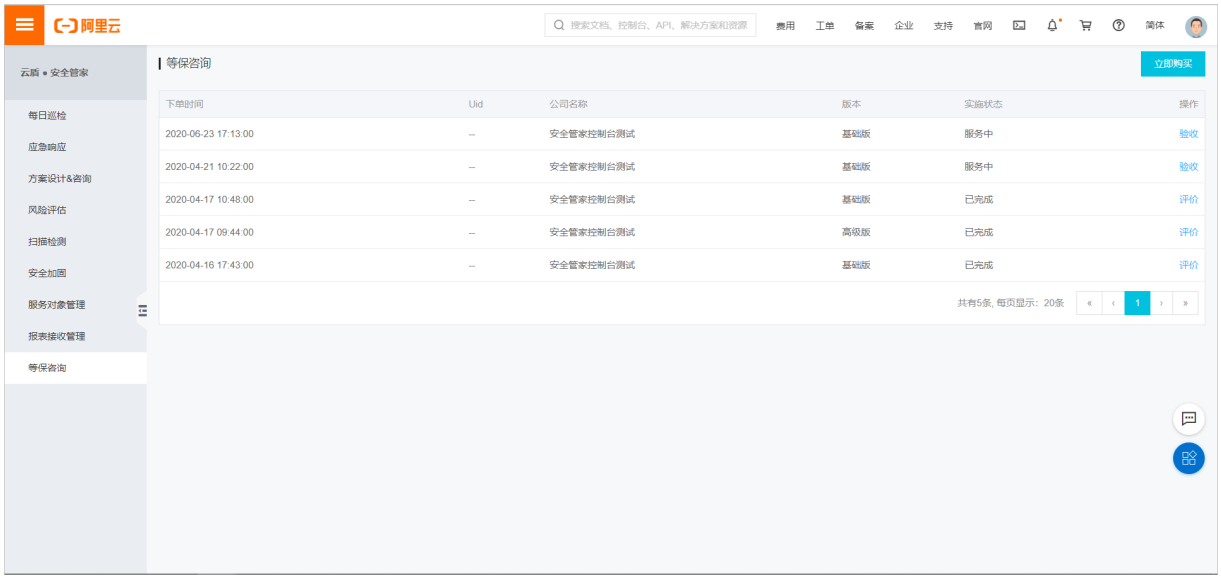
报表接收管理

用户可添加或删除联系人，联系人用于在发生安全事件时交付人员可以通过电话与相应负责人取得联系，邮箱用于接收每日安全巡检的日报。

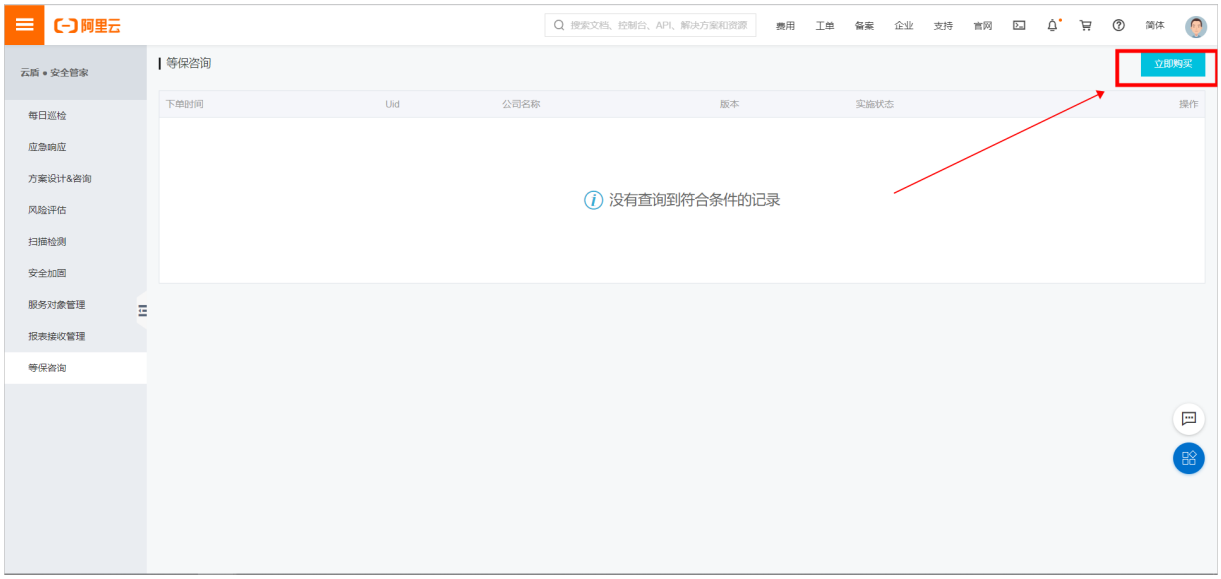


等保咨询

当用户购买了等保咨询服务，可以在这里进行查看和验收。



没有购买等保咨询服务的用户，可以通过单击**立即购买**跳转去购买服务。


阿里云
费用
工单
备案
企业
支持
官网
简体
云盾 • 安全管家
每日巡检
应急响应
方案设计&咨询
风险评估
扫描检测
安全加固
服务对象管理
报表接收管理
等保咨询
等保咨询
立即购买
下单时间
Uid
公司名称
版本
实施状态
操作
没有查询到符合条件的记录