# 配置核查（龙检）

## 产品文档

# 文档目录

# 产品简介

# 产品概述

最近更新时间: 2022-10-24 10:52:13

建行云基线核查（龙检）（Cloud Security Check）是一款独立于云上主机及其它安全产品的安全云产品，它以各资产安全配置是否合规的视角，从网络访问控制、基础安全防护、监控告警多个方面为用户提供云平台配置的基线核查功能，针对龙御WAF、负载均衡、龙卫士、龙堡垒、安全组等云产品的配置检测，帮助用户及时发现安全隐患并提供相应的修复建议

# 功能优势

最近更新时间: 2022-10-24 10:52:12

- 简单易用：提供云产品配置的基线核查功能，内置多种检查指标满足基本的安全要求，用户无需做其他配置。
- 全面检测：提供覆盖云服务器、网络、安全组等多种云产品的安全基线指标。
- 旁路审计：在业务低峰期通过云产品API实现配置获取和检查，不影响用户正常业务。
- 风险告警：针对每日检测结果及未通过的指标项发送短信告警，帮助用户快速知晓风险，及时整改。

# 应用场景

最近更新时间: 2022-10-24 10:52:12

建行云CSCC产品可以提供云平台配置的基线检查功能，并针对未通过的指标项提供相应的修复建议。

- 配置核查 用户开通基线核查（龙检）服务后，会使用默认策略对所有资产进行检测。检测后可看到账户的安全评分、安全排行、所有指标的检查结果及未通过的指标结果详情。
- 结果查看及导出 配置核查任务执行后，用户可在控制台查看此次检查结果，点击下载可导出检查结果XLS文件到本地。
- 工单管理 用户在使用基线核查（龙检）产品时，如果想在检查任务时忽略部分特殊配置，可使用工单管理功能，针对特定的检查指标的特定配置申请加白操作，审批通过过，在指标项中仍会显示此配置信息，但不会进行告警。
- 白名单管理 用户在使用基线核查（龙检）产品时添加的特殊配置，可在白名单管理中查看具体内容。如果此特殊配置已经无效，可以申请取消。

# 推荐简介方案

最近更新时间: 2020-05-07 10:38:44

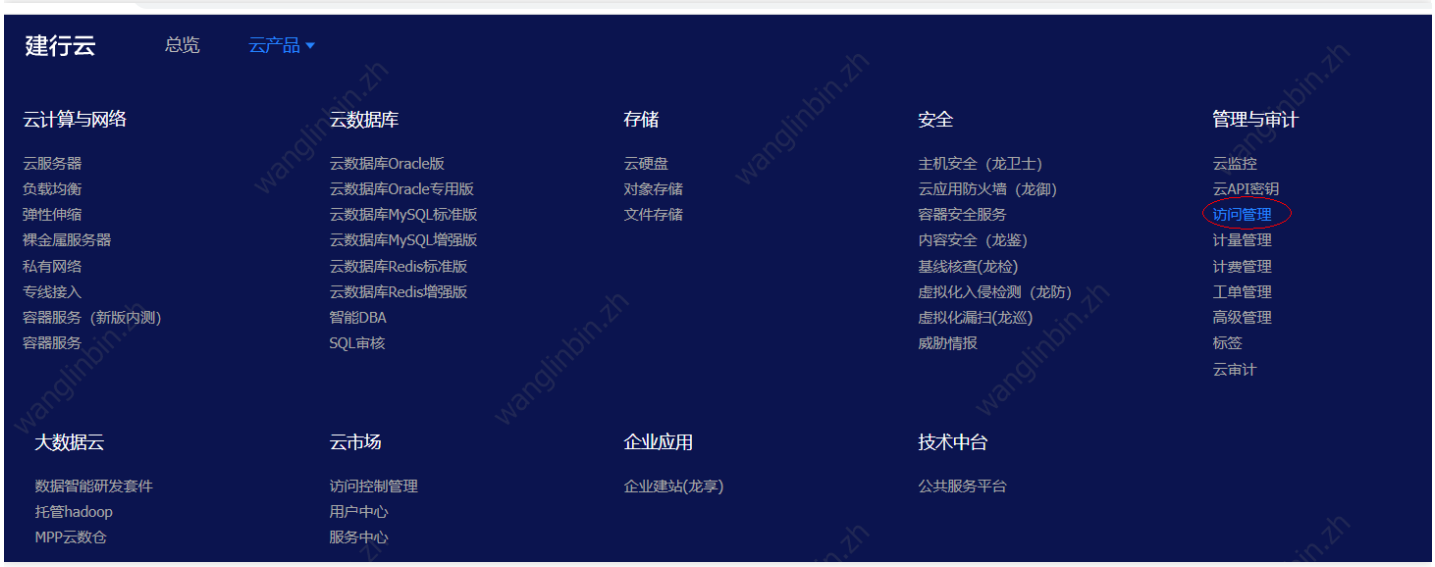
1.用户管理+龙检结合使用 龙检需使用账户的SecretId和SecretKey调用云产品的API接口完成云产品配置数据的获取。建议新建龙检产品专用的只读账户，只包含所有云产品的只读权限，这样既可满足产品检查的需要，又避免赋予过高的权限。

# 快速入门
# 开启龙检–配置核查服务

最近更新时间: 2022–10–31 18:13:54

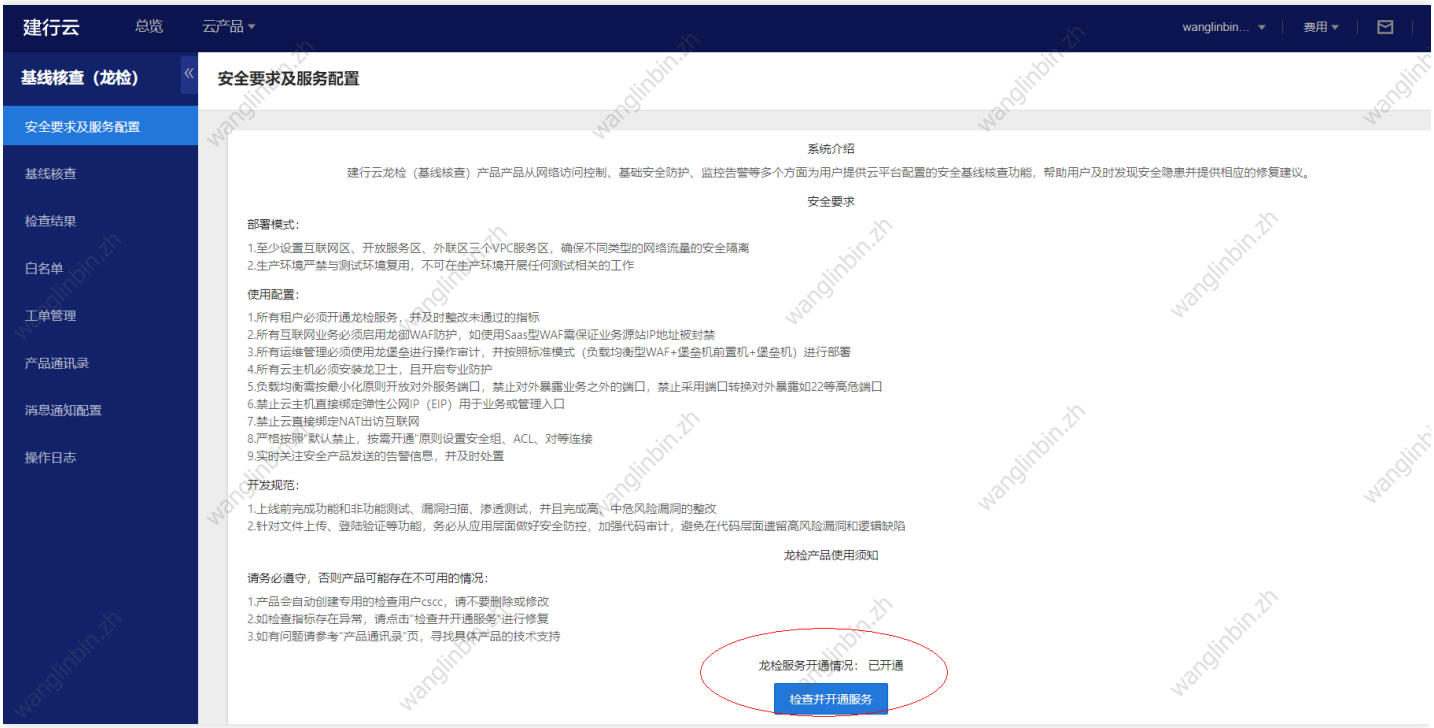
1. 开通服务 使用主账户登录建行云租户控制台，选择云产品–基线核查（龙检）–开通服务，点击立即开通。


2. 点击访问管理，查看是否cscc用户新增成功

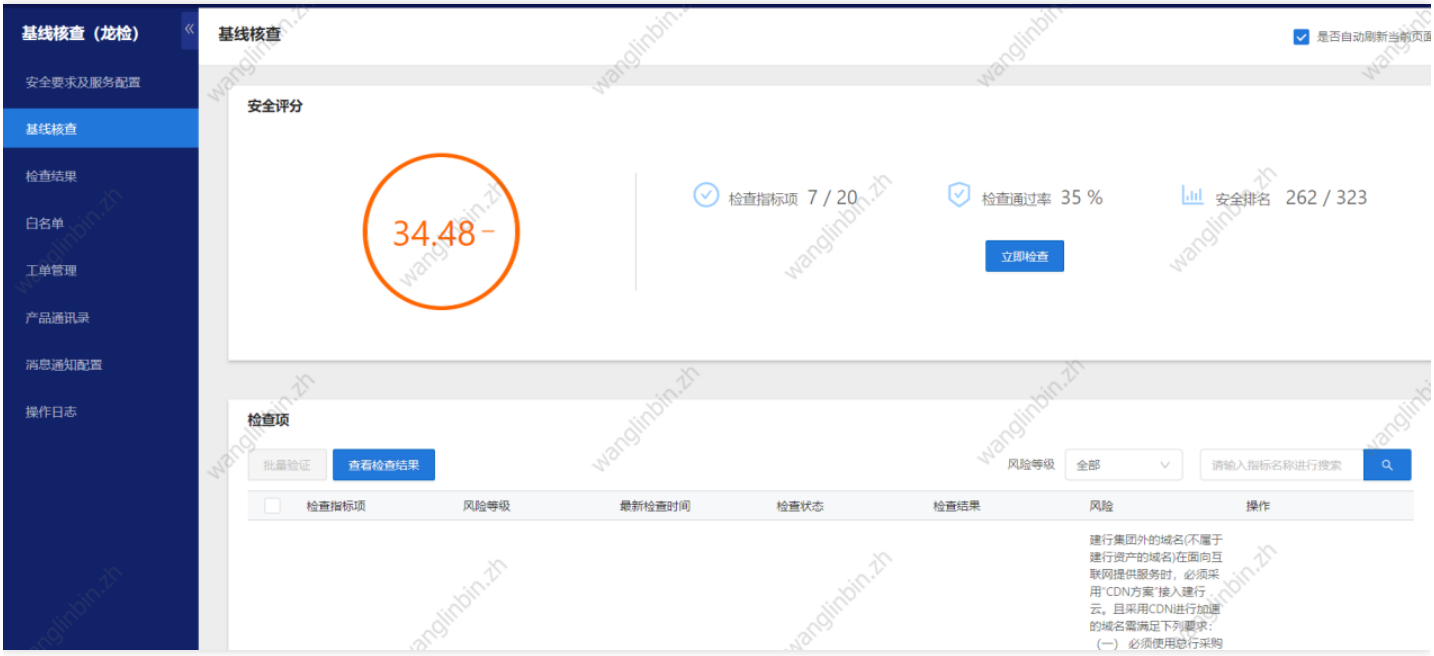




3. 如果用户不存在，进入安全要求及服务配置，点击检查并开通服务




## 4. 执行立即检查，查看基线检查结果是否正常显示分数



# 执行基线核查任务

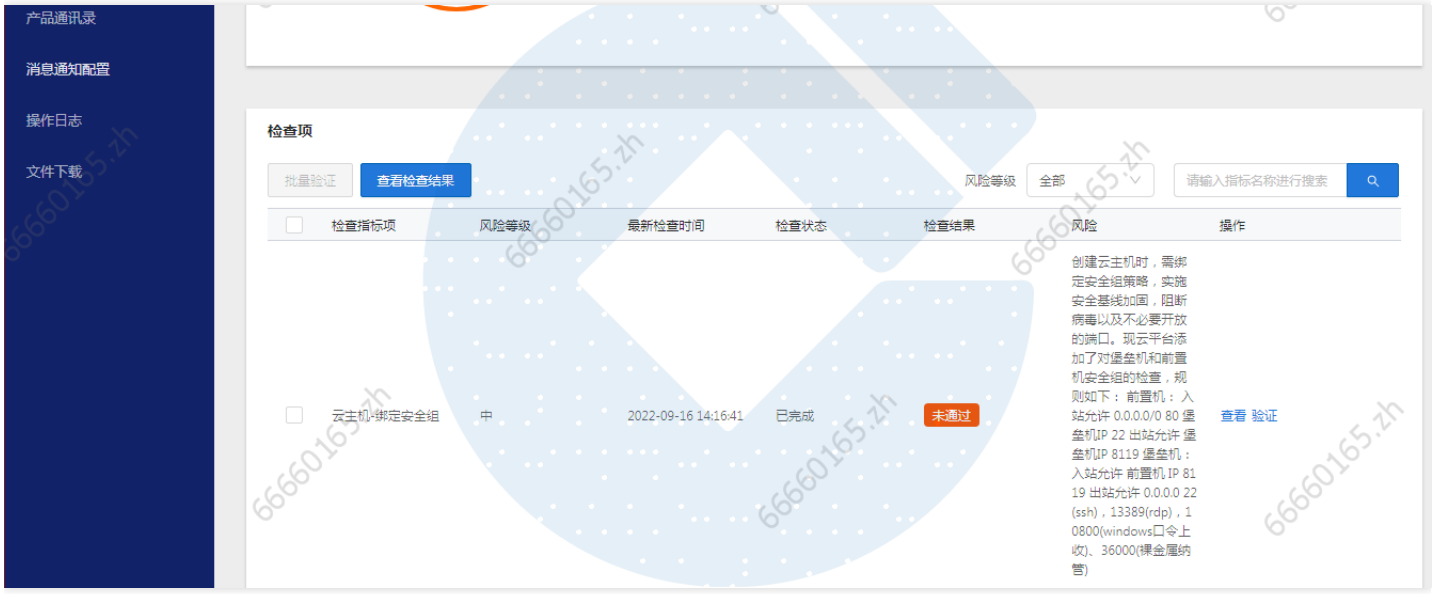
最近更新时间: 2022-10-31 18:13:54

登录建行云租户控制台，选择云产品-基线核查（龙检）-基线核查，点击立即检查

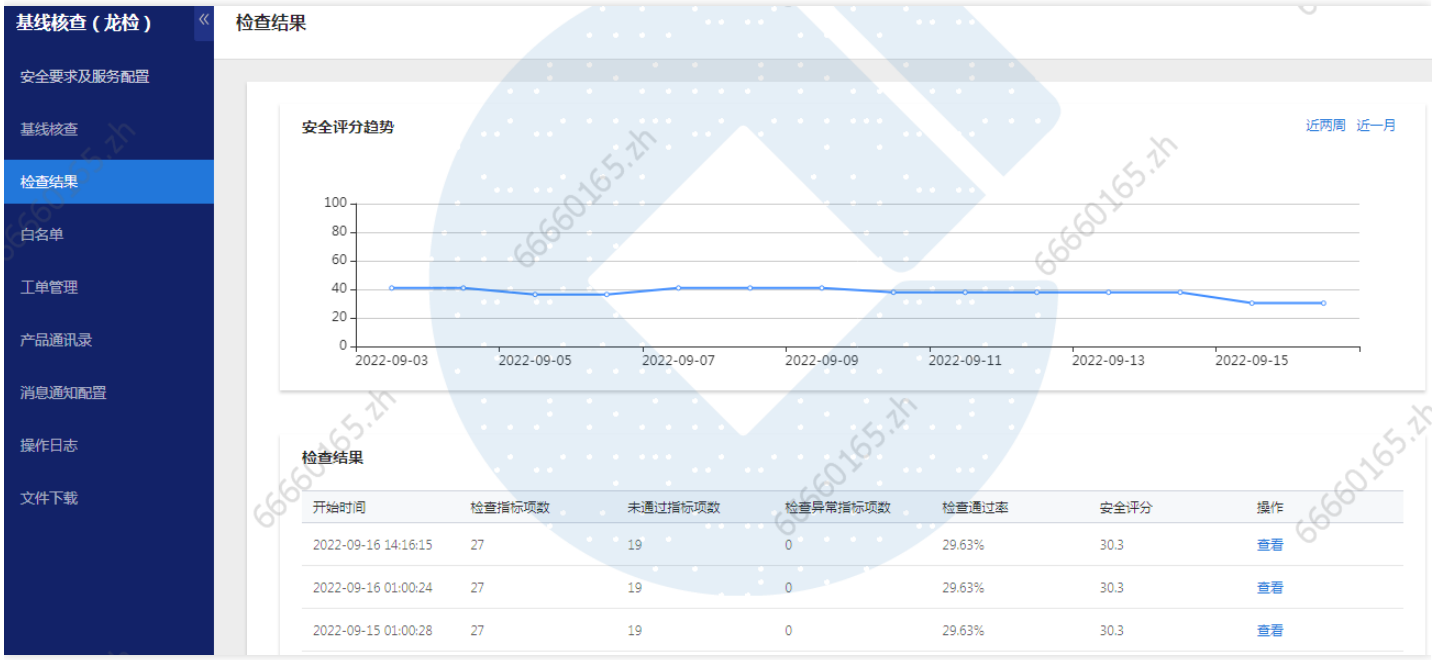
# 查看检查结果

最近更新时间: 2022-10-31 18:13:54

方式一：进入基线核查页面，界面中展示最近一次检查任务的执行结果，点击具体检查指标项的“查看”按钮，可查看该指标未通过明细详情。




方式二：进入检查结果页面，页面中展示龙检安全评分趋势图，以及所有任务检查结果列表，点击任务明细右侧“查看”按钮，展示该任务所有指标结果及未通过明细。




方式三：进入检查结果页面，点击任务明细右侧“查看”按钮后，可点击页面右上角“xls下载”按钮，出本次任务检查结果XLS文件到本地。

备注：xls下载点击后系统提交下载任务至后台，租户需进入文件下载页面中，查看下载任务执行进度，待文件生成后点击下载。


此外，龙检提供了龙卫士漏洞明细文件下载功能用于解决租户无法在龙卫士产品中下载所有漏洞明细数据的问题（该问题受限于cos产品网络访问控制）。

# 指标验证

最近更新时间: 2022-10-31 18:13:54

1.针对检测未通过的单指标进行验证

如果您对部分配置项进行了修改，在云产品-基线核查（龙检）-基线核查的检查项列表，定位到该配置检查项，单击”验证”，检查配置整改后是否还存在安全风险。


2. 针对检测未通过的多指标进行验证

如果您对部分配置项进行了修改，在基线核查的检查项列表，勾选配置检查项，单击批量验证，检查修改后是否还存在安全风险。


**备注：指标验证将不会对当前龙检分数产生影响，如果您希望获取问题整改后的最新龙检分数，请至基线核查页面点击“立即检查”，发起全量指标检查和分数计算任务。**

# 添加白名单

最近更新时间: 2022-10-31 18:13:53

1. 对检测未通过的指标进行临时加白

   目前可针对云WAF-自定义规则、弹性IP等指标进行加白操作，下面以云WAF-自定义规则举例。点击加入白名单即可创建工单进行加白申请。


备注：

 申请提交白名单时，因审核机制十分严格，一定要注明申请白名单原因，已经实施的安全措施，是否已向安全团队申报（特殊情况需要发正式的告知函及通知），以及备注联系人、电话及邮箱。

 设置生效时间：按需设置该白名单提交后的有效使用期限，当白名单申请在有效期内，指标项加白有效，反之无效

2.查看白名单

当运营端审批通过后，可在白名单菜单看到域名的白名单，已通过的白名单按指标分类到不同的指标组中，状态为“未失效“说明该指标项加白有效，状态为”已失效“，加白申请已过期，指标项恢复到未加白情况。


基线核查（龙检）
安全要求及服务配置
基线核查
检查结果
白名单
工单管理
产品通讯录
消息通知配置
操作日志
文件下载
白名单
弹性IP
云WAF-源站封禁配置
负载均衡-无WAF防护的业务
云WAF-WAF配置模式
云WAF-自定义规则
环境安全-存在开发环境
请输入IP进行搜索
创建时间
租户APPID
内网IP
EIP
生效指标
有效期至
状态
备注
操作
2022-07-14 19:20:51
1255000011
33.33.2.0
33.22.3.0
弹性IP
2022-07-15 00:00:00
已失效
test
取消加白
2022-07-14 19:20:51
1255000011
23.33.31.0
12.33.2.0
弹性IP
2022-07-15 00:00:00
已失效
test
取消加白
共 2 条
1
10 条/页

# 产品通讯录

最近更新时间: 2022-10-31 18:13:53

产品通讯录记录了指标项涉及的相关安全产品技术支持人员联系信息以提供资询

# 常见问题

# 配置核查服务包含哪些检查项?

最近更新时间: 2022-10-24 10:52:12

配置核查（龙检）检查项目前包含弹性IP、负载均衡、云主机、龙卫士、龙巢、龙御、龙堡垒、龙巡等云产品，共27个检查指标。

| 检查指标项 | 风险等级 | 风险 |
| --- | --- | --- |
| 外部域名接入规范 | 中 | 建行集团外的域名(不属于建行资产的域名)在面向互联网提供服务时，必须采用“CDN方案”接入建行云。且采用CDN进行加速的域名需满足下列要求： （一） 必须使用总行采购的CDN厂商（截止到2023年为网宿、阿里）。如果采购阿里CDN服务，需采购建行定制版服务。如果采购网宿CDN服务，需通知网宿将账号配置在ccb_cloud账号下，确保可有效进行联动封禁。（二） 采用CDN进行加速的必须为标准HTTP/HTTPS业务。 （三） 必须将真实的客户端IP通过XFF字段传给建行云。<br>此外已使用CDN方案的域名，在配置龙御WAF时需配置“是否使用代理模式”为“是”，以便WAF可以获取真实客户端地址。 |
| 弹性IP | 高 | 禁止云主机直接绑定弹性公网IP（EIP）用于业务或管理入口，可使用负载均衡对外提供服务，使用NAT实现互联网出访。 |
| 负载均衡–高危端口 | 高 | 应根据“最小化原则“开放对外服务端口，禁止对外暴露业务之外的端口。如将高危端口暴露在互联网，则存在暴力破解、漏洞利用等风险。 |
| 负载均衡–无WAF防护的业务 | 高 | 创建网站服务时，必须启用云WAF防护，以有效检测和防御针对WEB网站的入侵行为。 |
| 云WAF–外联业务防护配置 | 中 | 建行公有云支持通过PLA专线实现租户与自有数据中心、外联单位、建行私有云互通，当租户作为外联服务提供方时，必须启用云WAF防护，以有效检测和防御针对HTTP/HTTPS应用服务的入侵行为。 |

| | | |
|---|---|---|
| 云WAF–WAF启用 | 高 | 所有互联网业务必须启用云WAF，且WAF开关为开启。如不开启，WAF不会进行攻击检测，导致WAF防护失效。 |
| 云WAF–WAF配置模式 | 高 | 所有互联网业务必须启用云WAF，且开启拦截模式。如开启的为观察模式，则只会记录攻击日志，并不阻断攻击，导致WAF防护失效。 |
| 云WAF–门神规则 | 中 | 所有互联网业务必须启用云WAF，且开启所有检测功能。同时，不可关闭任何的内置规则。 |
| 云WAF–IP白名单 | 中 | 所有互联网业务必须启用云WAF，如果添加IP白名单，则此IP进行的访问请求都不会进行攻击检测和拦截。 |
| 云WAF–规则白名单 | 中 | 所有互联网业务必须启用云WAF，且开启所有检测功能。同时，不可加任何的规则白名单。 |
| 云WAF–自定义规则 | 中 | 所有互联网业务必须启用云WAF，且不可添加放行的自定义规则。如果添加了放行的自定义规则，则此规则匹配的请求将没有云WAF防护。 |
| 云主机–龙卫士防护 | 高 | 创建云主机时，需开启龙卫士主机安全的专业防护，以有效检测针对主机的暴力破解、异常登录和木马攻击等入侵行为。 |
| 云主机–龙卫士告警 | 中 | 龙卫士主机安全产品有效检测云主机的暴力破解、异常登录和木马攻击等入侵行为。 |
| 云主机–存在开发环 | 高 | 建行云不允许在生产环境进行开发测试，否则存在源码泄漏等风险；不允许部署高危服务，否在存在被攻击利用的风险。 |

| | | |
|---|---|---|
| 境/高危服务 | | |
| 龙巢–本地镜像配置 | 中 | 建行云提供龙巢（容器安全）产品，要求租户打开本地镜像扫描开关，保证可以及时发现本地镜像中的安全漏洞、敏感信息、木马病毒等。 |
| 龙巢–运行时安全配置 | 中 | 建行云提供龙巢（容器安全）产品，要求租户打开容器逃逸监控开关，保证可以及时发现容器逃逸事件。 |
| 龙巢–安全事件数量 | 中 | 建行云提供龙巢（容器安全）产品，可以有效检测运行时风险，包括容器逃逸、反弹shell、异常进程、文件篡改、高危系统调用，要求租户关注告警内容，及时处理。 |
| 龙巡–标准部署模式 | 高 | 建行云提供龙巡（漏洞扫描）产品，要求租户按部署规范在每VPC部署龙巡服务器。 |
| 龙巡定期漏扫 | 中 | 当主机资产发生变化，当不断有新漏洞被发现和利用，都会增加资产安全风险，如果不定期对资产进行漏洞扫描就无法发现这些新的安全风险。 |
| 云主机–漏洞 | 高 | 建行云定期对云服务器进行漏洞扫描，所有漏洞都应及时整改，否则存在利用漏洞进行攻击的风险。 |
| 龙堡垒–标准部署模式 | 高 | 建行云不允许将内网堡垒机直接面向互联网暴露,否则存在攻破利用等风险。 |
| 龙堡垒–应急通道配置 | 高 | 龙堡垒为运维产品，直接面向互联网存在巨大风险隐患。 |
| 龙堡垒–版 | 高 | 龙堡垒产品为运维审计产品，集中纳管后可实现后台统一版本管理及漏洞升级，从而避免低版本可能存在的漏洞风险。 |

| | | |
|---|---|---|
| 本及集中纳管 | | |
| 云主机–绑定安全组 | 中 | 创建云主机时，需绑定安全组策略，实施安全基线加固，阻断病毒以及不必要开放的端口。现云平台添加了对堡垒机和前置机安全组的检查，规则如下： 前置机： 入站允许 0.0.0.0/0 80 堡垒机IP 22 出站允许 堡垒机IP 8119 堡垒机： 入站允许 前置机 IP 8119 出站允许 0.0.0.0 22(ssh)，13389(rdp)，10800(windows口令上收)、36000(裸金属纳管) |
| 安全组–基础策略 | 中 | 需严格遵守“默认禁止，按需开通”的原则，合理约束网络访问策略，规避恶意访问和安全威胁，从而有效保障云上资源的安全稳定运行。 龙巡特定安全组（名称为ScannerSecurityGroup）的入站规则为0.0.0.0 端口为ALL 拒绝，出站规则为0.0.0.0 端口ALL 允许； 其他安全组的不可出现0.0.0.0 端口ALL 接受的入站或出站规则。 |
| 证书–过期提醒 | 低 | 客户访问证书过期的网站将显示网站不安全的提醒，影响企业信任度。且存在数据传输、数据泄露的风险。 |
| 资产探测–风险数据 | 高 | 建行云不允许面向互联网保留高危服务或风险路径，否则存在数据泄漏等风险。 |

*具体处置方案请参考基线核查>检查项>点击相应检查指标项后的“查看”，在最下方整改建议

# 配置核查服务是否需要手动执行?

最近更新时间: 2022-10-24 10:52:12

开通基线核查（龙检）服务后，会使用默认策略对所有资产进行检测。默认策略自动检测时间：每天00:00-08:00，默认检测对象：您账号下的资产，默认检测范围：所有配置核查检查指标。您也可以手动执行全面的检查或者执行特定指标。

# 云主机–绑定安全组指标不合规如何排查

最近更新时间: 2022–10–24 10:52:12

不合规详情中明细中的“正确的安全组”栏位已提示按要求该主机允许配置的安全组出入站规则的最大集合，（如只提示入站规则，则说明出站合规，租户仅需要排查入站规则），租户将本主机当前配置与提示内容进行比对，超过此范围内的安全组配置即导致指标不合规的原因，如ICMP入站规则等，删除后重新验证指标。

# 外部域名接入规范指标不合规如何排查（外部域名已经在CDN厂商进行加速）

最近更新时间: 2022-10-24 10:52:12

查看不合规详情中明细中提示的具体原因，如果“CDN厂商”已显示厂商名称，且“是否联动封禁”提示为是，但是“龙御WAF是否开启代理模式”为否，说明原因为WAF配置错误，租户需将域名的WAF配置模式中的“是否使用代理”修改为是；如果“CDN厂商”提示为“未上CDN”，可能存在两种原因，一是未按照我行要求将域名配置在建行账号下（此情况需联系网络协助解决），二是CLB+WAF侧和CDN侧配置的泛域名或子域名不一致导致。