VDI用户管理

**需求规格说明书**

**SRS**

|  |  |  |
| --- | --- | --- |
| 文件状态：  [ ] 草稿  [√] 正式发布  [ ] 正在修改 | 文件标识： |  |
| 当前版本： | 1.0 |
| 作 者： | 彭海军、毛照源、高旺 |
| 完成日期： | 2014-9-5 |



**版本历史**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 作者 | 审批者 | 发布日期 | 修改内容 |
| 1.0初稿 | 彭海军  毛照源  高旺 | 马晓超  苏永刚  薛蕊 | 2014-9-5 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目录**

[0．文档介绍 1](#_Toc397697732)

[0.1 文档目的 1](#_Toc397697733)

[0.2 文档范围 1](#_Toc397697734)

[0.3 读者对象 1](#_Toc397697735)

[0.4 参考文档 1](#_Toc397697736)

[0.5 术语与缩写解释 1](#_Toc397697737)

[1. 项目介绍 1](#_Toc397697738)

[2. 项目应用场景及相关概念说明 2](#_Toc397697739)

[3. 项目应当遵循的标准或规范 2](#_Toc397697740)

[4. 项目范围 2](#_Toc397697741)

[5. 项目中的角色 2](#_Toc397697742)

[6. 项目的功能性需求 3](#_Toc397697743)

[6.1.命名规范 3](#_Toc397697744)

[6.2.本地用户管理 3](#_Toc397697745)

[6.2.1.添加本地用户 3](#_Toc397697746)

[6.2.2.修改本地用户名 3](#_Toc397697747)

[6.2.3.修改本地用户口令 4](#_Toc397697748)

[6.2.4.修改本地用户信息 4](#_Toc397697749)

[6.2.5.本地用户查询 4](#_Toc397697750)

[6.2.6.本地用户批量导入 5](#_Toc397697751)

[6.2.7. 批量删除本地用户 5](#_Toc397697752)

[6.2.8.禁用用户账号 5](#_Toc397697753)

[6.2.9.解禁用户账号 6](#_Toc397697754)

[6.3.本地组织单元管理 6](#_Toc397697755)

[6.3.1.添加组织单元 6](#_Toc397697756)

[6.3.2.删除组织单元 6](#_Toc397697757)

[6.3.3.查询组织单元信息 6](#_Toc397697758)

[6.3.4.查询组织单元层次关系 7](#_Toc397697759)

[6.3.5.查看组织单元下的用户 7](#_Toc397697760)

[6.3.6.修改组织单元名 7](#_Toc397697761)

[6.3.7.编辑组织单元所属组织单元 7](#_Toc397697762)

[6.3.8.修改本地用户所属组织单元 8](#_Toc397697763)

[6.4.交付组 9](#_Toc397697764)

[6.4.1.交付组中添加用户 9](#_Toc397697765)

[6.4.2.交付组中移除用户 9](#_Toc397697766)

[6.4.3.交付组中添加组织单元 9](#_Toc397697767)

[6.4.4.交付组中移除组织单元 10](#_Toc397697768)

[6.4.5.添加交付组 10](#_Toc397697769)

[6.4.6.删除交付组 11](#_Toc397697770)

[6.4.7.查询交付组 11](#_Toc397697771)

[6.4.8.修改交付组组名 11](#_Toc397697772)

[6.5.用户登录 12](#_Toc397697773)

[6.5.1.本地用户的普通方式登录 12](#_Toc397697774)

[6.5.2.本地用户的管理方式登录 12](#_Toc397697775)

[6.5.3.域用户的普通方式登录 12](#_Toc397697776)

[6.5.4.域用户的管理方式登录 13](#_Toc397697777)

[6.6.LDAP服务器 13](#_Toc397697778)

[6.6.1.增加LDAP服务器 13](#_Toc397697779)

[6.6.2.删除LDAP服务器 14](#_Toc397697780)

[6.6.3.查询LDAP服务器 14](#_Toc397697781)

[6.6.4.修改LDAP服务器导入范围 14](#_Toc397697782)

[6.6.5.系统自动进行域同步 14](#_Toc397697783)

[6.6.6.域立即同步 15](#_Toc397697784)

[6.7.用户角色 16](#_Toc397697785)

[6.7.1.修改用户角色 16](#_Toc397697786)

[6.8.域用户 16](#_Toc397697787)

[6.8.1.添加域用户 16](#_Toc397697788)

[6.8.2.批量删除域用户 16](#_Toc397697789)

[6.8.3.修改域用户登录口令 17](#_Toc397697790)

[6.8.4.修改域用户基本信息 17](#_Toc397697791)

[6.8.5.查询域用户信息 17](#_Toc397697792)

[6.9.域组织单元 18](#_Toc397697793)

[6.9.1.增加域组织单元 18](#_Toc397697794)

[6.9.2.查看域组织单元详细信息 18](#_Toc397697795)

[6.9.3.查看域组织单元层次结构 18](#_Toc397697796)

[6.9.4.删除域组织单元 19](#_Toc397697797)

[6.10.域 19](#_Toc397697798)

[6.10.1.添加域信息 19](#_Toc397697799)

[6.10.2.删除域信息 20](#_Toc397697800)

[6.10.3.修改域信息 20](#_Toc397697801)

[6.10.4.修改域的连接信息 20](#_Toc397697802)

[6.10.5.查询域信息 20](#_Toc397697803)

[6.11.本地用户状态机 21](#_Toc397697804)

[6.12.本地组织单元状态机 22](#_Toc397697805)

[6.13.交付组状态机 24](#_Toc397697806)

[6.14.域状态机 25](#_Toc397697807)

[6.15.域用户状态机 27](#_Toc397697808)

[6.16.域组织单元状态机 30](#_Toc397697809)

[7. 项目的非功能性需求 32](#_Toc397697810)

[7.1.用户界面需求 32](#_Toc397697811)

[7.2.软硬件环境需求 32](#_Toc397697812)

[7.3.项目质量需求 32](#_Toc397697813)

[7.4.其他需求 33](#_Toc397697814)

[附录A 相关文档 33](#_Toc397697815)

[AD用户属性和系统用户属性对应关系表 33](#_Toc397697816)

[AD域属性和密码策略对应关系表 33](#_Toc397697817)

[LDAP服务器错误码 33](#_Toc397697818)

[附录B：需求建模与分析报告 36](#_Toc397697819)

[B.1 需求模型1 36](#_Toc397697820)

[B.n 需求模型N 36](#_Toc397697821)

[附录C：需求确认 36](#_Toc397697822)

# 0．文档介绍

## 0.1 文档目的

本文档力求把用户需求明晰化、技术化、确定化。

本文档作为项目开发流程的入口条件，为项目开发制定明确的技术规格，包括功能、特性以及其他规格要求。

本文档必须以满足用户需求为前提条件。

## 0.2 文档范围

本文档将从技术的角度描述用户需求，使得用户需求具体化和明确化。

本文档一旦经过专家评审后，不能随意更改、变动。如果必须改动，需要经过专家组组长签字确认。

## 0.3 读者对象

本文档的读者对象为项目软件开发人员以及专家评审组人员。

## 0.4 参考文档

[OPV-VDI][3.3.7][产品项目]产品总体设计

## 0.5 术语与缩写解释

|  |  |
| --- | --- |
| 缩写、术语 | 解 释 |
| VDI | Virtual Desktop Infrastructure |
| LDAP | Lightweight Directory Access Protocol |
| AD | Active Directory |

# 项目介绍

本项目主要根据[OPV-VDI][3.3.7][产品项目]产品总体设计的说明，分析VDI用户管理模块最新的需求，满足对VDI用户管理模块重构的计划。

# 项目应用场景及相关概念说明

略。

# 项目应当遵循的标准或规范

本项目开发必须遵循下面标准或者规范：

公司软件开发流程和规范；

VDI项目总体设计原则：

1）根据可靠性分级

2）高内聚，低耦合，可复用

3）机制与策略分离

# 项目范围

此项目开发完成后需要达到如下目标：

按照要求的时间点和交付要求交付项目。

交付文档：SRS，HLD，API手册，用户使用手册以及部署说明规范。

交付代码：jar包。

# 项目中的角色

|  |  |
| --- | --- |
| 角色名称 | 职责描述 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# 项目的功能性需求

## 命名规范

（1）用户名

➀字符集可使用任何Unicode字符。

➁长度不少于1个字符，不超过20个字符，不包含 \ / “ [ ] : | < > + = ; , ? \* @，首尾字符不能为空格,尾字符不能为中英文句号。

（2）交付组和组织单元名

➀字符集可使用任何Unicode字符

➁长度不少于1个字符，不超过64个字符，不包含 \ / “ [ ] : | < > + = ; , ? \* @，首尾字符不能为空格，尾字符不能为中英文句号。

（3）口令(本地域)

➀字符集可以是大写字母，小写字母，数字和符号（` ~ ! @ # $ % ^ & \* ( ) \_ + - = { } | \ : " ; ' < > ? , . /）

➁长度在6到64个字符之间

## 本地用户管理

### 添加本地用户

|  |  |
| --- | --- |
| 功能描述 | 支持添加本地用户 |
| 优先级 | 高 |
| 输入 | 必填项（用户名、口令、所属组织单元ID、用户角色），可选项（用户真实姓名、电话、邮箱、备注） |
| 操作序列 | 1. 检查用户名，口令的合法性，若不合法提示错误 2. 检查用户名是否已经存在，如果存在则提示用户名已存在错误；检查所属组织单元是否存在，如果该组织单元不存在则提示错误 3. 添加用户 |
| 输出 | 添加成功或错误信息 |
| 补充说明 | 注册时间从系统获取，默认为本地域  用户名，口令的命名规则，请参考需求文档中相关命名规则 |

### 修改本地用户名

|  |  |
| --- | --- |
| 功能描述 | 支持修改本地用户名 |
| 优先级 | 高 |
| 输入 | 用户ID，新用户名 |
| 操作序列 | 1. 检查新用户名的合法性，若不合法则提示错误 2. 检查新用户名是否已存在，如果已存在则提示错误 3. 修改用户名 |
| 输出 | 修改成功或错误信息 |
| 补充说明 | 用户名为用户的登录名或账号  用户名的命名规则，请参考需求文档中相关命名规则 |

### 修改本地用户口令

|  |  |
| --- | --- |
| 功能描述 | 支持修改本地用户口令 |
| 优先级 | 高 |
| 输入 | 用户ID，新口令，确认新口令 |
| 操作序列 | 1. 检查新口令的合法性 2. 检查新口令和确认新口令是否一样，如果不一样则提示错误 3. 更新用户口令 |
| 输出 | 修改成功或错误信息 |
| 补充说明 | 口令的命名规范，请参考需求文档中相关命名规则 |

### 修改本地用户信息

|  |  |
| --- | --- |
| 功能描述 | 支持修改本地用户信息 |
| 优先级 | 高 |
| 输入 | 必填（用户ID），可选项（用户姓名、电话、邮箱、角色、备注） |
| 操作序列 | 1. 更新用户信息 |
| 输出 | 修改成功 |
| 补充说明 | 无 |

### 本地用户查询

|  |  |
| --- | --- |
| 功能描述 | 支持本地用户查询 |
| 优先级 | 高 |
| 输入 | 用户ID（可选）  用户名 （可选，支持模糊查询）  用户姓名（可选，支持模糊查询）  邮箱（可选，支持模糊查询） |
| 操作序列 | 1. 查询用户信息 |
| 输出 | 用户信息（用户ID, 用户名，用户姓名，角色，所属域，组织单元，状态，联系电话，邮箱，备注） |
| 补充说明 | 支持分页和模糊查询，根据用户ID排序或添加时间排序 |

### 本地用户批量导入

|  |  |
| --- | --- |
| 功能描述 | 支持本地用户批量导入 |
| 优先级 | 高 |
| 输入 | 用户存储文件 |
| 操作序列 | 1. 读取Microsoft Excel 2003/2007格式文档 2. 检查用户名，口令的合法性。若不合法则跳过并记录错误 3. 导入的用户名已存在则跳过并记录错误 4. 检查提供的组织单元（组织单元为可选项），若不提供组织单元，用户将属于默认的顶层组织单元，若提供了组织单元，用户将属于该组织单元。若该组织单元尚未被建立，则将被建立在顶层组织单元之下 5. 添加用户（用户角色默认为普通用户，注册时间从系统获取，默认为本地域） 6. 返回所有没有添加成功的用户列表及失败原因 |
| 输出 | 本地用户导入成功或导入失败的用户 |
| 补充说明 | 在页面呈现导入失败的用户同时注明失败的原因，用户信息应包括：必填项（用户名，口令），可选项（组织单元，用户真实姓名，电话，邮箱），默认为本地域 |

### 批量删除本地用户

|  |  |
| --- | --- |
| 功能描述 | 支持批量删除本地用户 |
| 优先级 | 高 |
| 输入 | 用户ID列表 |
| 操作序列 | 1. 检查用户与虚拟桌面的状态，若用户与桌面已连接，则强制断开用户与桌面的连接 2. 删除用户的资源（与用户绑定的桌面进行重置，解除访问权限） 3. 删除用户 |
| 输出 | 删除成功 |
| 补充说明 | 无 |

### 禁用用户账号

|  |  |
| --- | --- |
| 功能描述 | 支持禁用用户账号 |
| 优先级 | 高 |
| 输入 | 用户ID |
| 操作序列 | 1. 检查用户与桌面的连接状态，若正在连接则强制断开连接 2. 修改用户状态为挂起状态 |
| 输出 | 禁用成功 |
| 补充说明 |  |

### 解禁用户账号

|  |  |
| --- | --- |
| 功能描述 | 支持解禁用户账号 |
| 优先级 | 高 |
| 输入 | 用户ID |
| 操作序列 | 1. 修改用户状态为正常状态 |
| 输出 | 解禁成功 |
| 补充说明 |  |

## 本地组织单元管理

### 添加组织单元

|  |  |
| --- | --- |
| 功能描述 | 支持添加组织单元 |
| 优先级 | 高 |
| 输入 | 组织单元名，所属组织单元ID |
| 操作序列 | 1. 检查组织单元名合法性 2. 检查组织单元名在所属组织单元下是否已存在，若已存在则提示错误，若不存在，则添加组织单元到所属组织单元 |
| 输出 | 添加成功或错误信息 |
| 补充说明 | 组织单元可以重名，但是同一个层次下的组织单元不能重名  创建时间从系统获取 |

### 删除组织单元

|  |  |
| --- | --- |
| 功能描述 | 支持删除组织单元 |
| 优先级 | 高 |
| 输入 | 组织单元ID |
| 操作序列 | 1. 查询该组织单元下的所有用户和下属组织单元 2. 批量删除该组织单元下的用户（参考批量删除本地用户） 3. 删除组织单元和下属组织单元 |
| 输出 | 删除成功 |
| 补充说明 |  |

### 查询组织单元信息

|  |  |
| --- | --- |
| 功能描述 | 支持查询组织单元信息 |
| 优先级 | 高 |
| 输入 | 组织单元ID |
| 操作序列 | 1. 查询组织单元基本信息（组织单元ID，组织单元名，所属域，创建时间，状态，添加的交付组） |
| 输出 | 组织单元基本信息 |
| 补充说明 |  |

### 查询组织单元层次关系

|  |  |
| --- | --- |
| 功能描述 | 支持查询组织单元层次关系 |
| 优先级 | 高 |
| 输入 | 组织单元ID |
| 操作序列 | 1. 查询该组织单元下的所有子组织单元 2. .将查询结果组织成树形结构 |
| 输出 | 组织单元层次关系 |
| 补充说明 |  |

### 查看组织单元下的用户

|  |  |
| --- | --- |
| 功能描述 | 支持查看组织单元下的用户 |
| 优先级 | 高 |
| 输入 | 组织单元ID |
| 操作序列 | 1. 查询该组织单元下的用户 |
| 输出 | 用户名列表 |
| 补充说明 | 用户为该组织单元下的直接子用户 |

### 修改组织单元名

|  |  |
| --- | --- |
| 功能描述 | 支持修改组织单元名 |
| 优先级 | 高 |
| 输入 | 组织单元ID，新组织单元名 |
| 操作序列 | 1. 检查组织单元的所属组织单元（父组织单元）下该新组织单元名是否已存在，若已存在则提示错误 2. 修改组织单元名 |
| 输出 | 修改成功或错误信息 |
| 补充说明 |  |

### 编辑组织单元所属组织单元

|  |  |
| --- | --- |
| 功能描述 | 支持编辑组织单元所属组织单元 |
| 优先级 | 高 |
| 输入 | 组织单元ID，新所属组织单元ID |
| 操作序列 | 1. 检查新所属组织单元下该组织的单元名是否已存在，若已存在，则提示错误 2. 检查组织单元是否已添加到某个交付组，若无则执行操作序列4，若有则执行操作序列3 3. 检查组织单元所属组织单元的交付组与新所属组织单元所属交付组(1)若相同则不做处理，则执行操作序列4   (2)若不同，则检查该组织单元与交付组的路径是直接相连还是通过父组织单元相连  1）若是直接相连则保留与原交付组的关系，继续执行操作序列4  2）若是通过父组织单元与交付组相连，则检查组织单元下用户与对应的桌面是否处于服务状态，若正在服务则强制断开连接，对组织单元下的用户拥有的桌面进行重置，解除权限，继续执行操作序列4   1. 修改组织单元的所属组织单元 |
| 输出 | 修改成功或错误信息 |
| 补充说明 |  |

### 修改本地用户所属组织单元

|  |  |
| --- | --- |
| 功能描述 | 支持修改本地用户所属组织单元 |
| 优先级 | 高 |
| 输入 | 用户ID，新组织单元ID |
| 操作序列 | 1. 检查用户是否已与某个交付组相连，若没有则执行操作序列3，若已与某个交付组相连则执行操作序列2 2. 检查新所属组织单元的所属交付组   （1）若两个交付组不同，则检查用户与交付组的路径是直接相连还是通过父组织单元相连  1）若是直接相连则保留与原交付组的关系，继续执行操作序列3  2）若是通过父组织单元与交付组相连，则检查组织单元下用户与对应的桌面是否处于服务状态，若处于服务状态则强制断开连接，对组织单元下的用户拥有的桌面进行重置，解除权限，继续执行操作序列3  （2）若相同则不做处理（保留所有的资源只是访问路径改变）继续执行操作序列3   1. 将用户添加到新组织单元中 |
| 输出 | 成功 |
| 补充说明 |  |

## 交付组

### 交付组中添加用户

|  |  |
| --- | --- |
| 功能描述 | 支持交付组中添加用户 |
| 优先级 | 高 |
| 输入 | 用户ID，交付组ID |
| 操作序列 | 1. 检查交付组是否有用户或组织单元   （1）若有则检查当前的用户与交付组中已存在的用户和组织单元是否是属于同一个域，如果是同一个域则可以添加，如果不是同一个域则禁止添加，提示用户错误  （2）若没有则可以直接添加无需往下执行操作序列   1. 检查用户的所属组织单元是否已添加到该交付组中   （1） 若已添加到该交付组中则提示用户该用户已添加到该交付组中  （2）若没有添加到该交付组中则将用户添加到交付组中 |
| 输出 | 添加成功或错误信息 |
| 补充说明 | 一个交付组里面的用户和组织单元必须是同一个域 |

### 交付组中移除用户

|  |  |
| --- | --- |
| 功能描述 | 支持交付组中移除用户 |
| 优先级 | 高 |
| 输入 | 用户ID，交付组ID |
| 操作序列 | 1. 检查用户的所属组织是否与交付组存在关联路径   （1）若存在，则解除用户与交付组的直接路径，用户依然可以通过组织单元的路径访问资源（桌面关系不解除）  （2）若不存在，则检查组织单元下用户与对应的桌面是否处于服务状态，若正在服务则强制断开连接，对组织单元下的用户拥有的桌面进行重置，解除权限   1. 将用户从交付组中移除 |
| 输出 | 移除成功 |
| 补充说明 |  |

### 交付组中添加组织单元

|  |  |
| --- | --- |
| 功能描述 | 支持交付组中添加组织单元 |
| 优先级 | 高 |
| 输入 | 组织单元ID，交付组ID |
| 操作序列 | 1. 检查交付组是否有用户或组织单元   （1）若有则检查当前的交付组与交付组中已存在的用户和交付组是否是属于同一个域，如果是同一个域则可以添加，如果不是同一个域则禁止添加，提示用户错误  （2）若没有则可以直接添加无需往下执行操作序列   1. 检查组织单元的所属组织单元是否已添加到该交付组   （1）若已添加到交付组，提示用户已添加  （2）若没有添加到交付组则执行操作序列2   1. 将组织单元添加到交付组中 |
| 输出 | 添加成功或错误信息 |
| 补充说明 | 一个交付组里面的用户和组织单元必须是同一个域 |

### 交付组中移除组织单元

|  |  |
| --- | --- |
| 功能描述 | 支持交付组中移除组织单元 |
| 优先级 | 高 |
| 输入 | 组织单元ID，交付组ID |
| 操作序列 | 1. 检查组织单元下的用户与交付组之间访问路径   （1）若只存在一条路径，则检查组织单元下用户的状态，若用户与桌面正在连接，则强制断开组织单元下用户与桌面的连接，用户连接断开后，直接解除与桌面的权限，桌面重置  （2）若存在多条路径，则删除所有通过该组织单元的路径（此时用户还是可以通过其它的路径访问交付组的桌面）   1. 交付组中移除组织单元 |
| 输出 | 移除成功 |
| 补充说明 |  |

### 添加交付组

|  |  |
| --- | --- |
| 功能描述 | 支持添加交付组操作 |
| 优先级 | 高 |
| 输入 | 组名(必填) |
| 操作序列 | 1. 检查组名合法性，如果不合法，则返回失败，提示组名不合法，如果合法则继续 2. 检查组名是否重复，如果重复，则返回失败，提示组名已存在，如果不重复则继续 3. 将交付组ID(自动生成)，组名，添加时间(系统获取)信息存入数据中心，返回添加成功 |
| 输出 | 添加成功或失败 |
| 补充说明 | 交付组内的用户、组织单元不能跨域存在，因此在创建交付组时就确其  属于哪个域  交付组的命名规则，请参考需求文档中相关命名规则 |

### 删除交付组

|  |  |
| --- | --- |
| 功能描述 | 支持删除交付组操作 |
| 优先级 | 高 |
| 输入 | 交付组ID(必填，系统中存在的组ID) |
| 操作序列 | 1. 如果选择强制断开该交付组下所有用户的连接 2. 立即解除该交付组所有用户(包括组织单元下的用户)访问与该交付组绑定的桌面池的权限，回收用户对应的桌面 3. 从数据中心删除该组的数据 |
| 输出 | 删除成功 |
| 补充说明 |  |

### 查询交付组

|  |  |
| --- | --- |
| 功能描述 | 支持查询交付组操作 |
| 优先级 | 高 |
| 输入 | 交付组ID（可选，不支持模糊查询，默认值为所有）  组名（可选，支持模糊查询，默认值为所有）  添加时间（可选，选择时间段，默认值为所有时间段） |
| 操作序列 | 1. 根据查询条件从数据中心查出满足条件的交付组 |
| 输出 | 如果查询结果为空，则输出没有满足条件的交付组  如果不为空，则输出以下内容：  1）交付组ID，组名，添加时间  2）交付组状态  3）交付组与桌面池的绑定状态  4）交付组下组织单元信息，用户信息 |
| 补充说明 | 支持分页，可按添加时间排序 |

### 修改交付组组名

|  |  |
| --- | --- |
| 功能描述 | 支持修改交付组组名操作 |
| 优先级 | 高 |
| 输入 | 组ID(必填)，修改后的组名(必填) |
| 操作序列 | 1. 检查组名合法性，如果不合法，则返回失败，提示组名不合法，如果合法则继续 2. 检查组名是否重复，如果重复，则返回失败，提示组名已存在，如果不重复则继续 3. 在数据中心修改组名信息 |
| 输出 | 修改成功或失败 |
| 补充说明 | 交付组的命名规则，请参考需求文档中相关命名规则 |

## 用户登录

### 本地用户的普通方式登录

|  |  |
| --- | --- |
| 功能描述 | 支持本地用户的普通方式登录 |
| 优先级 | 高 |
| 输入 | 用户名(必填)、密码(必填)、域名(必填，为本地域) |
| 操作序列 | 1. 检查本地域下是否有该用户及密码是否正确，如果用户名或密码错误返回登录失败，提示用户名或密码错误，如果正确则继续 2. 检查用户状态，如果不可用，则返回登录失败，提示用户状态错误，如果可用，则继续 3. 检查该用户是否已经登录，如果已登录，断开该用户的前一次登录，使本次登录成功，返回登录成功，如果未登录，则直接返回登录成功 |
| 输出 | 登录成功或登录失败及失败原因 |
| 补充说明 | Windows，Linux，Web客户端登录处理方式相同 |

### 本地用户的管理方式登录

|  |  |
| --- | --- |
| 功能描述 | 支持本地用户的管理方式登录 |
| 优先级 | 高 |
| 输入 | 用户名(必填)、密码(必填)、域名(必填，为本地域) |
| 操作序列 | 1. 检查该用户是否为管理员，如果不是，则返回登录失败，提示用户名或密码错误，如果是则继续 2. 检查本地域下是否有该用户及密码是否正确，如果用户名或密码错误返回登录失败，提示用户名或密码错误，如果正确则继续 3. 检查用户状态，如果不可用，则返回登录失败，提示用户状态错误，如果可用，则返回成功 |
| 输出 | 登录成功或登录失败及失败原因 |
| 补充说明 |  |

### 域用户的普通方式登录

|  |  |
| --- | --- |
| 功能描述 | 支持域用户的普通方式登录 |
| 优先级 | 高 |
| 输入 | 用户名(必填)、密码(必填)、域名(必填，系统中存在的域名) |
| 操作序列 | 1. 检查系统中是否存在该用户，如果不存在则返回登录失败，提示用户名或密码错误，如果存在则继续 2. 到对应的域服务器验证用户信息是否正确 3. 如果连接域服务器失败则返回登录失败，提示访问域服务器失败 4. 如果连接成功，根据验证的信息判断用户名及密码是否正确，如果用户米或密码错误，则返回登录失败，提示用户名或密码错误，如果用户名和密码正确，则继续 5. 检查用户状态，如果不可用，则返回失败，提示用户状态错误，如果可用，则继续 6. 检查该用户是否已经登录，如果已登录，断开该用户的前一次登录，使本次登录成功，返回登录成功，如果未登录，则直接返回登录成功 |
| 输出 | 登录成功或登录失败及失败原因 |
| 补充说明 | Windows，Linux，Web客户端登录处理方式相同 |

### 域用户的管理方式登录

|  |  |
| --- | --- |
| 功能描述 | 支持域用户的管理方式登录 |
| 优先级 | 高 |
| 输入 | 用户名(必填)、密码(必填)、域名(必填，系统中存在的域名) |
| 操作序列 | 1. 检查用户是否为管理员，如果不是，则返回登录失败，提示用户名或密码错误，如果是则继续 2. 到对应的域服务器验证用户信息是否正确 3. 如果连接域服务器失败则返回登录失败，提示访问域服务器失败 4. 如果连接成功，根据验证的信息判断用户名及密码是否正确，如果用户名或密码错误，则返回登录失败，提示用户名或密码错误，如果用户名和密码正确，则继续 5. 检查用户状态，如果不可用，则返回失败，提示用户状态错误，如果可用，则返回成功 |
| 输出 | 登录成功或登录失败及失败原因 |
| 补充说明 |  |

## LDAP服务器

### 增加LDAP服务器

|  |  |
| --- | --- |
| 功能描述 | 支持增加LDAP服务器操作 |
| 优先级 | 高 |
| 输入 | 域ID，导入范围 |
| 操作序列 | 1. 存储LDAP服务器信息（LDAP服务器ID，域ID,导入范围，添加时间（系统获取）） 2. 立即同步该域 |
| 输出 | 添加成功或失败及原因 |
| 补充说明 | 可读可写包括（域用户的增删改查，域组织单元的增删改查） |

### 删除LDAP服务器

|  |  |
| --- | --- |
| 功能描述 | 支持删除LDAP服务器操作 |
| 优先级 | 高 |
| 输入 | LDAP服务器ID(必填) |
| 操作序列 | 1. 删除LDAP服务器信息 2. 立即同步该域 |
| 输出 | 删除成功 |
| 补充说明 |  |

### 查询LDAP服务器

|  |  |
| --- | --- |
| 功能描述 | 支持查询LDAP服务器操作 |
| 优先级 | 高 |
| 输入 | LDAP服务器ID（可选，不支持模糊查询，默认值为所有）  域ID（可选，不支持模糊查询，默认值为所有）  添加时间（可选，选择时间段，默认值为所有） |
| 操作序列 | 1. 根据查询条件从数据中心查询满足条件的LDAP服务器 |
| 输出 | 如果查询结果为空，则返回没有满足条件的LDAP服务器  如果查询结果不为空，则返回以下信息：  LDAP服务器ID、域ID、添加时间、导入范围 |
| 补充说明 | 支持分页，可按添加时间排序 |

### 修改LDAP服务器导入范围

|  |  |
| --- | --- |
| 功能描述 | 支持修改LDAP服务器导入范围操作 |
| 优先级 | 高 |
| 输入 | LDAP服务器ID(必填)，新的导入范围 |
| 操作序列 | 1. 根据LDAP服务器ID和用户选择的导入范围，到数据中心修改数据 2. 立即同步LDAP服务器对应的域 |
| 输出 | 修改成功 |
| 补充说明 |  |

### 系统自动进行域同步

|  |  |
| --- | --- |
| 功能描述 | 支持系统自动进行域同步操作 |
| 优先级 | 高 |
| 输入 | 域ID（必填） |
| 操作序列 | 1. 根据同步时间执行以下操作 2. 根据LDAP路径，用户名，口令访问AD，如果访问失败，则不做任何处理，域进入异常状态 3. 获取该域的所有导入范围 4. 如果某个导入范围在AD中被删除，则删除对应的LDAP服务器 5. 获取新的所有的导入范围 6. 如果AD中删除了导入范围中的组织单元，则删除系统中的组织单元 7. 如果AD中在导入范围内增加了组织单元，则在系统中增加组织单元 8. 如果AD中删除了导入范围内的用户，则删除系统中的用户 9. 如果AD中在导入范围内添加了用户，则在系统中添加用户 10. 删除不属于导入范围的组织单元和用户 11. 更新域的密码规范 |
| 输出 | 同步成功或失败 |
| 补充说明 |  |

### 域立即同步

|  |  |
| --- | --- |
| 功能描述 | 支持域立即同步操作 |
| 优先级 | 高 |
| 输入 | 域ID(必填) |
| 操作序列 | 1. 根据LDAP路径，用户名，口令访问AD，如果访问失败，则不做任何处理，域进入异常状态 2. 获取该域的所有导入范围 3. 如果某个导入范围在AD中被删除，则删除对应的LDAP服务器 4. 获取新的所有的导入范围 5. 如果AD中删除了导入范围中的组织单元，则删除系统中的组织单元 6. 如果AD中在导入范围内增加了组织单元，则在系统中增加组织单元 7. 如果AD中删除了导入范围内的用户，则删除系统中的用户 8. 如果AD中在导入范围内添加了用户，则在系统中添加用户 9. 删除不属于导入范围的组织单元和用户 10. 更新域的密码规范 |
| 输出 | 同步成功或失败 |
| 补充说明 |  |

## 用户角色

### 修改用户角色

|  |  |
| --- | --- |
| 功能描述 | 支持修改用户角色操作 |
| 优先级 | 高 |
| 输入 | 用户ID(必填，系统中存在的用户ID)  角色类型(可选，只有两种类型普通用户与管理员，默认为当前用户的角色类型) |
| 操作序列 | 1. 根据用户ID和选择的角色类型，修改数据中心该用户的角色类型 |
| 输出 | 修改成功 |
| 补充说明 | 1. 系统建立时有一个默认的管理员，该管理员不可删除 2. 系统建立后，通过系统添加的管理员，有操作整个管理平台的权限，但是可以被删除 3. 管理员角色即可以管理方式登录，也可以普通方式登录 |

## 域用户

### 添加域用户

|  |  |
| --- | --- |
| 功能描述 | 支持添加域用户 |
| 优先级 | 高 |
| 输入 | 必填项（用户名、口令、所属组织单元ID、所属域ID，角色），可选项（真实姓名，邮箱，联系电话，备注）， |
| 操作序列 | 1. 验证输入信息的合法性，如果输入信息不合法，则提示用户输入信息不正确，请重新输入，如果输入信息正确则进入下一步 2. 在系统数据库和AD中添加用户信息，此用户的角色默认为普通用户，创建时间为当前系统时间。 |
| 输出 | 添加域用户成功或提示输入信息不正确，请重新输入 |
| 补充说明 | 用户名的命名规则请参考需求文档中相关命名规则；口令的命名规则要符合域用户 |

### 批量删除域用户

|  |  |
| --- | --- |
| 功能描述 | 支持批量删除域用户 |
| 优先级 | 高 |
| 输入 | 要删除的用户的ID列表 |
| 操作序列 | 1. 检查被删除用户中是否存在正在使用桌面的用户，如果没有，转到第4步，否则提示用户选择立即解除被删除用户对桌面池的访问权限还是等待被删除用户主动断开，如果是前者，则转到第2步，如果是后者，则转到第3步 2. 被删除用户立即断开与桌面的连接，权限关系被删除，原有桌面被重置，转到第4步 3. 被删除用户主动断开连接以后，权限关系被删除，原有桌面被重置 4. .系统中和AD中的用户的信息被删除，提示删除用户成功 |
| 输出 | 提示删除成功 |
| 补充说明 | 无 |

### 修改域用户登录口令

|  |  |
| --- | --- |
| 功能描述 | 支持修改域用户登录口令 |
| 优先级 | 高 |
| 输入 | 新登录口令和用户ID |
| 操作序列 | 1. 系统验证新口令是否符合域的密码策略，如果不符合则提示重新输入密码，否则进入下一步 2. .如果AD中修改域用户口令成功，则进入下一步，否则解析返回错误码，提示用户修改密码失败，请检查AD中域用户设定的安全组密码策略 3. .提示修改登录口令成功 |
| 输出 | 修改域用户登录口令成功或失败 |
| 补充说明 | 登录口令的命名规则要和用户所在域设定的密码策略相同 |

### 修改域用户基本信息

|  |  |
| --- | --- |
| 功能描述 | 支持修改域用户基本信息 |
| 优先级 | 高 |
| 输入 | 1. 用户的ID和要修改的基本信息（真实姓名，邮箱，联系电话，角色，备注） |
| 操作序列 | 1. 检查输入信息的合法性，如果合法就转到下一步 2. 修改AD中的该用户的信息，再修改本地数据库中用户的信息 |
| 输出 | 提示修改基本信息成功或失败 |
| 补充说明 | 输入的要修改的信息必须符合规则 |

### 查询域用户信息

|  |  |
| --- | --- |
| 功能描述 | 支持查询域用户信息 |
| 优先级 | 低 |
| 输入 | 查询条件（用户名，真实姓名，邮箱，所属组织单元ID），查询内容 |
| 操作序列 | 1. 如果查询内容为空，则查询出所有域用户信息；如果查询条件是按组织单元，则返回与此组织单元名类似的组织单元下的所有用户（不包括子组织单元下的用户）信息；如果查询条件是其他方式，则返回与此查询条件匹配的所有域用户信息 |
| 输出 | 用户信息（用户ID，用户名，真实姓名，所属域，角色，状态，联系电话，邮箱,添加的交付组）列表 |
| 补充说明 | 用户名、真实姓名、组织单元名支持模糊查询，结果支持分页 |

## 域组织单元

### 增加域组织单元

|  |  |
| --- | --- |
| 功能描述 | 支持增加域组织单元 |
| 优先级 | 高 |
| 输入 | 组织单元名，所属域，所属组织单元ID |
| 操作序列 | 1. 验证输入信息是否合法，如果是则进入下一步，否则提示重新输入 2. 检查组织单元名是否与所属组织单元中原有的组织单元名有冲突，如果有则提示重新输入 3. 保存组织单元信息到本地数据库和AD中 |
| 输出 | 提示添加成功或提示重新输入信息。 |
| 补充说明 | 域组织单元命名规则请参考需求文档中相关命名规则， |

### 查看域组织单元详细信息

|  |  |
| --- | --- |
| 功能描述 | 支持查看域组织单元详细信息 |
| 优先级 | 低 |
| 输入 | 查询条件（按域组织单元ID查，按组织单元名查，按组织单元状态查），查询内容 |
| 操作序列 | 1. 如果查询内容为空，则查询所有的域组织单元信息，否则按照查询条件和查询内容进行查询 |
| 输出 | 返回组织单元的详细信息（组织单元ID，组织单元名，所属域，创建时间，状态，添加的交付组）列表。 |
| 补充说明 | 组织单元名支持模糊查询，可按组织单元ID排序，支持分页 |

### 查看域组织单元层次结构

|  |  |
| --- | --- |
| 功能描述 | 支持查看域组织单元层次结构 |
| 优先级 | 高 |
| 输入 | 组织单元的ID |
| 操作序列 | 1. 选择要查看层次结构的组织单元 2. 返回本组织单元包含的组织单元信息 |
| 输出 | 返回本组织单元包含的组织单元（包括子组织单元中的组织单元）信息（组织单元ID，组织单元名） |
| 补充说明 | 无 |

### 删除域组织单元

|  |  |
| --- | --- |
| 功能描述 | 支持删除域组织单元 |
| 优先级 | 高 |
| 输入 | 组织单元的ID |
| 操作序列 | 1. 查询此组织单元下的所有用户（包括子组织单元下的用户）和子组织单元 2. .批量删除所有用户 3. 删除此组织单元和所有子组织单元 |
| 输出 | 删除成功 |
| 补充说明 | 无 |

## 域

### 添加域信息

|  |  |
| --- | --- |
| 功能描述 | 支持增加域操作 |
| 优先级 | 高 |
| 输入 | LDAP路径(必填)，用户名(必填)，口令(必填) ，BaseDN(必填)  操作类型(选择，只可查询，可读可写，默认为可读可写)  同步时间(可选，15m，30m，1h，2h，默认为15m)  DNS服务器地址(必填) |
| 操作序列 | 1. 判断操作类型，如果为只可查询到2步，否则转到第3步 2. 根据LDAP路径、用户名、口令，采用389端口访问LDAP服务器，如果访问失败则解析失败原因，返回失败及失败原因，如果成功则继续到第4步 3. 根据LDAP路径、用户名、口令，采用636端口访问LDAP服务器，如果访问失败则解析失败原因，返回失败及失败原因，如果成功则到第4步 4. 检查DNS是否正确，如果错误则返回失败，提示DNS错误，否则继续 5. 访问LDAP服务器获取密码规范以及域ID，域名 6. 如果该域已经存在，则添加失败，提示该域已存在 7. 存储域信息记录（域ID，域名，密码规范，DNS地址，同步时间，LDAP路径，用户名，口令，操作类型，BaseDN） |
| 输出 | 添加成功或失败及原因 |
| 补充说明 | 可读可写包括（域用户的增删改查，域组织单元的增删改查） |

### 删除域信息

|  |  |
| --- | --- |
| 功能描述 | 支持删除域信息 |
| 优先级 | 高 |
| 输入 | 域的ID |
| 操作序列 | 1. 删除域信息，及与该域相关的LDAP服务器信息，以及域下所有组织单元，用户（只删除系统中的数据不删除AD中的数据） |
| 输出 | 删除成功 |
| 补充说明 |  |

### 修改域信息

|  |  |
| --- | --- |
| 功能描述 | 支持修改域信息 |
| 优先级 | 高 |
| 输入 | 域的ID，新DNS地址，同步时间 |
| 操作序列 | 1. 检查新DNS地址是否正确，如果不正确，则返回失败，提示DNS信息有误 2. 如果正确，在数据中心修改该域的DNS信息及同步时间信息 |
| 输出 | 提示修改成功或提示修改失败 |
| 补充说明 |  |

### 修改域的连接信息

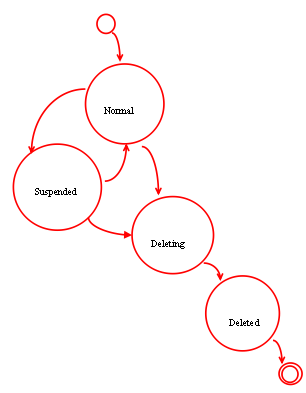
|  |  |
| --- | --- |
| 功能描述 | 支持修改域信息 |
| 优先级 | 高 |
| 输入 | 域的ID，LDAP路径，用户名，口令，BaseDN |
| 操作序列 | 1. 检查修改后的信息能否正常访问LDAP服务器，如果不能访问，则提示修改失败，返回失败原因 2. 如果访问成功，则修改数据中心该域的LDAP路径，用户名，口令，BaseDN信息 |
| 输出 | 提示修改成功或提示修改失败 |
| 补充说明 |  |

### 查询域信息

|  |  |
| --- | --- |
| 功能描述 | 支持查询域信息 |
| 优先级 | 高 |
| 输入 | 域的ID |
| 操作序列 | 1、从数据中心获取域的信息 |
| 输出 | 域ID，域名，密码规范，DNS地址，同步时间，操作类型  LDAP路径，用户名，口令，BaseDN |
| 补充说明 |  |

## 本地用户状态机

本地用户状态机



本地用户状态机跳转说明

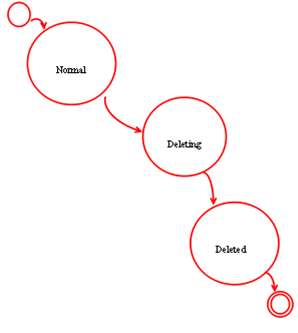
|  |  |  |
| --- | --- | --- |
| From | To | Condition |
| Normal | Suspended | **跳转行为：**  用户从正常状态到挂起状态  **状态：**  挂起  **跳转原因：**  管理员禁止用户账号使用 |
| Normal | Deleting | **跳转行为：**  用户从正常状态到正在删除用户  **状态：**  正在删除  **跳转原因：**  （A）管理员删除用户  （B）管理员删除用户所属组织单元 |
| Suspended | Normal | **跳转行为：**  用户从挂起状态到正常状态  **状态：** 用户状态正常  **跳转原因：**  管理员解除禁止用户 |
| Suspended | Deleting | **跳转行为：**  用户从挂起状态到正在删除用户  **状态：** 正在删除用户  **跳转原因：**  管理员删除用户  管理员删除用户所属组织单元 |
| Deleting | Deleted | **跳转行为：**  正在删除用户到删除完成  **状态：**  生命周期结束  **跳转原因：**  （A）用户的资源清理完成，已从系统中删除 |

用户状态与用户操作许可矩阵

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| User Status | Delete | Update | Query | Forbid | Unforbid | Edit Organtional Unit | Delivery Add | Delivery User |
| Normal | Admin | Admin  User | Admin  User | Admin |  | Admin | Admin | Admin |
| Deleting |  |  | Admin |  |  |  |  |  |
| Deleted |  |  |  |  |  |  |  |  |
| Suspended | Admin | Admin | Admin  User |  | Admin | Admin | Admin | Admin |

## 本地组织单元状态机

组织单元状态机



状态机跳转说明

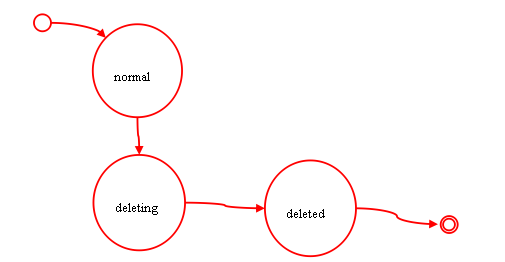
|  |  |  |
| --- | --- | --- |
| From | To | Condition |
| Normal | Deleting | **跳转行为：**  组织单元从正常状态到正在删除状态  **状态：**  正在删除  **跳转原因：**  管理员删除组织单元  管理员删除所属的上级组织单元 |
| Deleting | Deleted | **跳转行为：**  正在删除状态到删除完成  **状态：**  删除完成  **跳转原因：**  （Ａ）组织单元下的资源清理完成，已删除 |

组织单元状态与用户操作许可矩阵

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Organtional Unit Status | Delete | Update | Query | Edit | Delivery Add | Delivery Remove |
| Normal | Admin | Admin | Admin | Admin | Admin | Admin |
| Deleting |  |  | Admin |  |  |  |
| Deleted |  |  |  |  |  |  |

## 交付组状态机

交付组状态机

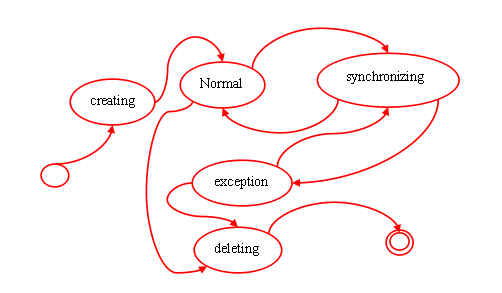


交付组状态跳转说明

|  |  |  |
| --- | --- | --- |
| From | To | Condition |
| start | normal | **跳转行为：**  成功创建交付组  **状态：**  交付组处于正常状态，可以添加（移除）用户和组织单元  **跳转原因：**  （A）管理员添加交付组 |
| normal | deleting | **跳转行为：**  交付组从正常状态到正在删除状态  **状态：**  正在删除，不可以添加（移除）用户和组织单元  **跳转原因：**  管理员删除交付组 |
| deleting | deleted | **跳转行为：**  正在删除状态到删除完成  **状态：**  删除完成，交付组不存在  **跳转原因：**  （Ａ）系统完成对交付组的删除 |

## 域状态机

域状态机

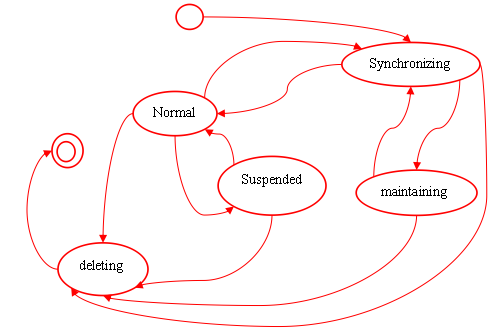


域状态机跳转说明

|  |  |  |
| --- | --- | --- |
| From | To | Condition |
| START | Creating | **跳转行为：**  系统正在添加域信息  **状态：**  进入正在添加状态  **跳转原因：**  （A）管理员添加了新域 |
| Creating | Normal | **跳转行为：**  系统成功添加了新域信息  **状态：**  进入正常状态  **跳转原因：**  （A）管理员成功添加了新域 |
| Normal | Synchronizing | **跳转行为：**  系统正在和AD进行域信息的同步  **状态：**  进入正在同步状态  **跳转原因：**  系统与AD自动同步或手动同步 |
| Synchronizing | Normal | **跳转行为：**  系统域信息和AD中信息同步完成  **状态：**  进入正常状态  **跳转原因：**  系统与AD自动同步或手动同步结束 |
| Synchronizing | Exception | **跳转行为：**  域同步时，出现异常，如无法连接服务器，连接信息错误  **状态：**  进入异常状态  **跳转原因：**  网络连接异常  AD中管理员密码被修改 |
| Exception | Synchronizing | **跳转行为：**  在上次同步时发生异常，但在本次同步时可以正常同步  **状态：**  进入正在同步状态  **跳转原因：**  系统与AD自动同步或手动同步 |
| Exception | deleting | **跳转行为：**  处于异常状态的域信息被删除，系统中对于的域组织单元和域用户都被删除，AD中相应的信息不变  **状态：**  进入正在删除状态  **跳转原因：**  管理员删除了处于异常状态的域信息 |
| Normal | deleting | **跳转行为：**  管理员删除了域信息，系统中对于的域组织单元和域用户都被删除，AD中相应的信息不变  **状态：**  进入正在删除状态  **跳转原因：**  管理员删除了域信息 |

## 域用户状态机

域用户状态机



状态机跳转说明

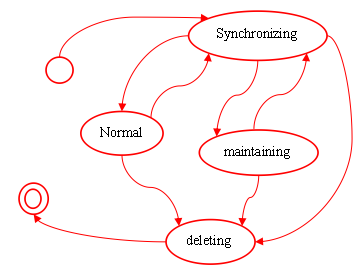
|  |  |  |
| --- | --- | --- |
| From | To | Condition |
| START | Synchronizing | **跳转行为：**  正在保持系统中和AD中新用户的信息一致  **状态：**  用户进入同步状态  **跳转原因：**   1. 管理员添加了新的域用户 2. 从AD中导入了新的域用户 |
| Synchronizing | Normal | **跳转行为：**  AD中用户的状态和系统中用户的状态处于一致状态，用户可以正常使用  **状态：**  用户进入正常状态  **跳转原因：**  系统与AD同步结束，用户进入正常状态 |
| Normal | Synchronizing | **跳转行为：**  为了保持AD中的用户状态和系统中处于一致状态，系统中的状态可能被修改，也可能被删除  **状态：**  用户进入正在同步状态  **跳转原因：**  系统与AD自动同步或手动同步 |
| Maintaining | Synchronizing | **跳转行为：**  之前处于维护状态中用户，在本次同步时，LDAP连接正常  **状态：**  域用户进入同步状态  **跳转原因：**  系统自动和手动同步时LDAP连接正常，可以正常同步 |
| Synchronizing | Maintaining | **跳转行为：**  域用户连接到了桌面，同步时发现LDAP服务器连接异常  **状态：**  域用户进入维护状态  **跳转原因：**  系统自动和手动同步时LDAP连接异常 |
| Maintaining | Deleting | **跳转行为：**  处于维护状态的用户被删除  **状态：**  域用户进入删除状态  **跳转原因：**  管理员删除了此用户 |
| Normal | Suspended | **跳转行为：**  域用户失去对VDI的访问权限，域用户信息被删除  **状态：**  正常域用户进入挂起状态  **跳转原因：**  管理员禁止了域用户的访问权限 |
| Suspended | Normal | **跳转行为：**  域用户重新对VDI的访问权限  **状态：**  域用户从挂起状态进入正常状态  **跳转原因：**  管理员解除了域用户的挂起状态 |
| Normal | Deleting | **跳转行为：**  域用户失去对VDI的访问权限，域用户信息被删除  **状态：**  正常域用户进入删除状态  **跳转原因：**  管理员删除了域用户 |
| Synchronizing | Deleting | **跳转行为：**  正在同步时，发现AD中的用户被删除，则系统中域用户信息被删除，权限关系被删除  **状态：**  域用户进入正在删除状态  **跳转原因：**  同步时，域用户被删除 |
| Suspended | Deleting | **跳转行为：**  挂起的用户被删除，系统和AD中域用户信息被删除，权限关系被删除  **状态：**  域用户进入正在删除状态  **跳转原因：**  管理员删除域用户 |

域用户状态与用户操作许可矩阵

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Desktop Status | delete | update | search | suspend | connect | login | Delivery(add,remove) |
| Normal | Admin | Admin  user | Admin | Admin | User  Admin | Admin  user | Admin |
| synchronizing |  |  | Admin |  |  |  |  |
| Suspended | Admin | Admin | Admin |  |  |  |  |
| maintaining | Admin |  | Admin |  |  |  |  |
| Deleting |  |  |  |  |  |  |  |

## 域组织单元状态机

域组织单元状态机error



状态机跳转说明

|  |  |  |
| --- | --- | --- |
| From | To | Condition |
| START | Synchronizing | **跳转行为：**  正在系统添加了和AD中信息一致的新域组织单元  **状态：**  组织单元处于同步状态  **跳转原因：**   1. 管理员添加新的域组织单元 2. 系统和AD同步时，导入了新的组织单元 |
| Synchronizing | Normal | **跳转行为：**  系统中组织单元信息和AD中已经一致  **状态：**  进入正常状态  **跳转原因：**  系统中组织单元的信息和AD中的信息同步结束 |
| Normal | Synchronizing | **跳转行为：**  正在将系统中组织单元的信息正在和AD中的信息进行同步  **状态：**  进入正在同步状态  **跳转原因：**  系统自动同步或手动同步 |
| Synchronizing | Maintaining | **跳转行为：**  同步时，LDAP服务器连接异常，组织单元进入维护状态  **状态：**  进入正在维护的状态  **跳转原因：**  系统和AD同步时，发现LDAP服务器连接异常 |
| Maintaining | Synchronizing | **跳转行为：**  上次同步时LDAP无法连接，在本次同步时LDAP可连接  **状态：**  进入同步状态  **跳转原因：**  系统自动或手动同步 |
| Maintaining | Deleting | **跳转行为：**  系统中域组织单元信息被删除  **状态：**  进入被删除状态  **跳转原因：**  管理员删除域组织单元 |
| Normal | Deleting | **跳转行为：**  系统中AD中域组织单元信息被删除  **状态：**  进入被删除状态  **跳转原因：**  管理员删除域组织单元 |

组织单元状态与用户操作许可矩阵

|  |  |  |  |
| --- | --- | --- | --- |
| OU Status | delete | search | Delivery(add,remove) |
| Normal | Admin | Admin | Admin |
| Synchronizing |  | Admin |  |
| Maintaining | Admin | Admin |  |
| Deleting |  |  |  |

# 项目的非功能性需求

## 用户界面需求

|  |  |
| --- | --- |
| **需求名称** | **详细要求** |
|  |  |
|  |  |
|  |  |
|  |  |

## 软硬件环境需求

|  |  |
| --- | --- |
| **需求名称** | **详细要求** |
|  |  |
|  |  |
| … |  |

## 项目质量需求

|  |  |
| --- | --- |
| **主要质量属性** | **详细要求** |
| 正确性 |  |
| 健壮性 |  |
| 可靠性 |  |
| 性能，效率 |  |
| 易用性 |  |
| 清晰性 |  |
| 安全性 |  |
| 可扩展性 |  |
| 兼容性 |  |
| 可移植性 |  |
| … |  |

## 其他需求

# 附录A 相关文档

## AD用户属性和系统用户属性对应关系表

|  |  |
| --- | --- |
| AD用户属性 | 系统用户属性 |
| sn | 真实姓名 |
| cn | 用户名 |
| telephoneNumber | 联系电话 |
| mail | 邮箱 |
| unicodePwd | 登录密码 |

## AD域属性和密码策略对应关系表

|  |  |
| --- | --- |
| minPwdLength | 密码最短长度 |
| pwdHistoryLength | 密码历史记录数（修改密码时不能和历史密码重复） |
| pwdProperties | 1表示启用了密码复杂度,0表示没有启用了密码复杂度 |
| minPwdAge | 密码最短有效时间 |
| objectGUID | 域ID |

## LDAP服务器错误码

|  |  |  |
| --- | --- | --- |
| 宏定义 | 错误代码 | 错误描述 |
| LDAP\_SUCCESS | 0 | 请求成功 |
| LDAP\_OPERATIONS\_ERROR | 1 | LDAP 库初始化失败 |
| LDAP\_PROTOCOL\_ERROR | 2 | 出现协议错误 |
| LDAP\_TIMELIMIT\_EXCEEDED | 3 | 超出时间限制 |
| LDAP\_SIZELIMIT\_EXCEEDED | 4 | 超出大小限制 |
| LDAP\_COMPARE\_FALSE | 5 | 比较结果为 FALSE |
| LDAP\_COMPARE\_TRUE | 6 | 比较结果为 TRUE |
| LDAP\_AUTH\_METHOD\_NOT\_SUPPORTED | 7 | 不支持此身份验证方法 |
| LDAP\_STRONG\_AUTH\_REQUIRED | 8 | 需要加强的身份验证 |
| LDAP\_REFERRAL\_V2 | 9 | LDAP 版本 2 检索 |
| LDAP\_PARTIAL\_RESULTS | 9 | 接收到部分结果和检索 |
| LDAP\_REFERRAL | 10 | 参照发生错误 |
| LDAP\_ADMIN\_LIMIT\_EXCEEDED | 11 | 超出服务器上的管理限制 |
| LDAP\_UNAVAILABLE\_CRIT\_EXTENSION | 12 | 没有精密扩展 |
| LDAP\_CONFIDENTIALITY\_REQUIRED | 13 | 需要保密 |
| LDAP\_SASL\_BIND\_IN\_PROGRESS | 14 | 多阶段绑定的中间绑定结果 |
| LDAP\_NO\_SUCH\_ATTRIBUTE | 16 | 请求的属性不存在 |
| LDAP\_UNDEFINED\_TYPE | 17 | 类型未定义 |
| LDAP\_INAPPROPRIATE\_MATCHING | 18 | 出现不适当的匹配 |
| LDAP\_CONSTRAINT\_VIOLATION | 19 | 出现约束冲突 |
| LDAP\_ATTRIBUTE\_OR\_VALUE\_EXISTS | 20 | 属性已存在或已被赋值 |
| LDAP\_INVALID\_SYNTAX | 21 | 语法无效 |
| LDAP\_NO\_SUCH\_OBJECT | 32 | 对象不存在 |
| LDAP\_ALIAS\_PROBLEM | 33 | 别名无效 |
| LDAP\_INVALID\_DN\_SYNTAX | 34 | 辨别名的语法无效 |
| LDAP\_IS\_LEAF | 35 | 该对象为叶对象 |
| LDAP\_ALIAS\_DEREF\_PROBLEM | 36 | 无法取消对别名的引用 |
| LDAP\_INAPPROPRIATE\_AUTH | 48 | 身份验证不正确 |
| LDAP\_INVALID\_CREDENTIALS | 49 | 提供的凭据无效 |
| LDAP\_INSUFFICIENT\_RIGHTS | 50 | 用户无足够的访问权限 |
| LDAP\_BUSY | 51 | 服务器忙 |
| LDAP\_UNAVAILABLE | 52 | 服务器不可用 |
| AD\_INVALID CREDENTIALS | 52e | 验证错误 |
| LDAP\_UNWILLING\_TO\_PERFORM | 53 | 服务器不处理目录请求 |
| LDAP\_LOOP\_DETECT | 54 | 引用链循环回至引用服务器 |
| LDAP\_NAMING\_VIOLATION | 64 | 存在命名冲突 |
| LDAP\_OBJECT\_CLASS\_VIOLATION | 65 | 存在对象类别冲突 |
| LDAP\_NOT\_ALLOWED\_ON\_NONLEAF | 66 | 不允许在非叶对象上操作 |
| LDAP\_NOT\_ALLOWED\_ON\_RDN | 67 | 不允许在 RDN 上操作 |
| LDAP\_ALREADY\_EXISTS | 68 | 对象已存在 |
| LDAP\_NO\_OBJECT\_CLASS\_MODS | 69 | 无法修改对象类别 |
| LDAP\_RESULTS\_TOO\_LARGE | 70 | 返回的结果太大 |
| LDAP\_AFFECTS\_MULTIPLE\_DSAS | 71 | 多个目录服务代理受到影响 |
| LDAP\_OTHER | 80 | 出现未知错误 |
| LDAP\_SERVER\_DOWN | 81 | 无法联系 LDAP 服务器 |
| LDAP\_LOCAL\_ERROR | 82 | 出现本地错误 |
| LDAP\_ENCODING\_ERROR | 83 | 出现编码错误 |
| LDAP\_DECODING\_ERROR | 84 | 出现解码错误 |
| LDAP\_TIMEOUT | 85 | 搜索超时 |
| LDAP\_AUTH\_UNKNOWN | 86 | 出现未知的身份验证错误 |
| LDAP\_FILTER\_ERROR | 87 | 搜索筛选器不正确 |
| LDAP\_USER\_CANCELLED | 88 | 用户已取消操作 |
| LDAP\_PARAM\_ERROR | 89 | 传递给例程的参数不正确 |
| LDAP\_NO\_MEMORY | 90 | 系统内存不足 |
| LDAP\_CONNECT\_ERROR | 91 | 无法建立到服务器的连接 |
| LDAP\_NOT\_SUPPORTED | 92 | 不支持此功能 |
| LDAP\_CONTROL\_NOT\_FOUND | 93 | LDAP函数找不到指定控件 |
| LDAP\_NO\_RESULTS\_RETURNED | 94 | 不支持此功能 |
| LDAP\_MORE\_RESULTS\_TO\_RETURN | 95 | 将返回其他结果 |
| LDAP\_URL\_ERR\_NOTLDAP | 96 | URL没有以LDAP开头 |
| LDAP\_URL\_ERR\_NODN | 97 | URL无DN |
| LDAP\_URL\_ERR\_BADSCOPE | 98 | URL字符串范围无效 |
| LDAP\_URL\_ERR\_MEM | 99 | 无法分配内存空间 |
| LDAP\_CLIENT\_LOOP | 100 | 检测到客户循环 |
| LDAP\_REFERRAL\_LIMIT\_EXCEEDED | 101 | 超出检索限制 |
| LDAP\_SSL\_ALREADY\_INITIALIZED | 112 | SSL初始化已完成 |
| LDAP\_SSL\_INITIALIZE\_FAILED | 113 | 初始化失败 |
| LDAP\_SSL\_CLIENT\_INIT\_NOT\_CALLED | 114 | 使用SSL之前必须初始化 |
| LDAP\_SSL\_PARAM\_ERROR | 115 | 参数错误 |
| LDAP\_SSL\_HANDSHAKE\_FAILED | 116 | 未能连接到SSL服务器 |
| LDAP\_SSL\_GET\_CIPHER\_FAILED | 117 | 不可使用 |
| LDAP\_SSL\_NOT\_AVAILABLE | 118 | 无法加载SSL库 |
| LDAP\_NO\_EXPLICIT\_OWNER | 128 | 不明确 |
| LDAP\_NO\_LOCK | 129 | 不能获得锁 |
| LDAP\_DNS\_NO\_SERVERS | 133 | DNS服务器不存在 |
| LDAP\_DNS\_TRUNCATED | 134 | DNS结果被删减 |
| LDAP\_DNS\_INVALID\_DATA | 135 | 无效的DNS数据 |
| LDAP\_DNS\_RESOLVE\_ERROR | 136 | 无法解析DNS域名 |
| LDAP\_DNS\_CONF\_FILE\_ERROR | 137 | DNS注册文件出错 |
| LDAP\_XLATE\_E2BIG | 160 | 输出缓冲区溢出 |
| LDAP\_XLATE\_EINVAL | 161 | 输入缓冲区被截断 |
| LDAP\_XLATE\_EILSEQ | 162 | 无法输入字符 |
| LDAP\_XLATE\_NO\_ENTRY | 163 | 代码集无法映射 |
| USER\_NOT\_FOUND | 525 | 用户不存在 |
| NOT\_PERMITTED\_TO\_LOGON\_AT\_THIS\_TIME | 530 | 此时不允许登录 |
| RESTRICTED\_TO\_SPECIFIC\_MACHINES | 531 | 在此工作站上不允许登录 |
| PASSWORD\_EXPIRED | 532 | 密码过期 |
| ACCOUNT\_DISABLED | 533 | 账户禁用 |
| ACCOUNT\_EXPIRED | 701 | 账户过期 |
| USER\_MUST\_RESET\_PASSWORD | 773 | 用户必须重置密码 |
| ERROR\_ACCOUNT\_LOCKED\_OUT | 775 | 用户账户锁定 |

# 附录B：需求建模与分析报告

## B.1 需求模型1

## B.n 需求模型N

# 附录C：需求确认

***提示：****需求确认规程请参见SPP-PROC-RM，主要分两步：（1）需求评审，（2）需求承诺。对需求的评审应当采用“正式技术评审方式”，将产生一份“需求评审报告”，规程请参见SPP-PROC-TR。在获取责任人（Stakeholders）对需求的承诺之前，该《产品需求规格说明书》必须先通过需求评审。*

|  |  |
| --- | --- |
| **需求评审报告摘要** | |
| 需求文档 | *输入名称，标识符，版本，作者，完成日期，…* |
| 需求评审报告 | *输入名称，标识符，评审日期，…* |
| 评审结论 | [ ] 工作成果合格，“无需修改”或者“需要轻微修改但不必再审核”。  [ ] 工作成果基本合格，需要作少量的修改，之后通过审核即可。  [ ] 工作成果不合格，需要作比较大的修改，之后必须重新对其评审。 |
| 评审意见 |  |
| 评审小组成员 | *输入评审小组成员* |

|  |  |
| --- | --- |
| **需求承诺** | |
| 需求文档 | *输入名称，标识符，版本，作者，完成日期* |
| 客户承诺 | *承诺…*  签字，日期 |
| 项目经理承诺 | *承诺…*  签字，日期 |