目录

概况

概况界面是服务器安全的信息展示处理中心，实时展示您的主机安全情况、待处理风险、风险趋势以及主机资产的动态走势。

概览

概览条目展示了您当前购买的产品版本及授权数量，以及升配和续费入口。

服务器安全整体统计

从主机总数、待处理入侵事件、待处理高危漏洞、已开启安全监控主机台数四个维度展示了服务器安全的整体概况。

主机总数

主机总数统计了您已安装Agent的主机总数，和当前在线的主机数。

待处理入侵事件

待处理入侵事件为您展示了当前待处理入侵事件的数量，以及今日增减数量。点击该展示卡，页面将跳转至**入侵概览**页。

待处理高危漏洞

待处理高危漏洞为您展示了当前待处理高危漏洞的数量，以及今日增减数量。点击该展示卡，页面将跳转至**风险概览**页。

已开启安全监控主机

已开启安全监控主机为您当时了当前已开启安全监控的主机个数。

系统漏洞发现及处置趋势

系统漏洞发现趋势及处置趋势通过折线图，为您展示近7天、近30天、近1年内的系统漏洞发生及处置情况，并且支持按时间范围进行查看。将鼠标在趋势图中悬停，将显示该日期漏洞发现和处置总数。

易受攻击主机

统计了检出漏洞最多的前7台主机，点击主机页面将跳转至系统漏洞详情页。

主机数量变更分析

统计了当前在线主机数和今日新增主机数，同时提供了本周、本月、全年主机数量随时间变化的趋势图，并且支持按时间范围进行查看，将鼠标在趋势图中悬停，将显示该日期主机总数。

30天内各资产数量变更分析

统计了各类资产在30天内的变更情况，点击资产类别，下方资产数量走势图也随之切换。将鼠标在走势图中悬停，将显示该日期该类资产数量。

主机资产

统计了当前主机总数、在线主机数和离线主机数，同时提供了主机总数、在线主机随时间变化的趋势图，将鼠标在趋势图中悬停，将显示该日期主机总数和在线主机数。

主机操作系统分布

从Linux，Windows操作系统维度，统计了各版本系统占操作系统类别的比重。展示了各子类操作系统的占比和台数。

安全体检

服务器安全的安全体检功能可以为您的主机提供安全体检评分。您可主动发起主机深度检测，检测的项目包括：系统漏洞、弱口令、高危账号、配置缺陷、病毒木马、网页后门、反弹shell、异常账号、日志删除、异常进程、系统命令篡改等。安全体检检测出的问题系统自动进行问题归类到漏洞风险及入侵威胁模块中。

建议您Agent安装后立即执行首次安全体检，并配置定时体检策略。

支持自定义体检项体检、自定义路径体检

登录服务器安全控制台，选择**安全体检** > **体检列表**。点击**新建策略**，可自行选择体检项目，其中病毒木马检测支持快速扫描、全盘扫描及自定义路径扫描三种方式，网页后门检测支持自定义路径扫描。

体检未完成时，鼠标悬停至体检进度条上方，将显示体检的详细进度。 

支持立即体检及定时体检

您可选择立即体检及定时体检两种体检模式，立即体检即检测命令下发后立即执行体检命令；定时体检需用户设置扫描周期、扫描时间段后系统会按照设置规则定时执行体检命令。

安全体检策略

选择**安全体检** > **安全体检策略**，统一管理已创建的体检策略。定时体检策略需开启后生效。

可设置批量体检策略下发，通过设置体检的类型、体检的项目、体检的主机范围进行批量体检策略下发。并且支持定时体检策略与即时体检策略两种类型。

支持体检报告生成导出

体检报告可生成及导出，体检报告展示了体检分数、健康指数，体检结果图表化展示及详细体检问题说明展示，可导出Word格式的体检报告。

支持体检结果自动评分

体检结果将进行自动评分，通过检测的结果与预置的体检评分规则进行匹配可自动对主机健康情况进行打分，0-59分为不健康主机，60-89分为亚健康主机，90-100为健康主机。

资产管理

资产管理功能定期获取并记录主机上的Web站点、Web容器、Web应用、Web应用框架、账号、计划任务、端口、数据库、进程、第三方组件、环境变量、Jar包、系统安装包、软件应用、内核模块等信息，进行统一的管理和清点。

资产概览

登录服务器安全控制台，在左侧导航栏，选择**资产管理** > **资产概览**，进入资产概览页面。该页面了包含资产搜索、主机资产查询、主机操作系统分布三个模块。

资产一键搜

输入资产或主机的关键词进行快速查询主机资产；支持主机视图、资产视图双维度查看。

主机资产

统计了当前主机总数、在线主机数和离线主机数，同时提供了主机总数、在线主机随时间变化的趋势图，将鼠标在趋势图中悬停，将显示该日期主机总数和在线主机数。

主机操作系统分布

从Linux，Windows操作系统维度，统计了各版本系统占操作系统类别的比重。展示了各子类操作系统的占比和台数。

资产搜索

登录服务器安全控制台，在左侧导航栏，选择**资产管理** > **资产搜索**，进入资产搜索页面。资产搜索可以通过点击资产所属类目下的相关资产进行资产信息查询。

资产变更分析

登录服务器安全控制台，在左侧导航栏，选择**资产管理** > **资产变更分析**，进入资产变更分析页面。该页面包含了主机数量变更分析和30天各资产数量变更分析的情况展示。

主机数量变更分析

统计了当前在线主机数和本周新增加主机数，通过折线图为您展示近7天、近30天、近1年内的主机总数变更情况。并且支持按时间范围进行查看，将鼠标在趋势图中悬停，将显示该日期主机总数。同时支持报表导出功能。

30天各资产数量变更分析

统计了各类资产在30天内的变更情况，点击资产类别，下方资产数量走势图也随之切换。将鼠标在走势图中悬停，将显示该日期该类资产数量。同时支持报表导出功能。

主机资产

登录服务器安全控制台，在左侧导航栏，选择**资产管理** > **主机资产**。该页面检测已安装授权的主机，可采集已经安装轻代理中的各类信息。鼠标悬停在主机IP上时，展示主机的主机内外网IP、主机名、操作系统、系统内核、MAC地址信息。同时支持报表导出功能。

资产采集设置

在**资产管理** > **主机资产**页面点击**资产采集设置**按钮，您可自主选择资产采集项和采集频率。采集频率包括：仅采集一次、1小时、8小时、24小时、7天、15天、24天、30天、60天和暂停更新。


选择某台主机，点击列表页上方的**更新资产信息**按钮，或点击某台主机操作列的第二个按钮，将重新下发资产采集命令。

资产价值

资产价值代表该资产的重要程度，重要程度越高则级别越高，最高为5级。您可手动调整每台主机的资产价值。选择某台主机，点击列表页上方的**资产价值**按钮，或点击某台主机操作列的第四个按钮，可修改当前主机的资产价值。

资产详情

点击主机资产列表操作列中的**详情**按钮，将跳转至资产详情页。资产详情页详细描述了所选主机的已采集到的硬件信息、资产信息、漏洞风险、入侵威胁、安全监控、安全防护、合规基线等信息。

Web站点

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > Web站点**。服务器安全将探测主机上的网站信息，可采集网站域名、网站安装路径、网站运行状态、运行用户、端口、配置路径、运行参数等站点详细信息。支持通过危险设置与服务类型进行站点信息过滤筛选。

Web中间件

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > Web中间件**。服务器安全将探测主机上的Web中间件，可采集Web中间件的版本、安装路径、监听地址及端口、端口协议类型、运行权限、配置文件路径、日志文件路径、错误日志文件路径、插件路径、数据路径、进程二进制路径、启动参数等信息；支持Web中间件有Apache、IIS、JBoss、Nginx、Tomcat、Weblogic等。

Web应用

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > Web应用**。服务器安全将探测主机上的Web应用信息，可采集到应用名、版本、应用语言、服务类型等信息，支持通过应用类型进行过滤筛选；支持Web应用有Blot CMS、CKEditor、DedeCMS、DiscuzX、Ecmos、MediaWiki、Navigate CMS、OneThink等。

Web应用框架

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > Web应用框架**。服务器安全将探测主机上的Web应用框架信息，可采集到应用框架名、框架语言、框架版本、服务类型、应用路径等信息，支持通过框架语言类型进行过滤筛选。

端口

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > 端口**。服务器安全将探测主机上对内端口及对外端口，可采集端口对应的服务及端口协议信息，支持通过内外端口、端口协议、常用端口进行过滤筛选；支持端口规则设置。

账号

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > 账号**。服务器安全将探测主机上的账号信息，可采集账号的用户名、是否Root权限、Shell、状态、上次登录时间、用户ID、所属用户组等信息；支持业务账号设置；支持通过账号类型、账号诊断、账号异常、密码异常、用户组、登录方式进行过滤筛选。

数据库

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > 数据库**。服务器安全将探测主机上的数据库信息，可采集数据库的版本、安装路径、监听地址及端口、端口协议类型、运行权限、配置文件路径、日志文件路径、错误日志文件路径、插件路径、数据路径、进程二进制路径、启动参数等；支持的数据有Hadoop、Memcahed、MySql、Redis等。

软件应用

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > 软件应用**。服务器安全将探测主机上的软件应用信息，可采集软件应用的软件应用名、当前版本、安装信息、状态、发现时间等信息；支持开机启动项、系统服务 、定时任务属性筛选。

第三方组件

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > 第三方组件**。服务器安全将探测主机上的第三方组件信息，可采

集第三方组件的版本、安装路径、相关网站等信息；支持的第三方组件有CKEditor、DedeCMS、Discuz、PHP、PHPMyAdmin、Struts2、WordPress、Zabbix等。

进程

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > 进程**。服务器安全将探测主机上的进程信息，可采集进程的路径、版本、hash值等；支持进程白名单设置、业务进程设置等；可通过运行状态、进程标签、进程权限、是否系统进程、是否自启动、是否包管理安装、是否服务进程等多个维度进行进程信息的筛选。

系统安装包

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > 系统安装包**。服务器安全将探测主机上的系统安装包信息，可采集系统安装包的包名、总述、版本、安装时间、类型、安装路径等信息，支持采集的安装包有rpm包、dpkg包、java包、system包等；支持通过安装包类型进行过滤筛选。

Jar包

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > Jar包**。服务器安全将探测主机上Jar包信息，可采集到包名、类型、是否可执行、版本号、绝对路径等信息，支持通过Jar包类型进行过滤筛选。

计划任务

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > 计划任务**。服务器安全将探测主机上的计划任务信息，可采集计划任务的计划任务名、执行周期、执行命令或脚本、执行用户、运行目录等信息；支持采集的计划任务有Crontab计划任务、At计划任务、TaskScheduler计划任务。

环境变量

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > 环境变量**。服务器安全将探测主机上环境变量信息，可采集到变量名、变量类型、用户名、变量值等信息，支持通过环境变量类型进行过滤筛选。

内核模块

登录服务器安全控制台，在左侧导航栏，选择**资产管理 > 内核模块**。服务器安全将探测主机上内核模块信息，可采集到模块名、模块大小、模块描述、模块版本、模块路径、引用计数、依赖项等信息。

漏洞风险

漏洞风险包含两个部分，一是主机自身的安全漏洞如系统漏洞、网页漏洞等；二是人为原因造成的风险因素如弱口令。漏洞风险模块会显示当前主机上的漏洞风险情况，同时提供修复方案供用户进行参考。

风险概览

登录服务器安全控制台，在左侧导航栏，选择**漏洞风险 > 风险概览**。风险概览展示了服务器安全采集到的漏洞风险情况，包括应急漏洞、系统漏洞、弱口令、风险账号和配置缺陷的数量。

系统漏洞发现及处置趋势

系统漏洞发现趋势及处置趋势通过折线图，为您展示近7天、近30天、近1年内的系统漏洞发生及处置情况，并且支持按时间范围进行查看。将鼠标在趋势图中悬停，将显示该日期漏洞发现和处置总数。

易受攻击主机

统计了检出漏洞最多的前7台主机，点击主机，页面将跳转至系统漏洞详情页。

应急漏洞

登录服务器安全控制台，在左侧导航栏，选择**漏洞风险 > 应急漏洞**。应急漏洞模块可采集近期爆发出的高危漏洞，通过应急漏洞的检测功能对主机资产进行快速检测，确认是否有资产受到影响。

漏洞发现

支持漏洞和主机过滤，通过漏洞类型、风险等级、修复影响、影响软件、漏洞名称、等进行漏洞过滤，通知主机分组、标签、状态、内核版本等进行主机过滤。

应急漏洞库

支持应急漏洞库设置，采集应急漏洞信息、统计应急漏洞总数。

检测任务

支持检测任务设置，可创建检测任务，设置检测漏洞及检测主机范围。

重要说明： 应急漏洞检测为被动触发，您需先创建检测任务。

系统漏洞

登录服务器安全控制台，在左侧导航栏，选择**漏洞风险 > 系统漏洞**。Windows漏洞通过订阅微软漏洞更新，当发现主机存在漏洞时推送微软官方补丁信息，支持漏洞修复、忽略。Linux漏洞通过检测主机上的软件版本信息，与CVE官方漏洞库进行匹配，检测出存在漏洞软件并推送漏洞信息，支持漏洞忽略；支持通过漏洞过滤（漏洞名称、漏洞类型、风险等级、修复影响、处理状态等）、主机过滤（主机名称、主机分组、主机标签、主机状态、内核版本等）双维度过滤漏洞信息；支持白名单设置，可查看白名单列表和添加白名单。

网站漏洞

登录服务器安全控制台，在左侧导航栏，选择**漏洞风险 > 网站漏洞**。服务器安全通过目录文件的检测方案，检测出Discuz远程代码执行漏洞、Discuz memcache+ssrf GETSHELL漏洞、DedeCMS注入漏洞、WordPress IP验证不当漏洞等多种网站漏洞，对发现的网站漏洞，提供修复和忽略操作；支持通过漏洞类型、漏洞风险等级进行漏洞信息过滤筛选。

弱口令

登录服务器安全控制台，在左侧导航栏，选择**漏洞风险 > 弱口令**。服务器安全提供的弱口令库或用户自定义的弱口令规则可发现识别操作系统弱口令、数据库弱口令、应用弱口令，支持弱口令忽略；支持通过风险过滤（风险等级、处理状态、账户名称等）、主机过滤（主机名称、主机分组、主机标签、主机状态、内核版本等）双维度过滤弱口令信息；支持白名单设置，可查看白名单列表和添加白名单。

风险账号

登录服务器安全控制台，在左侧导航栏，选择**漏洞风险 > 风险账号**。服务器安全通过账户防护引擎可识别发现可以高权限账号、空密码账号、用户名和密码相同的账号，支持高危账号忽略、禁用、信任；支持白名单设置，可查看白名单列表和添加白名单。

配置缺陷

登录服务器安全控制台，在左侧导航栏，选择**漏洞风险 > 配置缺陷**。拥有强大的操作系统、Web容器、数据库、及其他应用的配置缺陷检测检测能力，支持Windows2003、Windows2008、Windows2012、Windows2016等各种Windows系统配置缺陷检测，支持Memcached、CentOS、Ubuntu、Debian、OpenSUSE、RedHat等Linux操作系统配置缺陷检测；支持IIS、Apache、Nginx、Tomcat、Weblogic、Tengine、JBOSS等各类Web容器配置缺陷检测；支持Redis、Mongodb、Memcached、ElasticSearch、PostgreSQL、Oracle等数据库配置缺陷检测；支持FTP、SNMP、Samba等应用的配置缺陷检测；支持白名单设置，可查看白名单列表和添加白名单。

入侵威胁

入侵威胁管理用以展示及处理各类入侵事件及具有高度威胁的事件，支持识别并处置的入侵威胁事件包括：病毒木马、网页后门、反弹shell、异常账号、日志删除、异常登录、异常进程、系统命令篡改等。

入侵概览

登录服务器安全控制台，在左侧导航栏，选择**入侵威胁 > 入侵概览**，进入入侵概览页面。该页面整体展示了识别到的入侵威胁情况。

概览页上方集中展示了8类入侵事件的具体个数，点击每个入侵威胁事件可跳转至其详情页。

当前入侵威胁分布情况

直观展示了各入侵威胁事件数量的差异和每个入侵威胁事件在总体的占比。将鼠标在图中悬停，将显示该入侵威胁事件的数量、占比情况。

30天入侵威胁发现趋势

直观展示了30天内各类入侵威胁事件数量变化的趋势，将鼠标在图中悬停，将显示当前日期各类入侵威胁事件的具体数量。

威胁分析

登录服务器安全控制台，在左侧导航栏，选择**入侵威胁 > 威胁分析**。威胁分析可以分析出最近一个月的攻击趋势和攻击类型分布。展示不同类型威胁的攻击趋势和不同类型攻击威胁的详细攻击特征信息，并可以对攻击IP加入黑名单。

支持按用户自定义时间范围进行查看，支持按数据中心查看。

病毒木马

登录服务器安全控制台，在左侧导航栏，选择**入侵威胁 > 病毒木马**。服务器安全采集可疑病毒木马程序的哈希指纹到云端，通过云查杀模块对哈希进行检测识别。对于信任主机支持添加白名单设置，可查看白名单列表。

若确认文件是恶意的，可以对单个文件进行隔离，或者批量选择进行一键隔离，隔离成功后，原始恶意文件将被加密隔离，后期可以在隔离区进行恢复。如果文件非恶意的，可以选择信任操作，加入信任后，云眼将不再对该文件进行检测，后期可以在信任区对信任文件进行管理。

网页后门

登录服务器安全控制台，在左侧导航栏，选择**入侵威胁 > 网页后门**。服务器安全可以实时准确的查杀各类木马恶意文件，同时提供恶意文件检测和一键隔离等功能，第一时间清除木马后门文件，确保用户服务　的安全。提供对webshell文件隔离、信任、下载和查看。对于信任主机支持添加白名单设置，可查看白名单列表。

反弹shell

登录服务器安全控制台，在左侧导航栏，选择**入侵威胁** > **反弹shell**。服务器安全支持反弹shell检测识别及事件关闭，通过对反弹shell事件进行检测识别可入侵攻击；展示安全体检和实时防护的反弹shell进程、进程运行参数、父进程和父进程运行参数、本地地址和反弹的目的地址；对于信任主机支持添加白名单设置，可查看白名单列表。

异常账号

登录服务器安全控制台，在左侧导航栏，选择**入侵威胁** > **异常账号**。服务器安全支持影子账号、篡改系统账号的检测识别及事件关闭，影子账号支持禁用处理；对于信任主机支持添加白名单设置，可查看白名单列表。

日志异常删除

登录服务器安全控制台，在左侧导航栏，选择**入侵威胁** > **日志异常删除**。服务器安全支持日志异常删除的检测识别及事件关闭，对于信任主机支持添加白名单设置，可查看白名单列表。

异常登录

登录服务器安全控制台，在左侧导航栏，选择**入侵威胁** > **异常登录**。服务器安全支持异常地点登陆、异常IP段登录、异常时间登录、异常计算机名登录、暴力破解登录5种异常登录类型检测及事件关闭。

异常进程

登录服务器安全控制台，在左侧导航栏，选择**入侵威胁** > **异常进程**。服务器安全支持子进程权限高于父进程、隐藏进程、隐藏端口进程3种异常进程的检测识别及事件关闭。对于信任主机支持添加白名单设置，可查看白名单列表。

系统命令篡改

登录服务器安全控制台，在左侧导航栏，选择**入侵威胁** > **系统命令篡改**。服务器安全支持系统命令校验的检测识别及事件关闭。对于信任主机支持添加白名单设置，可查看白名单列表。

安全防护

服务器安全提供安全防护功能支持暴力破解防护、扫描防护、病毒防护、IP黑白名单、端口安全防护、反弹shell监控、远程登录防护。通过对各类攻击事件的采集分析生成攻击趋势图、攻击分布图等图表，直观展现各类攻击事件。

登录服务器安全控制台，在左侧导航栏，选择**安全防护** > **防护设置**，点击**防护模板**按钮，可创建自定义防护模板，对每个防护模块进行分别定义。

点击**防护策略**按钮，跳转至**防护策略**页签，可针对指定的主机或主机组，选用某个防护模板制定单独的防护策略。

点击某防护功能旁的**设置**按钮，可进入防护配置详情页，针对每种防护模块制定具体的防护规则。

暴力破解防护

支持FTP防暴力破解、远程登录防暴力破解、MySql数据库防暴力破解3种防护功能，支持记录并拦截、记录不拦截两种模式。

扫描防护

支持扫描攻击防护，能有效的防止入侵扫描，可选记录并拦截、记录不拦截两种模式。

病毒防护

支持云查杀引擎、网马查杀引擎、安天本地引擎、天安云引擎多引擎技术识别并查杀最新病毒；可设置轻巧、中度、严格三种防护等级，轻巧防护下监控程序执行和网页文件写入，确保病毒无法运行，对系统性能影响轻微；中度防护下监控程序执行、写入，网页文件写入，确保病毒无法入侵，对系统性能影响小；严格防护下监控对程序和网页文件任何形式的访问，对系统性能会有一定影响。支持自动隔离（在隔离区备份原文件）及不处理（只写日志）两种处理方式。

IP黑白名单

支持白名单及黑名单设置，支持黑白名单批量导出及倒入；黑名单下可设置记录并拦截、记录不拦截两种模式。

端口安全

支持端口安全规则设置，可选宽松模式及严格模式，宽松模式下开放所有端口，只关闭规则中的端口；严格模式下关闭所有端口，只开放规则中的端口。支持TCP、UDP、ICMP、IGMP、ICMP6五种协议。

反弹shell监控

支持反弹shell监控，通过对反弹shell事件进行检测识别可入侵攻击。

远程登录防护

支持远程登录防护功能，可修改远程登录的端口，并指定可远程登录的IP地址或IP段。

安全监控

安全监控中可对主机开启各类监控包括登录监控、完整性监控、操作审计、会话监控。从主机安全角度，全天候监控主机的运行情况，能确保第一时间发现服务器问题。安全监控发现的问题系统自动进行问题归类到漏洞风险及入侵威胁模块中。

登录监控

登录服务器安全控制台，在左侧导航栏，选择**安全监控** > **登录监控**，安全监控模块可对主机的登录日志进　分析，识别出主机登录流水中的异常计算机名登录、异常IP段登录、异常地点登录、异常时间登录、暴力破解登录等异常登录行为。根据主机的账户登录　为分析，对可疑的登录　为提供实时告警通知；支持登录监控配置。

完整性监控

登录服务器安全控制台，在左侧导航栏，选择**安全监控** > **登录监控**，安全监控模块支持进行完整性监控，支持监控文件完整性，可发现删除文件、修改文件、新增文件等文件完整性异常行为；支持监控账号完整性，可发现修改账号用户名、修改账号密码、修改账号权限等账号完整性异常行为；根据主机的完整性分析，对可疑的文件、账号完整性异常　为提供实时告警通知；支持设置完整性监控。

操作审计

登录服务器安全控制台，在左侧导航栏，选择**安全监控** > **操作审计**，安全监控模块可对用户的输入操作进行命令审计，实时发现用户的危险操作，不依赖于传统日志的命令审计，根据主机的操作审计分析，对可疑操作　为提供实时告警通知；支持监控配置，可以通过定义的规则进行筛选威胁的命令。

会话监控

登录服务器安全控制台，在左侧导航栏，选择**安全监控** > **会话监控**，安全监控模块支持监控主机上网络连接情况，采集会话连接的协议、本地地址、本地端口、外部地址、外部端口、进程等会话信息，并生成主机会话连接图表；支持会话监控配置。

合规基线

合规基线模块结合等级保护工作过程，对业务系统资产进行跟踪，根据资产定级自动进行对应级别的安全配置检查，对合规情况出具报告，保证系统建设符合相关要求，促使相关监督检查工作高效执行。使用服务器安全的合规基线功能进行基线检查即可轻松完成对业务系统的安全风险检查。

基线检查

登录服务器安全控制台，在左侧导航栏，选择**合规基线** > **基线检查**。合规基线模块支持对单台主机或多台主机开启基线检查和环境检查。同时展示了每台主机的检查进度、检查状态、异常项与总检查项的比值和完成时间。点击**基线模板**将跳转至基线模板页面，点击**检查策略**将跳转至检查策略页面。

对已完成基线检查的主机，点击操作列的**详情**按钮跳转至报告页面，可查看异常项目详情及导出报告。

基线模板

登录服务器安全控制台，在左侧导航栏，选择**合规基线** > **基线模板**。基线模板支持对官方模板和自定义模板的统一管理。

检查策略

登录服务器安全控制台，在左侧导航栏，选择**合规基线** > **检查策略**。检查策略模块支持制定针对主机或主机分组的基线检查策略。点击操作列的**立即检查**按钮，将立即执行该策略。支持自定义检查频率。

攻击告警

开通服务器安全后，您可以通过云监控设置安全事件告警策略，当检测到漏洞风险、入侵威胁、安全监控和基线检查异常时及时向您发送告警通知。

创建告警规则

1.登录云监控控制台，菜单栏选择**告警服务** > **告警策略**，切换至**事件告警**页签。 2.点击**创建告警策略**按钮，配置策略基本信息。

参数	说明
策略名称	必填，设置告警策略名称
描述	选填，填写策略名称描述

3.产品类型选择**服务器安全**。 4.选择关联资源。 5.选择事件名称，您可选择全部事件或自选事件。

事件类型	事件类型参数	事件名称	事件名称参数	事件等级
漏洞风险	VulnerabilityRisk	应急漏洞	UrgentVulnerabilities	CRITICAL
		弱口令	WeakPassword	CRITICAL
		系统漏洞	SystemVulnerabilities	CRITICAL
		网站漏洞	WebsiteVulnerabilities	CRITICAL
		风险账号	UnsafeAccounts	CRITICAL
		配置缺陷	ConfigurePermissions	CRITICAL
		病毒木马	Virus	CRITICAL
		网页后门	WebShell	CRITICAL
		反弹shell	ReverseShell	CRITICAL
		异常账号	AbnormalAccounts	CRITICAL
入侵威胁	IntrusionDetected			

		日志异常删除	AbnormalDeletion	WARN
		异常登录	AbnormalLogin	WARN
		异常进程	AbnormalProcess	WARN
		系统命令篡改	CommandTampered	CRITICAL
		登录监控异常	LoginMonitoring	WARN
安全监控	SecurityMonitoring	完整性监控异常	IntegrityMonitoring	WARN
		操作审计异常	OperationalAudit	WARN
		会话监控异常	SessionMonitoring	WARN
基线检查	BaselineCheck	基线检查异常	BaselineCheck	WARN

事件等级描述如下。

事件等级	说明
Critical	严重
Warn	警告
Info	提醒

添加告警接收人

选择对应的告警接收人，可以接收到实例触发规则后产生的警报信息，支持添加联系人组、联系人、回调地址。具体请参阅云监控-新建告警策略产品文档。