

# 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

深信服科技股份有限公司版权所有,并保留对本文档及本声明的最终解释权 和修改权。

本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容, 除另有特别注明外,其著作权或其它相关权利均属于深信服科技股份有限公司。未 经深信服科技股份有限公司书面同意,任何人不得以任何方式或形式对本文档内 的任何部分进行复制、摘录、备份、修改、传播、翻译成其他语言、将其全部或部 分用于商业用途。

#### 免责条款

本文档仅用于为最终用户提供信息,其内容如有更改,恕不另行通知。

深信服科技股份有限公司在编写本文档的时候已尽最大努力保证其内容准确 可靠,但深信服科技股份有限公司不对本文档中的遗漏、不准确、或错误导致的损 失和损害承担责任。



# 目 录

前	前言	1
1	1 立即体检	2
2	2 免费注册	
3	3 安全概况	4
4	4 合规体检	5
	4.1 创建子帐号	5
	4.1.1 登录阿里云-访问控制	5
	4.1.2 创建用户	5
	4.1.3 创建用户组并关联用户	6
	4.1.4 复制 AK 并保存	9
	4.2 填写 AK 帐号	11
5	5 体检结果	



# 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。

多云安全平台			直通产品经理 多云安全平台
深信服云等保合规体检 88955	等保2.0概述	云等保体检 云等保套餐特性	云等保建设流程 云等保合规套餐 立即体检
5分钟快速了解云上业务安全风险			
快速省心过等保,就造漂信服多云安全平台,深信服多云安全平台 解决方式,也不如企业理解、提升了,在成为,满足云上等保合规 续评估,也不以风险。全面满足,这个人工人,要求。	为用户提供高性价比的云上等保合规安全—站云 要求,通过智能、实时的安全洞察,帮助用户托		
	等保2.0是什么		
•		等保2.0	的概念
	国务院147号令 第一次提出等级保护的概念,要求对信	自1994年国家 国家的网络安 40.949-7.659	第一次提出等级保护概念以来,等级保护已经成为了 全基本制度、基本国策和基本方法。开展网络安全等 2010年9月20日
1999	息系统分等级进行保护。	数味护工作建 安全保障工作 《中华人尼共	味》后恶化及液、细胞后恶女王的银令殊躁,走信息 中国家意志的体现。随着经济社会发展和技术进步, 和回回终留会注入卫生生中回应终期会到这些少素三
CP17950			
GB17859 国家强制性标准发布。信息系统等级保 护建设必须遵循的标准。	····· <mark>· 2007</mark>	《甲華八氏共 会对国家落实 息安全技术网 全等级保护已	机固构的女主流》及中外中央网络女主和信息节女贝 网络安全等级保护制度都提出了明确要求,伴随《信 络安全等级保护基本要求》新国标正式发布,网络安 近人2.031代,
G817859 国家原制性标准发布。信息系统等级保 护建设必须遵循的标准。	·····································	》中华人民共 会对国家落实 息安全技术网 全等级保护已	机副附值发生加及 化中六中共称的发生加加的无效的 制度全学等级供护基本要求)新国核正式发布,网络安 进入2.03时代,
GB17859 国家强制性标准发布。信息系统等级保护建设必须遵循的标准。	2007 公通字 [2007] 43号 等级保护管理办法发布,明确如何提 设、如何监管以及如何选择服务商等。	4年4765人 会对国家隔荣 思安全技术网 全等极保护已 等保2.01	机晶体加速点的2004年5月8月2日,2016年5月2日日 開設生育發展的運動進力可能要求。作用《信 請定全等紛鳴沪基本要求》新回時正式來奇,同感受 进入2031代。 主要变化



# 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。

🐼 深信服云等保合规体检	01 免费注册 02 安全概况 03 合規体检 04 体检线	唐黑 直通产品经理 多云安全平台
为了给加	免费注册多云安全平台,即刻发起检查 彭提供更好的体检服务,请填写您的企业/个人信息、体化 2-2 知您,您也可联系产品经理进行免费 若您已经注册多云安全平台账号,请 立即登录	平台将通过短信通
	<b>登录信息</b> sangfor 通用次输入显录密码	
	<b>企业和个人信息</b> 请输入企业名称 请选择企业所属行业 请输入您的姓名 请输入您的我业名称	•
	<ul> <li>联系方式</li> <li>请输入邮箱地址</li> <li>488 请输入手机号码</li> <li>请输入把信告证码 获取效</li> <li>3 我已阅读开网意《服务协议》《用户数据处理协议》</li> </ul>	
	注册并登录	



# 3 安全概况

请填写您企业的云上安全概况。

诊 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 体检结界	直通产品经理 多云安全平台 📗 💽
	云上安至概况	
	为了更好地评估您云上业务的安全风险情况,请填写您企业的云化战略以 规情况。	<b>设</b> 元上安全合
	【令业于化建筑】	
	1.企业当前的公有云上的云主机规模是多少?	同行选择占比
	A 0-50	A 00 %
	C. 101-500#	C = 10 %
	〇 D. 500台以上	D 5 %
	2.企业止在使用的云外境有哪些? 多达	
		B 67 %
	□ C. 腾讯元	G 31 %
	D. 华为云	D 26 %
	E. 百度云	E 19 %
	F. AWS	F 17 %
	G. Azure	G 🔤 10 %
	H. Kubernetes	H 23 %
	I. 其他	22 %
	3.企业今年在云安全领域投入的资金规模?	同行选择占比
	○ A. 0-20万	A 53 %
	○ В. 21-50万	B 29 %
	○ C. 51~100万	C 📖 12 %
	○ D. 100万以上	D 🗉 6 %
	进入合规体检	



### 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"

RAM 访问控制	RA	AM 访问控制 / 用户							
概览	月	用户							
人员管理へ	▲ ▲ ● RAM 用户是一个身份实体,它通常代表您的组织中需要访问云资源的人员或应用程序。								
用户组		通常的操作步骤如下: 1. 创建用户,并为用户设置登录密码(用户图	登录控制台场景)或创建 AccessKey(应用	]程序调用 API 场景)。					
用户		2. 添加用户到用户组(需要先创建用户组并引	完成对用户组的授权)。						
设置		创建用户 输入登录名、用户 ID 或 AccessKe	y ID Q					d	5
SSO 管理		用户登录名称/显示名称	备注	最后登录时间 14	创建时间 11	操作			
权限管理 へ 授权				-	2021年6月23日 16:45:17	添加到用户组	添加权限	删除	
权限策略管理	<			-	2021年6月22日 11:04:20	添加到用户组	添加权限	删除	
RAM 角色管理				-	2021年6月22日 11:02:20	添加到用户组	添加权限	删除	
OAuth 应用管理(公测中)				-	2021年5月14日 14:54:33	添加到用户组	添加权限	删除	
		□ 添加到用户组 添加权限							
								(	

(2) 填写登录名称、显示昵称、选择"Open API 调用访问"并点击确定

RAM 访问控制		RAM 访问控制 / 用户 / 创建用户
概览		← 创建用户
人员管理	^	田户联号信息
用户组		* 登录名称 ③ * 显示名称 ③
用户		min-read @ 137 naliyur_)m 最小化读
设置		+ 添加用户
SSO 管理		
权限管理	^	访问方式 💿
授权		□ 控制台访问 用户使用账号密码访问阿里云控制台
权限策略管理		<b>Open API 调用访问</b> 启用 AccessKey ID 和 AccessKey Secret,支持通过 API 或其他开发工具访问
RAM 角色管理		确定 返回
OAuth 应用管理(公测中	)	<



#### 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

RAM 访问控制	RAM 访问控制 / 用户组	创建用户组    ×
概览	用户组	2 * 用戶組名称
人员管理 へ 用户组 用户	通过用户相对职责相同的 RAM 用户进行分类并接权,可以更加高效地管理用户及其权限, 对一个用户相进行复数后,用户相对的所有用户会自动提承该用户相约权限, 如果一个用户被加入到多个用户相,那么该用户将会继承多个用户组的权限。	minread 最大长度 64 个学符,允许英文学母、数字、 , , , , , , , , , , , , , , , , , , ,
没直 SSO 管理 权限管理 へ	创建用户组         用户组名称 ~ Q、请输入           用户组名的显示名称         备注	<b>藏小化读权限</b> 最大长度 24 个字符或汉字。
授权 权限策略管理 RAM 角色管理	a sd 全部读 	6注
OAuth 应用管理(公测中)		最大长度 128 个字符。
		8
		3 (Maz: R2)



(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"

RAM 访问控制	RAM 访问控制 / 用户组		
概览	用户组		
人员管理 へ 用户組	<ul> <li>通过用户组对职责相同的 RAM 用户进行分类并提权,可以更加高效地管理用户及其权限。</li> <li>对一个用户组进行授权后,用户组内的所有用户含自动继承该用户组的权限。</li> </ul>		
用户	如果一个用户被加入到多个用户组,那么该用户将会继承多个用户组的权限。		
设置 SSO 管理	创建用户组 用户组名称 >> Q、请输入		¢
权限管理 ヘ	用户编名称/显示名称 备注	创建时间	操作
授权 权限策略管理		2021年7月14日 21:12:22	添加组成员 添加权限 删除
RAM 角色管理	□ minread 量小化该	2021年7月14日 21:12:42	添加組成员 添加权限 删除
OAuth 应用管理(公测中)		2021年7月28日 21:06:19	添加组成员 添加权限 删除

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。

RAM 访问控制	RAM 访问控制 / 用户组	添加权限	×	
RAM 访问控制 変変 力力管理 へ 用户 设置 SSO 管理 反用管理 へ 投釈 取測態管理 RAM 角色管理 OAuth 品用管理 (公測中)	RAM (5時時期) 用户組 用户组 ● 満江用户組初販費相同的 RAM 用户進行分类并現代、 対果一个用户組进行硬权品,用户组行分类并現代、 対果一个用产組近入到多个用户組,那么该用户培会的 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	<ul> <li>添加权限</li> <li>指定告源组的模拟生纹前提是该云振务已支持资源组、查看当前支持资源组的云振务。(前往查看) 单次成权高多文持 5 余推稳,如果将定更多准确。成为多次进行。</li> <li>· 現权应用范围</li> <li>· 重な完整</li> <li>· 指定表源组</li> <li>· 请请将编辑人员意想《书选行理案》</li> <li>· 被授权主体</li> <li>· 加加 · 差到 · (p.122 · )509 · )702.0. jyun.co ×</li> <li>· 法将权限</li> </ul>		
		3 AllyunRAMReadOnlyAccess       3 AllyunOSSReadOnlyAccess         仅限推時名称       音注         AllyunRAMReadOnlyAccess       只该访问访问控制(RAM)的权限、即查看用户、组以及投权         AllyunRAMReadOnlyAccess       只该访问访问控制(RAM)的权限、即查看用户、组以及投权         AllyunVPNGatewayReadOnlyAccess       AllyunVPNGatewayReadOnlyAccess         AllyunVPNGatewayReadOnlyAccess       AllyunVPNGatewayReadOnlyAccess         AllyunVPNGatewayReadOnlyAccess       AllyunVPNGatewayReadOnlyAccess         AllyunVPNGatewayReadOnlyAccess       AllyunVPNGatewayReadOnlyAccess         AllyunRAMReadOnlyAccess       AllyunVPNGatewayReadOnlyAccess         5       5         100       取消	× s × k k s × k k x k k x	

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"

RAM 访问控制	RAM 访问控制 / 用户组		
概览	用户组		
人员管理 へ 用户组 用户	<ul> <li>通过用户组对职责相同的 RAM 用户进行分类并提权,可以更加高效地管理用户及其权限。</li> <li>对一个用户组进行贯权后,用户组为的所有用户会自动继承该用户启动权限。</li> <li>如果一个用户被加入到多个用户组,那么该用户将会继承多个用户组的权限。</li> </ul>		
设置 SSO 管理	創建用户組         用户组名称 ∨ Q 请输入	6(780+1/2	Ö
权限管理	□ //// 地口的//山小口が Wi/// □ 全部读	2021年7月14日 21:12:22	森加组成员 添加权限 删除
RAM 角色管理	minread 氟小化读	2021年7月14日 21:12:42	添加组成员添加权限 删除
CAULTER (22394)		2021年7月28日 21:06:19	添加组成员 添加权限 删除



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。

RAM 访问控制	RAM 访问控制 / 用户 / 创建用户	RAM 访问控制 / 用户 / 创造用户					
概览	← 创建用户	← 创建用户					
人员管理へ	若开通编程访问,请及时保存 AccessKey 信息,页面关闭后	后将无法再次获取信息。					
用户组	用户信息						
用户	下载 CSV 文件						
设置		هم م	1回日 Accession D	AcceseKay Secret	10.01		
SSO 管理		134 <u>1</u> 78	Accessively ID	Accessively Secret	DRTF		
权限管理 へ	创 shenxiaofue .onaliyun.com 开	創建用户:● 成功 无 干启编程访问:● 成功 500000000000000000000000000000000000	LTAI5tDmS7BVnw4uN1XwmpzD	1.000	□ 复制		
授权	添加到用户组 添加权限						
权限策略管理	<						
RAM 角色管理	返回						
OAuth 应用管理(公测中)							



#### 方式二:

1)前往【用户-用户详情-用户 AccessKey】创建。

	登录名称 min-read@123 350904 )2.c	rh.com 🗗 复制 UID	291 926 636					
RAM 访问控制	显示名称 最小化读	创建	时间 2021年7月14日 21:13:48					
概览	备注	手机	号码					
人员管理へ	邮箱							
用户组								
田户	认证管理 加入的组 权限管理							
H17"								
设置	控制台登录管理 启用控制台登录							
SSO 管理								
权限管理 ヘ	控制台访问	上次:	登录控制台时间					
授权	必须开启多因素认证	下次	登录重置密码					
权限策略管理								
RAM 角色管理	虚拟 MFA U2F 安全密钥							
OAuth 应用管理 (公测山)	<							
ONUTIONEDE (Z/09+7	虚拟多因素认证设备(VMFA) 应用虚拟 MFA 设备							
	遺植 TOTP 物准算法来产生 6 位数字级让纳约回用程序。							
	设备状态 禾启用			_				
				E				
	用户 AccessKey							
	创建 AccessKey			E				
	AccessKey ID	状态 最后使用时间 ⑦	创建时间	探				
	LTAI5tGmhQnLfx5SrfDN8DDz	已启用 2021年7月28日 21:44:43	2021年7月14日 21:19:47	禁用 删除				

2) 创建成功下载 CSV 文件或复制。

创建 AccessKey	$\times$
请及时保存或发送 AccessKey 信息至对应用户,弹窗关闭后将无法再次获取该信息,但您可以随时创建新的 AccessKey。	
⊘ 创建成功,请及时保存。	
AccessKey ID LTAI5t9C46UMyCLFVxeegs51 AccessKey Secret	
<ul> <li>坐 下载 CSV 文件 □ 复制</li> <li>关I</li> </ul>	闭



#### 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 安全橋	祝 03 合规体检	-> 04 体检结果	直通产品组	经理 多云安全平台 丨 💽
体 1	验进度 00%	<b>等保合规体</b> 机 조해국 <b>(-)</b> sherviat 检查标准 阿포조-ች(	<b>金完成</b> mu 第2.0三级			$\odot$
-1 体检详情						
<b>82</b> 检查项总数	<b>16</b> 未通过检查项数	<b>29</b> 规则总数	<b>9</b> 342 未通过规则数		<b>40</b> 已检查资源数	<b>37</b> 未通过资源数
安全物理环境	未通过检查项数: 0	未通过规则数: 0 未通过资源数: (	0			详情 >
安全通信网络	未通过检查项数: 3	未通过规则数: 2 未通过资源数: :	2			详情 >
安全区域边界	未通过检查项数: 5	未通过规则数: 1 未通过资源数: 1				详情 >
安全计算环境	未通过检查项数: 8	未通过规则数: 7 未通过资源数: :	37			详情 >
安全管理中心	未通过检查项数: 0	未通过规则数: 0 未通过资源数:	0			详情 >
安全应用推荐 深信服多云安全平台根据	您填写的云上安全概况信息,建设 LOSM	X购买使用以下6个应用组件。 一 二 売款業库安全审计DAS		云日志审计Loager		云Web应用防火墙WAF
全面解》 建问题	₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩	与大数据分析相结合的 防护	数据安全	及时、有效的发现安全事 计违规	i件及审 WAF	专注于网站与其系统的应用层安 全防护
SSL V	PN 业标准引领者	<b>云镜漏洞扫描</b> 全面提升客户网络 全性	3 <sup>夏体安</sup> 5-	4		
		下载合规	体检报告 前往多云	<b>安全平台</b> 进入多	云安全平台查看报告详情	

6	∽ 深信服云等得合	<b>规体检</b> 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   🌔
安全计算环境	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
	X11#1%	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
		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、管理和宣询等等 2 个检宣项。	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
	安全管理中心	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		品授理 报告结果, 但信扫码直通深信服云安全产品经理, 领取更多语料~ 规程告专业解读		
了.	解多云安全平台	<b>●</b>		
	快捷入口 下载资 多云安全控制台 《多云 相关文章	料 安全平台白皮书) 《多云安全深值服等保2.0合规材料》		
	CSA发布 深信服持	《多云安全风能图谱》深信服为主要参编单位之一 读加码云安全,为用户保证护纸	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