云盾 2.0 控制台帮助手册

1. 阿里云控制台云盾入口

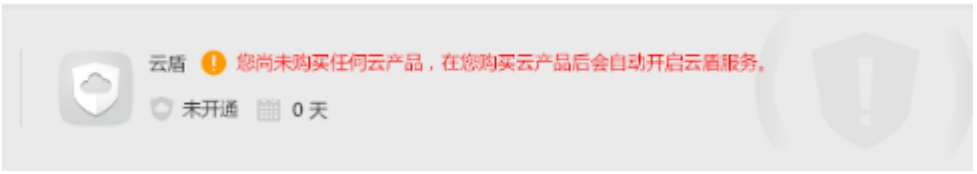
用户通过阿里云控制台 http://home.console.aliyun.com/ 进入到云盾控制台

没有攻击或异常的情况（安全）

- 用户点击查看安全周报，进入安全周报的详情页面
- 其中右侧 41 ,762 次是统计当前用户所有云服务器当天收到 DDoS+密码暴力破解 +Web 攻击次数
- 207 天显示的是用户自购买 ECS 当天起云盾防护的天数

有攻击或异常的情况（异常）

用户没有购买云产品的情况

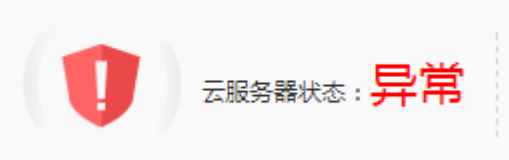


2. 云盾控制台首页

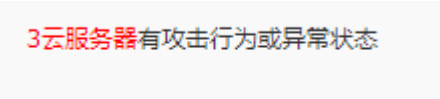
- 显示用户所有 ECS,SLB 实例列表 ,以 TAB 切换的方式展示不同类型实例的列表

安全概述

- 显示用户当前所有云服务器的安全状况，异常/安全



- 当用户的云服务器有攻击（DDoS 攻击，密码暴力破解，Web 攻击）或者有异常的情况(检测出后门，异地登录，存在 Web 漏洞)会显示异常

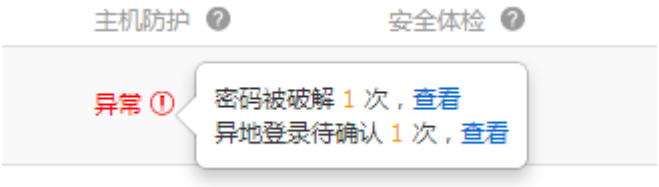


- 没有攻击或者异常的情况，会显示安全的状态
- 会提示用户当前有几台云服务器有异常问题
- 提示用户当前出现不同问题分类的云服务器台数，点击不同的分类会显示出现问题的云服务器列表，点击返回按钮可以返回到全部实例列表
- 每个不同问题分类显示出现攻击或者异常事件的总数，如 DDoS 攻击 100 次，数据统计周期为一天，拦截密码破解（7 天） 3 次，3 台云服务器出现密码破解，为 7 天内有 3 台云服务器出现 3 次拦截密码破解攻击

实例列表

- 显示某一类型的所有实例列表，显示每个实例的 IP 地址，实例名称，节点位置，DDoS 防护，主机防护，安全体检的异常信息，操作区显示查看监控报表和安全设置

- 用户可以通过点击 DDoS 防护，主机防护，安全体检项目查看每个防护项的异常数据



- 用户点击 IP 地址链接和查看监控报表进入某一个实例的实例详情页(DDoS 防护报表)，点击安全设置链接进入某一个实例的安全设置详情页

批量安全设置

用户在实例列表中选择多个实例后，点击列表下方的安全设置按钮可对多个实例进行安全设置

搜索实例

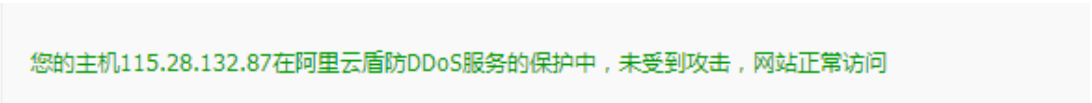
用户通过实例名称和云服务器 IP 可以进行精准搜索

3. 实例详情页

用户可以进入每个实例的详情页查看每项防护的监控报表和安全设置

DDoS 防护

- 用户可以通过 DDoS 防护页面查看一天内的 DDoS 防护情况
- 当用户没有 DDoS 攻击的时候显示



- 用户可以通过查看流量和报文速率两种类型的防护报表

主机防护

用户可以通过查看主机防护报表查看不同主机入侵防护类型的报表

- 攻击数据总览

  用户可以通过防护总览来查看每种防护类型的数据统计，如

检测出异地登录次数 1 次

- 密码破解拦截，异地登录，Web 攻击拦截的防护数据统计周期为 7 天内，后门检测为用户所有的后门数据
- 密码破解拦截

  用户可以查看攻击源 IP 的信息，攻击的时间，拦截状态（被破解/已拦截），拦截次数，同时可以进行删除该条记录的操作

- 后门检测

  用户可以查看后门的地址，检测出来的时间，后门的状态（待处理，已删除，已忽略），同时可以进行筛选，用户可以对后门进行删除，恢复，忽略三种操作
- 异地登录

  用户可以查看异地登录的信息，登录的地点，IP 地址，异地登录的时间，状态（已确认，待确认），同时可以进行筛选，用户可以确认某条异地登录信息为本人操作，同时可以取消确认操作

- Web 攻击拦截

用户可以查看某个实例下被保护的网站数量，拦截的 Web 攻击次数

用户可以添加，删除某个实例下被保护的网站域名

Web 攻击的类型包括：

sql 注入 XSS 跨站 文件包含 webshell 远程代码执行 服务器信息窃取 其他

安全体检

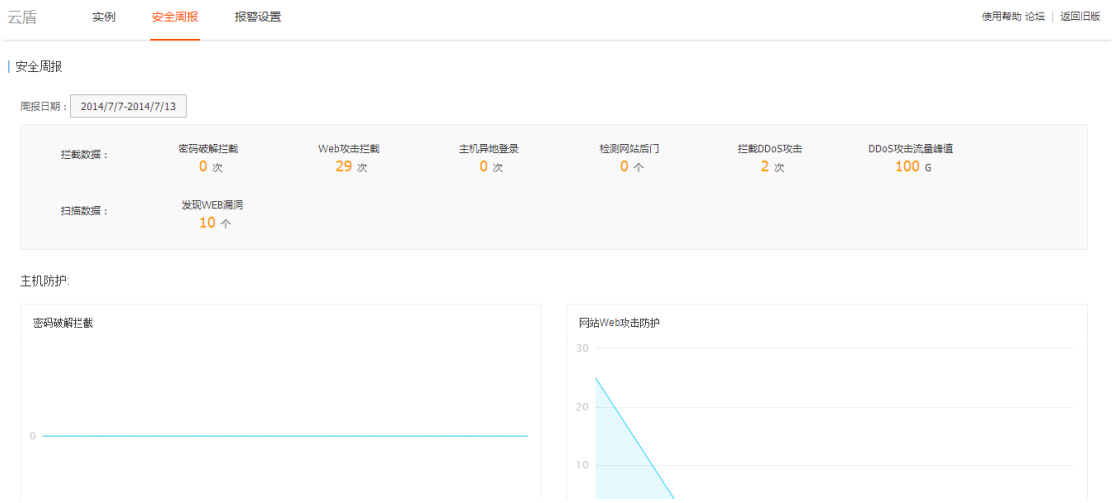
- 端口安全
  - 用户可以查看某个实例下的端口状态，查看每个端口，对应的服务，端口的状态（开启，关闭），同时可以进行停止检测，立即检测端口的操作
  - 查看端口列表数据的周期为 3 天
- Web 漏洞
  - 用户可以查看某个实例下的 Web 漏洞数据，每个漏洞的 URL,漏洞的类型，漏洞参数，状态（未修复/已修复），同时用户可以进行立即检测和查看详情的操作

安全设置

用户可以通过安全设置详情页对某一个实例进行安全设置，包括

- DDoS 防护设置
- 主机防护设置
- 安全体检设置

4. 安全周报



用户可以通过安全周报查看该用户下所有云服务器，一周内的安全状况数据报表，包括密码破解拦截，网站 Web 攻击防护，网站后门入侵防护，异地登录提醒，DDoS 防护，Web 漏洞体检

5. 报警设置

- 用户可以设置短信提醒设置和邮件提醒设置，针对密码破解拦截，DDoS 防护，端口安全检测，异地登录提醒，Web 漏洞检测，网站后门检测服务选择开启，关闭提醒服务
- 用户可以自行选择仅 10：00-20：00 接收提醒或者 24 小时内接受提醒

6. 其他

用户可以通过控制台右上角的“使用帮助”，“论坛”，“返回旧版”跳转到对应的页面，其中“返回旧版”返回到之前的云盾 1.0 控制台