

聚源资源管理系统白皮书

一. 系统概述:

系统基于计算和存储分离的原则, 针对目前网络发展现状及存在的数据安全问题, 设计为面向企事业的分布式的数据应用、存储共享、安全控制系统。

系统组成:

系统由三部分组成:

资源共享子系统 (SSS)、资源备份子系统 (SBS)、资源系统客户端 (Client)

系统设计目的:

SSS 子系统存储文件, 用户在 Windows 系列操作系统上, 通过网上邻居访问 SSS 子系统, 进行文件操作。

SSS 子系统可将文件备份到 SBS 子系统, 也可以从 SBS 子系统恢复文件。

SSS 子系统可启用 VPN 功能, 用户通过安装在 Windows 之上的 Client 建立与 SSS 子系统的加密隧道。

二. SSS 功能要求:

2.1 SSS 概述

SSS 是灵聚思聚源资源管理系统的核心子系统, 安装在 SSS 子系统的硬件和操作系统之上。设计目的为集成文件共享、通信加密、数据备份和 B/S 远程管理等多项功能的软件。

2.2 SSS 功能

2.2.1 安装

1. SSS 以★.tgz 格式封装提供;
2. 安装程序名称: SSMS-LINVS-2.1v.tgz
3. 可在 FreeBSD5.x 系统及 RHEL、CENTOS、SUSE 等发行版上使用 #pkg_add 命令安装;
4. 默认安装路径为: /usr/local/ssms ;
5. 可自定义安装路径;
6. 安装后可配置为独立运行模式;
7. 远程管理支持 WEB 访问, 并提供 SSL 加密, 服务端口: 80;
8. 远程管理登录参考界面:
9. 远程管理访问参考界面:

2.2.2 注册

1. 系统安装时将在安装目录下自动建立“linvs”目录；
2. 系统安装后自安装之日 90 天内提供完全功能使用；
3. 90 天后，若 “linvs” 目录下没有正确的注册文件，系统应不能运行；
4. 注册文件要求根据硬件独立特征文件生成；
5. 在远程管理界面中提供注册文件生成、注册文件导出、注册文件导入功能；
6. 远程界面：参照图 2

2.2.3 用户权限

SSS 系统用户包括：系统用户和普通用户，二者均为虚拟用户，即不是操作系统用户。

系统用户权限：

1. 系统设 admin 系统管理员和 log 日志管理员；
2. admin 用户不能删除 log；
3. admin 和 log 用户权限如下表：

系统用户	系统管理权限	用户管理权限	日志管理权限 文件备份权限	共享目录管理权限
Log	无	无	有	有
Admin	有	有	无	有

Admin 可指定某普通用户具有共享目录管理的权限。

admin 权限详述：（权限详述见 2.2.5 文件备份和 2.2.6 日志管理）

1. 系统管理部分：
 - ★ 查看和定义共享主机名、主机摘要；
 - ★ 查看和定义可访问本系统的客户端 IP（IP 段）
 - ★ 查看和定义禁止访问本系统的客户端 IP（IP 段）
 - ★ 查看和执行 SSS 共享服务启用/停用；
 - ★ 查看和执行 SSS 名字服务启用/停用；
 - ★ 查看和定义 SBS 系统的 IP 地址；
 - ★ 查看和定义 SBS 系统中对应本 SSS 系统的相对路径；
 - ★ 查看和定义用户身份认证方式；
2. 用户管理部分：
 - ★ 普通用户组的查看、新建、删除、停用；
 - ★ 普通用户的查看、新建、删除、停用；
 - ★ 可将普通用户加入指定组，要求 1 个用户可加入多个组；
3. 共享目录管理部分：
 - ★ 新建共享目录，要求可输入相对路径；
例：即不必输入类似 “/var/sss/xxx”，仅需输入 “xxx”
 - ★ 删除目录共享，若目录下有文件（包括目录和文件），则仅删除目录共享，真实目录不删除；

★ 可定义共享目录可见用户（组）、可访问用户（组）、属主用户（组）、可写入用户（组）和写入后文件所属用户（组）；

说明 1: 当系统一级目录较多时，对于某用户（组）而言，只需要看到其应该看到的目录，而不论其不该看到的目录是否允许他访问。

说明 2: 若某目录属主为普通用户，即表示该普通用户可在此目录下新建共享，删除共享并定义目录访问权限；其访问策略 **admin** 可查看，可更改；

1. 查询共享目录情况：可对根据时间段、属主查询共享目录相对路径、属主、访问策略等信息；

普通用户权限：

1. 普通用户可通过浏览器键入 <http://ip>，进行用户身份鉴别后可修改自己的口令（仅适用于 sss 认证方式）；
2. 普通用户可通过浏览器键入 <http://ip>，进行用户身份鉴别后可进行共享目录管理（仅适用于该普通用户具有某共享目录管理权限的情况）；

2.2.4 用户身份认证

用户身份认证支持 sss 认证和 radius 认证。

1. sss 认证：

Windows 客户端发送质询加密口令到 SSS 子系统，sss 将收到的口令+用户 ID 与 sss 后台口令表进行验证，允许或拒绝用户通过。

注：用户密码包括字母，数字和符号，字母区分大小写，密码长度 6-20 位，不允许空口令。

2. 实现 radius 认证需 windows 客户端向 SSS 子系统发送用户 ID+明文口令，因此需要我公司提供可使 Windows 发送明文口令的注册表文件，以便用户导入该注册表文件。

采用 radius 认证方式时，SSS 子系统作为 radius 认证代理转发用户认证请求。要求：

★ 可实现指定用户进行 radius 认证；

说明：若系统有 1000 用户，其中 200 用户使用 radius 认证，800 用户使用 sss 认证，要求可实现分别认证。

2.2.5 共享目录访问控制

1. 共享目录创建和信息查看：

★ **admin** 可查看所有共享目录信息，可对根据时间段、属主查询共享目录相对路径、属主、访问策略等信息；

★ 具有共享目录属主权限的用户可查看其具有属主权限的共享目录信息，可对根据时间段、属主查询共享目录相对路径、属主、访问策略等信息；

★ **admin** 和共享目录属主可在其各自权限范围内创建新共享目录；

2. 取消共享：

★ **admin** 和共享目录属主可取消其权限范围内共享目录的共享；

- ★ 若该共享目录下有子目录或文件，只取消共享；

- 3. 共享目录可见控制：
 - ★ admin 和共享目录属主可定义该共享目录哪个用户（组）可见，下级目录可见与否以上级目录为最终标准；
 - 举例：aaa 目录 tec 用户不可见，aaa/bbb 目录属主即使定义该目录 tec 用户可见，也无效。

- 4. 共享目录可访问控制：
 - ★ admin 和目录属主可定义，可访问该目录的用户和组；

- 5. 共享目录可写入控制：
 - ★ admin 和目录属主可定义可将目录和文件写入该共享目录的用户和组；

- 6. 共享文件（目录）写入后权限控制：
 - ★ admin 和目录属主可定义目录和文件写入后可编辑、删除的用户和组；

- 7. 共享目录磁盘配额
 - ★ admin 和目录属主可定义共享目录磁盘配额；

2.2.6 文件备份

SSS 子系统文件备份包括：实时增量备份、定时增量备份和手动增量备份三种方法；文件恢复可先设为全部数据覆盖恢复。

1. admin 可查询和定义远程 SBS 子系统的 IP 地址和相对路径；
2. log 可查询和定义采用哪一种增量备份方法；
3. 若采用手动增量备份方法，log 可执行该操作，admin 不可执行该操作；
4. 可手动从 SBS 子系统恢复数据，该恢复操作可先设为全部数据覆盖恢复；
5. 要求：SSS 子系统与 SBS 子系统间通过 VPN 通信；

2.2.7 日志管理

1. 以下操作记入日志：
 - 合法登录：**要求记入登录时间、IP、用户名；
 - 非法登录意图：**要求记入登录时间、IP、SSS 系统拒绝原因（如：密码错误或来自于拒绝客户端等）；
 - 系统管理变更：**要求记入时间、变更者、变更者 IP、变更内容；
 - 用户管理：**要求记入 admin 所作所有用户管理操作，包括：时间、操作者、操作者 IP、操作内容；
 - 共享目录访问控制：**要求记入 admin 和共享目录属主对共享目录的策略操作，包括：时间、操作者、操作者 IP、操作内容；
 - 共享目录访问：**要求记录内容：时间、访问者、访问者 IP、访问的共享目录名（包括相对路径）；

目录和文件操作：要求记录内容：时间、操作者、操作者 IP、操作行为（新建、更名、删除、编辑等）；

2. 日志信息只可以由 log 访问；
3. log 可按用户名、时间段、客户端 IP 查询日志；
4. 可列表显示日志，也可以饼图、柱状图图形化显示；
5. log 可导出、删除日志；
6. log 本身操作也需要记入日志。

三. SBS 功能要求

3. 1 sbs 概述

sbs 是存储资源管理系统的备份子系统，安装在 SBS 子系统的硬件和操作系统之上。设计目的：为多个 SSS 提供文件备份功能和 B/S 远程管理等多项功能的软件。

3. 2 sbs 功能要求

3. 2. 1 安装

1. sbs 以*.tgz 格式提供安装；
2. 安装程序名称：linvs-sms-1.2.tgz
3. 可在 CentOS, RHEL 系统上使用#pkg_add 命令安装；
4. 默认安装路径为：/usr/local/linvs-sms ；
5. 可自定义安装路径；
6. 安装后可配置为独立运行模式；
7. 远程管理支持 WEB 访问，并提供 SSL 加密，服务端口：80；

3. 2. 2 注册

1. 系统安装时将在安装目录下自动建立“linvs”目录；
2. 系统安装后自安装之日 90 天内提供完全功能使用；
3. 90 天后，若“linvs”目录下没有正确的注册文件，系统应不能运行；
4. 注册文件要求根据硬件独立特征文件生成；
5. 在远程管理界面中提供注册文件生成、注册文件导出、注册文件导入功能；
6. 远程界面：参照图 2

3. 2. 3 用户权限

sss 系统用户包括：sysadmin 系统管理员用户和 syslog 日志管理员用户，二者均为虚拟用户，即不是操作系统用户。

sbsadmin 系统管理员用户权限：

- ★ 创建对不同 SSS 的路径

- ★ 启用/停用文件备份服务
- ★ 更改口令
- ★ 查看磁盘空间使用状况
- ★ 限定对应不同 SSS 备份目录的磁盘配额

sbslog 日志管理员用户权限:

- ★ 查看 sbsadmin 操作行为
- ★ 更改口令
- ★ 导出和删除日志
- ★ 查看磁盘空间使用状况

3. 2. 4 备份目录访问控制

sbsadmin 和 sbslog 均可查磁盘空间利用状况，均不能访问备份目录。