深信服多云安全平台-云等保合规自检-阿里云说明文档

深信服科技股份有限公司

2021 年 11 月

版权声明

免责条款

目 录

前言

云等保合规体检是深信服多云安全平台推出的一款基于等保 2.0 二级、三级的公有云等保合规自检工具。

1 立即体检

（1）打开深信服多云安全平台体检链接

（2）进入“深信服多云安全平台-云等保合规体检介绍页”点击【立即体检】，即可快速开始“公有云等保合规体检”。

（3）点击【直通产品经理】，扫描二维码，可快速联系“深信服云安全专家-多云安全平台产品经理”。

（4）点击右上角【多云安全平台】，进入多云安全平台控制台，可快速体验更多云上安全能力。

2 免费注册

（1）填写帐号、密码、企业名称等企业/个人信息，即可免费注册企业帐号。注册帐号即为多云安全平台帐号。

（2）若您已注册【多云安全平台】企业帐号，请点击【立即登录】，快速进入下一步。

3 安全概况

请填写您企业的云上安全概况。

4 合规体检

说明：为了您能正常使用深信服多云安全平台-云等保合规体检服务，您需先接入阿里云等云环境各云帐号的 AccessKey，用于深信服多云安全平台连接各云环境同步云资产、云安全配置信息。同时，深信服多云安全平台建议您为每一个云帐号创建一个用于连接深信服多云安全平台的子帐号，并根据最小化授权原则赋予相关权限。深信服多云安全平台采用严格加密方式，不会泄露您的信息。

4.1 创建子帐号

4.1.1 登录阿里云-访问控制

登录链接：https://ram.console.aliyun.com/users

4.1.2 创建用户

（1）在【用户】列表点击“创建用户”

（2）填写登录名称、显示昵称、选择“Open API 调用访问”并点击确定

4.1.3 创建用户组并关联用户

为了您能正常使用深信服多云安全平台-云等保合规体检服务，您需创建用户组并选择“ReadOnlyAccess、AliyunECSFullAccess”策略或选择“最小化权限策略表”中的全部策略赋予子帐号。最小化读权限策略表如下：

序号	策略	描述
1	AliyunECSFullAccess	管理云服务器服务(ECS)的权限
2	AliyunRDSReadOnlyAccess	只读访问云数据库服务(RDS)的权限
3	AliyunMongoDBReadOnlyAccess	只读访问云数据库服务(MongoDB)的权限
4	AliyunKvstoreReadOnlyAccess	只读访问云数据库 Redis 版(Kvstore)的权限
5	AliyunSLBReadOnlyAccess	只读访问负载均衡服务(SLB)的权限
6	AliyunOSSReadOnlyAccess	只读访问对象存储服务(OSS)的权限
7	AliyunNATGatewayReadOnlyAccess	只读访问 NAT 网关(NAT Gateway)的权限
8	AliyunVPNGatewayReadOnlyAccess	只读访问 VPN 网关(VPNGateway)的权限
9	AliyunYundunCertReadOnlyAccess	只读访问云盾证书服务的权限
10	AliyunRAMReadOnlyAccess	只读访问访问控制(RAM)的权限，即查看用户、组以及授权信息的权限
11	AliyunCDNReadOnlyAccess	只读访问 CDN 的权限
12	AliyunVPCReadOnlyAccess	只读访问专有网络(VPC)的权限

操作步骤：

（1）在【人员管理-用户组】点击创建用户组并填写用户组信息

（2）添加权限

1）在【用户组】列表找到刚创建的用户组点击“添加权限”

2）在【添加权限】页-授权应用范围：选择“整个云帐号”

3）在“选择权限-系统策略”选择“ReadOnlyAccess”策略或选择“最小化读权限策略表”中的全部策略。

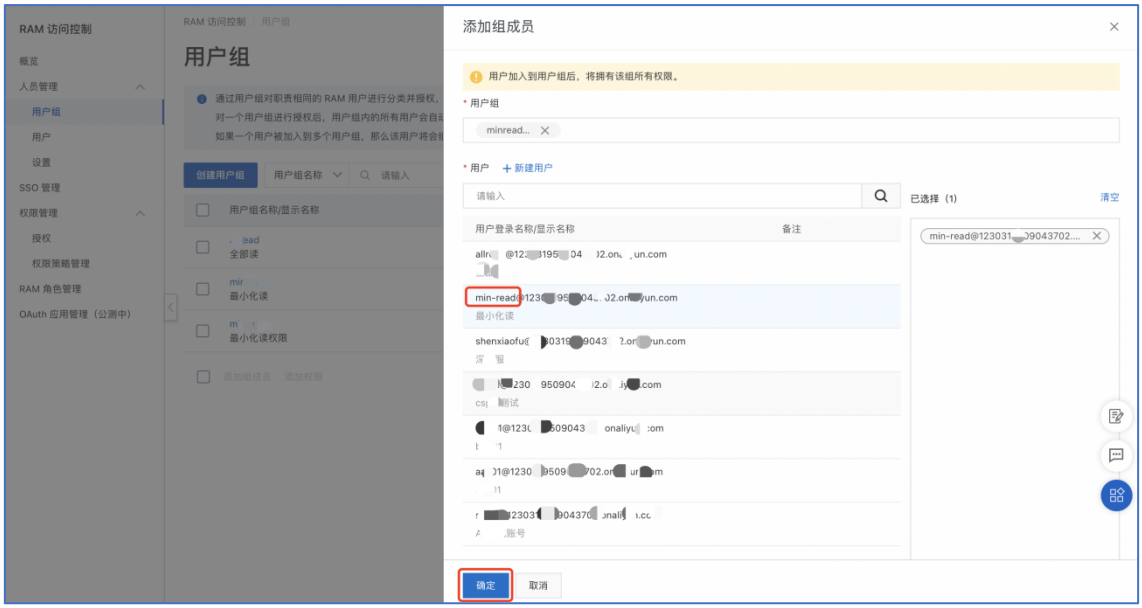
说明：如不能一次添加全部策略，可分批次添加，每次添加 5 个策略即可。

4）审阅后点击“完成”添加权限

（3）关联用户

1）在【用户组】列表找到刚创建的用户组点击“添加组成员”

2）选择刚创建具备“Open API 调用访问”的用户并点击确定。



4.1.4 复制 AK 并保存

方式一：成功创建用户时复制 AccessKey ID 和 AccessKey Secret。

方式二：

1）前往【用户-用户详情-用户 AccessKey】创建。

2）创建成功下载 CSV 文件或复制。

4.2 填写 AK 帐号

（1）打开登录链接并前往“合规体检”页

（2）选择云环境、自定义云帐号名称并填写 4.1.4 复制的 AccessKey 帐号。多个帐号点击“新增云帐号”继续填写。

（3）测试连通性：点击“开始测试”，当提示“连通性测试成功”则表示全部云帐号可接入。当存在任一云帐号权限不足时则会显示“查看权限检测详情”，权限不足可能会导致资产或配置同步不完整，您可根据检测详情前往阿里云平台配置所缺失的权限。

（4）根据您的业务需要选择等保类型并点击“开始体检”。体检时间受您云上资产数的影响。

说明：配置完成后请注意删除本地保存的 AK 信息。

5 体检结果

（1）完成体检后，可查看的检查项总数、未通过检查项数、规则总数、未通过规则数、已检查资源数、未通过资源数以及每个安全层面未通过的检查项数、规则数、资源数，更多报告详情您可前往多云安全平台查看或下载合规体检报告。

（2）深信服多云安全平台根据您填写的云上安全概况信息，为您推荐等保合规应用，您可参考推荐配置相关应用组件，或添加深信服云安全产品经理企业微信领取免费报告解读资格、合规材料等福利。


深信服云等保合规体检
01 免费注册
02 安全概况
03 合规体检
04 体检结果
直通产品经理
多云安全平台
6-1
安全计算环境
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等 2 个检查项。
—
云主机安全CWPP
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等 4 个检查项。
云日志审计Logger
云日志审计Logger
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。
—
云堡垒机OSM
安全管理中心
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、管理和查询等等 2 个检查项。
云日志审计Logger 云数据库安全审计DAS
云日志审计Logger 云数据库安全审计DAS
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 6 个检查项。
云堡垒机OSM
云堡垒机OSM
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。
—
云主机安全CWPP
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等 5 个检查项。
多云安全平台
多云安全平台
6-2
直通产品经理
详细咨询报告结果，微信扫码直通深信服云安全产品经理，领取更多福利~
合规报告专业解读
获取免费合规材料
获取更多云等保合规服务
了解多云安全平台
6-3
快捷入口
下载资料
多云安全控制台
《多云安全平台白皮书》
《多云安全深信服等保2.0合规材料》
相关文章
CSA发布《多云安全风险图谱》 深信服为主要参编单位之一
深信服持续加码云安全，为用户保驾护航
深信服发布下一代云安全能力矩阵 助力用户构建混合多云时代下简单有效的安全体系
守护每一朵云
下载合规体检报告
前往多云安全平台
进入多云安全平台查看报告详情