



Serv-U® 文件服务器 用户手册

Rhino Software, Inc.
P.O. Box 53
Helenville, WI 53137
U.S.A.



目录

| | |
|-----------------------------|------------|
| 目录..... | 2 |
| 注意..... | 8 |
| 如何购买 Serv-U..... | 9 |
| Serv-U 版本:..... | 10 |
| Serv-U Bronze Edition..... | 10 |
| Serv-U Bronze Edition..... | 错误! 未定义书签。 |
| Serv-U Gold Edition..... | 10 |
| 系统要求..... | 11 |
| 支持的平台..... | 11 |
| 建议使用的硬件..... | 11 |
| 推荐使用的硬件..... | 11 |
| 入门..... | 12 |
| 创建 Serv-U 首个域..... | 13 |
| 创建您的首个 Serv-U 用户..... | 14 |
| Serv-U 服务器理念..... | 15 |
| 用户账户类型..... | 15 |
| 用户集合..... | 15 |
| 服务器..... | 15 |
| 域..... | 15 |
| 群组..... | 16 |
| 用户..... | 16 |
| 用户界面约定..... | 17 |
| 了解用户界面约定..... | 17 |
| Serv-U 管理控制台..... | 18 |
| 管理控制台布局..... | 18 |
| 导航菜单..... | 19 |
| 选项卡式的配置页面..... | 19 |
| 启动 Web 客户端..... | 19 |
| 更改 Serv-U 主题..... | 19 |
| Serv-U 网络配置入门书..... | 20 |
| PASV IP 地址..... | 21 |
| 域名与描述..... | 23 |
| 域根目录..... | 23 |
| 域监听器..... | 24 |
| FTP——文件传输协议..... | 24 |
| FTPS——使用 SSL 的文件传输协议..... | 24 |
| SFTP——使用 SSH2 的安全文件传输..... | 24 |
| HTTP——超文本传输协议..... | 24 |
| HTTPS——使用 SSL 的超文本传输协议..... | 24 |
| 添加监听器..... | 25 |
| 类型..... | 25 |
| IP 地址..... | 25 |
| PASV IP 地址或域名（仅 FTP）..... | 25 |
| 仅用于 SSL 连接..... | 25 |
| 用于局域网（LAN）连接..... | 25 |
| 端口..... | 25 |
| 启用监听器..... | 25 |



| | |
|----------------------|----|
| 纯虚拟域 | 26 |
| 用户信息 | 27 |
| 登录 ID..... | 27 |
| 全名 | 27 |
| 密码 | 28 |
| 管理权限..... | 28 |
| 根目录..... | 28 |
| SSH 公共密钥路径..... | 29 |
| 账户类型..... | 29 |
| 默认的 Web 客户端..... | 29 |
| 电子邮件地址..... | 29 |
| 将用户锁定在根目录下..... | 29 |
| 启用账户..... | 30 |
| 总是允许登录..... | 30 |
| 说明 | 30 |
| 可用性..... | 30 |
| 目录访问规则 | 31 |
| 文件权限 | 32 |
| 读取 | 32 |
| 写入 | 32 |
| 追加 | 32 |
| 重命名..... | 32 |
| 删除 | 32 |
| 执行 | 32 |
| 目录权限 | 32 |
| 列表 | 32 |
| 创建 | 32 |
| 重命名..... | 32 |
| 删除 | 33 |
| 子目录权限 | 33 |
| 继承 | 33 |
| 作为 Windows 用户访问..... | 33 |
| 配额权限 | 33 |
| 目录内容的最大值..... | 33 |
| 强制访问控制 | 33 |
| 限制文件类型 | 34 |
| IP 访问规则 | 36 |
| 特定 IP——xxx | 36 |
| 范围——xxx-xxx | 36 |
| 通配符——* | 36 |
| 掩码——? | 37 |
| CIDR 阻止——/ | 37 |
| IPv6 支持..... | 37 |
| 启用排序模式..... | 37 |
| 示例文件——承包方..... | 38 |
| 示例文件——开通信息站..... | 38 |
| 示例文件——按名称访问..... | 38 |
| 传输比率和配额管理 | 39 |



| | |
|-----------------------------|----|
| 传输比率 | 39 |
| 配额 | 39 |
| 无传输比率限制的文件 | 40 |
| 虚拟主机 | 41 |
| 示例文件——虚拟主机 | 41 |
| 虚拟路径 | 42 |
| 物理路径 | 42 |
| 虚拟路径 | 42 |
| 包含于“最大目录大小”计算 | 42 |
| 示例文件——使用虚拟路径 | 43 |
| 示例文件——创建相对虚拟路径 | 43 |
| 群组 | 44 |
| 群组模板 | 44 |
| 配置 Windows 用户群组 | 44 |
| 加密 | 45 |
| 配置 FTPS 和 HTTPS 的 SSL | 46 |
| 使用现有证书 | 46 |
| 创建新证书 | 46 |
| 查看证书 | 47 |
| 高级 SSL 选项 | 47 |
| FIPS 选项 | 48 |
| SFTP（通过 SSH2 的安全文件传输） | 48 |
| 使用现有的私人密钥 | 48 |
| 创建私人密钥 | 48 |
| SSH 密码和 MAC | 48 |
| FTP 设置 | 49 |
| 全局属性 | 49 |
| 全局 FTP 响应 | 49 |
| 服务器欢迎消息 | 49 |
| 高级选项 | 49 |
| 编辑 FTP 命令与响应 | 49 |
| 信息 | 50 |
| FTP 响应 | 50 |
| 消息文件 | 50 |
| 高级选项 | 50 |
| 示例文件——定制 FTP 命令响应 | 50 |
| 数据库访问 | 52 |
| SQL 模板 | 52 |
| 用户和群组表格映射 | 52 |
| 示例文件——ODBC 验证 | 53 |
| SMTP 配置 | 54 |
| SMTP 服务器信息 | 54 |
| 验证信息 | 54 |
| Serv-U 事件 | 55 |
| 服务器事件 | 55 |
| 服务器与域事件 | 55 |
| 服务器、域、用户与群组事件 | 55 |
| 创建常规事件 | 56 |



| | |
|----------------------|----|
| 事件操作 | 56 |
| 电子邮件操作..... | 56 |
| 气球提示操作..... | 56 |
| 执行命令操作..... | 56 |
| 跟踪 Serv-U 中的活动 | 57 |
| 断开连接..... | 57 |
| 探查和聊天..... | 58 |
| 广播 | 58 |
| 中止 | 58 |
| 服务器与域统计 | 59 |
| 会话统计..... | 59 |
| 当前会话..... | 59 |
| 24 小时会话..... | 59 |
| 总会话..... | 59 |
| 最大会话数量..... | 59 |
| 平均会话长度..... | 59 |
| 最长会话 | 59 |
| 登录统计..... | 59 |
| 登录..... | 59 |
| 注销..... | 59 |
| 当前登录..... | 60 |
| 当前最大登录数..... | 60 |
| 上次登录时间..... | 60 |
| 上次注销时间..... | 60 |
| 平均登录持续时间..... | 60 |
| 最短登录持续时间秒数..... | 60 |
| 传输统计..... | 60 |
| 下载速度..... | 60 |
| 上传速度..... | 60 |
| 平均下载速度..... | 60 |
| 平均上传速度..... | 60 |
| 已下载..... | 61 |
| 已上传..... | 61 |
| 用户和群组统计 | 62 |
| 会话统计..... | 62 |
| 当前会话..... | 62 |
| 24 小时会话..... | 62 |
| 总会话..... | 62 |
| 最大会话数量..... | 62 |
| 平均会话长度..... | 62 |
| 最长会话 | 62 |
| 登录统计..... | 62 |
| 登录..... | 62 |
| 注销..... | 62 |
| 当前登录..... | 62 |
| 当前最大登录数..... | 63 |
| 上次登录时间..... | 63 |
| 上次注销时间..... | 63 |



| | |
|------------------------|----|
| 平均登录持续时间 | 63 |
| 最长登录持续时间 | 63 |
| 最短登录持续时间秒数 | 63 |
| 传输统计 | 63 |
| 下载速度 | 63 |
| 上传速度 | 63 |
| 平均下载速度 | 63 |
| 平均上传速度 | 63 |
| 已下载 | 63 |
| 已上传 | 64 |
| 保存统计 | 64 |
| 服务器与域日志 | 65 |
| 冻结日志 | 66 |
| 全选 | 66 |
| 清除日志 | 66 |
| 图例 | 66 |
| 过滤日志 | 66 |
| 下载日志 | 66 |
| 配置域日志 | 67 |
| 记录日志到文件设置 | 67 |
| 日志文件路径 | 67 |
| 启用“记录日志到文件” | 68 |
| 自动循环更新日志文件 | 68 |
| 清除旧的日志文件 | 68 |
| 不记录 IP | 68 |
| 数据库支持 | 70 |
| 许可证信息 | 71 |
| 名称 | 71 |
| 电子邮件地址 | 71 |
| Serv-U 版本 | 71 |
| 份数 | 71 |
| 购买日期 | 71 |
| 更新 | 71 |
| 版本信息 | 71 |
| 其他产品 | 71 |
| 注册 Serv-U | 71 |
| 系统变量 | 72 |
| 服务器信息 | 72 |
| 服务器统计 | 72 |
| 域统计 | 72 |
| 用户统计 | 73 |
| 上次传输统计 | 73 |
| 日期/时间 | 73 |
| 服务器设置 | 74 |
| 会话信息 | 74 |
| 文件信息 | 74 |
| 当前活动 | 75 |
| Serv-U 集成 DLL | 76 |



| | |
|----------------|----|
| 配置集成 DLL | 76 |
| 术语表 | 77 |



注意

版权所有 © 2010 Rhino Software, Inc. 保留所有权利。

该文档用于 Serv-U 文件服务器的安装与维护。

该手册按现状提供，不明示或暗示保证信息准确性或任何其它保证。因为 Serv-U® 可能安装于不同的硬件与软件环境，我们不提供适用于某一特定用途的保证。

良好的数据处理实践表明，任何新程序均需经过使用者以非关键数据充分测试后方可依靠。使用者必须承担使用此程序的所有风险。销售者的任何责任将仅限于更换产品。

联系方式

Rhino Software, Inc. 中国独家总代理商

Qast Software Group

地址：上海市江苏路 369 号兆丰世贸大厦 21 楼（200050）

电话：86-021-52550311

传真：86-21-52400179

电邮：support@rhinosoft.com.cn



如何购买 Serv-U

Serv-U 在初次安装日期后的 30 天内作为全功能的 Gold Edition 试用。为了继续使用拥有完整功能的 Serv-U，您必须购买 Serv-U 许可证。

访问以下网址可获得价格信息：<http://www.rhinosoft.com.cn/buy.htm>。

更多信息请咨询我们的销售代表：

Qast Software Group

地址：上海市江苏路369号兆丰世贸大厦21楼（200050）

电话：021-52550311

传真：021-52400179

电邮：support@rhinosoft.com.cn



Serv-U 版本:

Serv-U 文件服务器有三个不同版本，以满足当今服务器管理员的各项不同需求。RhinoSoft.com 提供的 Bronze Edition 拥有核心工具与功能，Silver Edition 中新增了 FTPS (SSL) 和虚拟主机支持，而 Gold Edition 拥有一款企业功能集，专供文件服务器通信量十分巨大的中大型企业使用。

Serv-U Bronze Edition

Serv-U Bronze Edition 提供的强健功能集包括用于文件管理和传输的所有工具：

- 一个域中可允许25个并发连接数
- 50个用户账户
- 支持 HTTP Web 客户端
- 支持虚拟路径映射
- 支持传输比率与配额

Serv-U Silver Edition

Serv-U Silver Edition 在 Bronze Edition 的基础上进行了功能扩展，添加了：

- 三个域中可允许100个并发连接数
- 250个用户账户
- 支持加密的 FTPS 连接
- 支持虚拟主机
- 通过 HTTP 登录页面实现用户密码恢复

Serv-U Gold Edition

Serv-U Gold Edition 致力于满足对企业级文件服务器的需求，它没有限制且能随企业的发展而不断扩展。除了支持 Silver Edition 中的加密 FTPS，Serv-U Gold Edition 还添加了 SSH 和 HTTPS 支持。鉴于此，Serv-U Gold Edition 企业版具有如下功能：

- 拥有无限并发连接数的无限域
- 无限用户数
- FIPS 140-2 支持，通过 OpenSSL 完成验证（证书 #1051）
- 自定义 HTTP 企业标志支持
- 支持用户和群组统计
- 支持加密的 HTTPS 连接
- 使用 SSH2 的 SFTP（通过安全外壳传输文件）
- 支持从一个位置远程管理多台服务器
- 支持用户和群组账户的 ODBC 数据库存储
- 支持基于用户账户的 NT-SAM /活动目录
- 支持电子邮件、外部程序和气球提醒事件
- 拥有无限并发连接数的无限域
- 无限用户数
- 自定义 HTTP 企业标志支持
- 支持用户和群组统计
- 支持加密的 HTTPS 连接
- 使用 SSH2 的 SFTP（通过安全外壳传输文件）



- 支持从一个位置远程管理多台服务器
- 支持用户和群组账户的 ODBC 数据库存储
- 支持基于用户账户的 NT-SAM /活动目录
- 支持电子邮件、外部程序和气球提醒事件
- 有关 Serv-U 文件服务器三个版本的更多信息，请访问 <http://www.Serv-U.com/>。

系统要求

支持的平台

Serv-U 独家支持以下 Windows 版本：

- Windows 2000 Professional / Advanced Server
- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008

支持 **32-位** 和 **64-位** (x64) Windows 版本。

建议使用的硬件

Serv-U 的最低硬件需求：

1 GHz+ Pentium / AMD CPU
256 MB 内存
70 MB 磁盘空间
800x600 VGA 视频卡和监视器
Internet Explorer 6+

推荐使用的硬件

3 GHz+ Pentium / AMD CPU
1 GB 内存
100 MB 磁盘空间
1024x768 VGA 视频卡和监视器
Internet Explorer 8

注意：Serv-U 是多线程的应用程序，通过有效使用资源从而为任何数量的用户提供快速的用户体验——尤其是繁重的下载/上传，因为这些操作都运行于其本身的线程中。不过，有效地运行 Serv-U 并不需要如此高的硬件规格。



入门

- 1) 从<http://www.Serv-U.com/dn.asp>页面上下载Serv-U 的最新版本，允许下载试用。您可以随时将该试用版注册成您购买的完整版本，且不需要任何额外配置。
- 2) 双击安装文件开始安装。如果您目前使用的是 Windows Vista、Windows 7 或 Windows Server 2008，您必须拥有管理员权限才可启动安装进程。您可能需要确认某个 Windows 用户账户控制对话框，以提醒您确实启动了此安装进程。
- 3) Serv-U 支持的安装语言包括英文、德文、法文、意大利文、日文和简体/繁体中文。请选择您偏爱的语言然后点击“确定”。注意：此时您选择的仅是管理控制台的默认语言。远程连接的用户可以选择他们想要的任何语言，然后使用 Serv-U 支持的语言连接到 Serv-U。
- 4) 请执行简单的安装步骤。您需要选择的选项包括：Serv-U 安装文件夹、开始菜单中所创建文件夹的名称、是否将 Serv-U 作为一项服务安装。推荐安装为一项服务，这样即使没有用户登录到服务器控制台，Serv-U 仍然可以运行。
- 5) 安装后点击“完成”以启动 Serv-U 管理控制台。



创建 Serv-U 首个域

Serv-U 的域是共享常规设置的用户和群组的集合，常规设置包括传输速率限制、服务监听器和目录访问规则等。大多数情况下，您的所有用户和设置位于同一个域中，无需创建单独的域。在“虚拟主机”部分讨论了使用不同域的情况。

注意：这并不表示所有用户共享相同文件的权限。Serv-U 中的每个用户对于您定义的目录拥有特殊权限，并且除非您明确给予其访问权限否则不能访问到任何文件或文件夹。

首次安装 Serv-U 后，不存在任何域。Serv-U 管理控制台会提示您创建第一个域。域向导会询问您如下信息：

- 域名：这是 Serv-U 中使用的临时名称，用来表示您的用户集合。也可以取名为类似 ftp.mydomain.com 或简单地称为“我的域”这些正式的名称
- 描述（可选项）：该域及其用途的文字描述。
- 监听器：Serv-U 支持 FTP、HTTP（所有版本）、FTP（Silver & Gold 版本）和带有 HTTPS 的 SFTP（仅限于 Gold 版本）。在安装过程中可以配置这些监听器。如果您已拥有 web 服务器，您可能需要将 HTTP/HTTPS 监听器设置为使用类似于 8080/8081 这样的非标准端口或“取消勾选”这些监听器从而将其禁用。
- IP 地址（可选项）：如果需要监听某个特定 IP 上的入站连接，请在这里输入。这必须是分配到服务器上网卡（NIC）的 IP 地址。大多数情况下应该是留空的。
- 密码加密模式：如果需要使用密码恢复功能（仅限于 Silver / Gold 版本），应将“密码加密模式”设置为“简单的双向”以允许 Serv-U 为用户恢复密码。还提供“无加密”选项，这是最不安全的存储用户密码的方式，不推荐使用。大多数情况下建议使用“服务器默认值”。
- 已完成！现在您可以点击“完成”以启动您的首个域。您可以根据 Serv-U 提示来创建新的用户账户。



创建您的首个 Serv-U 用户

Serv-U 用户是拥有访问权限的唯一账户，可以访问由管理员定义的一组特定文件夹和文件。如果要快速简便地创建用户帐户，请点击“域用户”菜单上的“向导”按钮并执行如下步骤：

- 1) 为您的用户账户选择唯一的登录 ID（又称“用户名”）。您还可以指定完整的名称和邮件地址（用于密码恢复或电子邮件事件）。
- 2) 为您的用户账户输入密码。
- 3) 选择该用户账户的根目录，如有需要可禁用“锁定根目录中的用户”选项。默认的（推荐）选项是“已启用”。
- 4) 选择该用户的权限。这两种选项是“只读”和“完全访问”。“完全访问”不允许该用户远程执行文件。
- 5) 点击“完成”。

随后该用户可以使用“域详情 | 监听器”菜单中启用的任何协议登录。



Serv-U 服务器理念

Serv-U 文件服务器使用一些概念，帮助您理解如何将文件服务器作为单一的分级单元进行配置和管理。Serv-U 文件服务器有四个相关的配置级别：服务器、域、群组 and 用户。其中，只有“群组”是可选的——所有其它级别是文件服务器的必要组成部分。下面提供了对每个级别的解释。

用户账户类型

在 Serv-U 文件服务器中定义用户账户的方法有多种，包括：

- 域用户——以域级别定义，域用户只能登录其所属的域。
- 全局用户——以服务器级别定义，全局用户可以登录文件服务器上的任何域。
- 数据库用户——能够以服务器和域级别定义，数据库用户存储在外部数据库中，能够通过 ODBC 访问，是本地账户数据库的补充。
- Windows 用户——能够以域级别定义，Windows 用户是 Windows 账户，可以位于本地系统也可通过域控制器访问，它作为本地账户数据库的补充，允许客户端使用 Windows 登录凭证登录到文件服务器。

由于能够使用相同的登录 ID 以各种级别指定用户账户，因此 Serv-U 使用层次结构确定哪种账户具有较高的优先级。以上列出的账户类型按其优先级高低顺序排列。如果能够以域和服务器级别指定用户账户，则域级别账户的优先级总是高于服务器级别指定的账户。

创建用户时，考虑它们需要何种访问类型，并相应选择合适的用户类型——以服务器级别输入设置节省了以域级别输入多个用户的时间和精力。

用户集合

不同于群组，用户集合对其包含的用户账户不提供任何级别的配置。

相反，它只是提供了一种方法将用户归类以便查看和管理。

例如，为了基于群组成员资格管理用户账户，可以创建用户集合，然而当用户账户更改群组成员资格时必须手动对其进行维护。

服务器

服务器级别是 Serv-U 文件服务器的基本单元，也是可用的最高配置级别。

它代表了文件服务器整体，并管理所有域、组和用户的行为。Serv-U

文件服务器带有一组默认选项，可逐个对其进行覆盖。因此，服务器是 Serv-U

配置等级的最高级别。域、组和用户从服务器继承了它们的默认设置。在每个较低级别可以覆盖继承的设置。不过，一些设置是服务器级别特有的，例如 PASV 端口范围。

域

一台服务器可以包含一个或多个域。通过域这个接口用户连接文件服务器并访问特定用户账户。

域的设置是从服务器继承而来。它也定义了其所有群组和用户账户能继承的设置集。

如果服务器级别的设置在域级别被覆盖，那么该域所有群组和用户账户将继承该值为其默认值。



群组

群组是进行额外配置的可选级别，通过它可以更为方便地对分享许多相同设置的相关用户账户进行管理。通过使用群组，管理员可以快速更改多个用户账户，而不必分别手动配置各个账户。群组从它所属的域中继承所有默认设置。它定义了所有群组成员用户继承的设置集。实际上，每个用户级别设置可在群组级别进行配置，或在用户级别被覆盖。

用户

用户级别处于等级底部。它可以从多个群组继承其默认设置（如果它是多个群组的成员），或从父域继承默认设置（如果它不是任何群组的成员或群组未定义默认设置）。用户账户标识了与文件服务器的物理连接，并定义了该连接的访问权限。以用户级别进行覆盖的设置别处不能被覆盖，并将永远应用于使用该用户账户进行验证的连接。



用户界面约定

Serv-U

文件服务器使用统一的方式显示配置选项，它不但表达了选项的当前值，也表达了该选项是否是默认（或继承）值。传统方式为使用所谓三态复选框达到上述目的。三态复选框有两个主要缺点：

1. 默认状态不能清晰地表达选项的当前值。在某些版本的 Windows 中，该选择框被选中并带灰色的背景色——即使当前未启用该选项！
2. 它们只能用来表示二进制值，即它们只能表示两个值——开或关。

Serv-U 文件服务器使用便于理解的不同协定克服了这些缺点。

当选项从父对象中继承值时，选项的文本将显示为常规的非粗体文本。

显示的值（无论是文本值还是复选框）随着父对象的更改而更改，因为该值是从父对象中继承而来。

不过，如果默认值被覆盖，其文本将以粗体显示。当前显示的值始终是选项的值，而与其父对象的更改无关。

了解用户界面约定

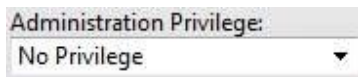
为了更好的说明用户界面约定，请参考以下案例文档。

Acme Technology Co. 是一家计算机维修公司，使用 Serv-U

文件服务器向出差工程师提供对共享企业资源的全局访问权限。每个工程师在文件服务器上都有自己的账户。

为便于管理用户账户，文件服务器管理员使每个用户账户成为“工程师”群组的成员。

该群组的管理权限被设为“无权限”，因为工程师没有管理文件服务器的责任。



一个工程师获得升职。

除了他当前的技术工作以外，他也被授予文件服务器的管理权限，以便协助其他工程师进行账户管理。

文件服务器管理员只需编辑该工程师的用户账户并将管理权限更改为“域管理员”。

该选项的文本变为粗体，表示它覆盖了默认值（无权限），该默认值是用用户账户从其“工程师”群组成员资格中继承得来。

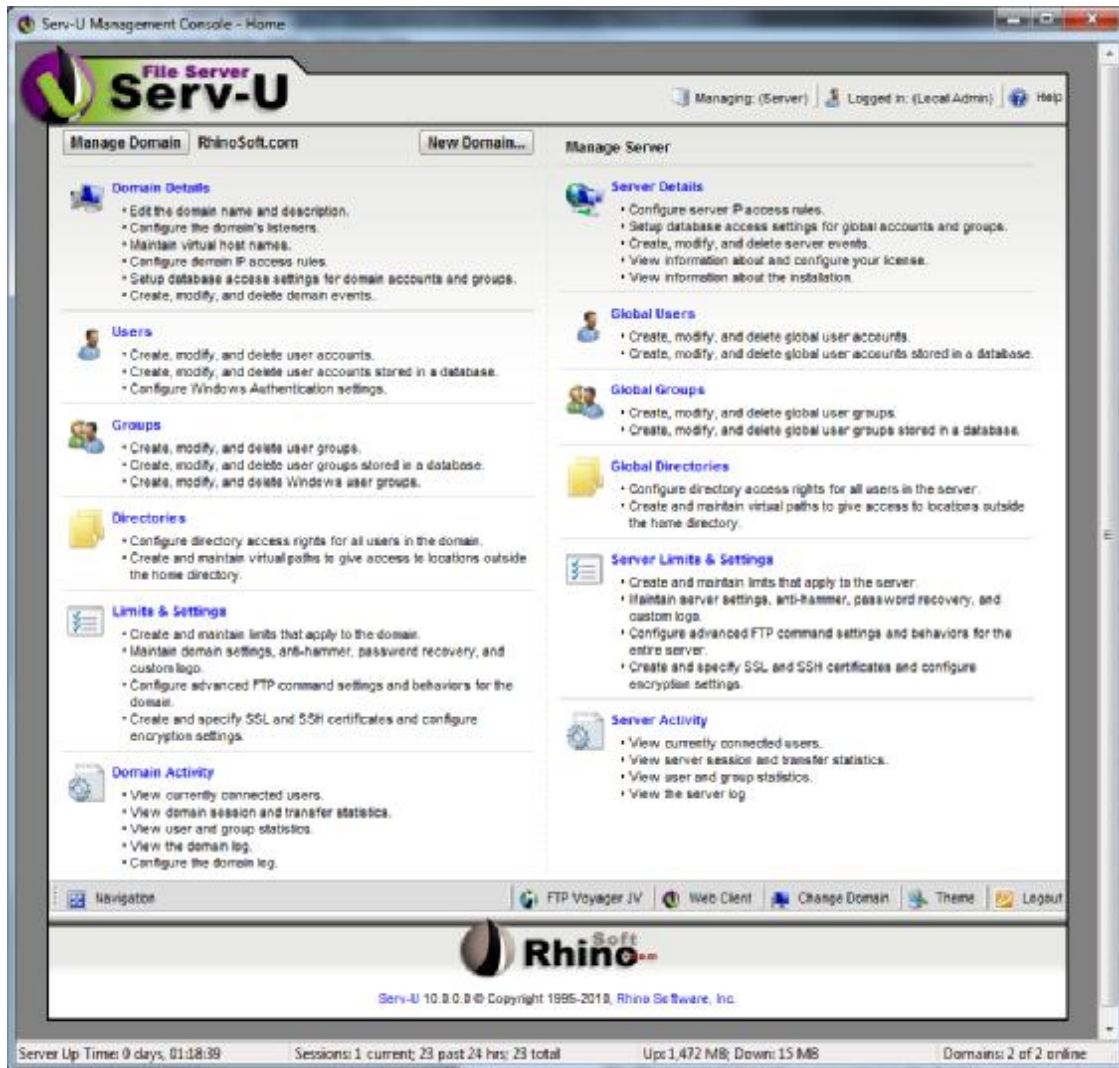


以后，通过选择“管理权限”下拉框中的继承默认值选项可以将管理权限恢复为从“工程师”群组继承而来的默认值。



Serv-U 管理控制台

Serv-U 管理控制台的设计旨在以熟悉的方式快速便捷地访问文件服务器配置选项。查看配置页面时，您可以通过点击左上角的 Serv-U 文件服务器标志在任何时候返回管理控制台主页面。



管理控制台布局

管理控制台显示为熟悉的控制面板类型的布局，并对相关选项进行归类。点击类别标题，例如“用户”，显示用户账户管理屏幕。从该屏幕可使用每个子类配置选项。也可选择子类以直接转到该子类的配置页面。

对于服务器管理员，管理控制台分两列显示。右列显示的类别与配置服务器范围的选项和设置有关。左列显示的类别与配置活动域有关。要更改活动域，请点击管理控制台左上角的“管理域”按钮，并选择另一个要管理的域。



另外，页脚的右下角提供了“更改域”按钮。可使用该方法从管理控制台的任何页面更改活动域。

域管理员只能访问适用于域的配置设置和选项，不能访问为系统管理员显示的服务器级别类项目。

导航菜单

导航菜单位于屏幕的左下角，提供了与 **Serv-U** 所有配置类别的直接链接。它是上下文相关的，显示了所选配置对象（域或服务器）的相关类别，以及当前所选类别的可扩展配置选项列表。

选项卡式的配置页面

当从管理控制台打开某个类别时，所有相关的子类别页面都在同一个屏幕上以选项卡形式显示。这允许在相关配置选项间快速导航。

启动 Web 客户端

当配置 **Serv-U** 文件服务器时，通过点击页面底部工具栏内合适的启动按钮，可在任何时候启动 HTTP 会话。如果获得使用授权，那么就可以在浏览器内运行 Web 客户端。如果获得使用授权，可以点击 FTP Voyager JV 按钮使用 Java 运行时环境启动 TP Voyager JV。

更改 Serv-U 主题

用来启动主题菜单的“主题”按钮位于该屏幕的右下角。该菜单列出了可用于更改 **Serv-U** 外观和风格的主题。只需选择下拉式组合框中的某个主题然后点击“确定”按钮。无需刷新页面即可加载该主题。



Serv-U 网络配置入门书

在理想的情况下，类似于 Serv-U 文件服务器的服务和应用程序以其专门的 IP 地址安装在专门服务器的 DMZ 区域。不过，鉴于对安全性问题的顾虑，现有的网络配置和可用 IPv4 地址的多次缺乏，Serv-U 必须安装在服务器的防火墙或路由器之后，并且使用“端口转发”来处理 FTP 流量。这就允许拥有有限公共 IP 地址的网络，在无需为额外公共 IP 地址、昂贵且无用的网络硬件支付额外费用的情况下，托管多项服务。与 Windows 活动目录集成时能实现最佳效果，因为活动目录集成要求该服务器是活动目录的成员之一。

如果您希望将 Serv-U

配置成与您的路由器或防火墙结合，您必须首先将该路由器（和/或防火墙）配置成可以转发您要的文件传输端口到您服务器的内部 IP 地址。虽然 FTP 是最普遍使用的协议，Serv-U 中同时包括其它协议。这些协议及其端口分别是：

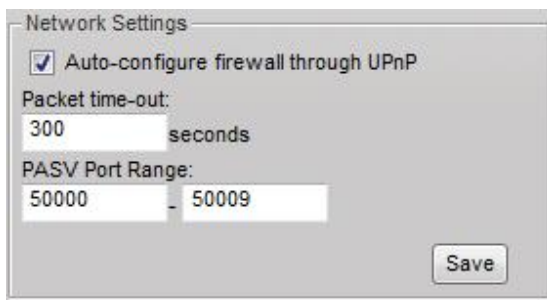
- FTP - FTP 端口号：21 和 PASV 端口范围：50000-50009
- FTPS（隐式）——FTP 端口号：990 和 PASV 端口范围：50000-50009
- SFTP——端口号：22
- HTTP——端口号：80
- HTTPS——端口号：443

| IP Address | Port | Type |
|------------------------------------|------|----------------------------|
| << All Available IPv4 Addresses >> | 21 | FTP and explicit SSL/TLS |
| << All Available IPv4 Addresses >> | 990 | Implicit FTPS (SSL/TLS) |
| << All Available IPv4 Addresses >> | 80 | HTTP |
| << All Available IPv4 Addresses >> | 443 | HTTPS (SSL encrypted HTTP) |
| << All Available IPv4 Addresses >> | 22 | SFTP using SSH |

可通过路由器路由文件传输流量并直接路由至 Serv-

U。路由器通常调用“端口转发”选项，一般出现在大多数家庭和较为简单的商用路由器的“高级”选项中。

您在配置端口转发时，请确保将“服务器限制与设置 | 设置”菜单中的“PASV 端口范围”也配置到 50000-50009。



Network Settings

Auto-configure firewall through UPnP

Packet time-out:
300 seconds

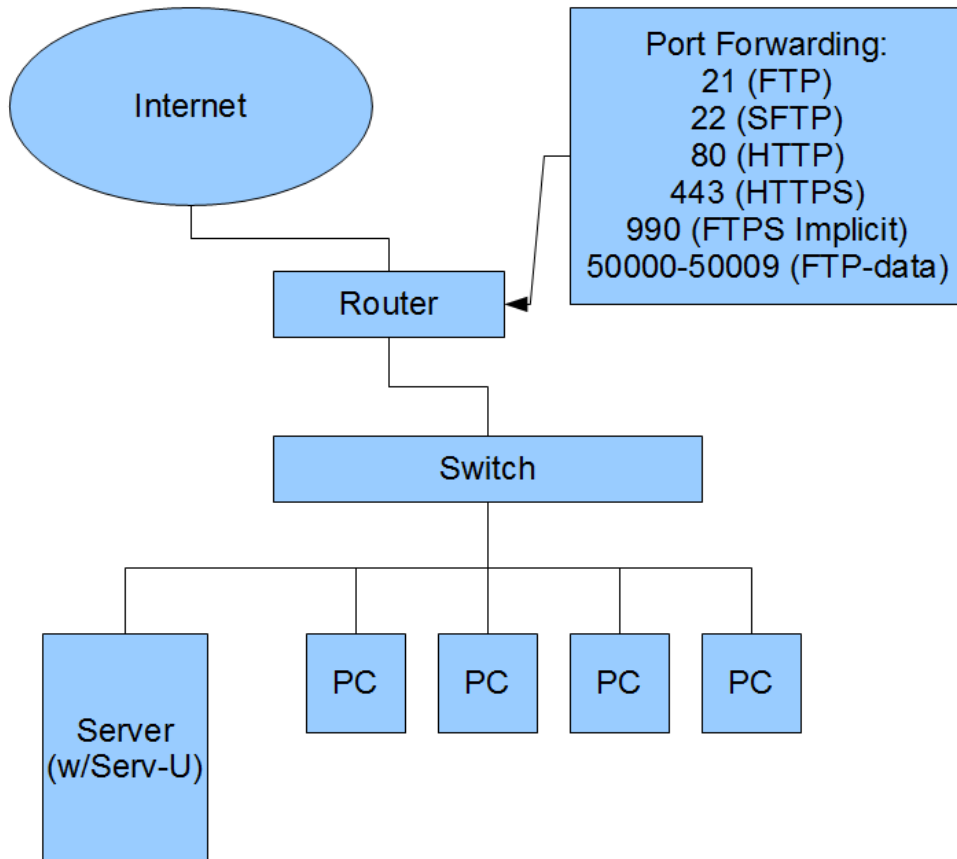
PASV Port Range:
50000 - 50009

Save



为了进一步简化流程，Serv-U 还支持名为“即插即用”的协议。从而允许 Serv-U 根据您的设置自动配置路由器或防火墙，您无需再亲手配置任何设置。不过在大多数情况下还是手动配置路由器比较好。

下方图表是 Serv-U 在小型/中型办公室网络中的应用。



PASV IP 地址

每个“FTP 和 显示 SSL/TLS”和“FTPS 隐式”监听器均包含名为“PASV IP 地址或域名”的配置选项。由于 FTP 和 FTPS 协议使用两种不同的连接来通信，所以就出现了这一配置选项。第一个连接最有名，且发生在 21 端口——被称为控制通道（Control

Channel），用于服务器与客户端之间的通信，传输了哪些数据，哪位用户正在登录等。

第二个连接的知名度较小，被称为数据通道（Data Channel），用于传输目录列表和文件。大部分客户端使用“PASV 模式”中的数据通道连接，发生该连接的端口范围是 50000-50009。

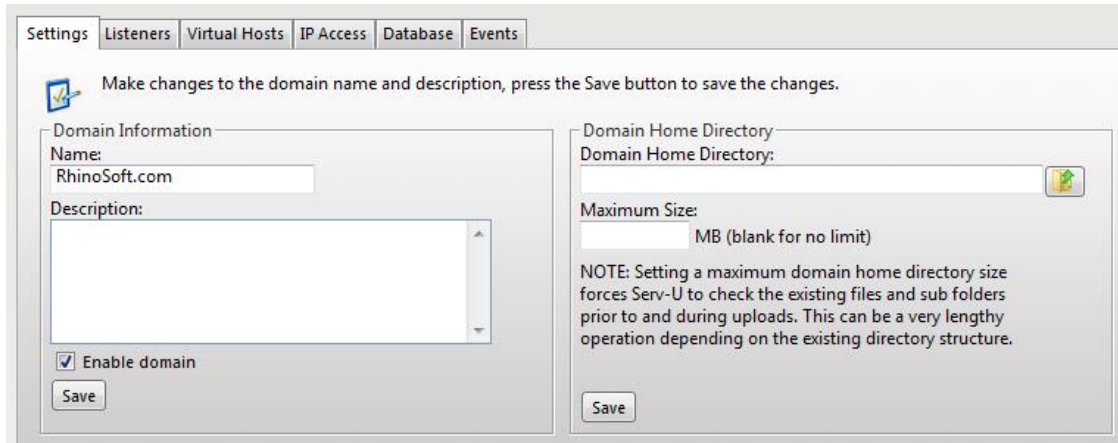
作为通过程的一部分，Serv-U 必须能够让客户了解应该如何连接到服务器，包括应该使用的端口号和 IP 地址。由于它与创建初始 FTP 连接时使用的 IP 地址不同，所以由 Serv-U 发送到客户端的通信信息是特殊的“227”信息。发出的 IP 地址通常是该服务器的私人 IP 地址，因为该服务器不知道路由器的 IP 地址。路由器随即自动调整此 227 信息并添加正确的 IP 地址。



路由器不执行这项任务或者客户端使用了加密连接都会导致路由器无法读取此 FTP 会话和执行该任务。在这种情况下，**Serv-U** 需要管理员来告知其哪些信息需要发送至客户端。要提供这些信息，必须以该服务器的公共 IP 地址或者服务器的域名更新“域详情 | 监听器” FTP 条目中的“PASV IP 地址”字段。大多数情况下，此域名实际上是最好的。因为如果通过这种方式更改 IP 地址，将会更新域名并且在没有任何干预的情况下更新 **Serv-U**。对于使用动态 DNS 服务的动态 IP 地址用户，该功能可发挥双倍的强大作用。



域名与描述



通过域名对各个域执行唯一标识。如果提供的名称不唯一，则会显示错误消息指出每个域需要唯一的名称。域名仅用于管理用户，对用户不可见且无法访问。

此外，通过使用说明字段，每个域可以拥有与其相关的附加说明性信息。类似于域名，说明文本也仅供有管理权限的用户使用。该字段用于说明域的目的，或总结文件服务器上由于存在域而变为可用的资源。

取消勾选启用域选择框，可以暂时禁用域。禁用时，所有用户都完全不能访问该域。该域仍存在于文件服务器上，所有设置被保存，且在禁用的同时仍能对其进行管理。要让用户可以再次访问该域，请勾选启用域选择框。

对上述域设置作出更改后，请点击“保存”按钮来应用更改。

域根目录

系统管理员可以为某个域配置一个根目录并且指定该目录的最大尺寸，从而限制该域的可用磁盘空间。该域的根目录并不影响用户目录访问规则，也不限制用户以任何方式可访问的路径。不过，为了计算一个域正在使用的磁盘空间，**Serv-U** 必须知道所有的域文件希望被存储的根目录。

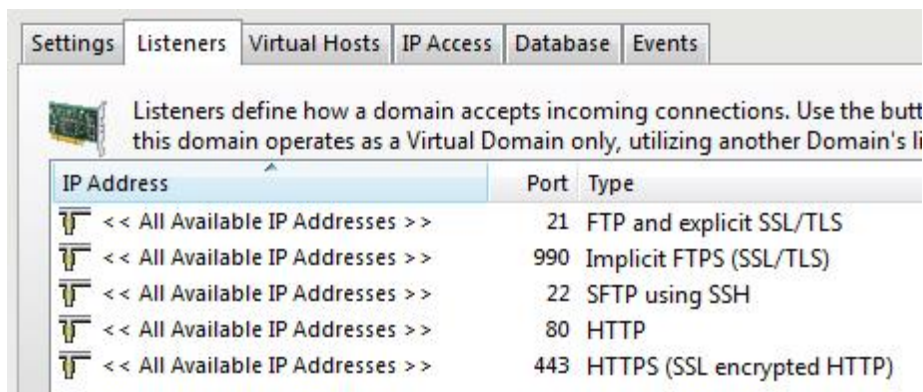
若要指定域的根目录，请在含有域根目录标签的字段输入一个路径。“浏览”按钮可用来选择路径。当您在为该域创建“域管理员”账户时，建议使其具有相同的根目录，从而确保该域的所有用户位于该域根目录的子目录中。以兆字节（**MB**）为单位输入该域允许使用的最大磁盘空间。将该字段留空或输入“**0**”表示该域没有最大值限制。当施加限制以后，该服务器就会拒绝可能导致超出最大值的任何上传。点击“保存”按钮应用这些更改。

注意：计算某个域正在使用的磁盘空间是一项费时的操作，这取决于根目录的结构。



域监听器

Serv-U 文件服务器提供高度可配置的界面，以便在域上启用不同的文件共享协议。使用适当标识的按钮可以添加、编辑和删除监听器。通过添加绑定于所需 IP 地址和端口的监听器，每个域可以监听多个端口和 IP 地址。除了选择监听器的连接属性之外，也必须选择文件共享协议。以下为 Serv-U 文件服务器支持的文件共享协议的列表和简短说明。



FTP——文件传输协议

FTP 是在因特网上传输文件的传统协议。它通常运作于默认的 21 端口。传统上，以纯文本形式处理 FTP，然而 SSL 连接通过使用 AUTH 命令获得明确支持。

FTPS——使用 SSL 的文件传输协议

FTPS 类似于 FTP，然而连接为 FTPS 配置的监听器，意味着执行任何协议通信前必须进行 SSL 连接。这一般被称为隐式 FTPS，它通常使用默认的 990 端口。

SFTP——使用 SSH2 的安全文件传输

SFTP 是通过安全外壳会话传输文件的一种安全方式。它在相同端口上执行所有协议通信和数据传输，而无需打开防火墙的多个端口，这一点不同于 FTP。SFTP 会话总是加密的。SFTP 使用默认的 22 端口。

HTTP——超文本传输协议

HTTP 是用于浏览网站的协议。它也是下载并传输文件的一种简单方法。向域添加 HTTP 监听器的优点是可以使用基本 Web 客户端，从而使用户无需独立的客户端就可以向文件服务器收发文件。HTTP 通常使用 80 端口。

HTTPS——使用 SSL 的超文本传输协议

HTTPS 类似于 HTTP，但其所有通信都用 SSL 进行保护。如同 FTPS，连接运行 HTTPS



协议的监听器意味着进行安全连接。HTTPS 的默认端口是 443。

添加监听器

点击“添加”按钮后，会显示监听器配置对话框。配置每个监听器选项后，点击“保存”按钮添加监听器到域。

类型

选择所需的该监听器所支持的文件共享协议。每个监听器只能支持单个协议。要向域添加更多文件共享协议，请为每个协议创建新的监听器。从上述可以找到对所支持的文件共享协议的简短说明。

IP 地址

在这里输入单个 IP 地址可以将其与监听器绑定。如果文件服务器没有外部 IP 地址（例如，它在路由器后面），该字段可以留空。该字段留空使 Serv-U 监听所有可用的 IP 地址。

PASV IP 地址或域名（仅 FTP）

如果监听器支持 FTP 协议，则可使用该附加字段来指定单独的 IP 地址用于 PASV 模式的数据传输。在这里输入 IP 地址保证 PASV 模式在不安全连接和安全连接上都能正常工作。如果文件服务器没有外部 IP 地址，请尝试使用 DNS4Me 并在该字段中输入您的 DNS4Me 域名。Serv-U 解析 DNS4Me 域名以保证总有正确的外部 IP 地址用于 PASV 命令响应。

仅用于 SSL 连接

该选项允许 PASV IP 地址或域名仅使用 SSL 连接，在提供 PASV IP 地址到连接的客户端时，SSL 连接总是必须的。启用该选项后，将不再向客户端提供专用于 PASV 模式的非 SSL FTP 连接的 IP 地址。

用于局域网（LAN）连接

通常情况下 Serv-U 不使用来自局域网（与 Serv-U 拥有相同网络的计算机）连接的 PASV IP 地址。启用该选项，PASV IP 地址同样可用于局域网连接。

端口

自动提供所选协议的默认端口。不过，可以使用 1 和 65535 之间的任何端口。当使用非标准端口时，客户端在试图连接域之前必须预先知道正确的端口。如果使用非标准端口，我们推荐使用 1024 以上的端口值以避免潜在的冲突。

启用监听器

取消勾选此选择框，从而临时禁用监听器。禁用时，监听器以不同的图标显示在列表中。



纯虚拟域

Serv-U 支持多个域“共享”相同的监听器。

换句话说，第一个域拥有必要的监听器配置，而其他域“驮靠”在第一个域之上。

这样，第二个域以虚拟方式存在。要使某个域“驮靠”在现有域的监听器配置上，请将该域的监听器列表留空。

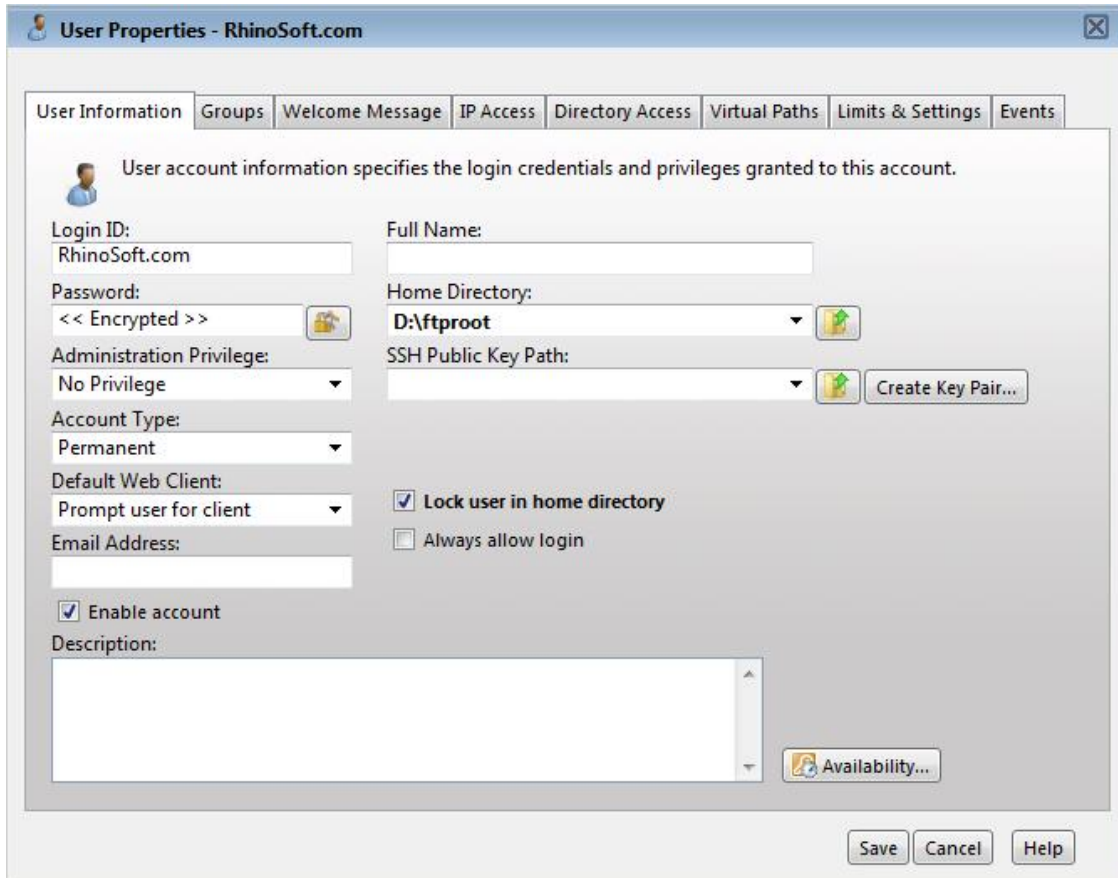
“驮靠”域必须至少定义了一个虚拟主机。

“驮靠”的方法仅作用于 **FTP** 和 **HTTP**

协议，因为只有这两个文件共享协议指定了建立连接后标识所需主机的方法。对于 **FTP** 连接，客户端必须发布 **HOST** 命令以标识所需域。对于 **HTTP** 连接，浏览器基于用来建立 **HTTP** 连接的域名，自动向 **Serv-U** 提供必需的主机报头。



用户信息



用户账户包括各种属性和设置。用户信息选项包含该用户账户的一般信息，如登录信息、根目录和账户类型。关于每种属性的详细信息请参见以下内容。

登录 ID

由客户端提供的登录 ID 是作为连接到文件服务器会话验证的一部分。除了登录 ID 之外，客户端还必须提供密码以完成验证。以某一级别指定的每个账户必须使用唯一的登录 ID。登录 ID 不得包含以下任一特殊字符： \ / < > | : ? *.

注意：有两种特殊登录 ID：“匿名”和“FTP”。这两个登录 ID 含义相同，可供访客访问文件服务器。这些用户无需密码，因此密码部分应该留空。虽然无需输入密码，但 Serv-U 会要求使用这些账户登录的用户提供其电子邮件地址以完成登录过程。

全名

可以使用账户的全名指定有关账户的更多识别信息。但不在客户端登录时使用。



密码

文件服务器会话验证所需的第二个项目是密码。密码应保密妥善保存，不应与除了账户所有者之外的人共享。强密码至少含有 6 个字符，包括大小写字母和至少一个数字。可以在限制中对密码的长度和复杂程度进行修改，制定限制。更多信息，请参见帮助文档中有关密码限制的内容。

另外，紧挨“密码”字段的“锁定”图标允许用户生成新的随机密码。这一新密码会遵循定义的密码长度要求。默认情况下，所有密码的长度是八个字符，且要求一定的复杂程度。如果“密码最小长度”少于或等于四个字符，该密码就是四个字符的长度——否则，生成的密码将遵照指定的域值。

管理权限

可以授予用户账户以下三种管理权限的其中之一：无权限、系统管理员或域管理员。该属性的值可以从群组成员继承。

无权限的用户账户就是一般的用户账户，只能从文件服务器上上传和下载文件。这些用户账户无法使用 Serv-U 管理控制台。

系统管理员可以执行任何的文件服务器管理活动，包括创建和删除域、用户账户，甚至可以更新文件服务器的许可证。通过 HTTP 远程管理登录的具有系统管理员权限的用户账户只要和计算机有物理连接，便能管理这台服务器。

域管理员只能管理其账户所属域中的事务。域管理员也无法执行可能影响其他域的和域相关的活动。域管理员无法执行的与域有关的活动包括配置域监听器或配置域的 ODBC 数据库访问。

Serv-U

还支持只读的管理员账户，允许管理员登录并查看域或服务器级别的配置选项，从而在与外方共事时为远程问题诊断做出了重大贡献。

只读的管理员权限等同于其完全访问的特权，唯一差别在于只读的管理员权限无法更改任何设置或创建/删除/编辑用户账户。

注意：配置具有管理权限的用户账户时，在指定其根目录时请谨慎处理。如果管理员的根目录不是“\”(根)且被锁定在根目录，则在配置文件服务器时将无法使用其根目录以外的文件路径。

根目录

用户账户的根目录是用户一旦登录到文件服务器后所处的位置。

必须为每个用户指定其根目录，如果用户是群组的成员，也可以在群组级别指定其根目录。

必须指定根目录的完整路径，包括驱动器字母或 UNC 共享名。如果找不到根目录，可以配置 Serv-U 为用户创建根目录。

指定根目录时，%USER% 宏可用于将登录 ID 插入到路径中。

最常用于配置群组级别或新用户模板中的默认根目录，从而确保所有新用户拥有唯一的根目录。当结合了用于 %HOME%

的目录访问规则，可以使用唯一的根目录配置新用户，且投入最少的精力即可拥有该位置的正确访问权限。



%DOMAIN_HOME% 宏也可以用来识别该用户的根目录。例如，将用户的根目录放入常规位置时，使用 %DOMAIN_HOME%\%USER%。

可以将根目录指定为“\”(根) 使用户获得系统级别的访问权限，能够访问所有的系统驱动器。为了使其正常工作，该用户必须不被锁定在其根目录中。

SSH 公共密钥路径

SSH 公共密钥可用于验证登录到 Serv-U 文件服务器的用户。
公共密钥路径必须指向服务器安全目录下的重要文件。该路径包含以下宏：

%HOME%——用户账户的根目录
%USER%——登录 ID，如果公共密钥以登录 ID 作为文件名的一部分使用
%DOMAIN_HOME%——该域的根目录，在域详情 |
设置中设置，如果这些密钥将放入与域根目录相关的中央文件夹

例如：

%HOME%\SSHpublic.pub
%HOME%\%USER%.pub
%DOMAIN_HOME%\SSHKeys\%USER%.pub

[点击这里](#)以了解有关创建 SSH 密钥对的更多信息。

账户类型

默认情况下所有账户都是永久账户，除非手动删除或禁用，将一直保留在文件服务器上。
可以配置账户在指定的日期被自动禁用或删除，只需配置账户类型。
选择合适的类型后，将显示账户过期日期控件。点击日历或过期日期选择将账户禁用或删除的日期。

默认的 Web 客户端

如果您的 Serv-U 许可证可以使用 FTP Voyager JV，则通过 HTTP 连接到文件服务器上的用户可以选择登录后使用哪种客户端。如果不需要询问用户使用哪种客户端，也可以使用默认客户端。如果该选项更改，将覆盖在服务器或域级别指定的选项。还可以通过群组成员的用户继承。使用继承默认值选项将其重新设置为相应的默认值。

电子邮件地址

当发送电子邮件通知到群组，以及执行密码恢复操作（使用 Web 客户端要求某个邮件地址发送恢复的密码给用户）时 Serv-U 事件可以使用“电子邮件地址”字段。在此输入电子邮件地址从而允许该用户账户的电子邮件通知或密码恢复操作。

将用户锁定在根目录下

被锁定在根目录的用户无法访问其根目录以上的路径。此外，根目录的实际物理地址显示为掩码，Serv-U



总是将其显示为“/”(根)。该属性的值可以从群组成员继承。

启用账户

取消选择该对话框将禁用当前账户。

禁用的账户仍然保留在文件服务器上，不过不能用来登录。如果希望重新启用该账户，请再次勾选启用账户选择框。

总是允许登录

启用该选项表示总是允许该用户账户登录，无论文件服务器级别设置的限制，如 IP 访问规则或最大会话数。这是非常有用的防止故障手段，以便确保关键的系统管理员账户总是能够在任何情况下远程访问文件服务器。由于该选项可以绕过任何访问规则，因此使用时需格外谨慎。该属性的值可以从群组成员继承。

说明

说明可以为条目添加更多注释，仅供管理员查看。

可用性

当用户连接到此服务器时，这项功能受到限制。可以根据一天中的某个时刻或者星期几设置限制。在给定可用时间以外的时间登录，会向用户发送“该用户账户目前不可用”消息。



目录访问规则

目录访问规则定义用户账户可以访问的系统区域。与传统的限制到用户和组级别的方式不同，Serv-U 通过全局目录访问规则的创建，将目录访问规则的使用扩展到域和服务器级别。

在服务器级别指定的目录访问规则可供文件服务器中的所有用户继承。

如果在域级别指定，则仅供该域内的用户继承。

继承的传统应用规则为，在较低级别指定的规则（如用户级别）可以覆盖在较高级别（如服务器级别）指定的冲突或重复的规则。

设置目录访问路径时，可以使用 `%USER%`、`%HOME%`、`%USER_FULL_NAME%` 和 `%DOMAIN_HOME%` 这些变量简化这一过程。例如，可以使用 `%HOME%/ftproot/`

创建目录访问规则，在用户根目录下指定“ftproot”文件夹。

以这种方式指定的目录访问规则具有“可移植性”，在实际的根目录更改时，能够保持原有的子目录结构。

这将减轻文件服务器管理员的维护负担。如果在路径中指定了 `%USER%` 变量，该变量将被替换为用户的登录

ID。变量在指定群组根目录时非常有用，可以确保用户继承符合逻辑且唯一的根目录。`%USER_FULL_NAME%` 变量可用于将“全名”值插入到该路径（用户必须拥有指定的“全名”才能使该功能发挥作用）。例如，用户“Tom Smith”在“D:\ftproot\Tom Smith”根目录中可以使用 `D:\ftproot\%USER_FULL_NAME%` 作为全名。


最后，`%DOMAIN_HOME%` 宏也可以用来识别该用户的根目录。例如，将用户及其根目录放入使用 `%DOMAIN_HOME%\%USER%` 作为全名的常规目录中。

目录访问规则按其列出的顺序应用。Serv-U

遇到的列表中第一条符合客户端路径的规则，即应用于该规则的规则。

换句话说，如果现有的规则拒绝访问某个子目录，但该规则列于授权访问父目录的规则之下，则用户仍无法访问该子目录。目录访问列表右边的箭头用于重新排列规则应用的顺序。

以下是列表和每种可用的访问权限的描述。



Directory Access Rule

Path:

Files

- Read
- Write
- Append
- Rename
- Delete
- Execute

Directories

- List
- Create
- Rename
- Remove

Subdirectories

- Inherit

Maximum size of directory contents: MB (leave blank for no limit)

Buttons: Save, Cancel, Help, Full Access, Read Only, Advanced >>



文件权限

读取

允许用户读取（例如：下载）文件。该权限不允许用户列出目录内容，执行该操作需要列表权限。

写入

允许用户写入（例如：上传）文件。该权限不允许用户修改现有文件，执行该操作需要追加权限。

追加

允许用户向现有文件中追加数据。该权限通常用于使用户能够对部分上传的文件进行续传。

重命名

允许用户重命名现有的文件。以前版本的 **Serv-U** 要重命名文件需要删除和写权限。从 7.0 版本开始，重命名是明确的权限。

删除

允许用户删除文件。

执行

允许用户远程执行文件。执行访问用于远程启动程序并通常应用于特定文件。这是非常强大的权限，在将该权限授予用户时需格外谨慎。具有“写入”和“执行”权限的用户实际上能够选择在您系统上安装任何程序。

目录权限

列表

允许用户列出目录中包含的文件。

创建

允许用户在目录中新建子目录。

重命名

允许用户在目录中重命名现有子目录。以前版本的 **Serv-U** 要重命名文件需要“删除”和“写入”权限。从 7.0 版本开始，重命名是明确的权限。



删除

允许用户在目录中删除现有子目录。注意：如果目录包含文件，用户要删除目录还需要拥有删除文件权限。

子目录权限

继承

允许所有子目录继承其父目录具有的不同权限。

继承权限适用于大多数情况，但是如果访问必须受限于子文件夹，例如实施强制访问控制（Mandatory Access Control）时，则取消继承并为文件夹逐一授予权限。

作为 Windows 用户访问

基于各种原因，可在外部服务器上保存文件和文件夹，从而集中化文件存储或提供额外的安全层。

在这种环境下，可以通过 UNC 路径（\\servername\folder\）而不是传统的“C:\ftproot\folder”路径来访问文件。

不过，在网络范围内访问已存储文件夹面临着另一挑战——默认情况下 Windows

服务在“本地系统”账户下运行，无法访问到网络资源。

要缓解所有 Serv-U 中的这一问题，可以将“Serv-U 文件服务器”服务配置成在某个网络账户下运行。

或者，如果拥有多台服务器或者 Serv-U

文件服务器服务基于安全性缘故需要在“本地系统”下运行，配置目录访问规则以使用指定的 Windows

用户执行文件访问。点击“高级”按钮可用来为各项个别目录访问规则指定特定的 Windows 用户。与 Windows 验证相似，目录访问受到 NTFS 权限的影响，不过 Serv-U 中的配置权限也是这种情况。

配额权限

目录内容的最大值

设置最大尺寸，动态地将目录内容大小限制在指定的值以内。

任何尝试的文件传输如果使目录内容超过这一限制值，则被拒绝。

它作为传统配额功能的替代功能，传统功能依赖于追踪所有的文件传输（上传和检测）以计算目录大小，且无法在用户文件服务器活动以外考虑对目录内容的更改。

强制访问控制

当用户需要访问相同根目录但不一定都能访问其下的子目录时，Serv-U 启用强制访问控制。

要在目录级别实施强制访问控制，只需禁用“继承”权限，如下所示（假设该规则应用于“D:\ftproot”）：





现在，用户可以访问“ftproot”文件夹但不能访问其下的子文件夹。必须为用户需要访问的子目录个别授予访问权限，从而在 Serv-U 文件服务器中提供强制访问控制的安全保护作用。

限制文件类型

如果用户使用 Serv-U 文件服务器上的存储空间保存与工作无关的文件，例如 MP3 音乐文件，通过配置目录访问规则并将其置于主目录访问规则之上（使用右边的箭头对规则重新排序）可以阻止传输 MP3 文件以杜绝上述操作，如下所示。在规则的文本条目中输入“*.mp3”并使用下列权限：



该规则拒绝传输任何以 **.mp3** 为扩展名的文件，并可作修改以显示任何文件扩展名。

同样，如果会计部门的员工只需要传输以 **.mdb** 为扩展名的文件，则可配置一对规则以授予传输 **.mdb** 文件的权限但拒绝对任何其他文件的访问，如下所示。

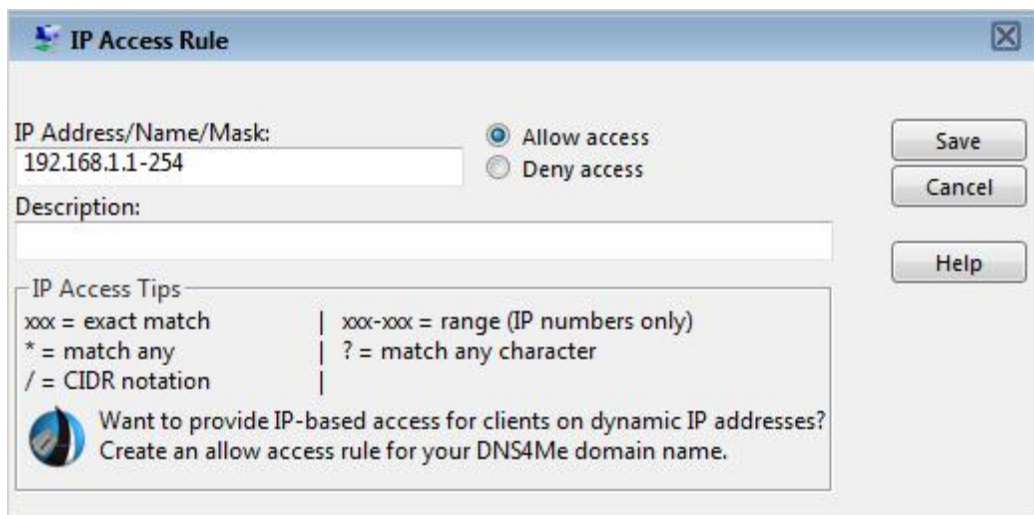
在第一条规则中输入用户根目录或需要访问的目录的路径，在第二条规则中输入需要访问的文件扩展名（例如“***.mdb**”）：



IP 访问规则

IP 访问规则是用户验证的一种补充形式，它可以限制登录特定 IP 地址、IP 地址群、甚至域。能够以服务器、域、群组 and 用户级别配置 IP 访问规则。以哪个级别指定 IP 访问规则也决定了连接在被拒绝前可以深入到哪个程度。发送欢迎消息前应用服务器和域级别的 IP 访问规则。当响应 HOST 命令以连接虚拟域时也应用域级别的 IP 访问规则。当客户端向服务器表明身份时，对 USER 命令的响应应用群组和用户级别的 IP 访问规则。

指定这些规则以确保特定网络内的客户端才能登录。要配置 IP 访问规则，首先要指定允许登录或不允许登录的客户端。点击“添加”按钮并指定应用该规则的 IP 地址或地址范围来添加规则。如果使用动态 DNS 服务，例如 DNS4Me，那么可以指定域名而不是 IP 地址，从而允许访问没有静态 IP 地址的移动客户端。也可使用反向 DNS 名称。如果创建了域名或反向 DNS 规则，Serv-U 必须执行反向 DNS 查询或 DNS 解析以应用这些规则。这可能会造成登录时少许时间的耽搁，这取决于系统 DNS 服务器的速度。



特殊格式允许使用范围和通配符，如下所示：

特定 IP——xxx

类似于 192.168.1.1 这样的完全匹配。

范围——xxx-xxx

类似于 192.168.1.10-19 这样的 IP 地址特定范围。

通配符——*

任何有效的 IP 地址值，例如 192.168.1.*，它类似于 192.168.1.0-255。



掩码——?

指定反向 DNS 名称的任何有效字符，例如 `server?.mydomain.com`。

CIDR 阻止——/

斜杠分隔符允许使用 CIDR 记数法来指定允许/阻止哪些 IP 地址。常见的 CIDR 块有 /8 (用于 1.*.*), /16 (用于 1.2.*.*) 和 /24 (用于 1.2.3.*)。块 /32 可用来指定单个 IP 地址。

IP 访问规则以显示的顺序依次应用。

因此可以将特定规则置于顶部，以便在以后应用列表中更宽泛的规则前允许（或拒绝）访问。

列表右侧的箭头可用来更改列表中单个规则的位置。

反恶意攻击规则不会自动阻止出现在该列表中的已认可地址。例如，本地 IP 地址 192.168.0.17 引起 Serv-U 启动其反恶意攻击规则来阻止此 IP 地址，但是该地址在列表中已明确认可，那么反恶意攻击规则不会自动阻止 192.168.0.17。

以下是它的工作方式。假定如下 IP 访问规则：

```
+ 192.168.0.17
+ *
```

当出现来自于 192.168.0.17 的活动，而用户搞错了密码，未发生自动 IP 阻止（通过超时、反恶意攻击、或由“会话活动”的系统管理员执行）是因为此 IP 地址已明确启用。末端项目 * 表示所有人都已认可，如果没有该值，那么将仅认可 192.168.0.17。如果反恶意攻击在不同的 IP 地址上发挥作用，会将阻止的 IP 地址添加到该列表的顶部，看起来就像：

```
- 10.10.10.1
+ 192.168.0.17
+ *
```

如果需要整段的 IP 地址，其工作方式如下所述：

```
+ 192.168.0.1-255
+ *
```

如果反恶意攻击在这些 IP 中的任何一个上发挥作用，将不会阻止此 IP。此处的关键就是通配符 *。Serv-U 将 *.* , *.*.* , *.*.*.* 检查为“任何”IP 地址。

IPv6 支持

Serv-U 同样支持基于 IPv6 地址范围、使用 CIDR 记数法的 IP 访问规则。应用 IPv4 标准，斜杠后的数字表示哪些地址可视为该范围的一部分，例如 `2001:db8::/32`。

启用排序模式

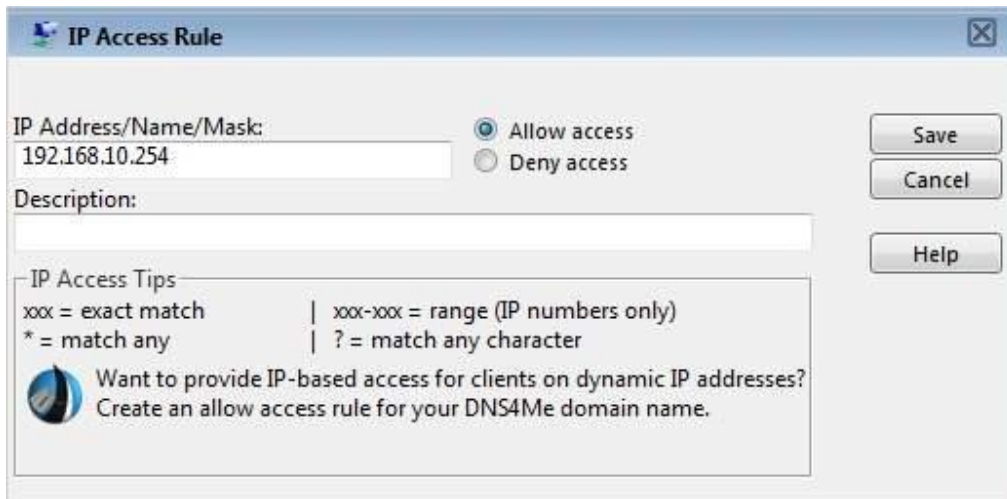
该选项允许 IP 访问列表按数字排序而不按处理顺序排序。以排序模式显示的 IP 访问列表不会更改规则处理的顺序——要查看规则优先级顺序，请禁用该选项。查看按数字排序的 IP



访问列表是一款有用的工具，可用于在查看冗长的访问规则列表时确定某个条目是否已经存在。

示例文件——承包方

临时雇佣了一名承包商，为了有效完成承包的工作需要访问 Serv-U 文件服务器。为了避免泄密，授权该承包商不能从工地办公室之外的位置访问服务器。办公室内的所有工作站分配到的 IP 地址为 192.168.10.2 到 192.168.10.254。因此，创建允许访问规则如下所示：



以上所示的规则允许承包商从办公室内访问文件服务器，但是因为创建了“允许访问”规则，因此添加了一条隐式的“拒绝所有访问”规则，该规则阻止从任何其它地方使用账户。他被授予其所处位置需要的访问权，但管理员拥有更高的控制权，可以控制从哪里能访问数据。

示例文件——开通信息站

用户需要从办公室内访问服务器，但出于安全考虑不能从办公楼内的一组开放式 PC 机房内进行登录。该机房分配到的 IP 地址为 192.168.15.100 到 192.168.15.110。因此，创建拒绝访问规则以拒绝对 192.168.15.100 到 192.168.15.110 的访问。请记住因为在使用 IP 访问规则时添加了隐式“拒绝所有访问”规则，在列表末尾必须添加“允许所有访问”规则允许用户从所有其它地址范围进行登录，这可以通过输入允许访问规则允许对“*.*.*”的访问来实现。列表末尾的这条规则保证了从所有其它 IP 地址可以进行连接。

示例文件——按名称访问

从 examplesite.com 域进行连接的用户应该是唯一可以访问该域的用户。为了限制可以访问该域的用户，采用基于反向 DNS 和主机名的 IP 访问规则。首先，创建新的访问规则允许访问 *.examplesite.com。

注意：为使这条访问规则起作用，相关 IP 地址的 PTR 记录必须匹配已创建的规则。一般来说，为使连接 IP 地址拥有这样的 PTR 记录，连接客户端必须从已分配了 IP 地址范围的大型公司进行连接——通常情况下，动态 IP 地址不能满足要求。



传输比率和配额管理

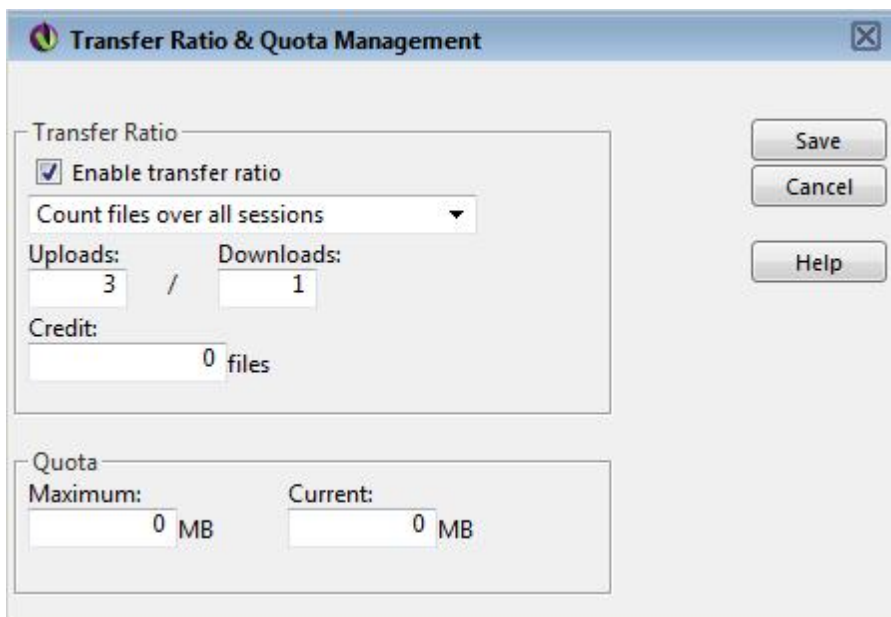
传输率和配额是在 Serv-U 文件服务器上管理文件传输的众多方式之一。有关这些选项的更多信息，请继续阅读本文档。

传输比率

传输比率是鼓励在文件服务器上共享文件的一种方便途径。通过指定合适的传输比率设置，您可以给用户指定“信用量”，用于传输指定数量的字节数或指定数量的完成文件。该方法通常用于使用户每上传下载“y”千兆字节的数据或文件，便能下载“x”千兆字节的数据或文件。

要为当前用户账户启用传输比率，请选中标记为启用传输比率的选择框。选择合适类型的传输比率应用于用户账户。传输比率可以按千兆字节或完成的文件进行追踪。还可以按每个建立的会话追踪，或为该用户账户创建所有会话追踪。

要配置比率，可以在比率的上传和下载两边都指定数值。例如，计算所有会话文件数的比率为 3/1 表示，用户账户要能够下载一个文件，必须上传三个文件。用户账户的当前信用量显示在信用值字段中。该值是当前值，可以将其初始化为非零的值以便授予用户初始信用值。



The screenshot shows a dialog box titled "Transfer Ratio & Quota Management". It is divided into two main sections: "Transfer Ratio" and "Quota".

- Transfer Ratio Section:**
 - There is a checked checkbox labeled "Enable transfer ratio".
 - A dropdown menu is set to "Count files over all sessions".
 - There are two input fields: "Uploads:" with the value "3" and "Downloads:" with the value "1", separated by a slash.
 - Below these is a "Credit:" field with the value "0 files".
- Quota Section:**
 - There are two input fields: "Maximum:" with the value "0 MB" and "Current:" with the value "0 MB".

On the right side of the dialog, there are three buttons: "Save", "Cancel", and "Help".

配额

配额是另外一种限制用户账户数据传输量的方法。如果为用户指定最大配额值，则该用户无法使用大于该值的磁盘空间。当前字段显示用户账户当前已使用的磁盘空间。初次配置配额时，这两个字段都不得留空。设置后，Serv-U 将追踪用户的文件上传和删除情况，并相应地更新当前字段值。

注意：使用配额有个明显的缺点，为了保持当前值的精确，不能对 Serv-U 以外的用户账户可以访问的目录内容进行更改。由于这些更改发生在文件服务器连接之外，Serv-U



无法追踪并更新当前的配额值。

除了配额以外，还可以考虑在为用户账户指定目录访问规则时限制目录内容的最大尺寸。
有关该选项的更多信息，请参见帮助文档中的“目录访问规则”部分。

无传输速率限制的文件

传输速率不限的文件列表中的文件不受任何传输速率的限制。

换句话说，如果用户必须上传文件以获取下载文件所需的信用量，则用户总是能够下载位于该列表中的文件，即使他们没有足够的信用量。通常用于特殊文件，如“自述文件”或目录信息文件，总能供用户访问。

指定传输速率不限的文件时，可以使用通配符“*”和“?”。使用“*”通配符可以指定任何长度的任意字符。

例如，输入“*.txt”可以自由下载任何后缀名是 .txt 的文件，无论其实际的文件名是什么。

“?”可以用于指定文件名或目录中的单个字符。

此外，设置传输速率不限的文件条目时可以使用完整路径或相对路径。

指定文件名时如果使用完整路径，则仅指定的文件不受传输速率限制。

如果使用相对路径，如只输入“readme.txt”，则无论其目录位于何处，该文件总是不受传输率限制。



虚拟主机

虚拟主机为多个域提供了一种方式，使它们可以共享相同的 IP 和监听器端口号。通常情况下，每个域监听器必须使用一组唯一的 IP 地址和端口号。利用虚拟主机，无需使用非标准端口号，就可以在仅有唯一 IP 地址的系统上使用多个域。通过正确使用虚拟主机，多个域可以共享相同的监听器。此功能仅在当前许可证支持托管多个域时可用。

要为域配置虚拟主机，点击“添加”按钮并输入域的虚拟主机名。虚拟主机名通常是用来连接域的全称域名，例如“ftp.Serv-U.com”。

客户端连接到所需虚拟主机所采用的方式取决于连接 Serv-U 所使用的协议。

FTP

FTP 用户可以使用这两种方式中的一种来连接特定虚拟主机。如果 FTP 客户端支持 HOST 命令，就可以在登录前向 Serv-U 发出此命令来识别虚拟主机。不然，可以使用以下格式的登录 ID 来提供虚拟主机：virtual_host_name|login ID。先输入虚拟主机名，接着输入竖线字符（“|”），最后输入登录 ID。

SFTP

希望连接到特定虚拟主机的 SFTP 用户必须使用指定的登录 ID 格式，如上方 FTP 部分中的描述。

HTTP

对于 HTTP 用户而言，浏览器会为 Serv-U 自动提供用于搜索站点的主机名，允许 Serv-U 从输入浏览器导航栏中完全符合要求的域名中识别虚拟主机。

示例文件——虚拟主机

多个域在同一个服务器上进行配置，该服务器有一个 IP 地址和两个全称域名（FQDN）指向它。由于用户必须使用端口 21 来连接到这两个域，请在每个域上配置虚拟主机，以使 Serv-U 能区分对这两个域的请求。在每个域上设置了相同的监听器属性后，请打开“虚拟主机”选项卡，点击“添加”，然后输入客户端用于连接域的 FQDN

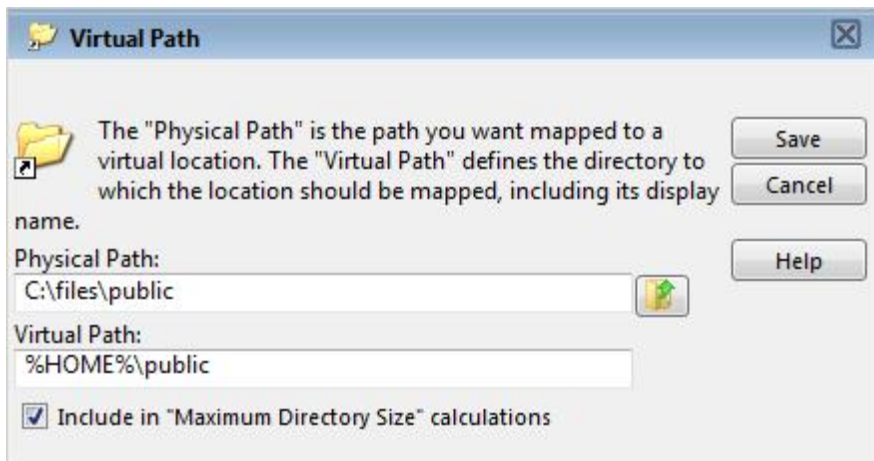
使用 FTP 连接服务器后，用户能发送 HOST ftp.Serv-U.com 命令以连接文件服务器上相应的域。FTP 和 SFTP 用户通过其 ftp.Serv-U.com|login ID 的登录 ID 来识别虚拟主机。如果通过 HTTP 进行连接，用户可以通过访问 http://ftp.Serv-U.com 来连接该域。



虚拟路径

虚拟路径允许用户访问根目录以外的文件和文件夹。

虚拟路径仅定义一种方式，将现有目录映射到系统中的其他位置，使用户能够在其可访问的目录结构中看到该目录。为了能够实际访问该映射位置，用户还是必须拥有虚拟路径的物理路径所指定的目录访问规则。



和目录访问规则一样，虚拟路径能够以服务器、域、群组 and 用户级别进行配置。

以服务器级别创建的虚拟路径可供文件服务器上的所有用户使用。

如果以域级别创建，则仅供该域内的用户访问。Serv-U

的细粒度文件访问控制甚至允许为个别用户或群组专门创建虚拟路径。

物理路径

物理路径是系统或网络中的真实位置，可以置于可供用户访问的虚拟位置。

如果物理路径位于同一计算机上，应使用完整路径，如“D:\inetpub\ftp\public”。也可以使用 UNC 路径，如“\\Server\share\public”。为了使用户能够看到虚拟路径，必须具有指定给物理路径的目录访问规则。

虚拟路径

虚拟路径是应该向用户显示的物理路径位置。通常在虚拟路径中使用宏 %HOME%

来取代在用户根目录中指定的物理路径。指定虚拟路径时，最后指定的目录作为用户目录列表中显示的名称。例如，虚拟路径“%HOME%/public”取代指定物理路径中名称为“public”的文件夹，该文件位于用户的根目录下。也可以使用不带任何宏的完整路径。

包含于“最大目录大小”计算

勾选此功能时，在“最大目录大小”计算中包含虚拟路径。

取消勾选此功能时，在“最大目录大小”计算中不包含虚拟路径。

“最大目录大小”限制影响可以上传多少数据的目录大小。



示例文件——使用虚拟路径

授予一组 Web 开发者可以访问目录“D:\ftproot\examplesite.com\”的权限，以便进行 Web 开发。开发者还需要访问位于“D:\corpimages\”的图片库。为了避免授予群组访问 D 盘根目录的权限，必须配置虚拟路径使图片库看起来包含在群组的根目录中。要在 Web 开发者的群组中添加虚拟路径以便“使用户能够访问目录”，可以将“D:\corpimages\”指定为物理路径，同时将“D:\ftproot\examplesite.com\corpimages”指定为虚拟路径。请确保也为“D:\corpimages\”添加群组级别的目录访问规则。开发者现在可以访问图片库，同时无需折衷安全性或重新安排共享的资源。

示例文件——创建相对虚拟路径

继续上面的例子，如果 Web 开发者群组的根目录被重新安排到其他驱动器，则不仅需要更新其根目录，还需要更新虚拟路径以反映这一更改。要避免此问题，可以使用 %HOME% 宏创建相对虚拟路径位置，便无需在根目录更改时更新虚拟路径。和使用“D:\ftproot\examplesite.com\corpimages”作为虚拟路径不同，可以使用“%HOME%\corpimages”。这将告诉 Serv-U 将“corpimages”虚拟路径置于群组根目录中——无论根目录处于什么位置。如果之后根目录有所更改，虚拟路径仍将出现在根目录中原来的位置。



群组

群组可以用来和多个用户账户共享相同的配置选项。配置群组的方法和配置用户账户类似。

基本上用于用户账户的每个配置选项都能够以群组级别进行设置。

用户要继承群组的设置，必须是该群组的成员。仍然能够以用户级别覆盖用户从群组成员中继承的权限和属性。一个用户可以是多个群组的成员以便获取多种权限，如目录或 IP 访问规则。

和用户账户一样，群组也能够以多个级别创建，包括：

- 全局群组
- 域群组
- 数据库群组——提供服务器级别与域级别

不过，群组仅可用于以相同级别定义的用户账户。

换句话说，全局用户（即以服务器级别定义的用户）只能是全局群组的成员。

以此类推，在特定域定义的用户仅可能是为该域创建的群组中成员。

这一限制还应用于在数据库中创建的群组，以相同级别在数据库中创建的用户才能是这些群组的成员。

使用“添加”、“编辑”与“删除”按钮来管理可用的群组。

群组模板

Serv-U 帮助管理员为新群组配置模板，只需点击“模板”按钮即可。

打开后，除了群组名称以外，可以像配置其他群组一样配置模板群组。

将设置保存到模板后，所有手动创建的新群组将使用模板中的设置作为其默认设置。

如果要将所有群组配置为默认使用一些基本设置，使用群组模板是一种在创建新群组时节省时间的好方法。

配置 Windows 用户群组

管理员能够允许客户端使用本地 Windows 用户数据库，或通过域服务器能够访问的账户登录到文件服务器。这些账户在本地 Serv-U 用户数据库中不存在，无法进行个别配置。

为了协助账户配置，所有通过这种方法登录的用户都属于默认 Windows 用户群组。

点击该按钮可以像配置普通群组一样配置该群组。不过，对该群组的更改将仅应用于 Windows 用户账户。



加密

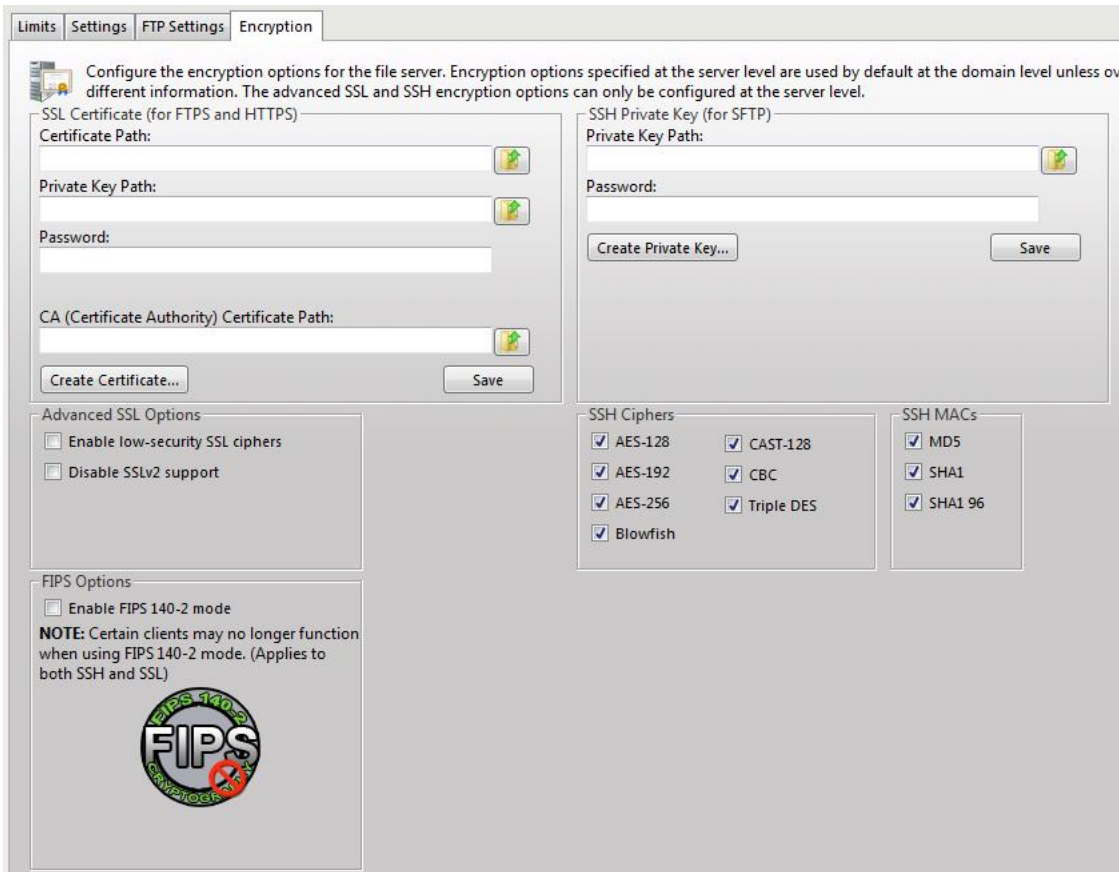
Serv-U 支持两种加密数据传输方式——安全套接层（SSL）和安全外壳 2（SSH2）。SSL

用于保护文件传输协议（FTP）和超文本传输协议（HTTP）。SSH2

是一种安全地与远程系统进行交互的方式，该远程系统支持通常称为 SFTP 的文件传输方式。除了名称，SFTP 与 FTP 协议自身没有任何共同之处。

为了使每种加密方法有效工作，必须提供证书和/或私人密钥。SSL 需要提供证书和私人密钥，而 SSH2 只需私人密钥即可。如果您没有所需文件，Ser-U 可以创建这些文件。

以服务器级别指定的加密选项被所有域自动继承。以域级别指定的加密选项自动覆盖相应的服务器级别选项。某些配置选项仅可用于服务器。



当在 Serv-U 中创建 SSL/TLS、SSH 和 HTTPS 加密域时，加密域不能共享监听器，了解这一点很重要。因为 SSL/TLS 和 SSH 加密是基于对在 IP

地址之间传送的通信进行加密，因此每个域都必须具有单独的监听器才能正确操作。

如果创建了多个加密域共享监听器，则第一个创建的域能优先使用监听器，造成其它加密域不能正确工作。

要操作多个加密域，请修改每个域的监听器以确保它们监听唯一的端口号。



配置 FTPS 和 HTTPS 的 SSL

使用现有证书

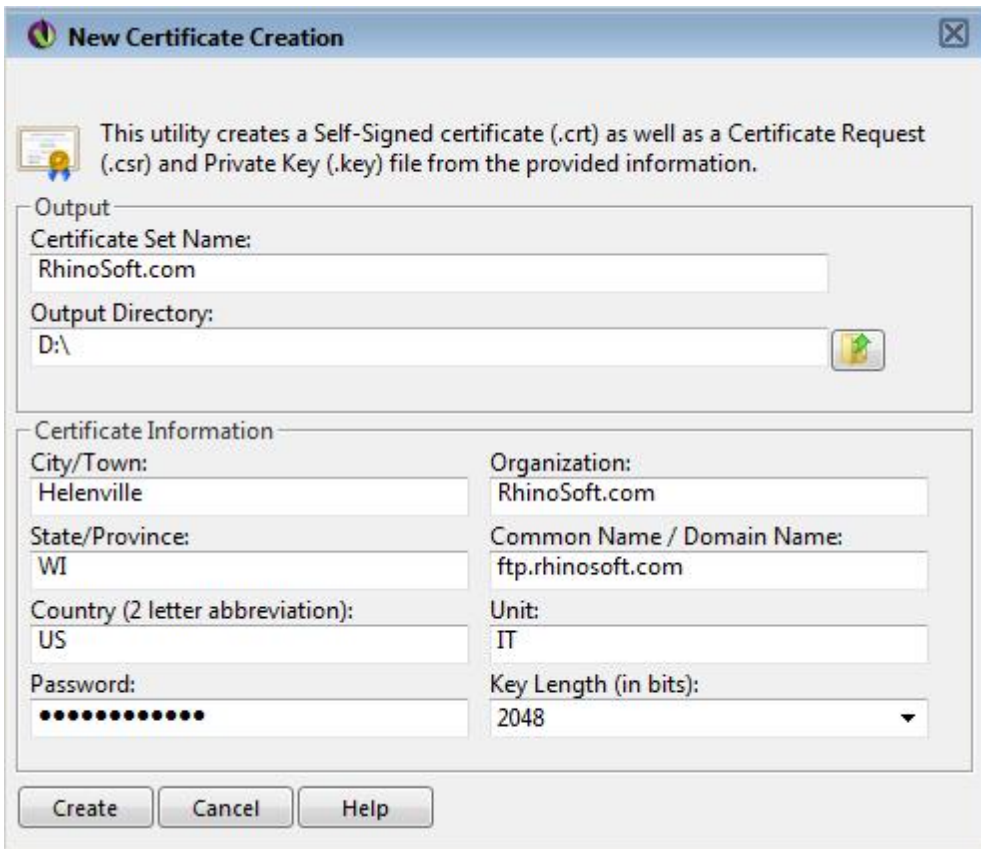
- 从证书颁发机构获取 SSL 证书和私人密钥文件。
- 将这些文件置于服务器内的安全目录中。
- 使用相应的浏览按钮选择证书和私人密钥文件。
- 如果已颁发 CA(证书颁发机构) PEM 文件，输入或浏览到此文件。
- 输入用来加密私人密钥文件的密码。
- 点击“保存”按钮。

如果所提供的文件路径和密码都正确，Serv-U 立即开始使用所提供的证书来保护 FTPS 和 HTTPS 连接。如果密码不正确，或 Serv-U 无法找到所提供的文件，则显示错误消息对所遇到的错误作出解释。

创建新证书

- 首先点击“创建证书”按钮。
- 指定“证书设置名称”，用于命名 Serv-U 创建的每个文件。
- 指定放置所创建文件的输出路径。在大多数情况下，安装目录是一个安全的位置（例如：C:\Program Files\RhinoSoft.com\Serv-U\）。
- 指定服务器或企业所在的市/镇。
- 指定服务器或企业所在省/自治区/直辖市（如果适用）。
- 指定服务器或企业所在国家的 2 位国家编码。
- 输入用来保护私人密钥的密码。
- 指定完整的机构名称。
- 指定证书的通用名称。此处必须列出用户连接所用的 IP 地址或全称域名（FQDN）。注意：如果通用名称不是客户端连接所用的 IP 地址或 FQDN，则客户端可能收到提示指出证书不匹配连接的域名。
- 指定服务器所在的企业单位。
- 点击“创建”按钮完成证书的创建。





Serv-U 使用所提供的信息创建3个文件：

一个自签名证书（.crt），它能在服务器上立即使用，但未通过任何已知证书颁发机构的验证；证书申请（.csr）可以提供给证书颁发机构用于验证；私人密钥文件（.key）则可用于保护以上两种证书文件。

将私人密钥保存在安全可靠的位置极其重要。如果您的私人密钥暴露了，怀有恶意的人士就能使用您的证书。

查看证书

配置完 SSL 证书后要查看证书，请点击“查看证书”按钮。

所有有关证书的标识信息，包括证书的有效日期，都显示在新对话框内。

高级 SSL 选项

只能以服务器级别配置这些高级 SSL 选项。所有继承该行为的域均不可单独进行覆盖。

启用低安全性密码——勾选该选择框启用低安全性 SSL 密码。一些较早的或国际客户端可能不支持当前最佳的 SSL 密码。因为现今的计算标准认为这些密码不安全，默认情况下 Serv-U 不接受这些密码。

禁用 SSLv2 支持——Serv-U 支持多种不同版本的 SSL。较早的 SSLv2 版本针对使其提供的安全性不如 SSLv3 与 TLS 的安全漏洞作了评注。不过，要兼容出口的客户端或较旧的客户端软件，还是很有必要支持 SSLv2。勾选此框来禁用对于较旧的 SSLv2 协议的支持。



FIPS 选项

启用 FIPS 140-2 模式——FIPS 140-2

是由美国国家标准技术研究院（NIST）设置的一套经过严格测试的加密规范。启用 FIPS 140-2 模式限制 Serv-U 使用符合 FIPS 140-2 认证的加密算法，并确保了解密连接拥有更高级别的安全性。

SFTP（通过 SSH2 的安全文件传输）

使用现有的私人密钥

- 获得私人密钥文件。
- 将私人密钥文件置于服务器内的安全目录中。使用 Serv-U 内的“浏览”按钮选择文件。
- 输入私人密钥文件的密码。
- 点击“保存”按钮。

创建私人密钥

- 点击“创建私人密钥”按钮。
- 输入私人密钥的名称（如“MyDomain Key”），该名称也用来命名保存文件。
- 输入证书的输出生成路径（如 C:\Program Files\RhinoSoft.com\Serv-U\）。
- 选择密钥类型（默认的 DSA 类型是首选，但也可使用 RSA）。
- 选择密钥长度（默认的 1024 位提供最佳性能，2048 位较为适中，而 4096 位提供最好的安全性）。
- 输入用来保护私人密钥文件的密码。

SSH 密码和 MAC

默认情况下，服务器启用所有支持的 SSH 密码和 MAC（消息验证码）。

如果您的特定安全需求规定只能使用某些密码或

MAC，您可以通过取消选中相应的选择框来单独禁用不需要的密码和 MAC。



FTP 设置

Serv-U 文件服务器允许定制其接受的 FTP 命令以及对收到的 FTP 命令的应答。当以服务器级别配置这些选项时，所有域将继承这些定制设置。要定制特定域的 FTP 行为，请选择相应域，打开该域的 FTP 设置选项卡，并点击“用户定制设置”按钮。任何时候，点击“用户默认设置”按钮即可将域还原为服务器的默认设置。

我们不推荐使用该方法定制 FTP 行为，除非用户非常熟悉 FTP 协议及其标准和扩展命令集。

全局属性

当使用定制设置时，“全局属性”按钮变为有效。

全局 FTP 响应

全局 FTP 响应是大多数 FTP 命令间共享的响应，例如未找到文件时发送的错误消息。定制全局 FTP 响应确保该响应为所有其它 FTP 命令所使用，而无需为每个单独 FTP 命令定制响应。FTP 命令响应可以包含特殊宏，该宏可以将实时数据插入响应。请参阅帮助文件中的“系统变量”部分获得更多信息。

服务器欢迎消息

当服务器和客户端首次连接时，除了发送标准的“220 欢迎消息”以向客户端标识服务器身份之外，还发送服务器欢迎消息。如果选中在消息文件文本中包含响应代码选择框，则指定欢迎消息的每一行均以 220 响应代码开头。要定制欢迎消息，请在消息文件路径输入框中输入文本文件的路径。使用“浏览”按钮选择计算机上的文件。Serv-U 打开该文件并将其内容发送给连接的客户端。

高级选项

阻止“FTP_bounce”攻击和 FXP（服务器间传输）——勾选该复选框阻止了所有涉及该 Serv-U 文件服务器的服务器间文件传输，只允许将文件传输到命令通道所用的 IP 地址。有关“FTP_bounce”的更多信息，请参见 CERT advisory CA-97.27。

在多行响应的所有行上包含响应代码——FTP 协议定义了 FTP 服务器发布多行响应的两种方法。如果多行响应的每一行不包含 3 位响应代码，一些较早的 FTP 客户端就无法对其进行解析。如果您所用的 FTP 客户端难以处理来自 Serv-U 的多行响应，请选择该复选框。

为所有发送及接收路径和文件名使用 UTF-8 编码——默认情况下，Serv-U 将所有文件名和路径处理为以 UTF-8 编码的字符串。它还将所有的文件名与路径发送为以 UTF-8 编码的字符串，例如在发送目录列表时。取消勾选此选项将阻止 Serv-U 以 UTF-8 编码这些字符串。取消勾选此选项时，不将 UTF8 包含进 FEAT 命令响应，以便向客户端指明该服务器不使用 UTF-8 编码。

编辑 FTP 命令与响应

要编辑 FTP 命令，请选择要编辑的 FTP 命令并点击“编辑”按钮。



信息

在“信息”选项卡下，显示了有关命令的基本信息，以及指向我们网站上更多信息的链接。通过选择“禁用命令”复选框，也可以禁用每条 FTP 命令。当从客户端接收到禁用的命令时，将其作为未识别命令进行处理。

FTP 响应

在“FTP 响应”选项卡下，通过点击每条响应的“编辑”按钮，可以修改服务器对命令发出的所有可能的 FTP 响应。FTP 命令响应可以包含特殊宏，该宏可以将实时数据插入响应。请参阅帮助文件中的“系统变量”部分获得更多信息。

消息文件

某些 FTP 命令允许关联消息文件。消息文件的内容与标准 FTP 响应将一并发送。此外，作为默认选项可使用次要消息文件路径。使用“消息文件”所在的用户根目录的相对路径可以指定消息文件。如果未找到第一个消息文件，Serv-U 就试图使用“次要消息文件”来代替。通过在次要文件位置指定绝对文件路径，可以保证每个用户收到消息文件。

以下为允许指定消息文件的所有 FTP 命令的列表：

- CDUP
- CWD
- QUIT

高级选项

某些 FTP 命令包含高级配置选项，它们提供了配置命令行为的更多方法。在管理控制台中可使用配置选项的地方，对它们作了详细描述。以下为包含高级配置选项的 FTP 命令列表：

- LIST
- MDTM
- NLST

示例文件——定制 FTP 命令响应

连接到服务器的用户需要知道当传输完成时给定的文件夹内有多少配额空间可用。为此，编辑对 STOR 命令的响应来包含有关可用空间的报告。默认情况下，对 STOR 命令（它将文件保存在服务器上）的 226（命令成功）响应为：

“传输完成。\$TransferBytes 字节已传送。\$TransferKBPerSecond 千字节/秒。”

修改该响应使其多包含一个变量：

“传输完成。\$TransferBytes 字节已传送。\$TransferKBPerSecond 千字节/秒。剩余存储空间为 \$QuotaLeft。”

最后一条语句向用户显示了每个文件上传完成后剩余多少存储空间。可通过相同的方式处理 DELE



命令，从而使每次用户删除文件后，显示更新的配额数值以反映可用空间的增加情况。可同样处理任何 FTP 命令响应。

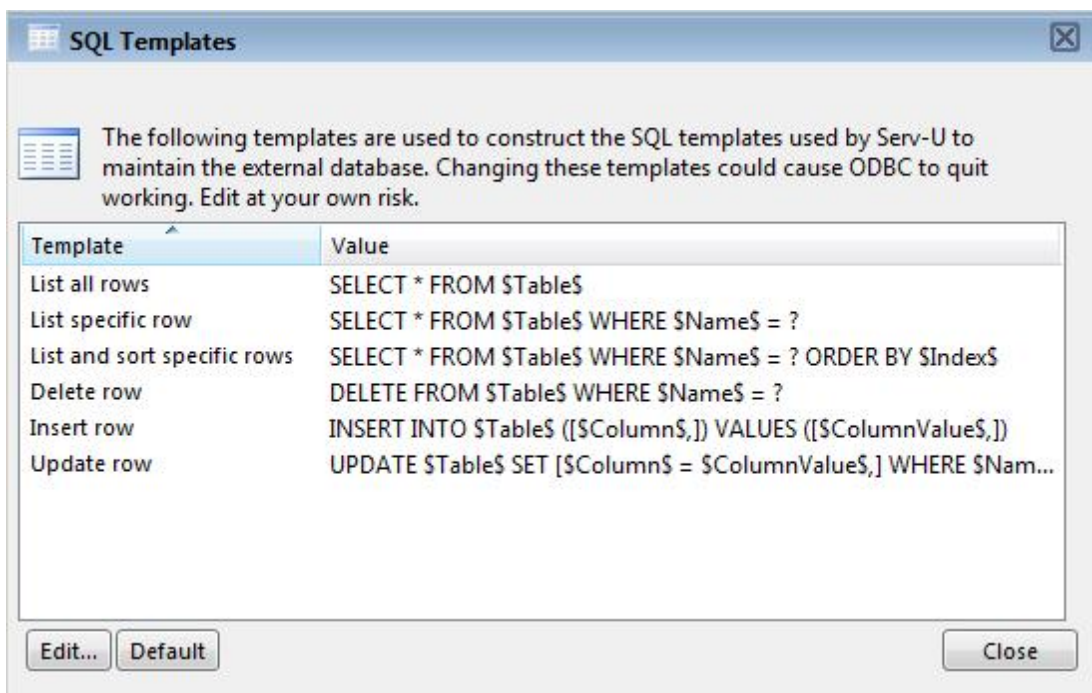


数据库访问

SQL 模板

Serv-U 使用多个查询来维护包含用户和群组信息的数据库。这些查询符合 SQL 语言标准。然而，如果您使用的数据库与 Serv-U 的协作有问题，可能需要更改这些查询。从 SQL 模板对话框，可以特别定制 Serv-U 使用的每条查询以符合数据库支持的标准。

注意：不正确地编辑这些 SQL 查询可能导致 Serv-U 内不再支持 ODBC。除非您擅长编写 SQL 语句，并肯定有必要启用数据库软件的 ODBC 支持，否则请勿擅自改动这些查询。



用户和群组表格映射

默认情况下，Serv-U 自动创建并维护在数据库中存储用户和群组信息所必需的表格和列。但如果试图将 Serv-U 连接到包含此信息的现有数据库，您需要定制表格和列的名称以符合现有数据库的结构。首先点击“用户表格映射”或“群组表格映射”。

Serv-U 在10个不同表格中保存用户或群组的信息。只有用户/群组信息表和用户/群组目录访问表是必需的。可以从“对象表”下拉框更改当前表格。“属性”列列出了当前表格中存储的属性。“数据库映射值”显示数据库中属性所映射到的列名。首行总是显示“表格名”，并可用来更改表格的名称。

某些表格中的条目顺序至关重要，这些表格列出了 SortColumn（排序列）属性。该列用于保存规则的应用顺序。

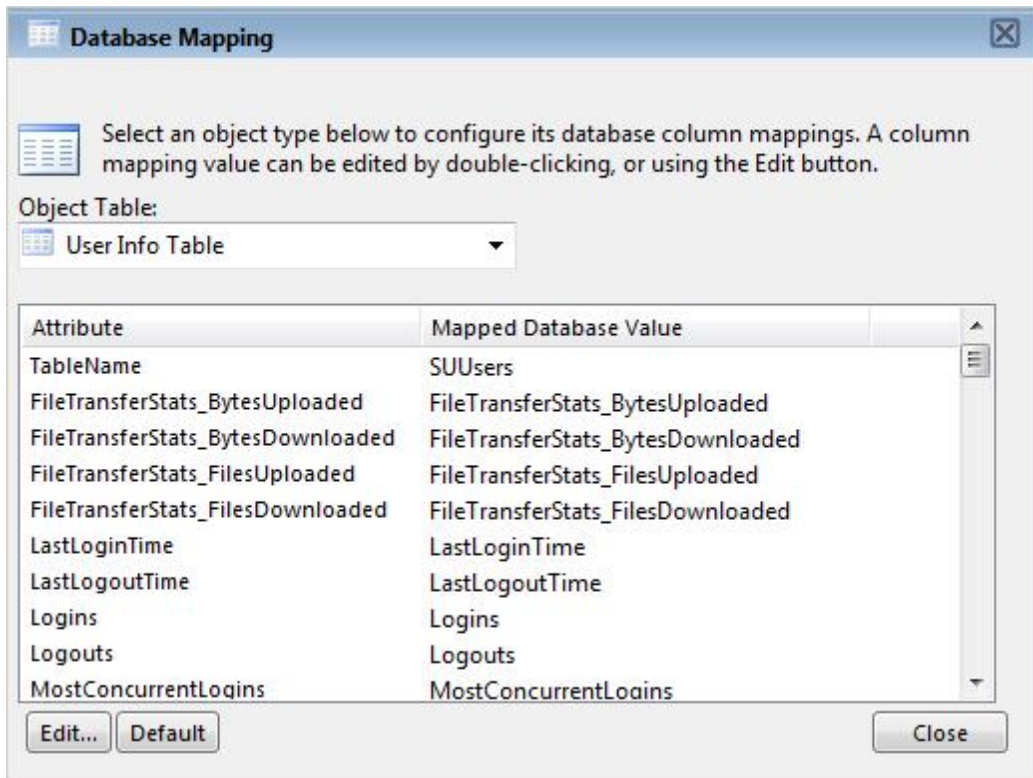
点击“编辑”按钮，或双击列名以编辑值。



启用此功能时，可以按需访问表格。在特殊情况下，可以禁用未使用的表格来减少 ODBC（数据库）的调用数量。

例如，如果不使用比率和配额的“用户无比率文件”、“每用户文件比率”、“每用户字节比率”、“每会话文件比率”以及“每会话字节比率”表格，便可将它们禁用以避免无用的 ODBC 调用。

请注意，在禁用表格时，这些字段将出现在对话框中，不过不会保存或加载这些字段。无法禁用“用户信息”与“群组信息”表格。



示例文件——ODBC 验证

通过 ODBC 数据库可以在 Serv-U 文件服务器中进行验证，允许脚本式账户管理和维护。为了使用 ODBC 功能，请转到数据库的 ODBC 验证。通过将凭证存入数据库的设置中，就可以在 Serv-U 管理控制台外部由脚本式数据库操作管理账户，该操作可以嵌入许多现有的账户设置系统中。首先必须在控制面板 | 管理工具 | 数据源（ODBC）中创建 DSN——如果 Serv-U 作为服务运行则使用“系统 DSN”，如果 Serv-U 作为应用程序运行则使用“用户 DSN”。一旦创建了正确的 DSN 后，请指定数据源名、登录 ID 和密码并选择“保存”。Serv-U 透明地创建表和列。可以从 Serv-U 的“数据库用户和数据库群组”区域（位于普通“用户和群组”选项卡旁）管理“数据库用户和群组”。



SMTP 配置

Serv-U 允许管理员这样配置 SMTP 连接：即为配置为使用电子邮件操作的事件发送邮件。SMTP 能够以服务器和/或域级别进行配置。域级别的 SMTP 配置可以从服务器级别继承。SMTP 配置对话框位于“域详细信息”与“服务器详细信息”页面上的“事件”选项卡。只需点击“配置 SMTP”按钮启动此对话框即可。

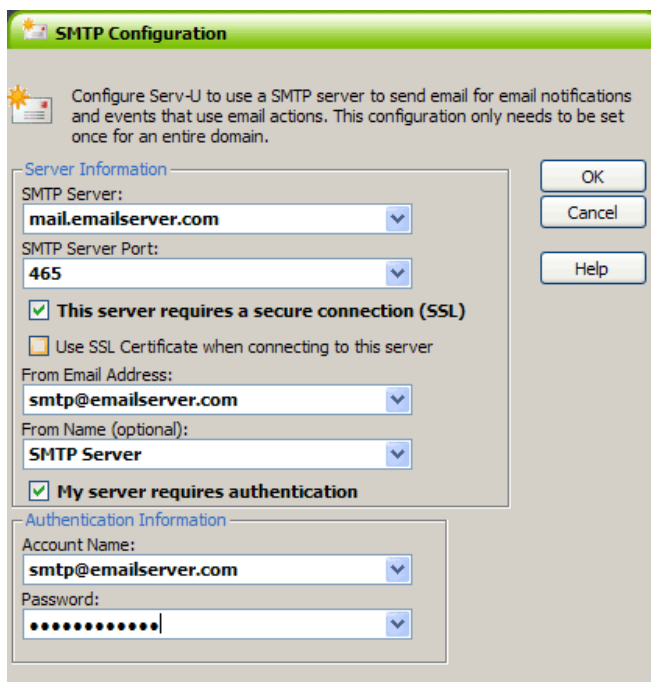
SMTP 服务器信息

- SMTP 服务器——SMTP 服务器的名称与 IP 地址
- SMTP 服务器端口——SMTP 服务器正在使用的端口
- 发件人电子邮件地址——用于出站邮件的电子邮件地址
- 发件人名称（可选）——用于出站邮件的名称
- 我的服务器需要验证——请勾选此框来启用验证
- 该服务器需要安全连接（SSL）——某些 SMTP 服务器要求所有的入站连接进行加密，以防可能存在的攻击。如果您的服务器要求入站 SMTP 连接进行加密，请启用此选项。用于已加密 SMTP 连接的默认端口号为 465。Serv-U 仅支持 Implicit SSL，不支持 Explicit SSL（587 端口）

验证信息

如果您的 SMTP 服务器要求验证，您必须输入以下信息：

- 账户名称——与 SMTP 服务器验证相关联的账户名称。
- 密码——账户的密码。



Serv-U 事件

Serv-U 支持使用事件处理，可以按选定的事件列表执行各种触发操作。以下是管理员可以执行的事件列表：

服务器事件

- 服务器启动
- 服务器停止

服务器与域事件

- 域启动
- 域停止
- 会话连接
- 会话断开
- 会话连接失败
- 删除日志文件

服务器、域、用户与群组事件

- 用户登录
- 用户注销
- 用户注销失败
- 用户密码更改
- 用户密码更改失败
- 启用用户
- 禁用用户
- 删除用户
- 阻止 IP
- IP 阻止时间
- 会话太多
- IP 上的会话太多
- 将 IP 自动添加到访问规则
- 添加用户
- 发送密码恢复
- 密码恢复失败
- 上传文件
- 文件上传失败
- 下载文件
- 文件下载失败
- 删除文件
- 移动文件
- 创建目录
- 删除目录
- 更改目录
- 移动目录
- 超出配额
- 超出磁盘空间



创建常规事件

Serv-U 允许管理员自动创建一系列最为常用的事件。

您可以选择使用电子邮件和/或气球提示操作来创建这些常规事件。

只需在“事件”选项卡中点击“创建常规事件”按钮即可。

针对您希望对常规事件执行的操作，选择“发送电子邮件”或“显示气球提示”单选按钮。

如果您选择“发送电子邮件”，您必须输入“收件人”地址以发送这些事件。

事件操作

在触发事件时，管理员可以选择执行三种不同的操作。以下列出了这些操作：

- 发送电子邮件
- 显示气球提示（仅限于服务器管理员）
- 执行命令（仅限于服务器管理员）

电子邮件操作

可以配置电子邮件操作在事件触发时将邮件发送至多位收件人与 Serv-U 群组。

要添加电子邮件地址，请在“收件人”或“密送”字段中输入。要将邮件发送至 Serv-U

群组，请使用“群组”图标来添加或删除分发列表中的 Serv-U 群组。必须使用逗号或分号来分隔电子邮件地址。

电子邮件操作包含“收件人”、“主题”与“消息”参数。特殊变量可用于发送与事件相关的特定数据。

请参阅“系统变量”部分的变量列表。

气球提示操作

可以配置气球提示操作在事件触发时在系统托盘中显示气球提示。

气球提示操作包含“气球标题”与“气球消息”参数。特殊变量可用于发送与事件相关的特定数据。

请参阅“系统变量”部分的变量列表。

执行命令操作

可以配置执行命令操作在事件触发时对文件执行命令。

执行命令操作包含“可执行程序路径”、“命令行参数”和“完成等待时间”参数。

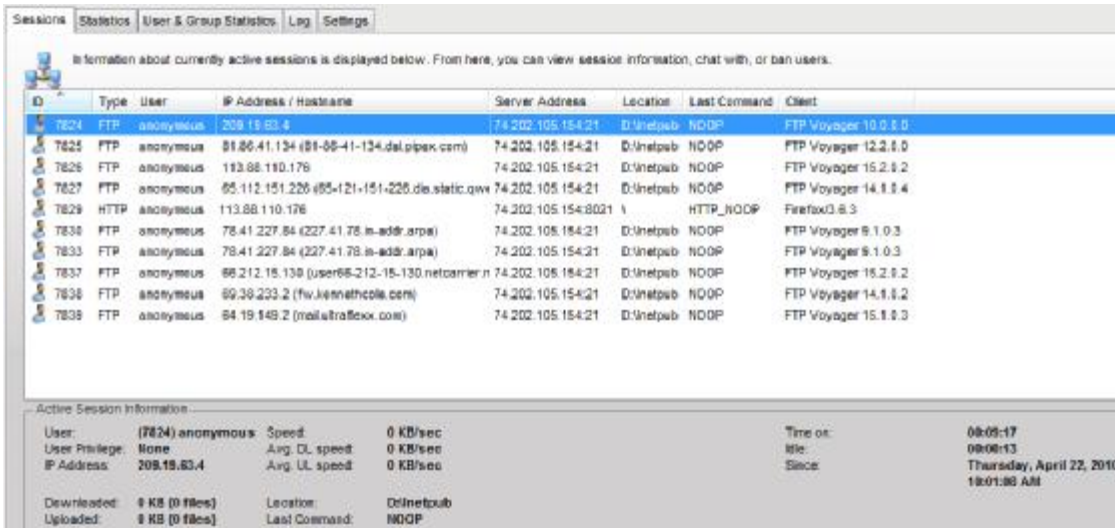
对于“完成等待时间”参数，您可以输入启动可执行程序路径后所等待的秒数。输入0值表示不等候。

注意：Serv-U 用于等候的任何时间量将延迟 Serv-U 可以执行的任何处理。

只可将等候值用于为外部程序提供足够的操作执行时间，例如在删除日志文件前移动该文件（比如用于“删除日志文件”事件的 `$LogFilePath`）。特殊变量可用于发送与事件相关的特定数据。请参阅“系统变量”部分的变量列表。



跟踪 Serv-U 中的活动



| ID | Type | User | IP Address / Hostname | Server Address | Location | Last Command | Client |
|------|------|-----------|--|---------------------|------------|--------------|----------------------|
| 7824 | FTP | anonymous | 209.19.83.4 | 74.202.105.154:21 | D:\inetpub | NOOP | FTP Voyager 10.0.8.0 |
| 7825 | FTP | anonymous | 81.86.41.134 (81-86-41-134.dal.pipex.com) | 74.202.105.154:21 | D:\inetpub | NOOP | FTP Voyager 12.2.8.0 |
| 7826 | FTP | anonymous | 113.88.180.176 | 74.202.105.154:21 | D:\inetpub | NOOP | FTP Voyager 15.2.8.2 |
| 7827 | FTP | anonymous | 65.112.151.226 (65-112-151-226.dia.static.qww) | 74.202.105.154:21 | D:\inetpub | NOOP | FTP Voyager 14.1.8.4 |
| 7829 | HTTP | anonymous | 113.88.110.176 | 74.202.105.154:8021 | l | HTTP_NOOP | Firefox/3.8.3 |
| 7830 | FTP | anonymous | 78.41.227.84 (227.41.78.s-addr.arpa) | 74.202.105.154:21 | D:\inetpub | NOOP | FTP Voyager 9.1.0.3 |
| 7833 | FTP | anonymous | 78.41.227.84 (227.41.78.s-addr.arpa) | 74.202.105.154:21 | D:\inetpub | NOOP | FTP Voyager 9.1.0.3 |
| 7837 | FTP | anonymous | 66.212.15.130 (user66-212-15-130.netcarrier.n) | 74.202.105.154:21 | D:\inetpub | NOOP | FTP Voyager 15.2.8.2 |
| 7838 | FTP | anonymous | 89.39.233.2 (fw.lignathcoke.com) | 74.202.105.154:21 | D:\inetpub | NOOP | FTP Voyager 14.1.8.2 |
| 7839 | FTP | anonymous | 54.19.149.2 (mail.ustraflex.com) | 74.202.105.154:21 | D:\inetpub | NOOP | FTP Voyager 15.1.8.3 |

| Active Session Information | | | |
|----------------------------|------------------|----------------|--------------------------|
| User: | (7824) anonymous | Speed: | 0 KB/sec |
| User Privilege: | None | Avg. DL speed: | 0 KB/sec |
| IP Address: | 209.19.83.4 | Avg. UL speed: | 0 KB/sec |
| Downloaded: | 0 KB (0 files) | Location: | D:\inetpub |
| Uploaded: | 0 KB (0 files) | Last Command: | NOOP |
| Time on: | 08:09:17 | File: | |
| Since: | 08:06:13 | Since: | Thursday, April 22, 2010 |
| | | | 18:01:56 AM |

“服务器和域会话”选项卡显示了当前的文件服务器会话活动。

当从服务器查看会话页时，显示来自所有域的所有连接会话。

如果在管理域的同时进行查看，则只显示该域的当前会话。从该页可以看到文件服务器上当前活动的概貌。

此外，可以查看单个会话，包括其当前状态、连接状况和传输信息。

要查看特定会话的详细信息，请选择该会话。“活动会话信息”组内包含了当前高亮显示的会话详情。

该信息被频繁更新以提供会话活动的最新精确快照。

根据会话的连接类型（例如 FTP、HTTP 或 SFTP），可以使用某些附加功能。

断开连接

通过点击“断开连接”按钮，可以随时断开任何类型的会话。

点击该按钮打开了另一个对话框，其中有其他选项用于设置断开方式。有3种断开连接选项可供选择：

- 断开连接——立即断开会话的连接。断开连接的客户端能立即建立另一个会话。这也称为“踢开”用户。
- 断开连接并禁用 IP——立即断开会话连接并禁用其 IP 地址达到指定的分钟数，以防止立即进行重新连接。
- 断开连接并永久阻止 IP——立即断开会话连接，并为其 IP 地址添加拒绝 IP 访问规则，以永久地防止从相同 IP 地址进行重新连接。

当从服务器会话视图中断开会话连接时，有称为“应用 IP 规则到”的附加选项可供使用。

该组合框允许您选择应用临时或永久 IP 禁令的位置——整个服务器或只是会话所连接的域。

除了断开会话连接，也可以通过选择标记为“禁用用户帐户”的选择框禁用会话使用的用户帐户。

如果当前会话使用 FTP

协议，通过在标记为“发送给用户的消息”的文本框内输入消息，可以在断开连接前将其发送给用户。HTTP 或



SFTP 会话不可使用该选项，因为这两个协议未定义与用户聊天的方法。

探查和聊天

通过点击“探查和聊天”按钮或双击列表中的会话可以探查任何类型的会话。

对用户进行查探显示了加亮会话时通常能看到的所有详细信息，但也包含了自会话开始与文件服务器建立连接起的完整会话日志。这帮助管理员浏览日志并查看会话用户所采取的所有操作。

如果当前会话使用 FTP 协议，则有附加的选项可以与用户聊天。

“聊天”组显示了开始“探查”会话后该会话收发的所有消息。

要向会话发送消息，请在标记为“消息内容”的文本框内输入消息文本并点击“发送”按钮。

当收到来自会话的消息时，也将在此自动显示。

注意：并非所有的 FTP 客户端都支持与系统管理员聊天。向服务器发送消息所用的命令为 **SITE MSG**。为了使客户端接收到消息，客户端应用程序必须能接收来自服务器的自发响应（而不是简单地删除它们）。

广播

通过点击“广播”按钮，可以向当前所有连接的 FTP 会话发送消息。通过广播发送消息等同于打开每个 FTP 会话的探查和聊天对话框并发送聊天消息。

中止

如果会话正在执行文件传输，通过点击“中断”按钮无需断开会话连接就可以终止文件传输。

确认中断命令后，服务器就终止该会话当前的文件传输。某些客户端，尤其是 FTP 和 SFTP

客户端，可以自动重启中断的传输，而使中断操作看上去似乎失败了。在这种情况下，请转而尝试“断开”会话。



服务器与域统计

域和服务器统计页面显示了有关服务器使用的详细统计信息，用于基准测试和记录保存。以服务器级别查看到的统计信息是服务器上所有域的累积统计信息的集合。单个域上查看到的统计信息只是该域的统计信息。显示的信息包括：

会话统计

当前会话

当前连接的会话数

24小时会话

过去24小时内连接的会话数

总会话

联机以来所连接的会话总数

最大会话数量

联机以来所记录的最大并发会话数量

平均会话长度

会话保持连接的平均时间长度。

最长会话

会话的最长记录时间。

登录统计

取决于当前正在查看的统计，可将这些统计应用到域或整个服务器。登录统计与会话统计不同，因为这些统计应用到与连接及断开相对的登录（提供登录 ID 和密码）。

登录

成功登录的总数

注销

注销总数



当前登录

当前登录的会话数。

当前最大登录数

同时登录会话的最大数

上次登录时间

上次记录的有效登录时间（并非上次创建连接的时间）

上次注销时间

上次记录的有效注销时间

平均登录持续时间

所有会话的平均登录时间

最长登录持续时间

会话的最长登录时间

最短登录持续时间秒数

会话的最短登录时间

传输统计

下载速度

当前累积占用的下载带宽

上传速度

当前累积占用的上传带宽

平均下载速度

联机以来占用的平均下载带宽

平均上传速度

联机以来占用的平均上传带宽



已下载

联机以来下载的数据总量和文件数目

已上传

联机以来上传的数据总量和文件数目



用户和群组统计

用户与群组统计页面根据个人用户或群组活动显示详细的统计信息。用户或群组的统计查看仅限于该用户或该群组。显示的信息包括：

会话统计

当前会话

当前连接的会话数

24小时会话

过去24小时内连接的会话数

总会话

联机以来所连接的会话总数

最大会话数量

联机以来所记录的最大并发会话数量

平均会话长度

会话保持连接的平均时间长度

最长会话

会话的最长记录时间

登录统计

取决于当前正在查看的统计，可将这些统计应用到一个或一组用户。登录统计与会话统计不同，因为这些统计应用到与连接及断开相对的登录（提供登录 ID 和密码）。

登录

成功登录的总数

注销

注销总数

当前登录

当前登录的会话数。



当前最大登录数

同时登录会话的最大数

上次登录时间

上次记录的有效登录时间（并非上次创建连接的时间）

上次注销时间

上次记录的有效注销时间

平均登录持续时间

所有会话的平均登录时间

最长登录持续时间

会话的最长登录时间

最短登录持续时间秒数

会话的最短登录时间

传输统计

下载速度

当前累积占用的下载带宽

上传速度

当前累积占用的上传带宽

平均下载速度

联机以来占用的平均下载带宽

平均上传速度

联机以来占用的平均上传带宽

已下载

联机以来下载的数据总量和文件数目



已上传

联机以来上传的数据总量和文件数目

保存统计

用户和群组统计可以直接保存为 **CSV** 文件，以便有计划地进行分析 and 检查。
要将统计保存为文件，首先选择您要生成统计文件的用户或群组，然后点击该页底部的“保存统计”按钮。



服务器与域日志

服务器和域日志选项卡显示服务器或域的活动记录。

服务器日志显示文件服务器的启动、配置和关闭信息。它不显示域活动信息。

要了解域活动信息，请查看相应域的日志。

除了文件服务器开始启动时所记录的有关库、授权和当前构建的状态信息，服务器日志也包含有关所有域监听器状态、通用即插即用（UPnP）状态和 PASV 端口范围状态的信息。

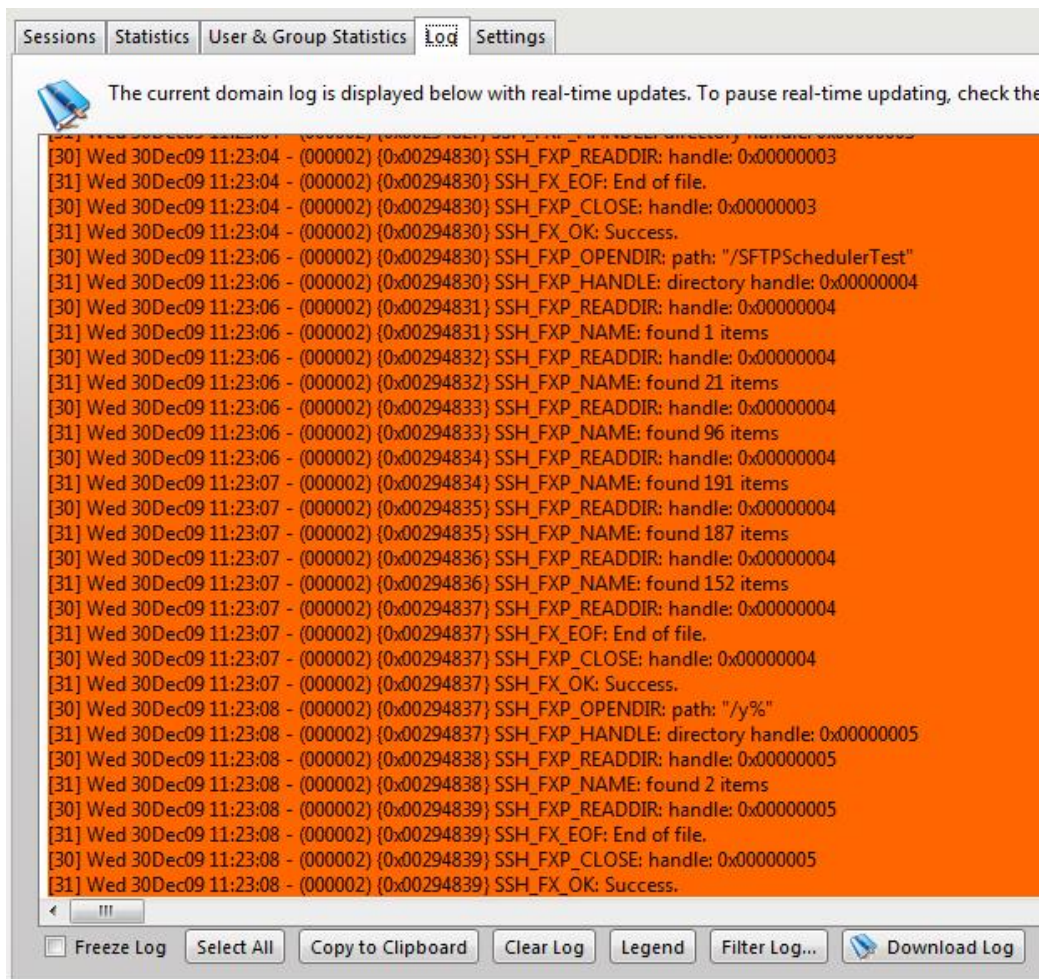
服务器日志中包含的信息也保存在安装目录中名为 **Serv-U-StartupLog.txt** 的文本文件中。每次启动 Serv-U 文件服务器时更新该文件。

域日志仅包含有关当前所管理域的活动信息。这包括域监听器的状态和任何已配置活动的日志信息。

要了解有关“域日志”中记录的活动类型信息的更多详情，请参见标题为“域日志设置”的帮助内容。

通过点击并在所需的日志部分上拖动鼠标可以高亮显示日志中包含的信息。

一旦高亮显示，就可以将所选部分复制到剪贴板。



冻结日志

选择该选择框可以暂时停止刷新日志。

这对于繁忙的系统很有用，因为在日志滚动到视窗之外前可以加亮并复制一部分日志。完成操作后，取消选择该选择框以恢复日志的自动更新。

全选

点击该按钮可以自动冻结日志并加亮当前显示的所有日志信息，以便将其复制到剪贴板中。

清除日志

当日志庞大到不能一目了然时，请点击该按钮删除当前显示的日志信息。只显示点击该按钮之后收到的日志信息。

图例

为了更方便地查看日志的不同部分，对每种不同类型的日志信息进行了色彩编码以利于快速识别。

点击该按钮在可拖拽的对话框中显示图例。将图例对话框拖拽到方便的位置，以便在浏览日志时可以参考图例。

过滤日志

要快速查找和通读日志的特定部分，可以根据搜索字符串来过滤日志。点击该按钮显示“过滤日志”对话框。输入搜索字符串并点击“过滤”按钮将刷新日志，使其只显示包含搜索字符串的日志条目。要再次查看完整的日志内容，请打开“过滤日志”对话框并点击“重置”按钮。

下载日志

要下载 Serv-U 中的完整日志文件，请点击“下载日志”按钮。如果您拥有文件下载权限，您的 web 浏览器将提示您选择保存该文件的位置，或开始自动下载该文件。



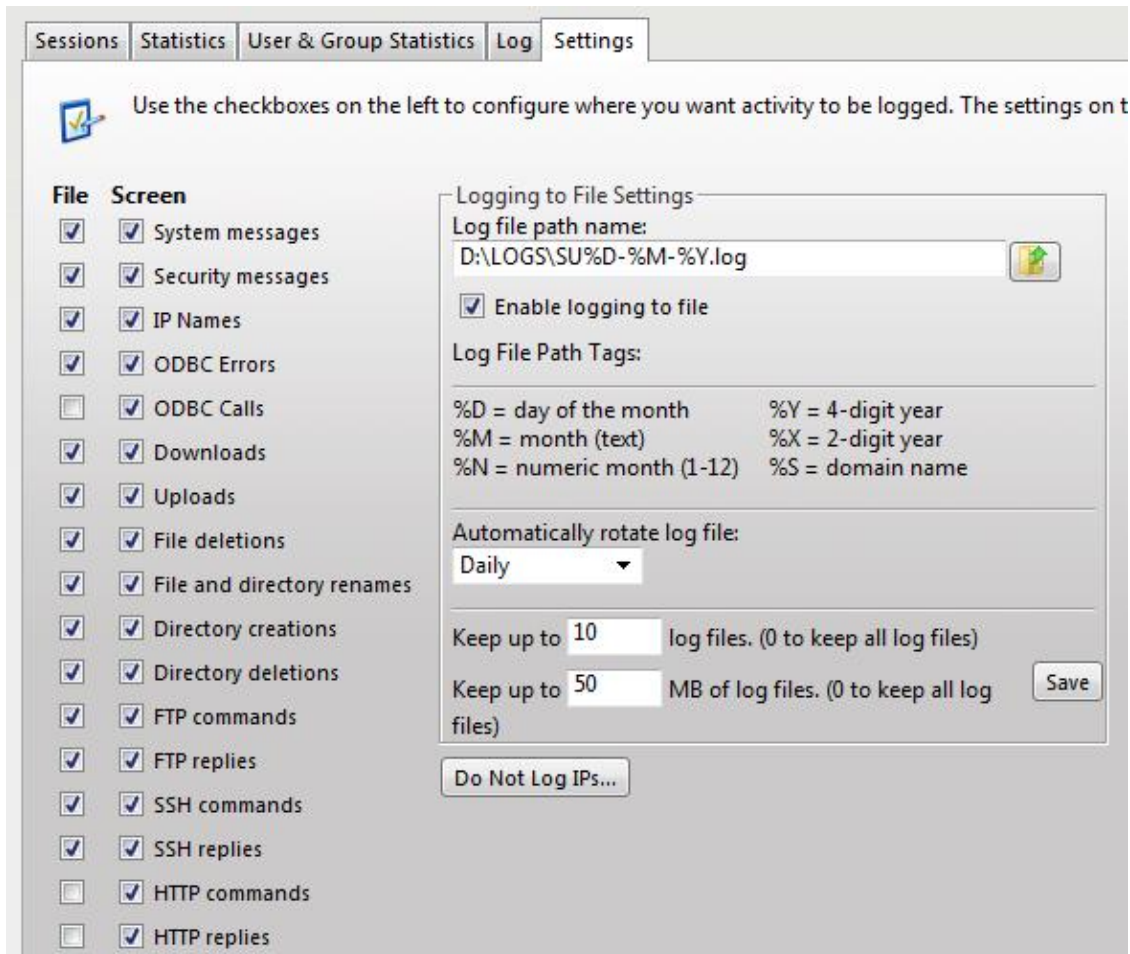
配置域日志

Serv-U 文件服务器允许大量定制操作，用于将域事件和活动记入日志。日志记录分为两个部分：文件和屏幕。要启用日志选项，请选中文件或屏幕列中相应的复选框。

从“文件”列中选中选项时，如果选中“启用记录日志到文件”，则相应的日志信息将保存到指定的日志文件中。

从“屏幕”列中选中选项时，从 Serv-U 管理控制台将看到在日志中显示的事件。

日志显示内容的多少可以根据您的需要进行配置。配置完需要的日志选项后，请点击“保存”按钮保存更改。



记录日志到文件设置

日志文件路径

将信息保存到文件之前，必须为日志文件命名。可以使用“浏览”按钮为日志文件选择已有的文件或目录位置。

日志文件路径支持以下列出的这些通配符。通配符字符表示日志文件创建的日期。

和“自动循环更新日志文件”选项结合使用时，通配符能够自动归档域活动用于审计，如 HIPAA 需要的活动日志。可用的通配符字符包括：

- %D——每月的当前日期



- %M——当前月份的名称
- %N——当前月份的数值（1-12）
- %Y——当前年份的4位数值（例如：2009）
- %X——当前年份的2位数值（例如：2009年表示为09）
- %S——正被记录活动的域名

启用“记录日志到文件”

选中该选择框，Serv-U 开始将日志信息保存到“日志文件路径”中指定的文件。如果未选中该选项，Serv-U 不会将任何日志记录到文件，除非在“文件”列中选中了个别选项。

自动循环更新日志文件

要确保日志文件维持可管理的尺寸，并且在审计时能够轻松引用，Serv-U 支持每隔固定的时间自动循环更新日志文件。通过指定“日志文件路径”时使用通配符表示当前日期，Serv-U 可以每日、每周、每月或每年循环更新日志文件并创建唯一的文件名。

清除旧的日志文件

Serv-U

支持自动清除旧日志文件的功能，只需设置要保存的最大文件数量或最大尺寸限制（MB）即可。将这些选项设置为“0”表示设置为无限且不应用限制。

注意：仅根据当前的日志文件路径名称清除日志文件。使用 Windows 通配符值替代日志文件变量，以便搜索匹配文件。例如：

```
C:\Logs\%Y:%N:%D %S Log.txt 搜索自 C:\Logs\????:?:?? * Log.txt
C:\Logs\%Y:%M:%D %S Log.txt 搜索自 C:\Logs\????*:?? * Log.txt
C:\Logs\%S\%Y:%M:%D Log.txt 搜索自 C:\Logs\--DomainName--\????*:?? Log.txt
```

日志变量的通配符化如下所示：

```
%D --> ??
%N --> ??
%M --> *
%Y --> ???
%X --> ??
%S --> *
```

可以清除匹配通配符路径名称的任何日志文件。

使用注意事项：最佳举措是将日志文件放置在单个目录中以避免意外的文件删除。

不记录 IP

Serv-U 支持指定 IP 地址，使其不被记入日志的功能。来自这些 IP 地址的活动将不被记录到规则指定的位置——记录到屏幕和/或文件。该功能能够使管理员忽略一些 IP 地址，否则将生产大量日志信息，从而使域活动和其他常规用户活动混淆。



还可以用于节省日志存储空间并减少管理成本。只需点击“不记录 IP”按钮并正确添加 IP 地址即可。



数据库支持

Serv-U 可以使用 ODBC 数据库来保存并维护域级别和服务器级别的群组 and 用户账户。可在两个地方配置 ODBC 连接：[域](#) | [域详情](#) | [数据库和服务器](#) | [服务器详情](#) | [数据库](#)。Serv-U 可以自动创建所有需要的表和列以便开始在数据库中保存用户和群组。因为 Serv-U 使用一组表格名来存储信息，所以必须为在数据库中保存详细信息的每个项目单独配置 ODBC 连接。换句话说，服务器和每个域必须有唯一的 ODBC 连接以确保分别对其进行存储。要配置数据库，请按以下步骤操作：

- 创建 ODBC 连接供 Serv-U 使用。RhinoSoft.com 推荐使用 MySQL，但也可使用任何具有 Windows ODBC 驱动程序的数据库。如果 Serv-U 作为系统服务运行则使用系统 DSN，如果作为常规应用程序运行则使用用户 DSN。
- 打开 Serv-U 管理控制台，转到相应的域或服务器数据库设置。输入数据源名称（DSN）、登录 ID 和密码，并点击“保存”。

如果是首次配制数据库连接，请选中“自动创建”选项。选中该选项后，Serv-U 文件服务器自动构建数据库表格和列。



许可证信息

“许可证详细信息”选项卡中显示了 Serv-U 文件服务器使用的当前注册 ID 中包含的信息。如果安装的是试用版，则将同时显示剩余试用天数的信息。该选项卡上包含的信息包括：

名称

当前许可证的名称

电子邮件地址

当前许可证的电子邮件地址

Serv-U 版本

当前许可证所支持的 Serv-U 版本。请参见 Serv-U 版本获得更多信息

份数

当前许可证允许的并发安装数。

购买日期

当前许可证的购买日期

更新

当前许可证允许免费更新到最新版本的截止日期。如果作为试用版运行，则显示剩余的试用天数

版本信息

显示获得授权的 Serv-U 版本所启用的功能和限制。

其他产品

更多 Serv-U 插件及其是否启用

注册 Serv-U

要注册 Serv-U 文件服务器，请点击底部工具栏上的“注册”按钮，并输入由文字和数字组成的注册 ID。如果您遗失了 ID，请点击“丢失 ID”按钮以便获得帮助找回 ID。如果您需要购买 ID，请点击“购买”按钮访问我们的网站来购买 ID。



系统变量

Serv-U 中的某些可配置的消息可以定制为包含各种变量，如以下列表中所示变量。这些变量在运行时会替换为相应的值，可以为登录的用户提供最新的统计和反馈。可以使用这些变量的地方包括事件消息、定制的 FTP 命令响应，或欢迎消息。

以下包含了所有可用的变量和每个变量的简要描述。如果没有另外指定，统计信息自上次启动 Serv-U 文件服务器后开始计算。

服务器信息

- `$ServerName`——服务器的全名（例如：Serv-U）
- `$ServerVersionShort`——Serv-U 文件服务器当前版本的前两位数字（例如：7.0）
- `$ServerVersionLong`——Serv-U 文件服务器的完整版本号（例如：7.0.0.3）
- `$OS`——操作系统的名称（例如：Windows XP）
- `$OSVer`——操作系统的完整版本号（例如：5.1.2600）
- `$OSAndPlatform`——操作系统的名称（例如：Windows XP）和平台名称（例如 32-位或 64-位）
- `$ComputerName`——从操作系统检索出的计算机名称，通常与 Windows 网络上的 UNC 名称相同（例如：WEB-SERVER-01）
- `$LogFilePath`——检索日志文件路径（仅限于删除日志文件事件）

服务器统计

- `$ServerDays`——服务器持续在线的总天数
- `$ServerHours`——服务器持续在线的小时数（0-24），推延到 `$ServerDays`
- `$ServerMins`——服务器持续在线的分钟数（0-60），推延到 `$ServerHours`
- `$ServerSecs`——服务器持续在线的秒数（0-60），推延到 `$ServerMins`
- `$ServerKBup`——上传的 KB 总数
- `$ServerKBdown`——下载的 KB 总数
- `$ServerFilesUp`——上传的文件总数
- `$ServerFilesDown`——下载的文件总数
- `$ServerFilesTot`——传输的文件总数，实际上为（`$ServerFilesUp` + `$ServerFilesDown`）
- `$LoggedInAll`——已创建的会话总数
- `$ServerUploadAvgKBps`——平均上传速率，单位 KB/秒
- `$ServerDownloadAvgKBps`——平均下载速率，单位 KB/秒
- `$ServerAvg`——平均数据传输速率（上传与下载），单位 KB/秒
- `$ServerUploadKBps`——当前上传传输速率，单位 KB/秒
- `$ServerDownloadKBps`——当前下载传输速率，单位 KB/秒
- `$ServerKBps`——当前数据传输率总计，单位 KB/秒
- `$ServerSessions24HPlusOne`——过去 24 小时内的会话总数再加一个会话
- `$ServerSessions24H`——过去 24 小时内的会话总数

域统计

- `$DomainKBup`——上传的 KB 总数
- `$DomainKBdown`——下载的 KB 总数
- `$DomainFilesUp`——上传的文件总数
- `$DomainFilesDown`——下载的文件总数
- `$DomainFilesTot`——传输的文件总数，实际上为（`$DomainFilesUp` + `$DomainFilesDown`）



- \$DomainLoggedIn——当前连接的会话总数
- \$DomainUploadAvgKBps——平均上传速率，单位 KB/秒
- \$DomainDownloadAvgKBps——平均下载速率，单位 KB/秒
- \$DomainAvg——平均数据传输速率（上传与下载），单位 KB/秒
- \$DomainUploadKBps——当前上传传输速率，单位 KB/秒
- \$DomainDownloadKBps——当前下载传输速率，单位 KB/秒
- \$DomainKBps——当前数据传输率总计，单位 KB/秒
- \$DomainSessions24HPlusOne——过去 24 小时内的会话总数再加一个会话
- \$DomainSessions24H——过去 24 小时内的会话总数

用户统计

应用到用户账户附带的所有会话

- \$UserKBUp——上传的 KB 总数
- \$UserKBDown——下载的 KB 总数
- \$UserKBTot——传输的 KB 总数
- \$UserLoggedIn——会话总数
- \$UserUploadAvgKBps——平均上传速率，单位 KB/秒
- \$UserDownloadAvgKBps——平均下载速率，单位 KB/秒
- \$UserAvg——平均数据传输速率（上传与下载），单位 KB/秒
- \$UserUploadKBps——当前上传传输速率，单位 KB/秒
- \$UserDownloadKBps——当前下载传输速率，单位 KB/秒
- \$UserKBps——当前数据传输率总计，单位 KB/秒
- \$UserSessions24HPlusOne——过去 24 小时内的会话总数再加一个会话
- \$UserSessions24H——过去 24 小时内的会话总数

上次传输统计

应用于最新完成的成功数据传输

- \$TransferBytesPerSecond——有效（已压缩）传输速率，单位：字节/秒
- \$TransferKBPerSecond——有效（已压缩）传输速率，单位：KB/秒
- \$TransferBytes——有效（已压缩）已传输字节数，进行格式化以便显示，例如 32,164
- \$NoFormatTransferBytes——有效（已压缩）已传输字节数，未经格式化，例如 32164
- \$TransferKB——有效（已压缩）已传输 KB 数，进行格式化以便显示
- \$ActualTransferBytesPerSecond——实际（未压缩）传输速率，单位：字节/秒
- ActualTransferKBPerSecond——实际（未压缩）传输速率，单位：KB/秒
- \$ActualTransferBytes——实际（未压缩）已传输字节数，进行格式化以便显示，例如 32,164
- \$NoFormatActualTransferBytes——实际（未压缩）已传输字节数，未经格式化，例如 32164
- \$ActualTransferKB——实际（未压缩）已传输 KB 数，进行格式化以便显示
- \$CompressionRatio——传输压缩率，表示为预计传输数据总量的百分比。例如，值 100.00 表示数据未经压缩。值 200.00 表示数据压缩为其原始大小的一半。
- \$CurrentCompressedTransferBytes——当前有效的（已压缩）已传输字节数，未经格式化，例如 32164（仅 FTP）
- \$CurrentUncompressedTransferBytes——当前实际的（未压缩）已传输字节数，未经格式化，例如 32164（仅 FTP）

日期/时间

- \$Date——根据 Serv-U 文件服务器显示的当前日期，使用系统本地日期格式
- \$Time——根据 Serv-U 文件服务器显示的当前时间，使用系统本地时间格式



服务器设置

- **\$MaxUsers**——允许登录的最大会话数，由许可证类型限制
- **\$MaxAnonymous**——允许登录的匿名用户最大数量

会话信息

应用于当前会话

- **\$Name**——用户账户的登录 ID
- **\$LoginID**——会话的登录 ID，运行方式类似 **\$Name**。**\$Name** 可以指目标用户账户的登录 ID，不过 **\$LoginID** 仅指会话的登录 ID。
- **\$IP**——客户端 IP 地址
- **\$IPName**——通过反向 DNS 查询 **\$IP** 获取的反向 DNS 名称
- **\$Dir**——会话的当前目录
- **\$Disk**——正被访问的驱动器盘符
- **\$DFree**——**\$Disk** 上的可用空间，单位 MB
- **\$FUp**——上传文件总数
- **\$FDown**——下载文件总数
- **\$FTot**——传输文件总数，实际上为 (**\$FUp** + **\$FDown**)
- **\$BUp**——上传的 KB 总数
- **\$Bdown**——下载的 KB 总数
- **\$BTot**——传输的 KB 总数
- **\$TConM**——会话持续连接的分钟总数
- **\$TConS**——会话持续连接的秒数 (0-60)，推延到 **\$TconM**
- **\$RatioUp**——应用比率中“上传”部分，如果不使用则为“N/A”
- **\$RatioDown**——应用比率中“下载”部分，如果不使用则为“N/A”
- **\$RatioType**——应用的比率类型，按每个会话或每个用户
- **\$RatioCreditType**——授予传输的信用量比率类型，按每个字节或完成的文件
- **\$RatioCredit**——应用比率的当前传输信用量，按 MB 或完成的文件
- **\$QuotaUsed**——显示当前已使用的磁盘空间配额，单位 MB，如果不使用配额则为“不限”
- **\$QuotaLeft**——显示还有多少可用的磁盘配额，单位 MB，如果不使用配额则为“不限”
- **\$QuotaMax**——显示可用使用的最大磁盘空间数，单位 MB，如果不使用配额则为“不限”
- **\$Protocol**——正在使用的当前协议 (FTP、FTPS、HTTP、HTTPS 或 SFTP (SSH2))
- **\$DomainName**——会话正在登录的当前域
- **\$DomainDescription**——会话正在登录的当前域的描述
- **\$TimeRemaining**——阻止某个 IP 地址一段时间的剩余时间 (仅限于事件通知)
- **\$LocalHomeDirectory**——本地根目录。只应用于需要此特定信息的事件，例如用户创建。
- **\$Password**——与用户账户相关联的密码。只能用于事件。不能用于欢迎消息。
- **\$UserEmailAddress**——用户的电子邮件地址。
- **\$FullName**——用户的全名，就如在“全名”字段为用户账户输入的名称一样。
- **\$SpaceFullName**——同“**\$FullName**”一样，不过在用户的全名前加了一个空格。当用户的全名为空时则留空 (无空格或名称)。
- **\$FullNameSpace**——同“**\$FullName**”一样，不过在用户的全名后加了一个空格。当用户的全名为空时则留空 (无空格或名称)。

注意：若在事件中或签署消息时使用 **\$IPName** 变量，在检索 **\$IP** 的反向 DNS 信息时会引起轻微的延迟。

文件信息

应用于最后远程访问的文件，并不一定是最后传输的文件



- **\$PathName**——检索完整的远程路径
- **\$FileName**——仅从 **\$PathName** 检索文件名
- **\$FileSize**——检索 **\$FileName** 文件的大小，单位字节
- **\$FileSizeFmt**——文件大小的格式化版本，包含数千个分隔符（取决于计算机的区域设置会使用逗号或句号）
- **\$FileSizeKB**——格式化的浮点值，表示文件大小，单位 KB
- **\$LocalPathName**——检索某个操作（与 Windows 相关时）的本地路径全名。
例如使用“C:\Temp\File.fid”替代“/Temp/file.fid”
- **\$LocalFileName**——检索文件名（当此文件存储在本地计算机上时）。请参阅 **\$LocalPathName** 获得详细信息
- **\$OldLocalPathName**——与 **\$LocalPathName** 相同，不过包含重命名前的路径。
- **\$OldLocalFileName**——与 **\$LocalFileName** 相同，不过包含重命名前的文件名。
- **\$OldPathName**——检索重命名前的远程路径名
- **\$OldFileName**——检索重命名前的远程文件名

当前活动

- **\$UNow**——Serv-U 文件服务器上的当前会话数量
- **\$UAll**——自 Serv-U 文件服务器上次启动以来已经连接到 Serv-U 的会话总数
- **\$U24h**——在过去24小时中已经连接到 Serv-U 文件服务器的会话总数
- **\$UAnonAll**——Serv-U 文件服务器上属于匿名用户的当前会话数
- **\$UAnonThisDomain**——连接域上属于匿名用户的当前会话数
- **\$UNonAnonAll**——Serv-U 文件服务器上不属于匿名用户的当前会话数
- **\$UNonAnonThisDomain**——连接域上不属于匿名用户的当前会话数
- **\$UThisName**——属于已连接用户账户的当前会话数

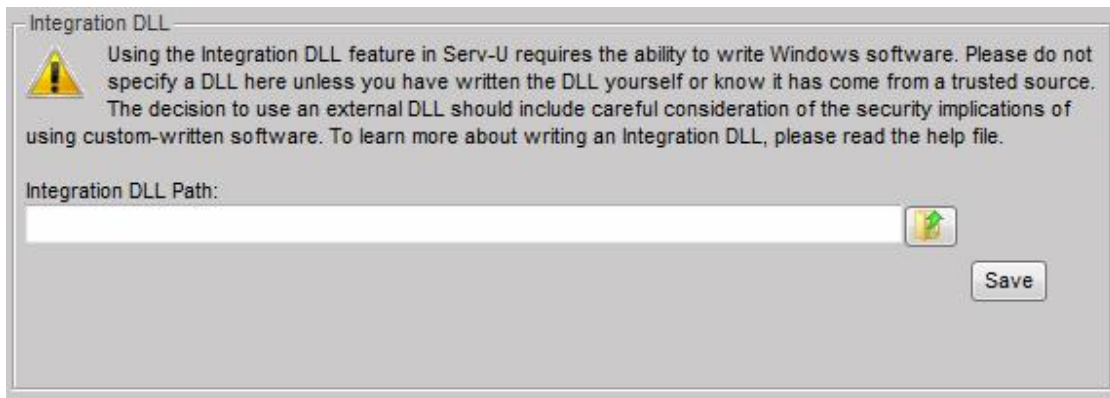


Serv-U 集成 DLL

Serv-U 文件服务器包含完全可扩展的集成 DLL，允许将 Serv-U 的几乎每个功能（用户登录、验证、密码更改等）通过易于构建的 DLL 授权给外部代码。可在 Serv-U 安装目录中的“Serv-U Integration Sample DLL（Serv-U 集成示例 DLL）”文件夹内找到通过代码提供详细说明书的 DLL。

配置集成 DLL

集成 DLL 能够以域与服务器级别进行配置。如果以服务器级别定义集成 DLL，还可将其用于尚未定义 DLL 的所有域。以域级别配置的集成 DLL 将覆盖那些以服务器级别配置的集成 DLL。可在“限制和设置 | 设置”菜单中以域或服务器级别配置集成 DLL。



注意：因为 Serv-U 提供 32-位和 64-位版本，在构建您的集成 DLL 时，必须考虑这一额外级别的复杂性。如果您正在运行 64-位版本的 Serv-U，您必须将您的 DLL 构建为 64-位 DLL，而不能构建为 32-位 DLL。如果您正在运行 64-位版本的 Windows，不过不确定您是否正在使用 64-位版本的 Serv-U，您可以在 Windows 任务管理器中进行检查。32-位版本的 Serv-U 将在可执行文件名称后包含“*32”，如下所示。

| | | | | | | | | | | |
|---------------------|--------|----|----------|-------|----------|--------|----|-----|----|-------------|
| Serv-U.exe *32 | thomas | 00 | 18,040 K | -24 K | 8,704 K | 27,366 | 0 | 331 | 21 | Serv-U® ... |
| Serv-U-Tray.exe *32 | thomas | 00 | 51,260 K | 0 K | 26,764 K | 68,234 | 20 | 496 | 21 | Serv-U® ... |



术语表

- 服务器——**Serv-U** 文件服务器，主要的 **Serv-U** 引擎处理入站 **FTP/FTPS/SFTP/HTTP/HTTPS** 请求。以服务器级别进行的设置将供所有的域、群组 and 用户继承。
- 域——用户和群组集合，使用相同的监听器和常规设置。
- 群组——共享常规设置（例如虚拟路径或目录访问规则）的用户组。
- 用户——单一账户，允许用户登录到 **Serv-U** 并访问文件和文件夹。
- 监听器——**Serv-U** 中的监听服务，可在域中配置为接受入站 **FTP、FTPS、SFTP、HTTP** 或 **HTTPS** 连接。监听器可以是 **IPv4** 或 **IPv6**，但不能同时使用这两种协议。
- 限制——配置选项，能够以服务器、域、群组或用户级别进行设置。可以为以下内容设置限制，包括密码复杂性要求、会话超时、**Web** 客户端定制等。
- **FTP**——“文件传输协议”的首字母缩写，它是一种率先出现的在因特网上共享文件的方式。目前仍然很常用，不过出于安全原因，常被安全协议（例如 **FTPS、SFTP** 或 **HTTPS**）所取代。
- **FTPS**——“通过 **SSL** 的 **FTP**”的首字母缩写，**FTPS** 连接与 **FTP** 连接相同，只不过 **FTPS** 连接使用 **SSL** 进行加密。**FTPS** 保护用户名、密码和文件在传输过程中不被窃取或拦截。**Serv-U Silver** 和 **Gold** 版本均提供 **FTPS** 支持。
- **SFTP**——“安全文件传输协议”的首字母缩写，**SFTP** 实际上与 **FTP** 毫不相关。**SFTP** 是传输文件的安全方式，它使用 **SSH** 协议，而且从本质上来说，它是 **SSH** 的子集，因为 **SFTP** 可以传输文件，但不能打开外壳（**shell**）会话。**Serv-U Gold** 版本提供 **SFTP** 支持。
- **HTTP**——“超文本传输协议”的首字母缩写，**HTTP** 是通过因特网共享网站的最常用协议。**Serv-U** 包含一个 **HTTP** 界面，以便用于 **Web** 客户端和 **FTP Voyager JV**。三种 **Serv-U** 版本均提供 **HTTP** 支持。
- **HTTPS**——“**HTTP** 安全”的首字母缩写，**HTTPS** 是连接 **Web** 服务器的安全方式。**Serv-U Gold** 版本提供 **HTTPS** 支持。
- 公共密钥验证——公共密钥验证，或 **PKA**，是 **SFTP** 中的一个过程，用户通过这种方式可以使用密钥对取代密码，对 **Serv-U** 进行验证。这是非常安全的连接方式，而且在基于 **Unix** 的操作系统中常供自动化的任务调度使用。
- 事件——**Serv-U**
事件主要包括事件类型（用户登录、文件上传失败等）与操作类型（显示气球提示、发送电子邮件、或执行命令）。**Serv-U** 事件用于自动化操作，并为重要的文件传输过程提供更为出色的可见度。
- 反恶意攻击——一项 **Serv-U** 功能，帮助管理员阻止使用错误凭证反复尝试连接的 **IP** 地址。“反恶意攻击”通过智能处理那些反复错误登录而导致失败的 **IP** 地址，允许管理员智能阻止病毒与黑客。
- **Web** 客户端——**Serv-U Web** 客户端是基于 **web** 的文件传输界面，所有的 **Serv-U** 版本均免费提供 **Web** 客户端。作为高级的 **Web 2.0** 服务，它能像任何其他客户端一样，供您上传、下载、删除与重命名文件。它还能用来拖/放文件、播放媒体文件、或将图像处理为幻灯片与缩略图格式。



- **FTP Voyager JV**——FTP Voyager JV 是高级的多平台文件传输客户端，作为 Serv-U 文件服务器的插件提供。它基于 Java，通过 HTTP/HTTPS 界面启动，允许完全的拖/放功能，并与桌面集成，给予您无缝的传输体验。
- **AES**——“高级加密标准”的首字母缩写。AES 是强加密标准，供美国政府与众多企业使用，以便在传输时加密数据。Serv-U 所提供的 AES 支持 128-位、192-位与 256-位密码。
- **目录访问**——包括应用于服务器、域、群组与用户的所有权限，允许和拒绝访问文件和文件夹。目录访问规则是文件访问权限的基础，确定一个用户可以访问什么，不能访问什么（以及如何进行访问）。
- **IP 访问**——Serv-U 中使用的 IP 访问规则帮助您确定谁可以连接到服务器。以服务器与域级别定义的规则确定谁可以创建与 Serv-U 的初始连接，而以用户和群组级别定义的规则确定谁可以使用给定的用户账户进行连接。
- **远程管理**——通过 Serv-U 中的 HTTP/HTTPS 服务，Serv-U Gold 版本的用户可以远程连接到 Serv-U 来管理服务与用户，无需实际登录到服务器本身。这实现了更为简便的远程服务器管理。
- **UPnP**——UPnP 表示通用即插即用，这是软件用来自动配置网络服务的路由器与防火墙的方式。Serv-U 包含针对 IPv4 与 IPv6 路由器的 UPnP 支持。

