红旗安全操作系统 4.0

安装分发手册

北京中科红旗软件技术有限公司

地址：中国北京海淀区万泉河路 68 号紫金大厦 6 层

Red Flag Software Co., Ltd.

http://www.redflag-linux.com

声明：

本软件受相应版权法保护，并在 GNU GPL 约束其使用、拷贝、发布及反编译的授权下发布。在未经红旗软件公司事先书面授权的情况下，文档的任何部分都不得以任何形式和途径进行复制、修改及分发。本手册在编写过程中由于已考虑了各种可能的预防措施，红旗软件公司对可能出现的内容错误及缺失不承担责任。

此出版物仅以其原有的存在形式提供，不含任何种类的明示或默示，包括但不仅限于那些隐含的用于商业目的的、为某种特定目的而定制的、或无特定目的的担保。此出版物可能会出现技术上的失误或印刷上的错误。其更正将不断添加于此，并合并到此出版物的最新版本中。

红旗软件公司保留在任何时刻对此出版物介绍的产品和/或程序进行添加和/或修改的权利。

本文档的最终解释权归属于红旗软件公司。

本产品使用了如下字库：

本产品使用了如下输入法：

目　　录

序

欢迎使用红旗安全操作系统！

《红旗安全操作系统安装分发手册》将帮助您顺利地在联网或非联网的机器上安装红旗安全操作系统。

红旗安全操作系统 4.0 采用图形化的安装方式，具有友好的安装界面、简捷的安装配置步骤。整个安装过程清晰明了，用户可以轻松自如地完成系统安装。

本书的适用对象

本手册适用于负责安装操作系统的系统管理员。它将帮您做好安装前的准备工作，并引导您完成整个安装过程。

如果您是一位有经验的 Linux 用户，而且以前使用过 Red Flag Asianux Server 系列产品，则可以跳过前两章，直接从***第 3 章：安装红旗安全操作系统***开始阅读。

提示与警告

为了强调《红旗安全操作系统 4.0 安装分发手册》中的某些重要的信息，我们使用下面两种方式加以重点说明：

一些有用的额外信息、使用中提示和帮助用户更加顺利地完成工作的小技巧等。

看到这一标记时应引起特别注意，它表示一些重要的警告和错误提示信息。

第1章 安装前的准备

安装红旗安全操作系统 4.0 之前，必须进行一些前期的准备工作。比如了解产品组成、制定安装计划、备份数据、硬件检查、制作安装引导盘和驱动盘、准备硬盘分区等。

1.1 产品组成

红旗安全操作系统 4.0 主要由四部分功能模块组成：安装于服务器上的 Linux 安全操作系统，是承载涉密数据和安全应用的运行载体；可选的安装于远程 Linux 终端上的安全和审计管理控制台，主要用于对于多节点的安全操作系统的远程集中化管理，包括安全和审计管理；以及可选的异常监测和报警组件，用于监测服务器端的异常事件和报警通告；最后是可选的 MySQL 审计备份数据库服务器，主要完成对审计记录进行可选的实时异地数据库备份导入。

我们首先将对安全操作系统的安装和前期配置做详细描述。关于可选的远程安全和审计管理控制台、异常监测和报警组件、以及可选的 MySQL 审计备份数据库服务器的安装和配置，将在第 4 章集中表述。

1.2 计划安装

在安装红旗安全操作系统 4.0 前，应做一个系统的工作计划。其中包括服务器硬件设备的选择、确定将要提供的服务类型、以及期望系统现在具有与将来具有的性能水平、物理上和人员上的安全规划等等。

对于基于关键任务的企业级服务平台，建议配置尽可能大的内存、采用 SMP 系统，并应建立某种冗余机制，如磁盘冗余阵列——RAID。

出于安全管理的需要，红旗安全操作系统 4.0 将系统管理、安全管理和审计管理按照职能进行了权能分立。因此，应安排至少三个有责任心的技术管理人员承担相应的管理任务，杜绝一人兼任多个管理职能的交叉管理行为发生。

在物理安全上，除保证机房的物理安全外，建议所有与安全服务器有网络连接的终端均使用防火墙等设施进行了访问控制。

1.3 备份数据

安装红旗安全操作系统 4.0 之前，最好先将硬盘上的重要数据备份到软盘、光盘、U 盘或磁带等介质上，以免在安装过程中发生意外时给您带来不必要的损失。通常要做备份的内容包括系统分区

表、系统中的重要文件和数据等。

1.4 了解计算机的硬件和网络信息

为保证后面的安装与配置能够顺利进行，在安装之前应收集以下几方面的机器信息。

※ 基本硬件配置信息	
硬盘	数量、容量大小、接口类型（IDE 或 SCSI）、参数（柱面数/磁头数/扇区数），如装有多个硬盘，要明确其主从顺序。
内存	计算机内存的大小。
光驱	接口类型（IDE、SCSI 或其它类型）；如果是非 IDE、非 SCSI 光驱，要明确其制造者和型号；如果是 IDE 光驱，它连接在第几个 IDE 口上。
SCSI 设备	记录其制造者和型号。
鼠标	类型（串口、PS/2、USB 或总线鼠标）、按键数目，串行鼠标连接的串行端口号。
※ 显示设备	
显卡	制造商、显卡型号（或使用的芯片组型号）、显存的大小。
显示器	制造商、显示器型号、水平和垂直刷新频率的范围。
※ 网络配置信息	
网卡	制造商、型号、中断号及端口地址。
调制解调器	制造商、型号及连接端口号。
其它	主机名称、所属域名、网络掩码、路由器（网关）地址、DNS 地址等。

红旗安全操作系统 4.0 基本系统基于红旗 Asianux Server 3 SP2 Linux 发行版，继承了其良好的硬件兼容性，保证与近年来生产的大多数硬件兼容。但是由于硬件的技术规范改变频繁，可能难以保证百分之百地兼容新的硬件。

关于最新的硬件支持信息，敬请访问红旗公司主页：http://www.redflag-linux.com。

1.5 确认安装环境要求

在红旗安全操作系统 4.0 安装之前，请确认如下安装环境要求是否具备：

CPU	最低 Pentium 3 800Mhz，推荐 Pentium 4 1G 以上 SMP 架构
内存	最低 1G，推荐 4G 以上
磁盘空间	推荐根分区 8GB 以上，交换区(swap)为内存 2 倍(最大不宜超过 2G)；

	推荐建立不低于 20G 的/var 日志分区

由于系统默认审计全部安全事件，将占用较大内存和日志记录空间。如果内存或者磁盘空间太少，审计记录有可能丢失。

1.6 制作安装引导盘

一般情况下，用户仅需从光盘引导安装即可。如果您的机器不支持从光盘引导，或有特殊的安装需求，便需要使用安装引导盘了。

红旗安全操作系统 4.0 中，安装光盘的/images 目录下，提供了一些映像文件。其中，有引导系统安装程序的引导盘映像，也有从一些非常规硬件上加载安装程序所需要的驱动程序盘映像。常用的是 diskboot.img 和 boot.iso，其中：

diskboot.img	安装引导盘。可以写入 U 盘或其他大容量可引导存储介质中，用来引导从本地光盘、网络、硬盘或 PCMCIA 设备的安装。
boot.iso	引导安装光盘。用于将同一套软件通过网络安装在很多机器上时使用。

根据将安装红旗安全操作系统 4.0 系统的主机的硬件配置、引导方式及安装介质的不同，请在安装前制作好所需的引导盘和驱动程序盘。关于如何选择引导和安装红旗安全操作系统 4.0 的方式，请参考本手册第 2 章：***启动安装程序*** 。

驱动程序盘为安装程序不支持的硬件添加支持，安装程序会在适当的时候提示您插入所需的驱动程序盘。

由于内核及驱动的体积变大，导致本版本无法再使用 3.5 英寸软盘来进行存储，于是将引导盘与驱动盘整合成一个镜像，以方便用户安装。

安装引导盘需要一个可用的 U 盘类设备。请准备好容量大于 12M 的 U 盘类设备，并确定计算机能够从该设备引导。

在 Linux 环境下，需要一台能够运行 Linux 系统中 dd 工具的计算机。

下面将介绍通过映像文件创建引导盘的方法。

下面的示例中都使用了“/”(斜杠)来分隔目录和文件，这是 Linux 系统的特点，Windows 中的分隔符是“\”(反斜杠)。

当计算机中已存在 Linux 环境，或借用一台 Linux 系统主机，执行下列的步骤：

1) 将光驱挂载到系统的/mnt/cdrom 目录上；

 # mount /dev/cdrom /mnt/cdrom

2) 插入一个 U 盘，然后输入：

 # dd if=/mnt/cdrom/images/diskboot.img of=/dev/sda1

使用 dmesg 命令检查物理设备的映像文件。（此处物理设备为 U 盘）

如果要制作其它引导盘或驱动程序盘，请再次运行 dd，并指定恰当的映像文件，选择目标设备，例如 U 盘（/dev/fd0）。

制作 Adaptec、HighPoint 控制器等特殊设备的驱动程序盘时，只需将以上命令中的映像文件换成相对应的映像文件，例如 Adaptec/aarich.img。

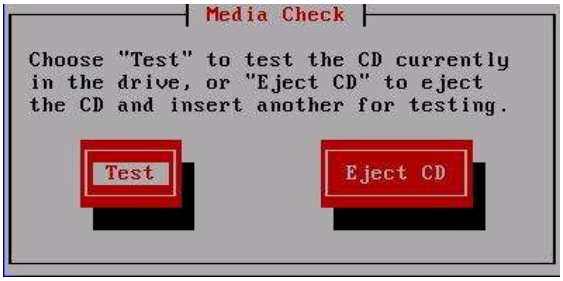
1.7 验证安装介质完整性

红旗安全操作系统 4.0 在产品发布盘上集成了 md5 码校验机制。任何第三方对红旗分发介质的变更将导致安装阶段的介质完整性校验失败。

用户可以在安装引导阶段在 boot:提示符前输入 redflag mediacheck 并回车启动介质完整性校验功能。在默认安装方式下，该功能也将自动默认启动。

介质完整性校验的启动页面如下图所示。点选”OK”按钮后将弹出介质完整性检查确认框。点选”Test”按钮验证当前光盘介质的完整性。

校验结束将提示完整性校验结果。如果校验失败说明该介质分发无效，请尽快与红旗软件公司进行联系。



介质完整性检查

除了在介质上进行完整性校验外，红旗安全操作系统还在 RPM 包一级进行了完整性校验和检测机制。由于系统在安装形式上主要由 RPM 包组成，为了有效防止系统分发阶段可能产生的分发修改，红旗安全操作系统在开发阶段就已经对系统 RPM 包的编译环境进行了私钥设置，除了部分集成的商业软件(如 SUN JDK)由于授权原因不能进行公钥设置外，所生成的 RPM 包均有一致的对外公钥。所有非一致性公钥的 RPM 包将被视为不可信。

用户可以在 Linux 系统下挂载红旗安全操作系统安装光盘并切换到相应的 RPM 包目录(RedFlag/RPMS)，执行如下命令检验 RPM 包的公钥是否一致来发现可疑的分发修改。如果发现可疑的分发不一致，请尽快致电红旗软件公司确认红旗安全操作系统分发的有效性。

rpm -qpi *.rpm |grep Signature

1.8 准备足够的磁盘空间

最好把红旗安全操作系统 4.0 安装在一个独立的硬盘上，如果不具备这一条件，也必须使用和其它操作系统（如 Windows、OS/2 以及不同版本的 Linux 系统）分隔开来的硬盘分区。

安装过程中会提示为红旗安全操作系统 4.0 分配适当的硬盘空间，因此了解当前计算机系统的使用情况并为创建这些分区准备足够的硬盘空间是至关重要的。

1.8.1 硬盘分区

一块硬盘可以被划分为多个分区，分区之间是相互独立的，访问不同的分区就像在访问不同的硬盘。分区有三种类型：主分区（primary-partition）、扩展分区（extended-partition）和逻辑分区（logical-partition）。一块硬盘最多可以有四个主分区，如果想在一块硬盘上拥有多于四个的分区，就要创建扩展分区，再在扩展分区上划分出逻辑分区。红旗安全操作系统 4.0 既可以安装在主分区上，也可以安装在逻辑分区上。

红旗安全操作系统 4.0 支持多个操作系统的共存并进行多重引导，但对于服务器来说，一般要全

天连续工作，因此额外的操作系统是不需要的，最好用干净的磁盘进行分区。

为了顺利地安装红旗安全操作系统 4.0，需要为根分区（/）（不包括 swap 分区）分配大于8G 的硬盘空间。另外，为了保存动态增长的运行系统日志和审计日志，推荐建立单独不少于 20G 的/var 日志分区。

如果确定将整块硬盘空间全部用于红旗安全操作系统 4.0，或在硬盘上有足够红旗安全操作系统 4.0 使用的未经分区的空闲空间或是未使用分区中的空间，那么就可以不阅读后面的内容，直接进入下一章：***启动安装程序***。

什么是未经分区的空闲分区？

已定义的分区没有占据整个硬盘，一个未经使用的硬盘也属于这种类型。这时可以简单地从未使用的空间中创建必要的分区。

什么是未使用分区中的空间？

过去曾将一个或多个分区用于其它的操作系统，而现在它们已不再被使用。这时应该先删除这些分区，然后在其上创建相应的 Linux 分区。可以用 DOS 下的 fdisk 命令完成，也可以在安装过程的配置分区步骤中实现。

1.8.2 重新分区的方法

如果系统中安装了其它操作系统，而且硬盘空间都被已安装的操作系统所占据，这种情况比较麻烦，除了增加一个新的硬盘外，还可以通过以下几种方式为红旗安全操作系统 4.0 分配硬盘空间。

- **方便的安装方法：无需对硬盘做太大改变**

必须有一个或一个以上的可删除分区，将上面的重要数据移到其它分区或备份后删除该分区，释放足够的磁盘空间来安装红旗安全操作系统 4.0。

只有当计算机上有两个硬盘驱动器或磁盘分区时，才可以使用这种方法。

- **破坏性的重新分区**

首先备份硬盘上的重要数据，然后对硬盘重新分区，分区时留下足够红旗安全操作系统 4.0 使用的空间。重新安装原有的操作系统及应用软件，之后再安装红旗安全操作系统 4.0。

- **使用分区工具划分**

使用分区魔术师 **PQMagic**、**FIPS** 等分区工具可以在保留数据的同时，安全地改变分区的大小。它将计算机的 DOS/WINDOWS 分区分为两个部分：DOS/WINDOWS 文件系统分区和一个空闲分区，这个空闲分区就可以用做安装新系统。

PQMagic 运行稳定、界面友好，可以在不损坏磁盘数据的情况下，任意地改变硬盘的分区及各分区的文件系统，具体信息请参照该工具的说明文档。

改变当前系统硬盘分区，在具体操作上是一件非常危险的事情，出现一点差错就可能导致整个硬盘数据的丢失，因此建议您提前将重要的数据备份好。

第2章 启动安装程序

为了开始红旗安全操作系统 4.0 的安装，需要进行安装程序的引导，可以使用光盘引导或 U 盘引导两种方式。

2.1引导安装程序的方法

根据系统硬件设备和将使用安装介质的不同，可以使用下列方式来引导红旗安全操作系统 4.0 的安装程序。

2.1.1 使用光盘引导

使用光盘引导、安装是安装红旗安全操作系统 4.0 最直接、最快捷、最方便的方法。它的前提是用户拥有系统安装光盘并决定使用光盘作为安装介质，且计算机支持从光盘引导的情况。

安装时，应首先设置当前计算机的 BIOS 启动顺序，把 DVD-ROM 作为第一个启动搜索选项。即保证引导搜索顺序为***光盘引导优先***。

2.1.2 使用 U 盘引导

如果计算机不支持光盘引导，或者您没有系统安装光盘，则需要使用安装引导盘来引导安装。安装引导盘的映像文件是安装光盘中的/images/diskboot.img 文件。

使用安装引导盘进行引导之前，需要改变系统的 BIOS 启动顺序，设置为 ***U 盘引导优先*** 。

如果需要安装引导盘，那么请事先准备好它。关于制作引导盘的详细信息，请参阅 *1.6 节*：***制作安装引导盘***。

引导和安装使用的介质没有本质的关系。事实上，使用光盘引导，也可以选择从硬盘或网络进行安装。具体实现如下：使用红旗安全操作系统 4.0 的安装光盘引导之后，在 boot：提示符下输入 redflag askmethod 引导选项，将出现安装介质的选择界面。有兴趣的用户可以实践一下。

2.1.3 成功引导

不论使用光盘还是 U 盘引导，成功引导后都将出现红旗安全操作系统 4.0 的安装启动界面，屏幕显示提示信息和 boot：提示符，按**<Enter>**键或等待一段时间不采取任何操作即可进入图形安装界面。

成功从光盘引导

如果需要使用文本安装方式，那么在 boot：提示符下输入 **redflag text**，然后按**<Enter>**键。

如果需要使用专家安装方式，那么在 boot：提示符下输入 **redflag expert**，然后按 **<Enter>** 键。

如果需要指定其他的安装方式，那么在 boot：提示符下输入 **redflag askmethod**，然后按 **<Enter>** 键。

我们推荐您使用图形安装方式执行安装。因为它具有界面友好、操作方便等优点。

正常情况下，只需使用默认选项。请留意引导信息以查看 Linux 内核是否检测到了计算机的硬件。如果硬件被正确地检测到，则进入后续的安装步骤。

- **关于文本安装方式**

文本安装方式与图形安装方式的操作步骤基本一致，仅仅是更换了操作界面，在配置和使用方面也大同小异。如果必须使用文本安装方式，参照下一章关于图形方式安装过程的介绍，您便能够很快地掌握。

目前，硬盘安装、FTP 安装及 HTTP 安装方式只提供了文本安装界面。

- **关于专家安装方式**

专家安装方式采用文本界面，用于提供某些安装程序不支持的特殊硬件的驱动支持。目前来说，这些特殊硬件大多数是 SCSI 适配器、RAID 设备或网络接口卡。红旗安全操作系统 4.0 安装程序中已

经为用户提供了上百种此类设备的驱动程序，但对于没有涵盖到的某些类型，就需要使用驱动 U 盘或驱动光盘通过专家安装方式为其加载驱动程序。

在专家安装方式中，安装程序会询问用户是否要使用驱动盘，然后选择从 U 盘或光驱中加载驱动程序。

驱动盘可以是由红旗公司制作的，也可根据红旗公司网站上发布的驱动程序映像自制，还可以是由硬件厂家提供的。

如果在安装红旗安全操作系统 4.0 时不需要某个不被支持的设备，就不必在此时使用驱动程序盘，可以在安装完成后添加对该设备的支持。

红旗安全操作系统 4.0 安装程序有自己的驱动 U 格式，如果不能满足格式的要求，可能将导致不能正确加载驱动。

2.1.4 EFI 系统的引导

EFI 作为 Intel 下一代的固件，红旗安全操作系统 4.0 已经为其提供了支持。

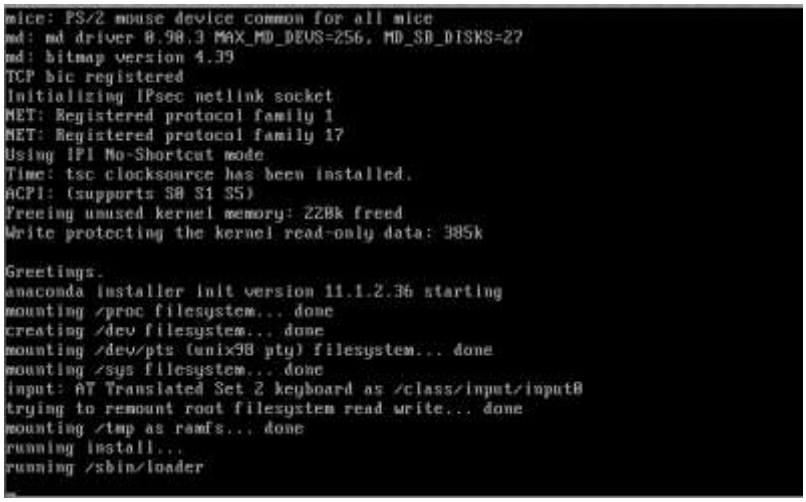
将光盘放入光驱后，重新启动计算机。当屏幕底端显示“start boot option”时按<**F2**>健，选择进入 Boot Manager。

选择 cdrom entry1，从光盘启动计算机。或直接从光盘启动计算机，输入 redflag efi 进入支持 efi 的安装模式。

安装时需建立一个 100M 的 vfat 分区，挂载点为/boot/efi。该分区必须是一个主分区，建议使用 hda1。其余的过程与一般的安装方式相同。

2.1.5 启动 Linux 安装程序

接下来的步骤是进行 Linux 核心的启动。下图是执行完 Linux 核心的引导，即将进入安装界面时的示意图。



Linux 核心的启动

图中最后一行 running /sbin/loader 表示正在运行安装程序的加载程序，也表示当前已经完成安装核心的启动。稍等片刻后，就会进入对应的安装程序。

安装过程中可以切换到不同的虚拟控制台，它们提供了各种有用的信息以及在 shell 下输入命令的方法。对于安装过程中所遇问题的定位和解决有很大帮助。

各个虚拟控制台的切换热键以及它们显示的内容如下：

<Ctrl+Alt+F1>	安装对话框	**<Ctrl+Alt+F4>**	与系统相关的消息
<Ctrl+Alt+F2>	shell 提示	**<Ctrl+Alt+F5>**	其它消息
<Ctrl+Alt+F3>	安装日志	**<Ctrl+Alt+F6>**	图形化显示

2.2选择安装方法

红旗安全操作系统 4.0 提供了多种不同的安装方式供用户选择，请根据具体情况选择一种合适的安装方法。

在一些场合，如机房中有大量的计算机需要同时安装系统，通过光盘逐个安装，不仅效率低，而且也不利于维护。

2.2.1 光盘安装

在计算机不支持从光盘引导的情况下，可尝试用 U 盘引导后，再用光盘进行安装。

安装引导 U 盘的映像文件是安装光盘中的/images/bootdisk.img 文件，关于制作引导盘的详细信息，请参阅本手册 ***1.6 节：制作安装引导盘***。

U 盘成功引导安装程序后，将出现如下图所示的“**Installation Method（安装介质）**”选择界面。

选择安装介质

选择“**local CDROM（本地光盘）**”，将红旗安全操作系统 4.0 的安装光盘插入光盘驱动器，一旦光盘已经在驱动器中，选择“**OK**”，然后按**<Enter>**键继续。

如果拥有安装光盘，并且计算机支持从光盘引导，建议使用安装光盘引导，成功引导后将直接进入图形化的光盘安装方式。

2.2.2 硬盘安装

如果没有红旗安全操作系统 4.0 的安装光盘，也可以将安装光盘的 ISO 映像下载或复制到本地硬盘驱动器中，执行硬盘安装。

使用硬盘安装也需要一个安装引导 U 盘，此外根据硬件设备的不同，还可能需要制作块设备驱动程序盘。关于制作安装引导盘和驱动程序盘的详细信息，请参阅本手册 ***1.6 节：制作安装引导盘***。

硬盘安装需要使用系统安装光盘的 ISO 映像文件。执行安装之前，先把红旗安全操作系统 4.0 安装光盘的 ISO 映像文件一起存放到本地硬盘中的某一位置下，***注意：该目录下不能包括有其他.iso 文件***。

U 盘成功引导安装程序后，在“**Installation Method（安装介质）**”界面中选择“**Hard drive（硬盘）**”，然后按**<Enter>**键继续。

接下来要为安装程序指定 ISO 映像文件所在的位置，如下图所示。

从硬盘安装

在“**select Partition**（**选择分区**）”界面中指定包含 ISO 映像文件的分区设备名。如果 ISO 映像不在该分区的根目录中，则需要在“**Directory holding images**（**包含映像的目录**）”中输入映像文件所在的目录路径。例如，ISO 映像在/dev/hda3 中的/download/redflag 中，就应该输入：/download/redflag。

存放 ISO 映像文件的分区必须是 ext2、ext3 或 FAT 文件系统格式，否则将无法执行硬盘安装。如 reiserfs、NTFS 都是不可以的。

2.2.3 网络安装

红旗安全操作系统 4.0 提供了 NFS、FTP、HTTP 三种网络安装方式。网络安装所用的 NFS、FTP、HTTP 服务器必须能够提供完整的红旗安全操作系统 4.0 安装树目录，即安装光盘中的所有必须的文件都存在且可以被使用。

要把安装光盘中的内容复制到网络安装服务器上，执行以下步骤：

```
# mount /dev/cdrom /mnt/cdrom

# cp -var /mnt/cdrom/*    /filelocation  （/filelocation  代表存放安装树的目录）

# umount /dev/cdrom/
```

如果你直接提取光盘中的 vmlinuz 及 initrd.img 然后使用其它引导器（如其它介质中的 grub 等）来进行安装引导，你需要在内核参数中追加 selinux=0 参数。

2.2.3.1 配置 TCP/IP

进行网络安装需要一张安装引导盘外，还需要准备网络驱动盘。关于制作安装引导盘和驱动程序盘的详细信息，请参阅本手册 ***1.6 节：制作安装引导盘***。

U 盘成功引导安装程序后，在“**Installation Method（安装介质）**”界面中选择要从哪个网络服务器上安装红旗安全操作系统 4.0，即“**NFS image（NFS 映像）**”、“**FTP**”或“**HTTP**”，然后按**<Enter>**键继续。

无论采用哪一种网络安装方式，都需要在如下图所示的“**Configure TCP/IP（配置 TCP/IP）**”对话框中，进行本机的 TCP/IP 配置。

TCP/IP 设置

系统支持 IPv4 和 IPv6 两种协议，用户可以选择 IPv4 或 IPv6，然后进行相关的 IP 地址配置。

如果用户选择了手工配置，将弹出上图所示的对话框。请输入本机的 IPv4 或 IPv6 地址、网关、名称服务器，然后按“**OK**”进入下一步。

2.2.3.2 NFS 安装

进行 NFS 安装的前提是网络中要有提供红旗安全操作系统 4.0 安装映像输出的 NFS 服务器，系统管理员如果要配置支持安装的 NFS 服务器，请参阅本手册附录 B 中的 ***NFS*** 网络安装的筹备工作。

NFS 安装除了可以利用安装树之外，还可以使用 ISO 映像文件，把红旗安全操作系统 4.0 安装光盘的 ISO 映像文件一起存放到 NFS 服务器的某一目录（该目录不能包括有其他.iso 文件），然后把该目录作为 NFS 安装指向的目录。

下图所示为 NFS 设置界面，请在此输入 NFS 服务器的信息。

NFS 安装

在“**NFS server name**

（NFS 服务器名称）”中输入 NFS 服务器的域名或 IP 地址，在“**RedFlag SecOS 4.0 directory（红旗安全操作系统 4.0 目录位置）**”中输入包含红旗安全操作系统 4.0 安装树或安装光盘镜像的目录名。

例如，NFS 服务器将红旗安全操作系统 4.0 的安装树或安装光盘的映像文件保存在 product/redflag/cdrom 目录中，则在“**RedFlag SecOS 4 directory**”中输入“**/product/redflag/cdrom**”。

2.2.3.3 FTP 安装

如果选择从 FTP 服务器中安装，将会出现如下图所示的 FTP 设置对话框。

FTP 安装

在“**FTP site name（FTP 站点名称）**”中输入 FTP 站点名称或 IP 地址，在“**RedFlag SecOS 4.0 directory**”中输入包含红旗安全操作系统 4.0 安装树的目录名。

例如，FTP 服务器将红旗安全操作系统 4.0 的安装树保存在/ftp/product/redflag 目录中，则在“**RedFlag SecOS 4.0 directory**”中输入“**/ftp/product/redflag**”。

2.2.3.4 HTTP 安装

如果选择从 HTTP 服务器中安装，将会出现如下图所示的 HTTP 设置对话框。

HTTP 安装

在“**HTTP site name（HTTP 站点名称）**”中输入 HTTP 站点名称或 IP 地址，在“**RedFlag**

SecOS 4.0 directory”中输入包含红旗安全操作系统 4.0 安装树的目录名。

例如，HTTP 服务器将红旗安全操作系统 4.0 的安装树保存在 product/redflag 目录中，则在“**RedFlag SecOS 4.0 directory**”中输入“**product/redflag**”。

第3章 安装红旗安全操作系统

前面已经讲过，红旗安全操作系统 4.0 的安装程序除了提供了图形安装方式外，还可以使用文本界面的安装方式。

本章将以图形安装方式为例，介绍安装红旗安全操作系统 4.0 系统的具体步骤，我们强烈推荐您使用图形安装方式来执行安装；因为它具有界面友好、操作方便的优点。

如果必须使用文本方式进行安装，也可以参照本章的图形化安装说明来获得必要的信息。

3.1 开始安装

完成安装程序的引导，将进入如下图所示的图形化安装界面。

开始安装

红旗安全操作系统 4.0 提供统一的图形化安装界面风格，屏幕下方列出了整个安装过程要经历的每一个步骤，并显示出当前所处的安装步骤；屏幕中上部是对应安装步骤的配置选项和参数设置界面。

屏幕的中下方有三个按钮：“**Back**”表示回到上一个安装界面；“**Next**”表示已经确定了当前的选择，要进入下一个安装步骤；“**Exit**”表示可以在任一时间退出安装程序，重新启动计算机。

在没有进行语言选择之前，界面文字缺省使用英文显示。

单击“**Next**”按钮继续，进入语言选择界面。

3.2 语言选择

此时选择的语言，决定了安装过程中使用的语言类型以及安装完成后在使用系统过程中默认的语言类型。您可以选择简繁体中文或英语。

语言选择

在此以选择“**Chinese Simplified（简体中文）**”为例，然后单击“**Next**”按钮。

安装完毕后，如果用户需要修改环境语言，可以运行 system-config-language 命令。根据提示选择，脚本会自动修改相关的文件。之后，用户必须注销后重新登录方能生效。

3.3 许可协议

接下来显示如下图所示的《软件协议书》界面。

软件许可协议

请仔细阅读其中的内容，如果愿意继续安装，选中“**接受**”，并单击“**下一步**”按钮进入后面的安装步骤。

如果选择“不接受”，将不能继续进行安装。如果由于某些原因需要取消本次操作，可以按下屏幕底部的“退出”按钮，将安全地取消本次安装。

3.4 设置键盘

红旗安全操作系统 4.0 提供了英文和日文两种键盘的选择，对于中文用户来说，选择英文键盘即可。

3.5 设置分区

对于大多数用户来说，设置分区是安装 Linux 系统过程中的最大难题。在此步骤中，必须告诉安装程序要在哪里安装系统，即为将要安装红旗安全操作系统 4.0 的一个或多个磁盘分区上定义挂载点。这时，需要根据实际情况创建、修改或删除分区。

2.5.1 分区的命名设计

Linux 通过字母和数字的组合来标识硬盘分区，具体如下：

前两个字母	分区所在设备的类型	hd：IDE 硬盘 sd：SCSI 硬盘

第三个字母	分区在哪个设备上	hda：第一块 IDE 硬盘 hdb：第二块 IDE 硬盘 sdc：第三块 SCSI 硬盘
数字	分区的次序	数字 1-4 表示主分区或扩展分区，逻辑分区从 5 开始。

例如：/dev/hda3 是指第一个 IDE 硬盘上的第三个主分区或扩展分区；/dev/sdb6 是第二个 SCSI 硬盘上的第二个逻辑分区。

注意：如果硬盘上没有分区，则一律不加数字，代表整块硬盘。

2.5.2 分区的组织

分区的目的是在硬盘上为系统分配一个或几个确定的位置，Linux 系统支持多分区结构，每一部分可以存放在不同的磁盘或分区上。

一般情况下，服务器系统都会规划多个分区，这样可以获得较大的灵活性和系统管理的方便性。

至于如何规划服务器上的 Linux 硬盘空间，建议考虑如下几个因素：

- 首先，Linux 根文件系统需要一部分的硬盘空间，挂载为/的根分区。
- 其次，交换分区需要一部分的硬盘空间。交换分区的大小取决于需要多少虚拟 RAM。一般来说，交换分区的大小为物理 RAM 的 1~2 倍。1G 以上的内存，将交换分区设置为 2G 即可。
- 最后，作为服务器用途，建议根据实际情况将根分区与/usr、/home、/var、/boot 等分区单独放在不同的磁盘分区或设备上，这是因为将每个关键性的区域存放在独立的分区，可为日后的移植、备份、系统恢复与管理提供方便。

分区功能简介

/	整个系统的基础（必备）
swap	操作系统的交换空间，用来支持虚拟内存，当系统没有足够的内存来储存正在处理的数据时，就要使用交换分区的空间。（必备）
/boot	在根下创建，用来单独保存系统引导文件
/usr	用来保存系统软件
/home	包含所有用户的主目录，可保存几乎所有的用户文件
/var	保存邮件文件、新闻文件、打印队列和系统日志文件
/tmp	用来存放临时文件，对于大型、多用户的系统和网络服务器有必要

安装红旗安全操作系统 4.0 至少需要创建以下三个分区：

- **根分区（/）**

Linux 根文件系统驻留的地方。***为了顺利安装，需要为根分区分配大于 8G 的硬盘空间***。

- **交换分区（swap）**

交换分区的大小一般设置为计算机内存的 1~2 倍。具体来说，如果系统内存不大于 1GB，交换分区就应该至少和系统内存相等，最多是其两倍；如果内存大于 1GB，推荐使用 2GB 的交换分区。

- **日志分区（/var）**

红旗安全操作系统 4.0 的审计日志增长很快，为了保证系统能够保留足够的系统日志和安全审计日志供日后监测和分析使用，建议单独创建不低于 20G 的日志分区。

2.5.3 配置分区方式

安装过程需要对硬盘进行分区。默认情况下，系统会提供一个合理的分区结构，您可以选择使用该分区结构或建立一个自定义的分区结构。

在红旗安全操作系统 4.0 进行自动分区时，系统提供了四种对原分区的处理方式：

- 在选定磁盘上删除所有分区并创建默认分区结构
- 在选定在选定驱动上删除 Linux 分区并创建默认的分区结构
- 使用选定驱动器中的空余空间并创建默认的分区结构
- 建立自定义的分区结构

如需进行手动重新分区，请选择“**建立自定义的分区结构**”。具体情况还请根据自身情况决定选项，并点击“**下一步**”按钮。

分区方式

2.5.4 配置分区

在下图中可以根据用户的要求，创建、修改和删除硬盘分区，并对每个分区设置装入点。

分区工具

可以看到，系统当前的硬盘分区情况以树状的目录层次结构列出，最上面的一级是硬盘，如果存在多个硬盘，分别以 hda、hdb、sda、sdb…表示。

如果分区设备名前面带有 符号，表示它下面还包含未显示的分区；如果分区设备名前面的符号为，表示它所包含的分区已全部显示。

分区列表中显示了系统中硬盘驱动器的详细信息，每一行代表一个硬盘分区，包括五个不同的

域：

设备：	当前硬盘和硬盘分区的名称
类型：	分区的文件系统类型
挂载点/RAID/Volume：	分区在目录树中的加载位置、RAID 设备名、LVM 卷组名称
格式化：	是否要对当前的分区进行格式化
大小：	当前分配给这个分区的空间（以 MB 为单位）
开始：	分区在物理块中的起始位置
结束：	分区在物理块中的结束位置

如果不想看到列表的 RAID 设备成员和 LVM 卷组成员，选中“**隐藏 RAID 设备/LVM 卷组成员**”。

分区列表底部的一排按钮用来控制 **Druid Disk** 分区工具的行为，用途如下：

新建：在空闲分区上申请一个新分区，选择后出现一个对话框，按要求输入所需的项；

编辑：选中分区后按下该按钮，用来修改当前分区表中已创建好的分区的某些属性；

删除：用来删除所选分区；

重设：取消所做的修改，将分区信息恢复到用户设置之前的布局。

RAID：用来给部分或全部磁盘分区提供冗余性。只有当您具备 RAID（磁盘冗余阵列）的相关经验时才应使用。

要创建一个 RAID 设备，必须首先创建文件系统类型为“software RAID”的分区。一旦已经有了两个或两个以上的软件 RAID 分区，选择“RAID”按钮来把软件 RAID 分区连接为一个或多个 RAID 设备。

LVM：用于创建一个 LVM 逻辑卷。

要创建 LVM 逻辑卷，必须首先创建文件系统类型为物理卷（LVM）的分区。一旦已创建了一个或多个物理卷（LVM）分区，即可选择“LVM”按钮来创建 LVM 逻辑卷。

不要把/boot 分区创建为 LVM 分区类型。红旗安全操作系统 4.0 中包括的引导装载程序无法读取 LVM 分区。

➢ 删除分区

如果硬盘上没有剩余的磁盘空间，或是重新设置 Linux 类型分区，那么需要先删除原有的分区，

为安装红旗安全操作系统 4.0 提供足够的空间。

例如，要删除主机中已经存在一个 Windows 分区，可以先在当前分区列表中选中该分区，然后按下“**删除**”按钮。

➢ 添加新分区

在分区列表中选定空闲空间，双击或点击“**新建**”按钮，即出现如下图所示的对话框。

添加分区

“**挂载点**”：输入将创建的分区在整个目录树中的位置，可以从下拉菜单中选择正确的挂载点。如果创建的是根分区，输入“/”；如果是交换分区，不需要输入装入点；如果创建的是根文件系统和交换分区以外的分区，应根据实际情况输入，如/boot、/home 等。

“**文件系统类型**”：在下拉菜单中选择将创建分区的文件系统类型，如果创建的是交换分区，选择“**swap**”；如果创建的是根文件系统或其他分区，可选择“**ext2**”、“**ext3**”、“**vfat**”，默认的类型为“**ext3**”。

红旗安全操作系统 4.0 允许根据分区将使用的文件系统来创建不同的分区类型。下面的是对不同文件系统以及它们的使用方法的简单描述。

分 区 类 型	使 用 方 法 描 述
ext2	支持标准 Unix 文件类型（常规文件、目录、符号链接等）。支持长达 255 个字符的文件名。
ext3	ext2 的升级版本，可方便地从 ext2 迁移至 ext3。主要优点是在 ext2 的基础上加入了记录数据的日志功能，且支持异步的日志。
物理卷（LVM）	创建一个或多个物理卷（LVM）分区用于创建一个或多个 LVM 逻辑卷。

分 区 类 型	使 用 方 法 描 述
软件 RAID	创建两个或多个软件 RAID 分区用来创建一个或多个 RAID 设备。
swap	用于支持虚拟内存的交换空间。
vfat	一个与 Microsoft Windows 的 FAT 文件系统的长文件名兼容的 Linux 文件系统。

“**允许的驱动器**”：包括了系统上安装的硬盘列表。硬盘被选中表示在该硬盘上可以创建想要的分区。如果某个硬盘没有被选中，那么新分区一定不会在该硬盘上被创建。

“**大小（MB）**”：输入分区的大小，以 MB 为单位。

“**其它大小选项**”：“**固定大小**”表示将分区保留为固定大小；选择“**指定空间大小（MB）**”，并在该选项右侧的字段中给出大小限制，这会允许你在硬盘驱动器上保留更多的空间以备将来使用；如果选择“**使用全部可用空间**”，上面输入的分区大小将是该分区的最小值，指定的 Linux 分区将占据整个剩余硬盘空间。如果后面再创建分区时也使用这个选项，系统将根据这两个分区最小值的比例自动分配空间大小。

“**强制为主分区**”：选择将创建的分区是否为硬盘上的四个主分区之一。如果没有选择，新创建的分区将是一个逻辑分区。

如果系统中已经存在有一个其它 Linux 系统的 Swap 分区，那么红旗安全操作系统 4.0 也可以使用它，就不需要再创建一个交换分区了。

单击“**确定**”按钮后屏幕上将显示新创建的分区信息。当所有操作正确完成后，单击“**下一步**”按钮即可。

- **编辑分区**

选择当前分区列表中的一个分区，单击“**编辑**”按钮，将看到一个与“**添加分区**”类似的对话框，在对话框中修改此分区的设置。

如果一个分区已经存在于硬盘上时，那么只能修改这个分区的挂载点和文件系统类型。要想进行其它的修改，如改变大小，就必须先删除此分区，然后再重建。

3.5.4.1 软件 RAID 配置

如果您具有使用软件 RAID 设备的经验，可以在安装过程中进行软件 RAID 的配置。本节将讨论如何在 **Disk Druid** 界面中进行软件 RAID 的配置。

在建立一个 RAID 设备之前，必须首先创建软件 RAID 分区，步骤如下：

在 Disk Druid 分区工具界面中，单击“**新建**”按钮以创建一个新的分区；出现如下图所示的“**添加分区**”对话框。

创建一个新的 RAID 分区

此处不能输入挂载点，只有已经创建了软件 RAID 设备后才能为其设置挂载点。在“**文件系统类型**”选择列表中选择“**software RAID**”。

“**允许的驱动器**”：选择将在其上建立 RAID 的硬盘。如果机器上带有多个硬盘，此处会默认全部选中，如果一定不会在某一硬盘上建立 RAID 阵列，则必须取消对该硬盘的选中。

“**大小（MB）**”：输入分区的大小（以 MB 为单位）。

“**其它大小选项**”：“**固定大小**”表示将分区保留为固定大小；选择“**指定空间大小（MB）**”，并在该选项右侧的字段中给出大小限制，这会允许你在硬盘驱动器上保留更多的空间备将来使用；如果选择“**使用全部可用空间**”，上面输入的分区大小将是该分区的最小值，指定的 Linux 分区将占据整个剩余硬盘空间。如果后面再创建分区时也使用这个选项，系统将根据这两个分区最小值的比例自动分配空间大小。

“**强制为主分区**”：选择将创建的分区是否应为硬盘上的四个主分区之一。如果没有选择，新创建的分区将是一个逻辑分区。

单击“**确定**”按钮返回到 Disk Druid 分区工具的主界面。

重复上述步骤，创建其他需要制作为软件 RAID 设备的分区。

并不是所有的分区都要采用 RAID 冗余机制，只有对数据可靠性和系统性能要求较高的分区才这么做。例如，可以将/home 分区设置为软件 RAID 设备。

已经将所有需要制作成 RAID 设备的分区创建为“**software RAID**”分区后，执行下面的步骤以建立 RAID 设备：

1) 在 Disk Druid 工具的主界面中，单击“**RAID**”按钮，出现如下图所示的“**RAID 选项**”对话框；

RAID 选项

2) 选择“**创建 RAID 设备**”，单击“**确定**”按钮后，将弹出“**创建 RAID 设备**”对话框；

如果选择“创建软件 RAID 分区”，则出现一个用来添加 software RAID 分区的界面，允许用户创建更多的软件 RAID 分区。

建立 RAID 设备

3) 输入或从下拉菜单中选择该设备的挂载点；

4) 在“**文件系统类型**”中选择 RAID 设备将采用的文件系统类型，默认的类型是 ext3；

5) 选择 RAID 设备的名称，例如：md0；

6) “**RAID 级别**”中，可以选择建立 RAID0、RAID1 或 RAID5 三种级别之一；

如果要将 RAID 设备挂载到/boot 上，则必须选择 RAID1 级别；同理，如果不打算创建单独的/boot 分区，而是将整个/分区建立成 RAID 设备，那么也必须选择 RAID1 级别。

7) 用于创建的 RAID 设备的软件 RAID 分区显示在“**RAID 成员**”列表中，从列表中选择将使用哪几个分区来建立 RAID 设备；

8) 如果创建的是 RAID1 或 RAID5 级别类型，可以在“**备件数量**”字段中指定备用分区的数量；

9) 单击“**确定**”按钮，新建的 RAID 设备将显示在如下图所示的 Disk Druid 工具主界面的“**RAID 设备**”列表中。

RAID 磁盘阵列已建立

3.5.4.2 LVM 配置

如果您具有使用 LVM 设备的经验，可在安装过程中进行 LVM 的配置。本节将讨论如何在 **Disk Druid** 界面中进行 LVM 的配置。

创建和配置 LVM 逻辑卷的步骤概括来讲包括以下三步：

- 在硬盘分区上创建用于 **LVM** 的**物理卷**；
- 由一个或多个**物理卷**组成**卷组**；
- 在卷组上创建**逻辑卷**，并为**逻辑卷**设置挂载点。

在创建一个 LVM 逻辑卷之前，首先必须选择和创建用于 LVM 的物理卷。只有这样，它们才可以被 LVM 系统识别。其步骤如下：

创建一个新的分区，只需在 Disk Druid 分区工具界面中，单击“**新建**”按钮，将弹出如下图所示的“**添加分区**”对话框。

创建一个物理卷

此处不能输入挂载点，只有创建了 LVM 卷组后才能为其上的逻辑卷设置挂载点。在“**文件系统类型**”的选择列表中，请单击“**physical volume（LVM）**”。

可以根据需要将一个或多个硬盘分区创建为用于 LVM 的物理卷，已创建的软件 RAID 设备也可以设置为物理卷。

“**允许的驱动器**”：选择将在其上建立 LVM 物理卷的硬盘。如果机器上带有多个硬盘，此处默认会全部选中，如果一定不会在某一硬盘上建立 LVM 物理卷，请取消对该硬盘的选中。

“**大小（MB）**”：输入分区的大小（以 MB 为单位）。

“**其它大小选项**”：“**固定大小**”表示将分区保留为固定大小；选择“**指定空间大小（MB）**”，并在该选项右侧的字段中给出大小限制，这会允许你在硬盘驱动器上保留更多的空间为将来使用；如果选择“**使用全部可用空间**”，上面输入的分区大小将是该分区的最小值，指定的 Linux 分区将占据整个剩余硬盘空间。如果后面再创建分区时也使用这个选项，系统将根据这两个分区最小值的比例自动分配空间大小。

“**强制为主分区**”：选择将创建的分区是否设置为硬盘上的四个主分区之一。如果没有选择，新创建的分区将是一个逻辑分区。

单击“**确定**”按钮后，返回到 Disk Druid 分区工具的主界面。

重复上述步骤，创建其他需要用于 LVM 的物理卷。如果想将多于一个的分区组成一个 LVM 卷组，那么就要分别将它们创建为物理卷。

/boot 分区不能建立在卷组上，如果要将根文件系统建立在一个逻辑卷上，那么必须在非逻辑卷分区上单独为/boot 划分一个分区。

已经建立了所有需要的物理卷后，执行下面的步骤：

可以在一个卷组上创建多个逻辑卷，但是一个物理卷只能属于一个卷组。

1. 在 Disk Druid 工具的主界面中，单击“**LVM**”按钮，用于将一个或多个物理卷组成一个卷组。如下图所示的“**制作 LVM 卷组**”窗口；

创建一个 LVM 卷组

2. 如有需要，可在“**卷组名称**”文本框中改变卷组的名称；

3. LVM 逻辑卷以大小相等的“**块**”为单位分配存储量，4MB 是默认的大小，这样逻辑卷的空间一定是 4MB 的整数倍。可以从“**物理范围**”选择列表中选择其它的值，但缺省的设置对于大多数情况来说相当理想，建议不要更改；

4. 在“**要使用的物理卷**”列表中，选择组成本卷组的物理卷；

5. 现在可以在卷组上创建逻辑卷了。在“**逻辑卷**”区域，按“**添加**”按钮，将出现如下图所示的“**制作逻辑卷**”界面，用于在已建立的卷组上创建新的逻辑卷，并为其设置挂载点、指定文件系统类型、确定名称和分配空间。当然，也可以对逻辑卷进行编辑和删除操作。

创建一个逻辑卷

在创建逻辑组时应考虑在卷组上留有一些空闲空间，以方便今后对逻辑卷进行扩展。

6. 单击“**确定**”按钮，新建的 LVM 卷组和逻辑卷将显示在如下图所示的 Disk Druid 工具主界面的分区列表中。

Logical Volumes 已建立

3.6 配置引导

GRUB（GRand Unified Bootloader）是红旗安全操作系统 4.0 的引导装载程序，它支持红旗安全操作系统 4.0 与多种操作系统共存，可以在多个系统共存时选择引导哪个系统，例如：Linux、Solaris、OS/2、Windows9x/2000/NT 等。

可以将 GRUB 安装在以下两个位置之一：**MBR**（主引导记录）或**引导分区的第一个扇区**（例如，/dev/hda1）。

MBR 是硬盘上的一个特别的区域，会自动被 BIOS 装载，是安装 GRUB 引导记录的默认位置。

如果系统已经在使用其他启动管理器（如 System Commander、Boot Manager 等），才把 GRUB 装到引导分区的第一个扇区中。这时，需要设置从其他的启动管理器来启动 GRUB，然后再启动红旗安全操作系统 4.0。

GRUB 配置界面如下图所示：

引导程序设置

GRUB 配置工具的使用说明如下：

引导程序的安装位置：用来设置安装 GRUB 的位置。如上所述，我们可以选择在主引导记录中安装，也可以选择在引导分区的第一个扇区中安装。

如果有多个 SCSI 硬盘，或者既有 SCSI 硬盘又有 IDE 硬盘，利用“**改变驱动器顺序**”选项，安装程序会根据 BIOS 中驱动器的顺序重新确定主引导记录（MBR）的位置。

标签：当 GRUB 启动后，在菜单中显示的可引导操作系统的标识，或者是在非图形化引导装载程序的引导提示下输入的信息。

默认情况下，红旗安全操作系统 4.0 的引导标签是“RedFlag Security OS 4.0”。

利用“**添加**”按钮可以在引导程序菜单中加入新的可引导分区，如果想修改或删除当前的某个引导标签，选中该项中后单击“**编辑**”或“**删除**”即可。

选中“**默认**”，对应的可引导映像将是计算机启动后默认进入的操作系统，只有选定了默认的引导映像后，才能继续安装。

引导程序密码提供了一种安全机制，用来防止其它可以进入系统的用户改变传递给内核的参数。为安全起见，建议您设置引导程序密码以加强系统的安全性。选择“**使用引导程序密码**”复选框，输入密码并加以确认。

3.7 配置网络

如果安装程序检测到了主机中的网卡类型，就会显示如下图所示的网络配置界面。

配置网络

安装程序能自动检测计算机中的网络设备，并在“**网络设备**”列表中列出。选择一个网络设备项，按下“**编辑**”按钮，将弹出一个如下图所示的该网络接口设备的编辑窗口。

编辑网卡

DHCP 是动态主机配置协议，用来自动配置当前网络的参数。如果当前网络中有 DHCP 服务器的存在，可以选中“**使用 DHCP 进行配置**”，为当前的网络设备提供 IP 地址和子网掩码。如果没有选择“**使用 DHCP 进行配置**”，则需要手工输入 IP 地址和子网掩码参数。

红旗安全操作系统 4.0 支持 IPv4 和 IPv6 两种协议，用户可以选择“**启动 IPv4 支持**”或“**启动 IPv6 支持**”。

IPv6 是 "Internet Protocol Version 6"的缩写，ipv6 是 IETF 协议设计出来的"下一代"互联网协议，它将取代当前使用的 ipv4 。

选择“**引导时激活**”，该网络接口设备会在系统引导时被启动；否则需在系统启动后手工启动。

接下来为机器设置一个主机名，如果不是“**通过 DHCP 自动配置**”，则需要在“**手工配置**”字段中填入主机名。

如果没有在此步骤中设置一个主机名，系统将使用缺省的主机名：localhost。

最后，如果手工设置了 IP 地址和子网掩码，还需要手工输入网关、主要、次要、和第三 DNS 服务器的地址。

网关的作用是配置路由信息，完成主机和 Internet 的连接。三个 DNS 选项用来配置使用的主要、次要和第三域名服务器，系统会按照顺序搜索域名服务器。

如果安装程序不能检测到您的网卡类型，那么网络配置界面就不会出现，用户可在安装完成后再进行网卡配置。

3.8 设置时区

红旗安全操作系统 4.0 提供了对各国时区的支持。对于大多数国内用户来说，保持默认的北京时间即可。

配置时区

3.9 设置 root 密码

root 用户是系统的默认系统管理者用户。root 用户是系统管理者，可以对系统进行管理操作。因此，root 用户口令是决定系统安全性的重要参数之一。

在下图所示的安装界面中，安装程序会提示设置系统的 root 用户密码。

在“**密码**”字段中输入口令，然后于“**确认**”字段再次输入相同的口令以确保口令的正确；否则安装将无法继续。

设定管理员密码

密码必须至少包括 8 个字符，并且区分大小写。系统管理员应劳记自己的密码，并且养成定期更改密码的好习惯。

系统管理员可以在使用系统的过程中，利用 passwd 命令或用户管理工具修改自己的密码。

出于安全考虑，红旗安全操作系统 4.0 默认不允许 root 用户直接登录系统，用户可以以普通用户身份登录后，再执行 su 命令切换至 root。

3.10 软件包安装方式

用户可以在该界面中选择安装哪些免费的中间件软件包。

软件包安装方式

3.11 即将安装

完成必要的配置工作，开始正式安装之前，将进入如下图所示的安装确认界面。

检查安装选项

完整的安装日志将被保存在/root/install.log 文件中。

请确认前面的安装选项设置无误，这里是安装过程中最后一个可以使用“上一步”按钮返回或取消安装的地方；一旦单击“下一步”按钮，将正式开始格式化分区并安装软件包。

3.12 安装软件包

安装程序会读取将要安装的软件包信息，进行必要的准备工作，然后开始软件包的复制过程。安装所需的时间由软件包数量、硬件的速度等多个方面决定，大概需要十几到几十分钟不等。下图是安装过程中的一幅画面。

安装软件包

屏幕左下方显示了安装的总体进度，屏幕右侧是对系统的简单介绍，可以在安装的过程中通过它们来了解红旗安全操作系统 4.0 的系统特征。

3.13 配置显示器

软件包安装完成之后，将进行显示器的配置，默认的分辨率为 800x600 上千颜色，用户也可根据自身需求自行选择。在“**硬件**”标签项中，用户可以配置显示器类型和视频卡类型。

登录类型取决于计算机的用途，开启 X 图形界面登录对于系统来说是一个负担，如果作为一台个人使用的工作站，可以选择图形登录，但作为服务器，处于稳定和性能考虑，建议您还是使用默认的文本登录界面。

配置显示器以及登录方式

3.14 管理员密码及安全模式设置

在红旗安全操作系统中，按照特权分立原则通过角色划分机制将传统 root 用户的权限分立为三个管理员用户，分别是系统管理员、安全管理员和审计管理员。对应的用户名分别是 sysadm、secadm 和 auditadm，分别完成日常的系统管理、安全管理和审计管理工作。

选择安全模式并进行密码配置

在本设置页中，将配置系统安全机制的运行模式并设置三个默认管理用户的初始密码。三个管理用户的密码在安装阶段被默认设置为同一个初始密码。日后管理员的密码更改，可以通过 rolepasswd 命令进行。

三个管理员用户是红旗安全操作系统保留用户，他们口令的变更只能通过 rolepasswd 进行，包括 root 用户在内的其他用户的口令修改，仍通过 passwd 命令进行。

管理员密码的安全对于系统安全至关重要。建议各管理员在首次登陆时立即使用 rolepasswd 命令将密码设置为较高强度的密码。

关于 rolepasswd 命令的使用，请参见《红旗安全操作系统 4.0 安全管理手册》第 4 章。

本页可选的安全机制的运行模式有：

生效(enforcing)模式：在该模式下，所有配置的安全机制严格生效，所有违规操作将被禁止并记录到审计日志中。

警告(Permissive)模式：在该模式下，违规操作可以成功执行，但均被完整记录到审计日志中。一般该模式用于安全策略配置后的初期调试和有效性验证。

关闭(Disabled)模式：该模式下，安全机制处于关闭和不工作状态。违规事件也不被记录入审计日志中。

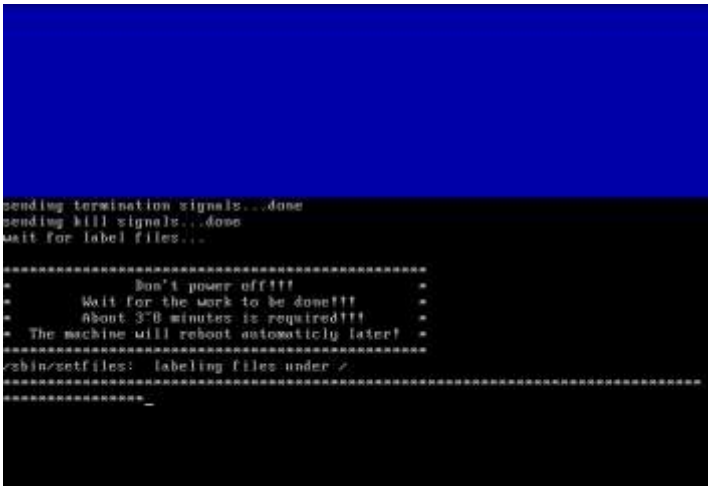
如果安装时选择警告或者关闭模式，则安装完成后所有安全控制功能失效。

3.15 安装结束

以上步骤完成后将显示下图所示的重新引导界面。

重新引导

在你点击重新引导按钮后，系统会弹出安装过程中使用的光盘，退出 X 环境进入控制台模式，进行安装运行环境的清理工作，并为系统的第一次使用生成所有文件的初始安全上下文标记。由于文件较多，生成系统初始安全上下文标记将需要花费一定的时间，依照机器性能一般会需要大约 3~8 分钟，请耐心等待。



重启前为第一次运行生成文件标记

这些工作完成之后，系统会自动重启。建议你在系统重启之前不要手工关机或者热重启，这样会造成文件标记过程不完整，影响第一次使用。

在红旗安全操作系统4.0 中，系统上的每一个文件都会有一个适当的安全上下文，系统正常启动后将依照安全上下文比对机制进行安全访问控制。

如果系统引导后需要重新设置所有安全标记，请以安全管理员身份执行命令：touch /.autorelabel 然后重启系统。重新设置安全标记不会影响系统安全访问控制的一致性。

至此，您已将红旗安全操作系统 4.0 的基本系统成功地安装到计算机中。

3.16 启动、引导和许可证注册

安装完成并重新启动计算机，系统自检结束后，会出现一个 GRUB 默认启动引导选择菜单，引导可选项如下：

RedFlag Security OS 4.0

引导菜单项只有一个，按**<Enter>**键将引导安全核心。

如果不进行任何操作，系统等待一段时间后也会自行引导，以默认的安全核心引导系统。

正常引导完成后，将出现 login 登录界面。此时，输入正确的用户名和登录口令即可正常使用系统。

需要说明的是，出于安全考虑，系统禁止 root 用户的控制台登录，如果要进行系统管理，可以先以系统安装时创建的三个管理员用户登录后再运行 su 命令切换至 root 环境。

登录进入红旗安全操作系统 4.0 基本系统后，建议的第一步操作是运行红旗许可证管理器注册正式许可证。红旗许可证管理器可以通过点击“管理程序”->“系统管理”->“红旗许可证管理器”，或者在字符终端下执行 rflicmgr 命令进行。由于系统安装时生成的测试许可证默认半年后会过期并挂起系统，因此安装系统后请第一时间注册正式许可证。

许可证注册需要启动图形环境。由于启动图形环境需要调用大量的系统服务和应用程序，出于安全性考虑，默认模式下将禁止系统管理员之外的用户运行于图形环境下。管理员用户也可以暂时将安全运行模式切换到警告或者关闭模式以获得图形环境。

关于如何切换安全运行模式，请参阅《红旗安全操作系统 4.0 安全管理手册》第 2.1 节。

第4章 远程管理端的安装和配置

出于安全性的考虑，默认安全生效模式下红旗安全操作系统 4.0 禁止系统管理员外的其他用户运行图形环境。为了便于管理员进行安全和审计管理，红旗安全操作系统 4.0 提供了具备远程集中化管理特性的图形化管理控制台。

本章主要介绍作为安装选件的红旗安全操作系统远程管理控制台的安装，包括安全和审计管理控制台、异常监测报警模块。

4.1 管理端安装

远程管理端的硬件安装要求和 1.5 节描述的红旗安全操作系统 4.0 的安装要求基本相同。在软件环境要求上，需要安装在红旗 Asianux Server 3 系列服务器系统或者红旗桌面 6.0 SP2 系统，或者其他与之兼容的通用 Linux 系统上。

选择一台通用 Linux 服务器，启动到图形界面下，插入安装光盘至光驱中。系统会自动挂载该光盘。打开光盘下的 Client_Tools 目录，可以看到有两个目录：i386 和 x86_64，并有一个自动安装脚本 install.sh。在此路径下面进入 shell(即使用 cd 命令切换到光盘的 Client_Tools 目录下)，运行 sh install.sh，安装脚本会根据当前是 32 位系统还是 64 位系统自动选取合适的安装文件进行安装。

脚本运行后会提示你是否安装审计客户端，输入 y 进行安装，输入 n 跳过；之后提示是否安装 prelude 系列工具，输入 y 进行安装，输入 n 跳过；最后提示是否安装安全管理客户端，输入 y 进行安装，输入 n 跳过。

至此，安全和审计管理控制台安装完毕。关于管理控制台的使用，请参阅《红旗安全操作系统 4.0 安全管理手册》第 5、6 章。

安装光盘的 Client_Tools/i386 和 Client_Tools/x86_64 下都有一个 install.sh 文件，分别是 32 位和 64 位工具的安装脚本。你可以手动选择合适的版本进行安装，这将允许你在 64 位系统上安装 32 位管理工具。如果使用 Client_Tools 目录下的 install.sh，在 64 位系统上默认安装的是 64 位管理工具。

出于特权分立的需要，不建议安全管理控制台和审计管理控制台安装在同一台控制终端上。异常监测及报警模块，可以与审计管理控制台一同安装部署到同一台控制终端上。相关终端的安全性分别由安全管理员和审计管理员掌控。

4.2 异常监测和报警模块的前期配置

异常监测和报警模块需要作额外配置，分别为安全操作系统端（**服务器端**）和报警终端（**客户端**）的相关配置：

- **服务器端配置**

修改 /etc/prelude/default/client.conf，将 server-addr 项改为客户端的 IP 地址。

- **客户端配置**

修改 /etc/prelude-manager/prelude-manager.conf，将 listen 项改为本机 IP，并将 TextMod 和 db 段的注释打开，如下是个示例：

```
[TextMod]
logfile = stderr
logfile = /var/log/prelude.log

[db]
type = mysql
host = localhost
port = 3306
name = prelude
user = prelude
pass = prelude
```

- **服务器端 snort 规则配置**

安全操作系统提供了示例 snort 规则，存放在服务器端的/etc/snort/目录下。完整和详细的 snort 规则，需要用户自己注册下载(http://www.snort.org/snort-rules)。

```
tar zxvf snortrules-snapshot-2.8.tar.gz
cp -rf rules /etc/snort/
```

然后修改服务器端 snort 配置文件/etc/snort/snort.conf，加载 prelude 支持。

```
output alert_prelude:profile=snort
```

- **添加 prelude 管理器代理**

在客户端输入下列命令：

```
prelude-admin add "prelude-manager" --uid 0 --gid 0
```

- **注册 auditd 服务会话**

在**服务器端**中输入命令，注册 auditd 服务会话：

```
prelude-admin register auditd "idmef:w admin:r" CLIENT_IP
```

其中 CLIENT_IP 为**客户端**机器的 IP 地址。

将提示输入注册密码，该密码由下一步操作生成。

在**客户端**中输入命令，将生成注册会话密钥：

```
prelude-admin registration-server prelude-manager
```

在**服务器端**输入该密钥以完成会话注册，从而成功建立客户端与服务器端的安全服务连接。

- **注册 pam 服务会话**

在**服务器端**输入命令，注册 pam 服务会话：

```
prelude-admin register pam "idmef:w admin:r" CLIENT_IP
```

其中 CLIENT_IP 为**客户端**机器的 IP 地址。

将提示输入注册密码，该密码由下一步操作生成。

在**客户端**中输入命令，将生成注册会话密钥：

```
prelude-admin registration-server prelude-manager
```

在**服务器端**输入该密钥以完成会话注册，从而成功建立客户端与服务器端的安全服务连接。

- **注册 snort 服务会话**

在**服务器端**输入命令，获得 snort 用户的 uid 和 gid：

```
id snort
```

在**服务器端**输入命令，注册 snort 用户服务会话：

```
prelude-admin register snort "idmef:w admin:r" CLIENT_IP --uid SNORT_UID --gid SNORT_GID
```

其中 CLIENT_IP 为**客户端**机器的 IP 地址。SNORT_UID 为 snort 用户的 uid，SNORT_GID 为 snort 用户的 gid。

将提示输入注册密码，该密码由下一步操作生成。

在**客户端**中输入命令，将生成注册会话密钥：

```
prelude-admin registration-server prelude-manager
```

在**服务器端**输入该密钥以完成会话注册，从而成功建立客户端与服务器端的安全服务连接。

- **在客户端创建 preludedb 数据库**

连接 mysql 数据库并建库：

$ mysql -u root

Enter password:

mysql> CREATE database prelude;

GRANT ALL PRIVILEGES ON prelude.* TO prelude@'localhost' IDENTIFIED BY 'prelude';

quit;

退出 mysql。

然后，创建 preludedb 数据表：

$ mysql -u prelude prelude -p <

/usr/share/libpreludedb/classic/mysql.sql

Enter password：prelude

- **在客户端创建 prewikka 数据库**

连接 mysql 并建库：

$ mysql -u root

Enter password:

mysql> CREATE database prewikka;

mysql>GRANT ALL PRIVILEGES ON prewikka.* TO prewikka@'localhost' IDENTIFIED BY 'prewikka';

退出 mysql。

然后，创建 prewikka 数据表：

$ mysql -u prewikka prewikka -p < /usr/share/prewikka/database/mysql.sql

Enter password: prewikka

- **注册 prelude-notify 服务会话**

在**客户端**的命令终端中输入如下命令：

```
prelude-admin register prelude-notify "idmef:r"    localhost --uid 0 --gid 0
```

此时 prelude-notify 为 root 运行，所以 uid、gid 为 0。其它用户请用对应的 uid 和 gid。

在**客户端**的其他命令终端中输入：

```
prelude-admin registration-server prelude-manager
```

输入产生的认证密钥，成功建立安全服务连接并完成会话注册。

- **重启 auditd、snortd 服务**

在**服务器端**键入如下命令重启服务：

```
service auditd restart
service snortd restart
```

- **开启异常监测报警**

在**客户端**另外开启三个命令终端，分别运行如下命令（注意必须先执行 prelude-manager）：

```
prelude-manager
prelude-notify
prewikka-httpd
```

至此，异常监测和报警模块的前期配置已经完成并成功开启。

关于异常监测和报警模块的功能，请参考《安全操作系统 4.0 安全管理手册》第 3.5.5 节。

1.建议异常监测报警组件安装在安全操作系统以外的终端上。

2.在终端上运行 prelude-notify 时，首次连接如果本机 ip 地址不是 127.0.0.1 会提示拒绝连接。解决办法是，右键点击右下角托盘下的 prelude-notify 的图标，选择 configure，将 Manager Addresses 改为自己的 ip，例如 192.168.80.5.然后，重启 prelude-nitify。

3.在终端上运行 prewikka-httpd 时，如果提示默认端口 8000 已经被使用，可以加参数 -p 指定端口，例如 prewikka-httpd -p 8080，然后右键点击右下角托盘下的 prelude-notify 的图标，选择 configure，将 Priwikka Url 改为 http://localhost:8080***）。***

4.3 审计日志的远程实时输出配置

红旗安全操作系统 4.0 的审计日志存放于/var/log/audit 目录下，默认情况下，只有审计管理员可以访问该目录，系统管理员和安全管理员只能通过 aureport 命令查询审计记录。

由于安全系统中审计记录的增长很快，可能存在着占满本地磁盘空间导致审计记录溢出情况。另外，也不排除本地硬盘扇区损坏导致审计数据无法恢复的情况发生。为了保证审计数据的可用性，红旗安全操作系统 4.0 提供了远程审计记录异地实时输出功能。这样，即使发生上述异常事件，审计管理员仍可以通过远程异地实时备份查询和分析审计数据。

红旗安全操作系统 4.0 审计系统支持两种异地实时输出接口：MySQL 数据库方式和 Kerberos 文件方式，用户可根据自身需求选择输出接口。

两种审计记录异地输出接口均支持加密传输方式，具体配置步骤，请联系红旗软件。

4.3.1 审计记录 MySQL 数据库输出接口配置

审计记录的远程 MySQL 数据库实时备份的配置步骤如下，所有操作均以 MySQL 数据库服务器的系统管理员用户进行：

1．执行如下命令启动 mysql 数据库服务：

```
service mysqld start
```

2．使用任意文本编辑器创建如下 sql 文件 audit_backup.sql：

```
DROP database IF EXISTS `aubackup`;
CREATE DATABASE aubackup;
USE aubackup;
DROP TABLE IF EXISTS `aulog`;
CREATE TABLE `aulog` (
        `id` bigint(20) NOT NULL auto_increment,
          `host` varchar(100) NOT NULL,
            `timestamp` decimal(13,3) NOT NULL,
              `context` text NOT NULL,
            PRIMARY KEY  (`id`)
    ) ENGINE=MyISAM DEFAULT CHARSET=latin1;
USE aubackup;
GRANT insert ON aulog TO auadm@"%" IDENTIFIED BY "abc123";
```

其中 abc123 是 MySQL 用户 auadm 的初始口令，您可以设置成任意复杂口令。

该 sql 脚本也可以在安装光盘 Client_Tools/i386/install_scripts 目录中找到。

3．执行如下命令导入并执行 audit_backup.sql，创建审计数据库表结构：

mysql -u root -p <audit_backup.sql

如有提示输入密码，则输入 MySQL root 用户密码。

4．修改安全操作系统端配置：

修改/etc/audisp/audisp-backup.conf 文件，添加 MySQL 服务器端 ip 地址，例如 192.168.0.3，则加入如下示例配置：

database = auadm@192.168.0.3:abc123

其中 abc123 是为第 2 步执行的 auadm 用户的密码

修改/etc/audisp/plugins.d/au-backup.conf 将其中的 active = no 改为 active = yes

然后在安全操作系统端执行如下命令重新启动 auditd 服务：

service auditd restart

5．验证审计记录实时备份是否生效：

执行 mysql -u root -p 登录后，执行下列命令：

use aubackup;

select * from aulog;

如果没有错误提示并成功输出审计记录则表示配置成功，输入 quit 退出 mysql 交互界面。

至此，远程 MySQL 数据库审计记录实时备份的配置工作已经完成。

4.3.2 审计记录 Kerberos 文件无加密输出接口配置

系统提供了对审计记录文件的实时分布式的远程备份功能，系统产生的审计日志将会被实时集中地备份到远程审计日志文件下。远程审计信息的记录格式由配置文件/etc/audisp/audispd.conf 中 name_format 字段控制。默认备份到远程的审计信息以远程主机名作为区分。

配置示例如下。需要说明的是，修改配置后必须以审计管理员身份重启 auditd 服务。

1. 服务器端(安全操作系统端)配置

审计配置文件/etc/audit/auditd.conf 示例：

```
# This file controls the configuration of the audit daemon
```

#远程审计日志集中备份到该服务器中/var/log/audit/audit.log中。

log_file = /var/log/audit/audit.log

#审计服务侦听端口

tcp_listen_port = 60

#双方审计传输不进行加密

enable_krb5 = no

krb5_principal = auditd

krb5_key_file = /etc/audit/audit.key

2. 客户端(异地备份端)配置

审计分发程序配置文件/etc/audisp/audispd.conf示例：

name_format = hostname

#name = mydomain

文件/etc/audisp/plugin.d/au-remote.conf 控制客户端审计日志发往远程备份服务器功能是否开启。

This file controls the audispd data path to the

remote event logger. This plugin will send events to

a remote machine (Central Logger).

#是否开启审计日志实时备份插件

active = yes

实时审计日志备份子系统配置文件/etc/audisp/audisp-remote.conf 示例：

This file controls the configuration of the audit remote

logging subsystem, audisp-remote.

#远程备份服务器主机 ip 地址和端口

remote_server = 192.168.80.114

port = 60

#采用加密方式，进行实时备份审计数据

enable_krb5 = no

##krb5_principal =

krb5_client_name = auditd

krb5_key_file = /etc/audisp/audisp-remote.key

4.3.3 审计记录 Kerberos 文件加密输出接口配置

一 配置准备：

服务器端　　192.168.34.66 kdc.example.com

客户端　　192.168.33.114　　kdcsrv.example.com

＝＝

二.服务器端

(1)修改/etc/hosts 配置文件

192.168.34.66　　kdc.example.com

192.168.33.114　　kdcsrv.example.com

(2)执行命令

hostname kdc.example.com

(3)修改配置文件/etc/krb5.conf

kerberos 认证服务器/etc/krb5.conf

[realms]

EXAMPLE.COM = {

kdc = 192.168.34.66:88

admin_server = 192.168.34.66:749

default_domain = example.com

}

(4)配置启动认证服务器

配置客户端与服务器端加密密钥

#!/bin/sh

cd /var/kerberos/krb5kdc/

rm principal.kadm5.lock principal.kadm5 principal.ok principal kadm5.keytab -rf

kdb5_util create -s

kadmin.local -q "addprinc auditd/kdc.example.com@EXAMPLE.COM"

kadmin.local -q "addprinc auditd/kdcsrv.example.com@EXAMPLE.COM"

kadmin.local -q "ktadd -k /var/kerberos/krb5kdc/kadm5.keytab kadmin/admin"

kadmin.local -q "ktadd -k /var/kerberos/krb5kdc/kadm5.keytab kadmin/changepw"

/etc/init.d/kadmin restart

/etc/init.d/krb5kdc restart

导出密钥客户端并测试正确性

#!/bin/sh

kadmin.local -q "ktadd -k /etc/audisp/audisp-remote.key auditd/kdcsrv.example.com"

chmod 400 /etc/audisp/audisp-remote.key

kinit -k auditd/kdcsrv.example.com -t /etc/audisp/audisp-remote.key

kvno auditd/kdcsrv.example.com

klist -k /etc/audisp/audisp-remote.key

scp /etc/audisp/audisp-remote.key 192.168.33.114://etc/audisp/audisp-remote.key

导出服务器端密钥并测试正确性

#!/bin/sh

kadmin.local -q "ktadd -k /etc/audit/audit.key auditd/kdc.example.com"

chmod 400 /etc/audit/audit.key

kinit -k auditd/kdc.example.com -t /etc/audit/audit.key

kvno auditd/kdc.example.com

klist -k /etc/audit/audit.key

拷贝认证文件到客户端覆盖掉原有的配置文件

scp /etc/krb5.conf 192.168.33.114://etc/krb5.conf

(5)修改审计配置文件/etc/audit/auditd.conf

审计配置文件/etc/audit/auditd.conf

tcp_listen_port = 60

enable_krb5 = yes

krb5_principal = auditd

krb5_key_file = /etc/audit/audit.key

==========

三.客户端配置

(1)修改/etc/hosts 配置文件

192.168.34.66 kdc.example.com

192.168.33.114 kdcsrv.example.com

(2)执行命令

hostname kdcsrv.example.com

(3)配置/etc/audisp/audispd.conf

客户端审计日志分发插件配置文件/etc/audisp/audispd.conf

name_format = hostname

#name = mydomain

(4)配置/etc/audisp/audisp-remote.conf

客户端审计日志远程备份/etc/audisp/audisp-remote.conf

remote_server = kdc.example.com

enable_krb5 = yes

#krb5_principal = auditd

krb5_client_name = auditd

krb5_key_file = /etc/audisp/audisp-remote.key

(5)配置/etc/audisp/plugins.d/au-remote.conf

客户端审计日志远程备份/etc/audisp/plugins.d/au-remote.conf

active = yes

==========

四 客户端与服务器端配置完成后。

（1）服务端启动服务

启动认证服务器服务

/etc/init.d/kadmin restart

/etc/init.d/krb5kdc restart

启动审计服务

/etc/init.d/auditd restart

是否正确查看/var/log/message 日志

Jan 12 00:59:15 kdc auditd[5131]: GSS-API Accepted connection from: auditd/kdcsrv.example.com@EXAMPLE.COM

（2）客户端启动审计服务

/etc/init.d/auditd restart

是否正确查看/var/log/message 日志

Jan 12 00:59:14 kdcsrv audisp-remote: kerberos principal: auditd/kdcsrv.example.com@EXAMPLE.COM

Jan 12 00:59:14 kdcsrv audisp-remote: Connected to kdc.example.com

==========

五 在/var/log/message 日志中如果看到上面信息之后，说明配置成功。

（1）查看审计日志中显示下面信息说明日志已经备份成功。

node=kdcsrv.example.com type=AVC msg=audit(1277283848.200:153): avc: denied { unlink } for pid=2348 comm="vim" name=".audit.log.swx" dev=sda10 ino=487855 scontext=root:staff_r:staff_t:s0-s15:c0.c1023 tcontext=root:object_r:auditd_log_t:s0 tclass=file krb5=auditd/kdcsrv.example.com@EXAMPLE.COM

（2）通过 wireshark 软件抓报可以验证是否加密传输。

附　录

附录 A　缺省配置和安全策略

与安全有关的缺省配置如下表所示：

配 置	说 明	缺省配置
强口令要求	对口令认证的强制要求	8 位以上、数字、字符或特殊字符混合、非字典口令
失败登录	重复失败登录次数及行为	连续失败登录次数 10 次后帐号被锁定 8 小时
空闲登出时间	字符终端空闲时间	字符终端空闲 300 秒后自动登出到 login 界面

此外，红旗安全操作系统 4.0 中默认提供如下安全策略：

1. 系统实行三权分立。

   新建系统管理员 sysadm、安全管理员 secadm 和审计管理员 auditadm，分别对应安全用户 sysadm_u、secadm_u 和 auditadm_u。

   系统管理员完成通常的与安全和审计管理无关的传统系统管理功能，如配置和启停系统服务、设置网络、文件系统维护等。安全管理员负责安全环境的设置和安全策略的部署。审计管理员负责审计环境的配置、审计日志的分析和报表生成等。三个管理员相互制约、互相监督。

2. 系统默认内建了三个安全用户：sysadm、secadm 和 auditadm，分别与三个内置安全用户进行映射。管理员无法删除这三个用户，也无法用 passwd 命令修改密码。管理员密码的修改，必须以对应管理员身份登录后使用 rolepasswd 命令进行。

3. 系统正常引导后，相关重要配置文件、设备文件、可执行程序和库被设置安全标记，受系统保护。

   具体的文件列表和对应的安全标记，见配置文件/etc/selinux/mls/contexts/files/file_contexts。

附录 B　常见问题

本附录讨论系统安装过程中可能遇到的一些问题及其解决办法。

➢ 配置一个多引导系统

可利用多重引导让红旗安全操作系统 4.0 与其他操作系统共享计算机。每个操作系统都从它自己的硬盘或分区中引导，但是使用时只可以引导其中之一，不能同时引导多个操作系统。

下面以红旗安全操作系统 4.0 和 MS Window 共存为例，其它操作系统的情况也与之相仿。

如果计算机上没有安装任何操作系统，请先安装 Windows（注意请为安装红旗安全操作系统 4.0 留出足够的空闲空间），然后再安装红旗安全操作系统 4.0。

如果将安装红旗安全操作系统 4.0 的计算机上已经装有 Windows（或某种其它操作系统），则需要根据具体情况按本手册 ***1.5 节***中所述的方法为红旗安全操作系统 4.0 准备足够的空间，然后进行安装。

➢ NFS 网络安装的筹备工作

进行 NFS 网络安装需要网络上有输出红旗安全操作系统 4.0 完整安装树或安装光盘映像文件的 NFS 服务器，下面介绍如何设置支持安装的 NFS 服务器。

首先，需要将红旗安全操作系统 4.0 安装光盘的映像文件或安装树复制到 NFS 服务器上，这一操作的详细说明请参见本手册第 2 章。在此，我们假设***/aa/bb/cc*** 为存放安装树或安装光盘映像文件的目录。

下一步，使***/aa/bb/cc*** 能够被安装程序读取（用 NFS 服务导出该目录），编辑/etc/exports 文件，添加下面一行：

/aa/bb/cc　*(ro)

然后，运行下面的命令启动 NFS 守护进程，使***/aa/bb/cc*** 能够被网络中每台要安装系统的主机只读地挂载：

 # /etc/rc.d/init.d/nfs restart

在使用 NFS 服务器和 NFS 客户端功能之前，需要先启动 portmap 服务。

➢ 如何在安装过程中创建扩展分区

分区工具在安装文件系统类型中没有提供扩展（extended）分区类型，即用户不能根据需要手工创建扩展分区。

安装程序提供了在创建完 3 个主分区后，自动将第四个分区创建为扩展分区的功能，即只能将第四个分区创建为扩展分区。

➢ 如何卸载系统

卸载红旗安全操作系统 4.0 需要两个步骤：

1、 删除硬盘上的所有红旗安全操作系统 4.0 分区，或用其它的操作系统代替。

2、 从计算机的主引导记录（MBR）中删除有关 GRUB 的信息，可以在 DOS 下运行 fdisk /mbr 命令完成，如果是其它操作系统，敬请参考该系统的文档完成同样的工作。

➢ 如果安装程序不支持 USB 键盘或鼠标，该如何处理

建议用户在安装系统时先使用 PS/2 的键盘或鼠标操作，安装完成后再换回 USB 接口的键盘或鼠标并进行相应的配置。

➢ 不能在安装过程中创建引导盘

红旗安全操作系统 4.0 系统的安装程序中取消了创建引导盘的步骤。

如果由于某些原因造成系统不能正常引导，可以使用安装光盘引导，在安装引导提示符 boot:下输入命令：**redflag rescue**，引导进入救援模式。

➢ 安装完毕等待很长时间才能重启引导

红旗安全操作系统 4.0 安装完毕后，会对系统进行首次自动化安全标记，这个过程需要 4-8 分钟时间，因此需要用户耐心等待直到标记过程完成。

需要说明的是，在某些机型尤其是显卡芯片为 Intel GM965 机器上，标记过程可能会出现黑屏，这是因为显卡驱动造成的问题，请用户耐心等待十分钟左右，机器应该能成功自动启动。

➢ 配置审计实时备份的安全连接

1. 生成证书

mkdir -p /usr/local/mysql_ssl/private

mkdir -p /usr/local/mysql_ssl/newcerts

cd /usr/local/mysql_ssl

touch index.txt

echo “01” > serial

cp /etc/pki/tls/openssl.cnf /usr/local/mysql_ssl/

修改/usr/local/mysql_ssl/openssl.cnf，将 dir = ../../Ca 改为 dir = /usr/local/mysql_ssl/

openssl req -new -x509 -keyout private/cakey.pem -out cacert.pem -config openssl.cnf

按照提示输入您的信息，请记住您输入的密码，后面会有操作提示输入密码，输入该密码即可。

＃ openssl req -new -keyout key.pem -out req.pem -days 3600 -config openssl.cnf

按照提示输入您的信息，请记住您输入的密码，后面会有操作提示输入密码，输入该密码即可。出现输入附加信息的提示时，请不要输入，直接回车即可。

＃ openssl rsa -in key.pem -out key.pem

＃ openssl ca -policy policy_anything -out cert.pem -config openssl.cnf -infiles req.pem

完成后，在/usr/local/mysql_ssl 文件中有 cacert.pem 为 CA 证书，key.pem、cert.pem 为密钥与证书

请重复两次上述步骤，生成两份 cacert.pem, key.pem 和 cert.pem，分别用于服务器和客户端。但是两次中凡是要求输入 common name 的字段不可相同。

2. 安全服务器端

mkdir -p /etc/audisp/keys

将 key.pem, cert.pem 和 cacert.pem 拷贝到/etc/audisp/keys/目录下。

修改/etc/my.cnf，加入下列配置

[client]

ssl-ca=/etc/audisp/keys/cacert.pem

ssl-cert=/etc/audisp/keys/cert.pem

ssl-key=/etc/audisp/keys/key.pem

service auditd restart

3. 接收备份端

mkdir /etc/mysql-ssl-keys/

将 key.pem，cert.pem，cacert.pem 拷贝到/etc/mysql-ssl-keys/

修改/etc/my.cnf，添加下列配置

[mysqld]

ssl-ca=/etc/mysql-ssl-keys/cacert.pem

ssl-cert=/etc/mysql-ssl-keys/cert.pem

ssl-key=/etc/mysql-ssl-keys/key.pem

service mysqld restart

- **系统启动时出现大量 avc 提示后无法引导**

系统启动时出现大量 avc 提示，并无法继续引导的话，可能是当前文件系统安全标记与系统安全标记库出现了不一致问题，需要对整个文件系统进行重新安全标记。

重新标记的步骤是：

1. 在 grub 引导项上按 e 键移动方向键至 kernel 行后再按 e 键，在行尾追加核心参数 selinux=0 后回车，然后按 b 键正常引导。
2. 登录后切换到 root 环境并执行 touch /.autorelabel 命令。
3. 执行 reboot 命令重启主机，系统会提示进行文件系统重新标记，标记完毕会成功引导。

Oracle 10g 安装和中文显示问题

在红旗安全操作系统 4.0 上安装 Oracle 10.2.0.1 版本时，请以安全管理员将运行模式设置于 Permissive 模式后以系统管理员身份按如下步骤进行安装和部署：

在安装 Oracle 时，在 oracle 用户的主目录的.bash_profile 文件末尾加入：

unset LANG

unset LANGUAGE

export LANG=C

然后在 shell 下执行 source /home/oracle/.bash_profile

安装 Oracle 完毕后，再修改 oracle 用户的主目录的.bash_profile 文件，删掉上面加入的三行。

然后在 shell 下执行 source /home/oracle/.bash_profile

重启 Oracle 管理工具 dbca 和 netca 即可显示中文。