ALIBABA CLOUD

# 阿里云

## 配置审计

## 等保预检

文档版本：20200925

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<br>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<br>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<br>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<br>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`<br>*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}` |

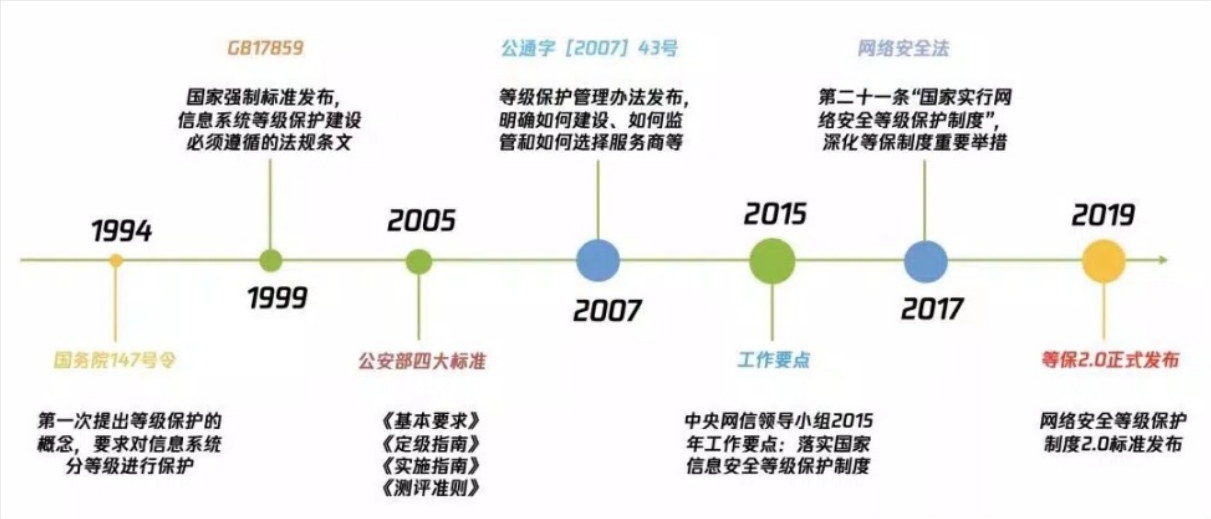
# 目录

# 1.等保2.0解读

本文为您解读等保2.0的具体内容，介绍配置审计的等保预检能力。

## 什么是等保2.0

等保2.0是指网络安全等级保护制度2.0国家标准，该标准已于2019年5月13日正式发布，并于2019年12月1日正式实施。目前58%的国家已制定国家网络安全战略，主要国家和地区都已制定专门的网络立法。等保2.0的发展和演进史如下图所示。




## 等保2.0的重要变化

- 云上信息系统纳入检测范围。

  基于等保1.0的网络和信息系统，新增了云计算平台、大数据平台、物联网、移动互联技术系统、工业控制系统。充分考虑了当前企业信息系统的业务多样性和复杂性。

- 云上租户的信息系统区别于云平台成为独立的检测对象。

  在等保1.0中，企业托管资源的云平台通过相应等保等级，即认为相应云上租户通过了相应等级。随着云上服务的复杂度和灵活性日渐成熟，云上租户对托管的资源具有越来越高的控制权，所以从等保2.0开始，云上租户使用云平台服务所构建的云上信息系统将作为独立的检测对象。

- 强调持续的安全能力构建，而非一次性检测。

  等保1.0主要关注在检测当时系统的合规状态，检测完成后，系统是否能持续保持安全合规是无法监管的。等保2.0在制定过程中，将对系统的持续合规要求融入到条例中，引导并监督企业构建一个可持续保护信息系统的安全能力。以PPDR（以策略为中心，构建防护、检测和响应防护机制）为核心思想、以可信认证为基础、以访问控制为核心，构建可信、可控和可管的立体化纵深防御体系。

| 分类 | 说明 |
| --- | --- |
| 可信 | 以可信计算技术为基础，构建一个可信的业务系统执行环境，即用户、平台、程序都是可信的，确保用户无法被冒充、病毒无法执行、入侵行为无法成功。可信的环境保证业务系统永远都按照设计预期的方式执行，不会出现非预期的流程，从而保障了业务系统安全可信。 |
| 可控 | 以访问控制技术为核心，实现主体对客体的受控访问，保证所有的访问行为均在可控范围之内进行，在防范内部攻击的同时有效防止了从外部发起的攻击行为。对用户访问权限的控制可以确保系统中的用户不会出现越权操作，永远都按系统设计的方式进行资源访问，保证了系统的信息安全可控。 |

| 分类 | 说明 |
| --- | --- |
| 可管 | 通过构建集中管控、最小权限管理与三权分立的管理平台，为管理员创建了一个工作平台，使其可以借助于本平台对系统进行更好的管理，从而弥补了我们现在重机制、轻管理的不足，保证信息系统安全可管。 |

等保2.0以“一个中心，三重防护”为网络安全技术设计的总体思路，其中一个中心即安全管理中心，三重防护即安全计算环境、安全区域边界和安全通信网络。

- 安全管理中心要求在系统管理、安全管理、审计管理三个方面实现集中管控，从被动防护转变到主动防护，从静态防护转变到动态防护，从单点防护转变到整体防护，从粗放防护转变到精准防护。
- 三重防护要求企业通过安全设备和技术手段实现身份鉴别、访问控制、入侵防范、数据完整性、保密性、个人信息保护等安全防护措施，实现平台的全方位安全防护。

等保1.0和2.0的差异如下表所示。

| 等保1.0 | 等保2.0 |
| --- | --- |
| 事前预防、事中响应、事后审计的纵深防御思路。 | 在“一个中心、三重防护”的理念基础上，注重全方位主动防御、安全可信、动态感知和全面审计。 |
| 0分以上基本符合。等保三级每年检测一次，等保四级每半年检测一次。 | 75分以上基本符合，等保三级和四级每年检测一次。 |

## 云上信息系统过等保的五大困难

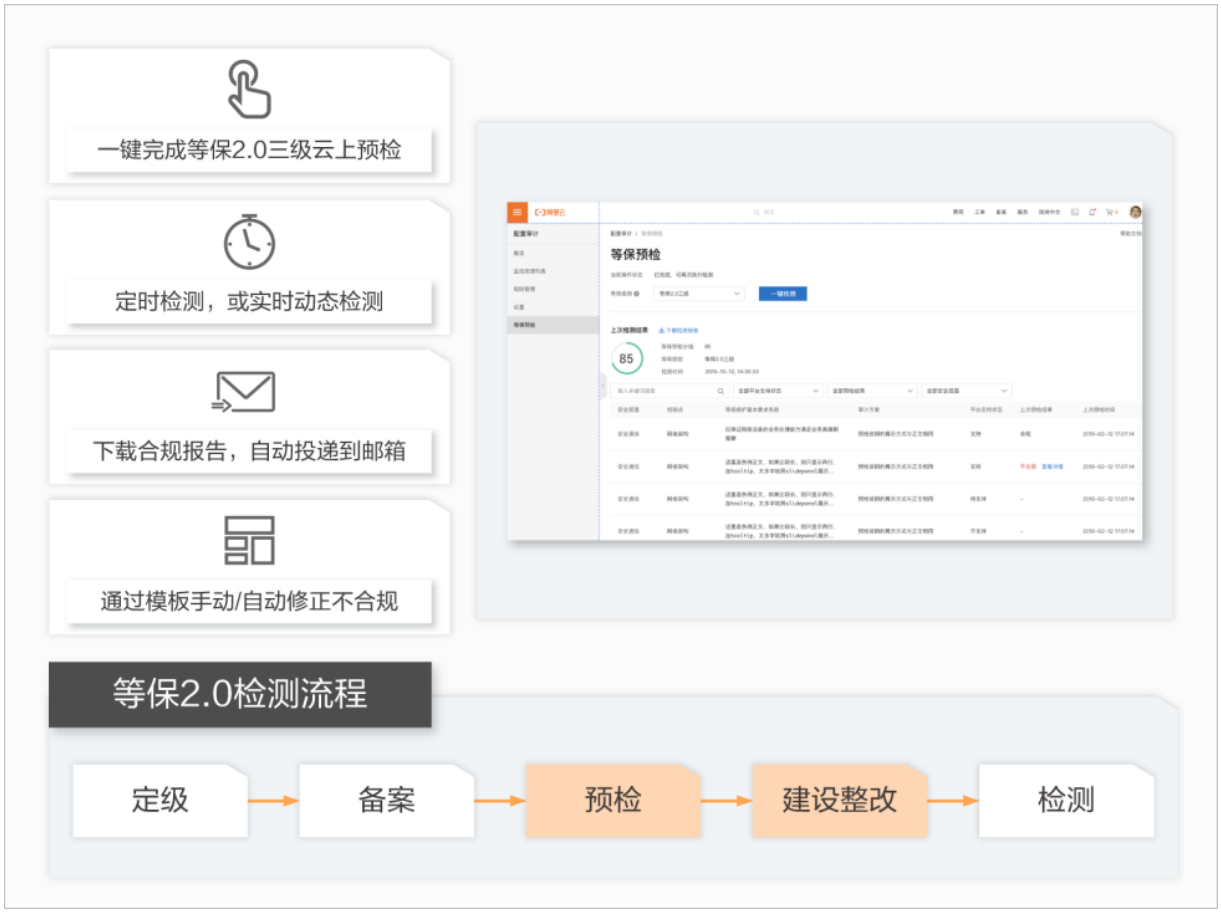
等保2.0侧重视持续的合规监管能力，且要求等保三级和等保四级均每年检测一次。但资源托管在云端，云上信息系统过等保，具体困难如下表所示。

| 困难 | 说明 |
| --- | --- |
| 云上检测范围不明确 | 虚拟化IT设施与传统IT的部分概念不同，面对复杂的云上配置，无从下手。 |
| 无集中的资源管理 | 云平台如果不提供配置管理数据库（CMDB）能力，在等保的反复检测和整改过程中，仅向检测结构举证和演示云上系统详情，操作就非常繁琐。 |
| 自己不掌握系统数据 | 资源托管在云端，等保2.0要求举证管理行为的日志和合规情况，需要依赖云平台对审计数据的输出。 |
| 无法自建自动化检测 | 通常云下企业都有自己的配置管理数据库CMDB（Configuration Management Database），只要合规和要求明确，完全可以自己写脚本扫描配置完成自检和监控。现在资源托管在云上，如果想通过脚本实现自检，则需要持续同步云上配置到云下，仅配置同步就消耗巨大的成本。 |
| 混合云截断成两部分 | 混合云的技术选型导致同一个业务系统部分在云上，部分在云下，无论是自检、扫描、监控或检测，都必须分开两次，人力和时间成本巨大。 |

## 借助云平台能力，实现持续监管

针对以上五大困难，阿里云在配置审计服务中，为您提供免费的等保预检能力，在等保预检和建设整改环节为企业助力。

配置审计将等保2.0条例解读为云上的合规检测规则，并持续监控资源的变更，动态实时的执行合规评估，及时推送不合规告警，让企业能时刻掌握云上信息系统的合规性。




## 功能特性

配置审计中等保2.0的功能特性如下：

- 等保2.0条例解读为检测规则：将云上等保2.0条例实现为一组监控规则，只需一键即可启动持续的等保预检，为正式检测做好准备。
- 动态、持续、可控的检测：通过持续追踪资源的变更，实时地触发相关联规则的评估。等保2.0要求达到75分即可通过，所以支持停止或忽略规则操作，避免持续出现无需关注的不合规告警。
- 不合规告警与修正：可以订阅等保2.0检测的不合规告警，收到告警后上云进行整改，或为具体的条例设置修正逻辑，在不合规发生时自动修正。
- 下载检测报告：可将检测结果下载到本地，便于云下分配任务并跟进整改，也可作为向检测机构举证时的辅助素材。

# 2.开启等保预检

配置审计提供等保2.0预检能力，为您动态且持续地监控阿里云上资源的合规性，从而避免正式检测时反复整改，帮助您快速通过等保检测。

## 背景信息

等保预检的使用限制如下：

- 等保2.0条例所需的产品未能完全接入配置审计，部分条例的检测尚不能支持。
- 等保检测仅能在预检和整改环节为您提供辅助信息，所得的检测报告并不能直接用于等保2.0的正式检测。您仍需请公安部授权的检测机构为您做最终认证。

## 操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**启用合规场景 > 法则标准 > 等保预检**。
3. 单击**开启持续检测**，为当前账号开启持续的等保预检。

## 后续步骤

- 您可以在**等保预检**区域，单击**暂停检测**，暂停等保预检功能。当您需要恢复等保预检功能时，单击**恢复检测**。
- 您可以在**等保预检**区域，单击**取消并删除报告**，删除规则、条例及已生成的检测报告。

# 3.查看等保预检结果

开启等保2.0预检后，配置审计自动为您新建了多条等保规则，您可以在规则列表中看到以level3为前缀的等保规则。等保预检持续检测资源的合规性，您每次刷新页面均会看到最新检测结果。您可以在等保预检列表中直接查看检测结果，并根据修改建议修正规则，使等保条例合规。

## 背景信息

一条等保条例可能对应一个或多个规则，只要其中一个规则检测不合规，则该预检结果不合规。

> 说明
>
> - 由于等保2.0的具体评分细则尚待公安部发布，配置审计仅为您统计了不合规的条例数。
> - 由于部分条例所需的产品尚未接入，配置审计只为您检测部分条例，且不支持的条例均默认统计为合规。

## 操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**启用合规场景 > 法则标准 > 等保预检**。
3. 在**等保预检**页面，您可以查看等保预检的所有规则和等保报告。
   - 在**规则列表**页签，您可以查看等保预检涉及的所有规则。您还可以对规则执行查看详情、调试参数、修改和停用的操作。
   - 在**等保报告**页签，针对预检结果为**有风险**的条例，您可以单击**改进建议**列的改进建议链接，根据文档中提供的方法，修改资源或审计规则，使其合规。您还可以查看条例的预检结果详情，或跳过无需预检的条例。

# 4.下载检测报告

本文为您介绍下载检测报告的方法。

## 前提条件

请确保您已开启等保预检，操作方法请参见开启等保预检。

## 操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**启用合规场景 > 法则标准 > 等保预检**。
3. 单击**等保报告**页签。
4. （可选）在**等保报告**页签，单击**生成最新报告**。
5. 在**等保报告**页签，单击**下载检测报告**。您可以获得一份Excel格式的检测报告。在该检测报告中，您可以查看不合规资源详情。

# 5.常见问题

## 5.1. 等保预检结果有风险怎么办？

当等保预检结果为有风险时，您可以根据文档中提供的方法修改资源或规则，使预检结果正常。

### 操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，选择**启用合规场景 > 法则标准 > 等保预检**。
3. 单击**等保报告**页签。
4. 在**等保报告**页签，单击**改进建议**列的改进建议链接。