**北京沃丰时代数据科技有限公司**

**网络安全方案**

**文档信息：**

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** | 网络安全方案 | | |
| **文档编号** | WF-DM007 | | |
| **文档密级** | 内部 | **发布范围** | 公司内部 |
| **编制人** | 韦昭 | **编制日期** | 2019-12-19 |
| **评审人** | 周毅 | **评审日期** | 2023-03-23 |
| **批准人** | 张磊 | **批准日期** | 2023-04-23 |

**修订历史记录：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **状态** | **修订内容说明** | **修订日期** | **编制人** |
| V1.0 | 新建 | 新增 | 2019-12-19 | 韦昭 |
| V1.1 | 修订 | 修订文档信息 | 2023-04-23 | 张帆 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 目录

1. 概述 3

1.1. 目标 3

1.2. 范围 3

1.3. 术语 3

2. 账号及登录管理 3

2.1. 云平台账号管理 3

2.2. jumpserver 4

3. 网络访问控制(ACL) 4

3.1. 生产网络 4

3.2. 办公网络 5

3.3. 测试网络及服务器 6

4. 项目配置管理 6

5. 主机病毒防护 6

# 概述

本文档描述Udesk 在生产和开发过程中如何保证安全,防止信息泄漏,病毒或黑客的侵犯等.

## 目标

防止公司资产,包括代码,主机,网络不受信息泄漏,病毒或黑客的攻击

## 范围

资产范围包括:代码,主机,网络

活动范围包括: 开发,生产,运维及办公

## 术语

* Udesk: 即沃丰时代数字有限公司
* 开发组接口人: 为各项目或项目组负责人
* 安全运营: 负责研发安全运营

# 账号及登录管理

Udesk 的运维账号主要包括: 阿里云,腾讯云,jumpserver，所有账号以人为ID的原则建立，可以做到可追踪。

# 云平台账号管理

云平台账号包括阿里云账号,腾讯云账号

* 由研发主管管理,各开发组接口人可向研发主管申请子账号
* 阿里云账号要求使用多因素认证(MFA),各开发组接口人向研发主管申请配置
* 默认开发组接口人只有只读权限

# jumpserver

jumpserver 为生产主机的入口,账号由运维组进行管理和维护.

* 运维组负责jumpserver账号的创建,维护和离职清除
* jumpserver 要求使用多因素认证,配置由运维负责
* 权限分配为最小权限原则

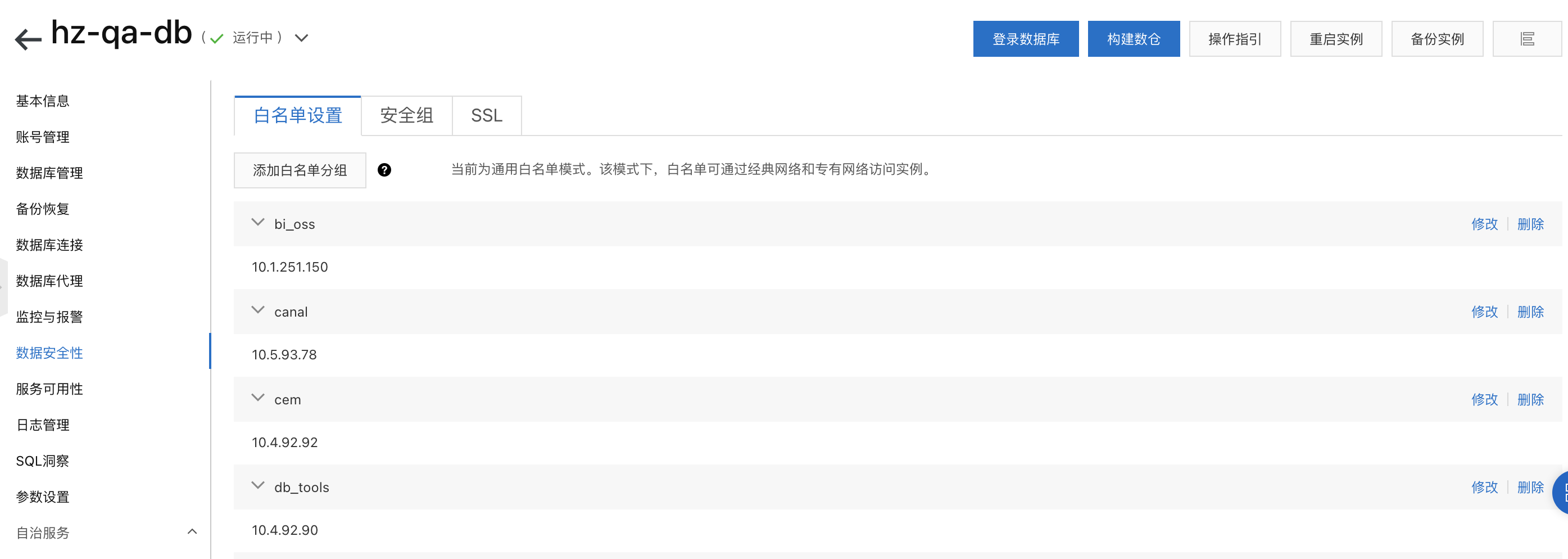
# 网络访问控制(ACL)

ACL 主要保证网络及主机安全.

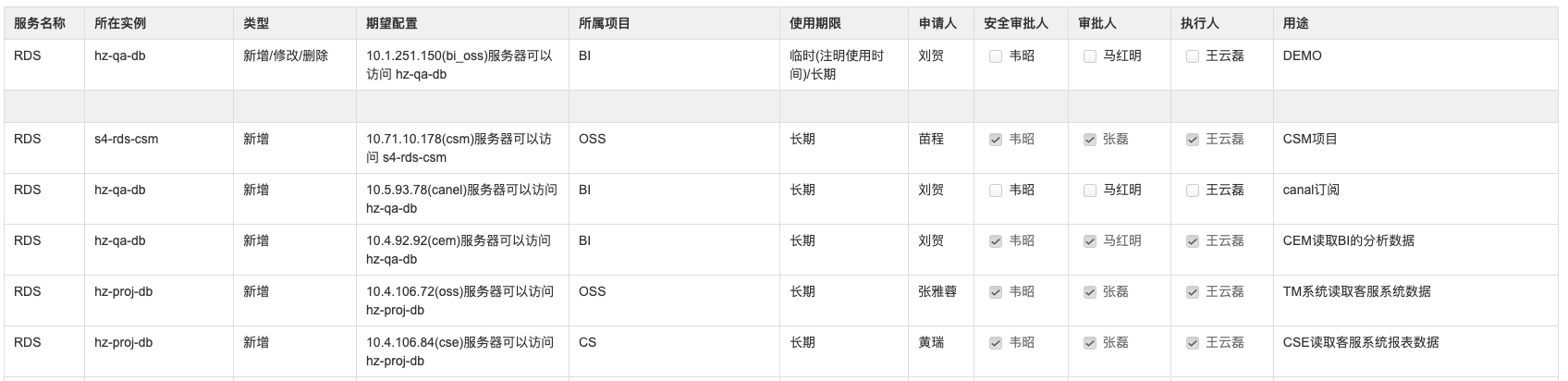
Udesk 的服务器分为三部分,生产,测试及办公系统.

# 生产网络

* Udesk 生产网络由阿里高防提供 DDOS 防护,生产入口必须经过高防
* Udesk http 服务由阿里Web应用防火墙(WAF)提供应用防护,WAF 在高防之后
* 生产网络维护入口(ssh)管理
  + 要用安全组保护,仅允许公司办公室 IP 及研发 VPN ip 登录
  + 研发人员查线上问题,需要登录服务器的,通过 jumpserver 登录
  + 管理人员(运维,安全运营,研发主管,发版主管)登录,可以通过跳板机(bastion) 登录
  + bastioin/jumpsever 均由运维组进行维护
* 生产网络严禁对外网开启高危端口
  + 包括: 3389,3306,6379,27017,5432,135,137,138,139,445,21
  + 安全运营每天对生产进行扫描,并巡检,见 udesk\_greatwall->ip->高危端口
* 生产网络服务组件管理
  + 服务组件不可以通过公网访问，只可以在服务器集群内部访问。
  + 服务组件禁止使用默认端口。
  + 服务组件需要被服务器集群内部机器访问需要配置IP白名单，服务组件IP白名单配置示例如下。



* + 服务组件IP白名单配置必须提交变更申请，由研发业务线技术负责人提交申请，由安全负责人和技术总监审批，由运维人员完成配置。服务组件IP白名单配置审批记录如下。



# 办公网络

办公网络包括自建运营运维及第三方 jira等

* 办公系统端口均需要安全组保护,仅限公司 ip 访问,安全组由运维组维护
* 办公系统域名需要经过confluence/域名配置备案(申请域名),安全运营确保已经受到安全组保护才可放行
* 办公系统有特殊要求需要外网访问,必须在备案中由开发组接口人说明
* 办公系统服务器维护走 ssh 入口,权限由运维组管理,ssh 入口仅允许公司 ip 访问

# 测试网络及服务器

测试网络及服务器是用于测试组 QA 测试的环境

* 测试环境维护部署由使用 ssh,ssh 入口仅公司 ip 可以访问
* 测试环境ssh证书可由开发/测试人员添加
  + 由运维组对已离职人员证书进行清除
  + 安全运营对所有机器上证书进行评审,见udesk\_greatwall->键值,保证证书都是本公司成员.

# 项目配置管理

项目配置管理负责保护公司源代码资产的安全

详见<<沃丰时代软件配置管理（2019）.doc>>

# 主机病毒防护

本公司服务器主机需要安装

* 主机入侵检查系统(hids): wazuh,见 https://oss.udesk.cn
* 反病毒rootkit软件: clamav/rkhunter
* 由安全运营负责安装