# 系统部署环境安全方案

# 目 录

[系统部署环境安全方案 1](#_Toc22282)

[目 录 1](#_Toc4045)

[1. 前言 3](#_Toc25332)

[1.1. 概述 3](#_Toc21278)

[1.2. 目标 3](#_Toc24557)

[1.3. 范围 3](#_Toc4873)

[1.4. 版本信息 3](#_Toc22736)

[1.4.1. 当前版本 3](#_Toc26394)

[1.4.2. 版本历史 3](#_Toc26250)

[1.5. 名词、解释 4](#_Toc19903)

[1.6. 参考资料 4](#_Toc31297)

[2. 采用解决方案 4](#_Toc22089)

[3. 资源权限初步分配 5](#_Toc17852)

[3.1. 角色列表 5](#_Toc13360)

[3.2. 资源类型列表 6](#_Toc7193)

[3.3. 角色资源类型权限 6](#_Toc19842)

[4. 资源权限详细分配 7](#_Toc13579)

[4.1. 云主机管理UI 7](#_Toc9621)

[4.1.1. 权限列表 7](#_Toc20281)

[4.1.2. 角色权限说明 7](#_Toc20084)

[4.1.3. 角色权限详单 7](#_Toc21117)

[4.2. 云主机Shell 7](#_Toc7848)

[4.2.1. 权限列表 8](#_Toc22789)

[4.2.2. 角色权限说明 8](#_Toc5701)

[4.2.3. 角色权限详单 9](#_Toc30053)

[4.3. 数据库 11](#_Toc22393)

[4.3.1. 权限列表 11](#_Toc16163)

[4.3.2. 角色权限说明 12](#_Toc530)

[4.3.3. 角色权限详单 13](#_Toc28973)

[4.4. OSS对象存储 14](#_Toc19222)

[4.4.1. 权限列表 14](#_Toc6876)

[4.4.2. 角色权限说明 15](#_Toc22909)

[4.4.3. OSS权限详单 15](#_Toc112)

[5. 开发角色对应设置 15](#_Toc23813)

[5.1. 开发环境 15](#_Toc9512)

[5.2. 测试环境 16](#_Toc31877)

[5.3. 生产环境 16](#_Toc19152)

[6. 附注说明 17](#_Toc30652)

# 前言

## 概述

针对目前开发环境，测试环境及生产环境中部署中的资源（含云主机，数据库及部署的程序等）需要统一进行安全管理，以保证系统系统在日常运维和使用中的安全。

## 目标

为目前部署的开发环境，测试环境及生产环境提供一套行之有效的日常运维的安全方案，以切实保障各环境的系统安全。

## 范围

* 公司决策管理层
* 运维护人员
* 测试人员

## 版本信息

### 当前版本

* 编 制 人：张洪波
* 编制日期：2018年10月23日
* 当前版本：1.0
* 版本说明：初始发布版本

### 版本历史

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **版本号** | **类型** | **说明** | **撰写人** | **发布日期** | **备注** |
| 1 | V1.0 | 创建 | 初始版本 | 张洪波 | 2018/10/23 |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |

## 名词、解释

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名词** | **英文缩写** | **解释** | **备注** |
| 1 | 对象存储服务 | OSS | 阿里云对象存储服务（Object Storage Service，简称OSS），是阿里云对外提供的海量、安全、低成本、高可靠的云存储服务。您可以通过本文档提供的简单的REST接口，在任何时间、任何地点、任何互联网设备上进行上传和下载数据。基于OSS，您可以搭建出各种多媒体分享网站、网盘、个人和企业数据备份等基于大规模数据的服务。 |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |

## 参考资料

暂无

# 采用解决方案

对目前环境中的资源采用权限“最小化原则”按角色进行授权，统一进行权限管理以切实保证系统的安全。



注：在实际中采用“角色权限为为主 + 用户权限为辅”的方式使得权限管理更加灵活，方便和实用。

# 资源权限初步分配

## 角色列表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **资源角色说明** | | | | | | | | |
| **序号** | **角色** | **资源权限** | | | | | | **备注** |
| **涉及所有权限** | **可能涉及常用权限** | **常用权限** | **用到的权限** | **公开资源** | **是否可授权** |  |
| 1 | 超级管理员 | **有** | 有 | 有 | 有 | 有 | 是 |  |
| 2 | 管理员 |  | **有** | 有 | 有 | 有 | 否 |  |
| 3 | 项目超级管理员 |  | **有** | 有 | 有 | 有 | 否 |  |
| 4 | 项目管理员 |  |  | **有** | 有 | 有 | 否 |  |
| 5 | 普通用户 |  |  |  | **有** | 有 | 否 |  |
| 6 | 匿名用户 |  |  |  |  | 有 | 否 |  |
| 7 | **备注说明** |  | | | | | |  |

## 资源类型列表

|  |  |  |  |
| --- | --- | --- | --- |
| **环境中资源权限控制** | | | |
| **序号** | **资源** | | **备注说明** |
|  | **环境** | **主机资源** |
| 1 | 开发环境 | 云主机管理UI |  |
| 2 | 云主机Shell |  |
| 3 | 数据库 |  |
| 4 | OSS对象存储 |  |
| 5 | 测试环境 | 云主机管理UI |  |
| 6 | 云主机Shell |  |
| 7 | 数据库 |  |
| 8 | OSS对象存储 |  |
| 9 | 生产环境 | 云主机管理UI |  |
| 10 | 云主机Shell |  |
| 11 | 数据库 |  |
| 12 | OSS对象存储 |  |
| 13 | 其它公共资源 | 如域名，邮箱，微信服务号等 |  |
| 14 | **备注说明** |  |  |

## 角色资源类型权限

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **环境中资源权限控制** | | | | | | | | |
| **序号** | **资源** | **权限** | | |  |  |  | **备注说明** |
| **主机资源** | **超级管理员** | **管理员** | **项目超级管理员** | **项目管理员** | **普通用户** | **匿名用户** |
| 1 | 云主机管理UI | 有 |  |  |  |  |  |  |
| 2 | 云主机Shell | 有 | 有 | 有 | 有 |  |  |  |
| 3 | 数据库 | 有 | 有 | 有 | 有 | 有 |  |  |
| 4 | OSS对象存储 | 有 |  |  |  | 有 | 有 |  |
| 5 | 其它公共资源，如域名，邮箱，微信服务号等 | 有 |  |  |  |  |  |  |
| 6 | **附注说明** | 标灰色的内容表示不存在的 | | | | | |  |

# 资源权限详细分配

## 云主机管理UI

云主机管理UI是云主机供应商官方提供的云主机管理UI，可以对虚拟主机，虚拟主机网络，安全组等进行管理。

### 权限列表

|  |  |  |  |
| --- | --- | --- | --- |
| **云主机管理UI** | | | |
| **序号** | **权限** | **权限说明** | **备注说明** |
| 1 | 主机管理 | 主机状态查看，关闭和启动系统，重装系统，设置安全组等 |  |
| 2 | 备注说明 |  |  |

### 角色权限说明

* 超级管理员

该云主机管理UI只有一个超级管理员帐号。因此云主机管理UI目前只针对超级管理员。

### 角色权限详单

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **云主机管理UI权分配** | | | | | | | |
| **序号** | **权限** | **超级管理员** | **管理员** | **项目超级管理员** | **项目管理员** | **普通用户** | **备注说明** |
| 1 | 主机管理 | √ |  |  |  |  |  |
| 2 | **备注说明** |  |  |  |  |  |  |

## 云主机Shell

主机Shell含目前的Xshell以及Xftp工具在内权限。

### 权限列表

详见本章节中的《角色权限详单》

### 角色权限说明

* 超级管理员

云主机Shell是云主机提供的控制台命令窗口（借助工具可以进行文件资源管理），该Shell由云主机供应商提供帐号，该帐号针对目前的超级管理员。

* 管理员

此外在操作系统中设置管理员用户对目前环境中项目涉及到的目录文件（含可执行Sh文件及安装环境中的文件在内）设置管理员用户。

* 项目超级管理员

项目超级管理员则针对本项目涉及的目录文件。

* 项目管理员

项目管理员由针则针对本项目涉及到一般情况下经常使用的目录及文件。

### 角色权限详单

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **云主机权限** | | | | | | | | | |
| **序号** | **资源类型** | | **权限** | **超级管理员** | **管理员** | **项目超级管理员** | **项目管理员** | **普通用户** | **备注** |
| 1 | 磁盘 | 磁盘文件（一般磁盘文件） | 读 | √ | √ |  |  |  |  |
| 2 | 写 | √ | √ |  |  |  |  |
| 3 | 删 | √ | √ |  |  |  |  |
| 4 | 执行 | √ | √ |  |  |  |  |
| 5 | 环境程序文件如Tomcat,Nginx，Redis等 | 读 | √ | √ | √ |  |  |  |
| 6 | 写 | √ | √ | √ |  |  |  |
| 7 | 删 | √ | √ | √ |  |  |  |
| 8 | 执行 | √ | √ | √ |  |  |  |
| 9 | 部署程序文件 | 读 | √ | √ | √ | √ |  |  |
| 10 | 写 | √ | √ | √ | √ |  |  |
| 11 | 删 | √ | √ | √ | √ |  |  |
| 12 | 用户权限 | 用户授权（创建，删除，用户，授权用户等） | 用户授权 | √ |  |  |  |  |  |
| 13 | 用户组授权（创建，删除，用户，授权用户组，加入用户等） | 用户组授权 | √ |  |  |  |  |  |
| 14 | 主机管理 | 安全组 | 加入安全组 | √ |  |  |  |  |  |
| 15 | 密钥绑定 | 绑定密钥 | √ |  |  |  |  |  |
| 16 | 修改密码 | 修改密码 | √ |  |  |  |  |  |
| 17 | 主机管理 | 查看主机状态，重启服务器等 | √ |  |  |  |  |  |
| 18 | 其它 | 其它操作 | √ |  |  |  |  |  |
| 19 | 域名 | 绑定IP | √ |  |  |  |  |  |

## 数据库

### 权限列表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **数据库权限说明** | | | | | |
| **序号** | **权限** | **权限说明** | **ServerPlivilegs** | **Plivilegs** | **备注** |
| 1 | Alter | 更改表，比如添加字段、索引、修改字段等 | √ | √ |  |
| 2 | Alter Routine | 更改存储过程权限 | √ | √ |  |
| 3 | Create | 创建数据库、表或索引权限 | √ | √ |  |
| 4 | Create Routine | 创建存储过程权限 | √ | √ |  |
| 5 | Create Temporary Tables | 允许创建临时表的权限 | √ | √ |  |
| 6 | Create User | 创建用户权限 | √ |  |  |
| 7 | Create View | 创建视图权限 | √ | √ |  |
| 8 | Delete | 删除数据权限 | √ | √ |  |
| 9 | Drop | 删除数据库或表权限 | √ | √ |  |
| 10 | Event | 表示拥有创建，修改，执行和删除事件（event）的权限 | √ | √ |  |
| 11 | Execute | 允许执行存储过程的权限 | √ | √ |  |
| 12 | File | 服务器主机上的文件访问 文件访问权限 | √ |  |  |
| 13 | Grant Option | 允许把你自已所拥有的权限再转授给其他用户 | √ | √ |  |
| 14 | Index | 索引权限 | √ | √ |  |
| 15 | Lock Tables | 锁表权限 | √ | √ |  |
| 16 | Process | 查看进程权限 | √ |  |  |
| 17 | References | 外键权限 | √ | √ |  |
| 18 | Reload | 允许进行一些数据库管理操作的权限，如FLUSH，RESET等 | √ |  |  |
| 19 | Replication Client | 允许查询镜像机制中主服务器和从服务器的位置 | √ |  |  |
| 20 | Replication Slave | 允许某个客户连接到镜像机制中的主服务器并请求发送二进制变更日志 | √ |  |  |
| 21 | Select | 查询权限 | √ | √ |  |
| 22 | Show Databases | 查看数据库权限 | √ |  |  |
| 23 | Show View | 查看视图权限 | √ | √ |  |
| 24 | Shutdown | 关闭数据库权限 | √ |  |  |
| 25 | Super | 执行kill线程权限 | √ |  |  |
| 26 | Trigger | 触发器权限 | √ | √ |  |
| 27 | Update | 更新权限 | √ | √ |  |
| 28 | Insert | 插入权限 |  | √ |  |
| 29 | 附注说明： | ServerPlivilegs:服务器权限，针对该数据库服务器上的所有数据库均有效。Plivilegs：数据库权限：只针对设置的数据库有效。 | | |  |

### 角色权限说明

* 超级管理员

具有所有数据库的一切权限。

* 管理员

具有对所有数据库常用权限。

* 项目超级管理员

具有本项所在数据库常用可能权限。

* 项目管理员

具有本项所在数据库目前正在使用的常用权限。

* 普通用户

具有本项目使用目前正在使用的资源。

### 角色权限详单

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **用户数据库权限分配** | | | | | | | | |
| **序号** | **权限** | | **角色及权限** | | | | | **备注** |
| **权限类型** | **权限** | **超级管理员** | **管理员** | **项目超级管理员** | **项目管理员** | **普通用户** |
| 1 | ServerPlivilegs | Alter | √ | √ | √ | √ |  |  |
| 2 | ServerPlivilegs | Alter Routine | √ | √ | √ | √ |  |  |
| 3 | ServerPlivilegs | Create | √ | √ | √ |  |  |  |
| 4 | ServerPlivilegs | Create Routine | √ | √ | √ |  |  |  |
| 5 | ServerPlivilegs | Create Temporary Tables | √ | √ | √ |  |  |  |
| 6 | ServerPlivilegs | Create User | √ | √ | √ |  |  |  |
| 7 | ServerPlivilegs | Create View | √ | √ | √ |  |  |  |
| 8 | ServerPlivilegs | Delete | √ |  |  |  |  |  |
| 9 | ServerPlivilegs | Drop | √ |  |  |  |  |  |
| 10 | ServerPlivilegs | Event | √ | √ | √ | √ |  |  |
| 11 | ServerPlivilegs | Execute | √ | √ | √ | √ |  |  |
| 12 | ServerPlivilegs | File | √ | √ | √ | √ |  |  |
| 13 | ServerPlivilegs | Grant Option | √ |  |  |  |  |  |
| 14 | ServerPlivilegs | Index | √ | √ | √ | √ |  |  |
| 15 | ServerPlivilegs | Lock Tables | √ |  |  |  |  |  |
| 16 | ServerPlivilegs | Process | √ | √ |  |  |  |  |
| 17 | ServerPlivilegs | References | √ | √ |  |  |  |  |
| 18 | ServerPlivilegs | Reload | √ |  |  |  |  |  |
| 19 | ServerPlivilegs | Replication Client | √ |  |  |  |  |  |
| 20 | ServerPlivilegs | Replication Slave | √ |  |  |  |  |  |
| 21 | ServerPlivilegs | Select | √ | √ | √ | √ | √ |  |
| 22 | ServerPlivilegs | Show Databases | √ | √ | √ | √ | √ |  |
| 23 | ServerPlivilegs | Show View | √ | √ | √ | √ | √ |  |
| 24 | ServerPlivilegs | Shutdown | √ |  |  |  |  |  |
| 25 | ServerPlivilegs | Super | √ |  |  |  |  |  |
| 26 | ServerPlivilegs | Trigger | √ | √ | √ |  |  |  |
| 27 | ServerPlivilegs | Update | √ | √ | √ |  |  |  |
| 28 | Plivilegs | Select | √ | √ | √ | √ | √ |  |
| 29 | Plivilegs | Insert | √ | √ | √ | √ | √ |  |
| 30 | Plivilegs | Update | √ | √ | √ | √ | √ |  |
| 31 | Plivilegs | References | √ | √ | √ | √ | √ |  |
| 32 | Plivilegs | Delete | √ |  |  |  |  |  |
| 33 | Plivilegs | Create | √ | √ | √ | √ | √ |  |
| 34 | Plivilegs | Drop | √ |  |  |  |  |  |
| 35 | Plivilegs | Alter | √ | √ | √ | √ | √ |  |
| 36 | Plivilegs | Index | √ | √ | √ | √ | √ |  |
| 37 | Plivilegs | Trigger | √ | √ | √ | √ | √ |  |
| 38 | Plivilegs | Create View | √ | √ | √ | √ | √ |  |
| 39 | Plivilegs | Show View | √ | √ | √ | √ | √ |  |
| 40 | Plivilegs | Grant | √ | √ | √ | √ | √ |  |
| 41 | Plivilegs | Execute | √ | √ | √ | √ | √ |  |
| 42 | Plivilegs | Alter Routine | √ | √ | √ | √ | √ |  |
| 43 | Plivilegs | Create Routine | √ | √ | √ | √ | √ |  |
| 44 | Plivilegs | Create Tmp. Tables | √ | √ | √ | √ | √ |  |
| 45 | Plivilegs | Lock Tables | √ |  |  |  |  |  |
| 46 | Plivilegs | Event | √ | √ | √ | √ | √ |  |
| 47 | **备注说明** |  | | | | | |  |

## OSS对象存储

### 权限列表

详见本章节的《OSS权限详单》

### 角色权限说明

* 超级管理员

由阿里云主机的OSS对象存储的帐号。

* 普通用户

普通用户是指能上传和下载OSS文件的权限。该部分目前有待于进一步和OSS供应商沟通看是否可设置子帐户。

* 匿名用户

匿名用户具有OSS资源公开的资源的访问权限。

### OSS权限详单

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **OSS权限分配** | | | | | | | | |
| **序号** | **权限** | | **超级管理员** | **管理员** | **项目超级管理员** | **项目管理员** | **普通用户** | **备注** |
| 1 | OSS管理 | 管理权限 | √ |  |  |  |  |  |
| 2 | OSS访问 | 上传 | √ | √ | √ | √ | √ |  |
| 3 | 下载 | √ | √ | √ | √ | √ |  |
| 4 | 备注说明 |  |  |  |  |  |  |  |

# 开发角色对应设置

## 开发环境

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **开发环境资源权限** | | | | | | | | |
| **序号** | **资源** | **权限** | | |  |  |  | **备注说明** |
| **主机资源** | **超级管理员** | **管理员** | **项目超级管理员** | **项目管理员** | **普通用户** | **匿名用户** |
| 1 | 云主机管理UI | 运维经理 |  |  |  |  |  |  |
| 2 | 云主机Shell | 运维经理 | 运维人员 | 项目经理 | 项目组长 |  |  |  |
| 3 | 数据库 | 运维经理 | 运维人员 | 项目经理 | 项目组长 | 开发人员 |  |  |
| 4 | OSS对象存储 | 运维经理 |  |  |  | 开发人员 | 其它 |  |
| 5 | 其它公共资源，如域名，邮箱，微信服务号等 | 运维经理 |  |  |  |  |  |  |
| 6 | **附注说明** | （1）标灰色的内容表示不存在的 （2）开发人员含程序。 | | | | | |  |

## 测试环境

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **测试环境资源权限** | | | | | | | | |
| **序号** | **资源** | **权限** | | |  |  |  | **备注说明** |
| **主机资源** | **超级管理员** | **管理员** | **项目超级管理员** | **项目管理员** | **普通用户** | **匿名用户** |
| 1 | 云主机管理UI | 运维经理 |  |  |  |  |  |  |
| 2 | 云主机Shell | 运维经理 | 测试经理 | 项目经理和测试经理 | 项目组长 |  |  |  |
| 3 | 数据库 | 运维经理 | 测试经理 | 项目经理和测试经理 | 项目组长 | 开发人员 |  |  |
| 4 | OSS对象存储 | 运维经理 |  |  |  | 开发人员 | 其它 |  |
| 5 | 其它公共资源，如域名，邮箱，微信服务号等 | 运维经理 |  |  |  |  |  |  |
| 6 | **附注说明** | （1）标灰色的内容表示不存在的 （2）开发人员含程序。 | | | | | |  |

## 生产环境

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **生产及开发环境资源权限** | | | | | | | | |
| **序号** | **资源** | **权限** | | |  |  |  | **备注说明** |
| **主机资源** | **超级管理员** | **管理员** | **项目超级管理员** | **项目管理员** | **普通用户** | **匿名用户** |
| 1 | 云主机管理UI | 运维经理 |  |  |  |  |  |  |
| 2 | 云主机Shell | 运维经理 | 运维人员 | 项目经理 |  |  |  |  |
| 3 | 数据库 | 运维经理 | 运维人员 | 项目经理 |  |  |  |  |
| 4 | OSS对象存储 | 运维经理 |  |  |  |  |  |  |
| 5 | 其它公共资源，如域名，邮箱，微信服务号等 | 运维经理 |  |  |  |  |  |  |
| 6 | **附注说明** | （1）标灰色的内容表示不存在的 （2）开发人员含程序。 | | | | | |  |

# 附注说明