**阿里云配置安全检查**

# 身份认证及权限

## 云平台-主账号双因素认证配置检查

检查描述

在只使用单一密码认证的情况下，黑客可能通过暴力破解等手段获取您的云平台管理密码。建议对云平台管理员账号开启密码加手机短信双重身份认证，防止密码泄露带来的安全隐患。

指导方案

[进入阿里云后台，顺序操作：管理控制台-账号管理-安全设置-虚拟MFA-设置](https://account.console.aliyun.com/#/selectVerificationMethod)

帮助资源

1、使用多重机制保护主账户安全原理：

<https://help.aliyun.com/document_detail/28643.html>

2、设置MFA方法：

<https://help.aliyun.com/document_detail/28635.html>

# 网络访问控制

## SLB-高危端口暴露检查

检查描述

应依据“最小服务”原则设定SLB转发策略，只转发必要的公共服务端口（如：80、443等）至公网，其他端口不应进行转发，如被SLB发布到公网会增加系统遭受外部黑客攻击的风险。

指导方案

进入“管理控制台-负载均衡-SLB实例-监听”处进行配置。

帮助资源

<https://help.aliyun.com/document_detail/27541.html>

## 安全组-RDS白名单配置检查

检查描述

数据库服务（RDS）端口不应直接对公网所有地址开放，应设定严格的访问控制策略，只允许特定的IP（如WEB应用服务器）可以访问数据库服务。

威胁影响

| 所在可用区 | 数据库实例ID | 数据库实例描述 | 白名单名称 | 问题条目值 |
| --- | --- | --- | --- | --- |
| 暂无风险 | | | | |

指导方案

进入管理控制台-云服务器数据库RDS-数据安全性-添加白名单分组，删除'0.0.0.0/0'条目，添加可信IP条目。

帮助资源

<https://help.aliyun.com/document_detail/26198.html>

# 日志审计

## 云平台-操作审计配置检查

检查描述

云安全体系要求云平台开启操作审计功能，操作日志需保存在对象存储服务(OSS)中，并合理设置日志的访问权限，以实现高危操作可追溯。

1.未开通操作审计时系统对管理员在平云台的操作行为不进行记录，当发生恶意操作时将无审计数据可查，难以定责；

2.不满足合规要求，例如：等级保护、ISO/IEC27001、PCI-DSS

指导方案

[进入管理控制台-操作审计，开启操作审计服务，并按照页面提示和相关帮助文档配置OSS Bucket存储日志。](https://actiontrail.console.aliyun.com/?#/trail/config)

帮助资源

<https://help.aliyun.com/document_detail/28810.html>

# 数据安全

## RDS-数据库安全策略检查

检查描述

1、云安全体系要求数据库开启SQL审计功能，以保证发生脱库、数据篡改或误操作事件时有据可查。

2、云安全体系要求数据库开启加密传输（SSL）功能，以确保数据在传输、存储过程中的安全性,防止攻击者窃取数据库账号和密码。

3、云安全体系要求数据库开启透明数据加密（TDE）功能，以确保数据在存储过程中的安全性，防止攻击者直接拿到明文数据库文件。

指导方案

进入管理控制台-云服务器数据库RDS-数据安全性，进行下列配置：

1.点击标签""SQL审计""，开启SQL审计；

2.点击标签”SSL“，设置SSL，依据向导和帮助文档进行设置；

3.点击标签”TDE“，开通TDE（需先开通秘钥管理服务KMS）

更多说明请参见帮助文档。

帮助资源

1、SQL审计：

<https://help.aliyun.com/document_detail/26197.html>

2、设置 SSL 加密：

<https://help.aliyun.com/document_detail/32474.html>

3、设置透明数据加密（TDE）：

<https://help.aliyun.com/document_detail/33510.html>

## OSS敏感文件泄露

检查描述

根据oss文件管理相关策略，对于存储某些重要信息的文件需要设置相关访问权限

指导方案

请自查上述oss对应实例中的文件权限设置是否合理，建议增加访问权限控制

帮助资源

[https://help.aliyun.com/document\_detail/31929.html](https://help.aliyun.com/knowledge_detail/57754.html)

# 基础安全防护

## WEB防护-云盾WAF

检查描述

云安全防御体系中需要部署WAF，用于解决WEB防护问题。

未部署云盾WAF服务会使系统缺乏对各种Web攻击行为的防护能力，黑客有可能利用WEB漏洞对您的业务系统进行攻击，进而造成数据泄露、网页篡改等安全事件发生。

指导方案

[建议购买更高级别的云盾WAF服务，并将所有网站域名加入WAF防护列表中。](https://yundun.console.aliyun.com/?p=waf#/waf/main/setting)

帮助资源

<https://help.aliyun.com/product/28515.html>