**AMR管理平台服务器离线备份及还原指导手册**

V1.0.0

# 前言

符号约定

在本文档中可能出现下列标识，代表的含义如下。

| 标识 | 说明 |
| --- | --- |
|  | 表示有高度潜在危险，如果不能避免，会导致人员伤亡或严重伤害。 |
|  | 表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。 |
|  | 表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。 |
|  | 表示静电敏感的设备。 |
|  | 表示高压危险。 |
|  | 表示强激光辐射。 |
|  | 表示危险运动部件，请远离运动风扇叶片。 |
|  | 表示设备部件机械伤人。 |
|  | 表示能帮助您解决某个问题或节省您的时间。 |
|  | 表示是正文的附加信息，是对正文的强调和补充。 |

修订记录

| 版本号 | 修订内容 | 发布日期 |
| --- | --- | --- |
| V1.0.0 | 首次发布 | 2024.06 |
|  |  |  |
|  |  |  |

目录

[前言 I](#_Toc169359631)

[第 1 章 软件安装 1](#_Toc169359632)

[第 2 章 移动硬盘分区 2](#_Toc169359633)

[2.1 移动硬盘分区 2](#_Toc169359634)

[第 3 章 烧制镜像文件 6](#_Toc169359635)

[3.1 刻录镜像文件 6](#_Toc169359636)

[第 4 章 物理服务器的离线备份及还原 8](#_Toc169359637)

[附录1 法律声明 12](#_Toc169359638)

[附录2 网络安全建议 13](#_Toc169359639)

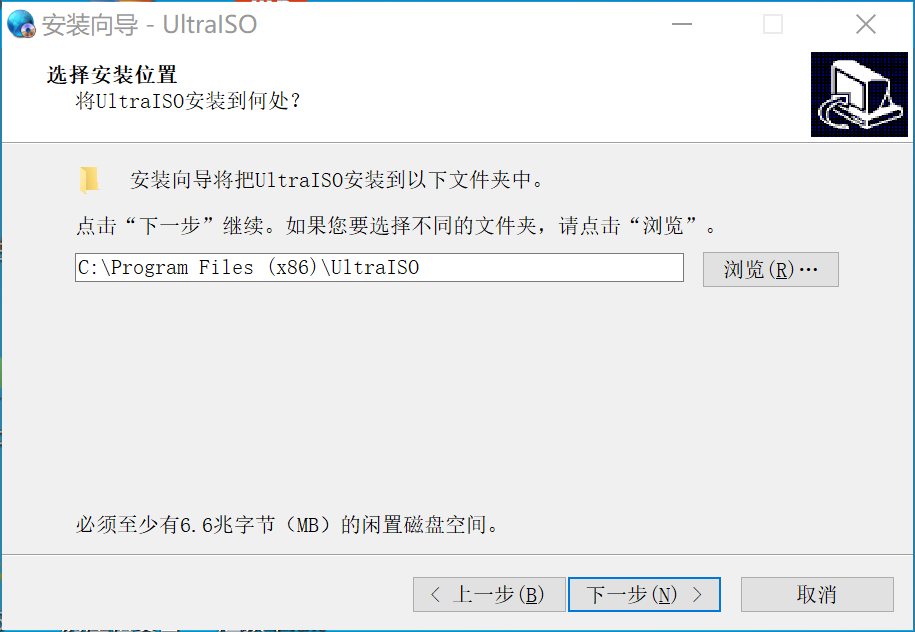
第 1 章 软件安装

用户需要安装UltraISO软件用于烧制镜像文件。

步骤1 打开UltraISO软件安装包，双击安装。

选择合适的安装路径，点击“下一步”。

图1-1 安装路径



步骤2 根据弹窗提示完成软件安装。

第 2 章 移动硬盘分区

使用DiskGenius对准备好的不小于1T的移动硬盘进行分区， 用于实现服务器的离线整机备份及还原。

2.1 移动硬盘分区

步骤1 将空的移动硬盘插入电脑，使用DiskGenius对移动硬盘进行分区。

步骤2 打开DiskGenius后选择移动硬盘，然后鼠标右键移动硬盘空闲处弹出对话框点击建立新分区。

图2-1 建立新分区

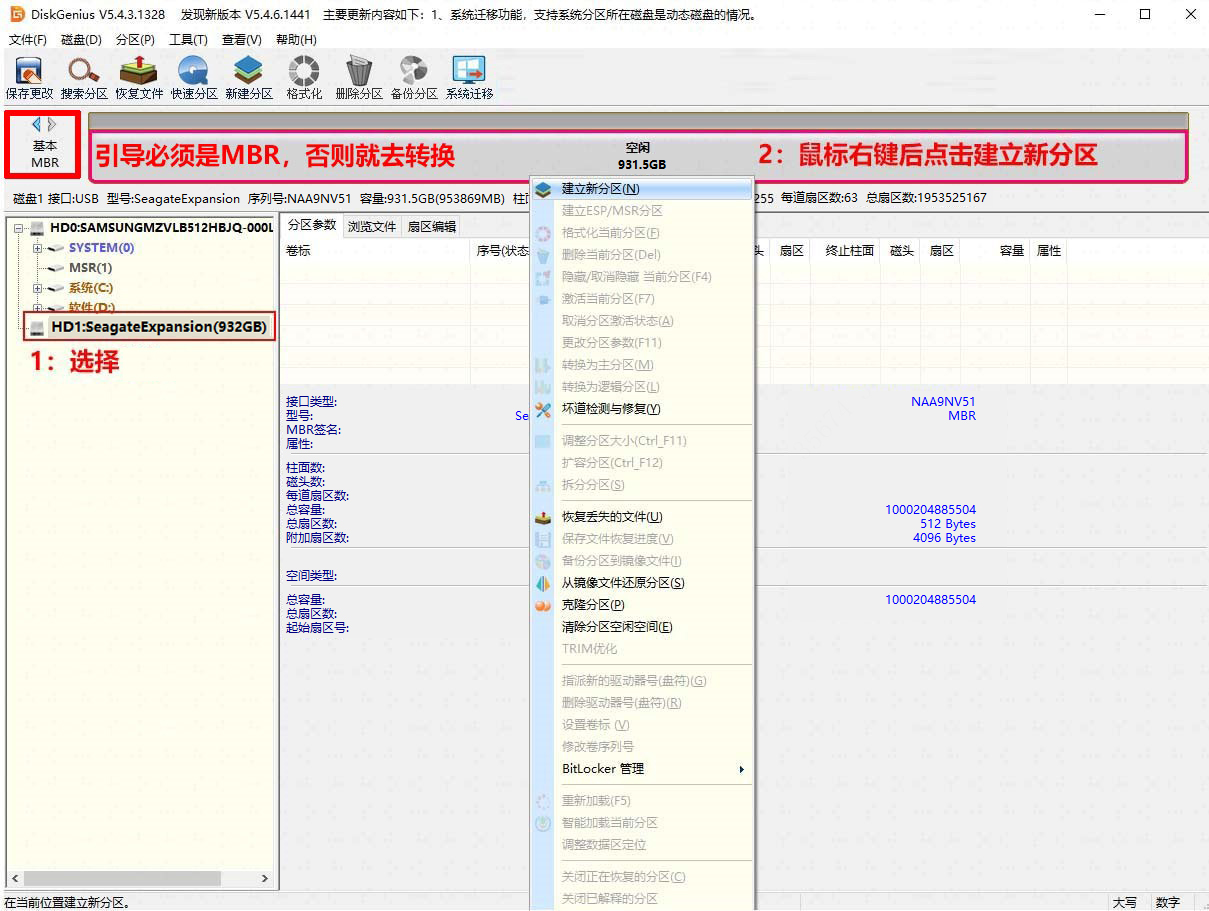
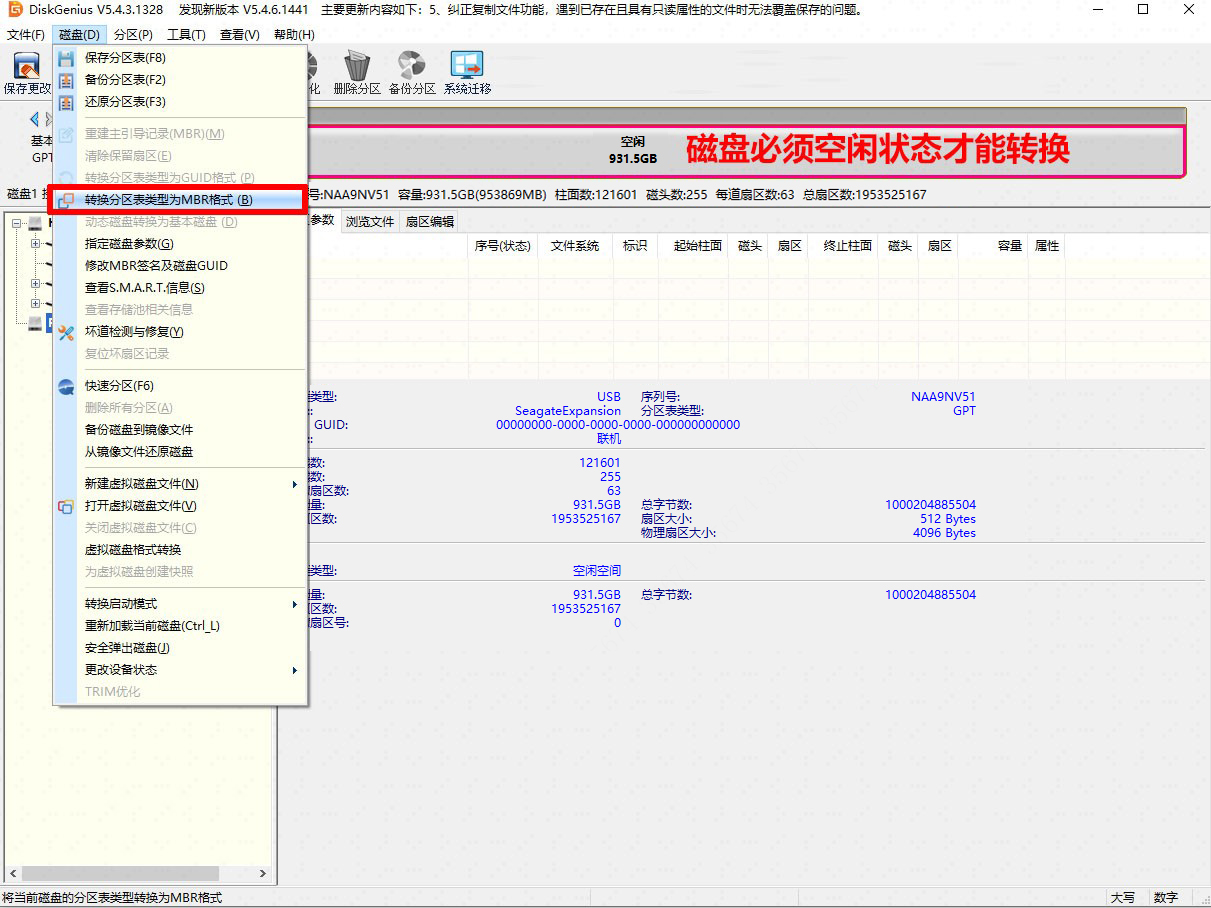


图2-2 引导转换

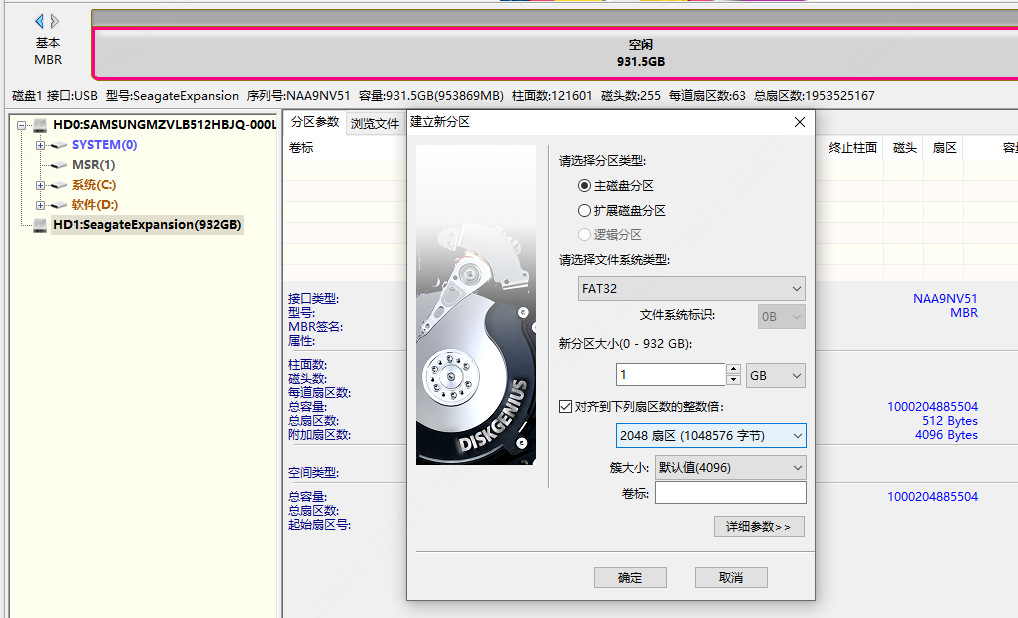




如移动硬盘已有分区则删除后重新建立。

步骤3 依次选择主磁盘分区>文件系统类型FAT32>新分区大小1GB后点击确定。

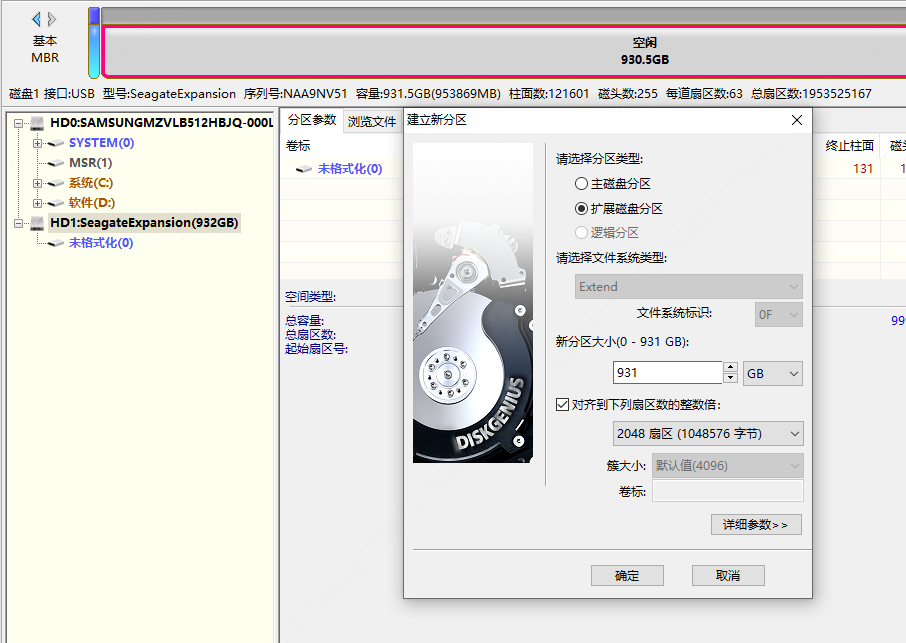
图2-2 新分区大小设置



步骤4 再次鼠标右键移动硬盘空闲处弹出对话框点击建立新分区。

步骤5 依次选择扩展逻辑分区>分区大小填写剩下所有空间>确定。

图2-3 建立扩展逻辑分区



步骤6 再次鼠标右键移动硬盘空闲处弹出对话框点击建立新分区。

步骤7 依次选择文件系统类型NTFS>分区大小填写剩下所有空间>卷标GHOST>确定。

图2-4 建立逻辑分区



步骤8 依次点击保存更改>弹出对话框选“是”>再次弹出对话框选“是”。

图2-5 保存更改



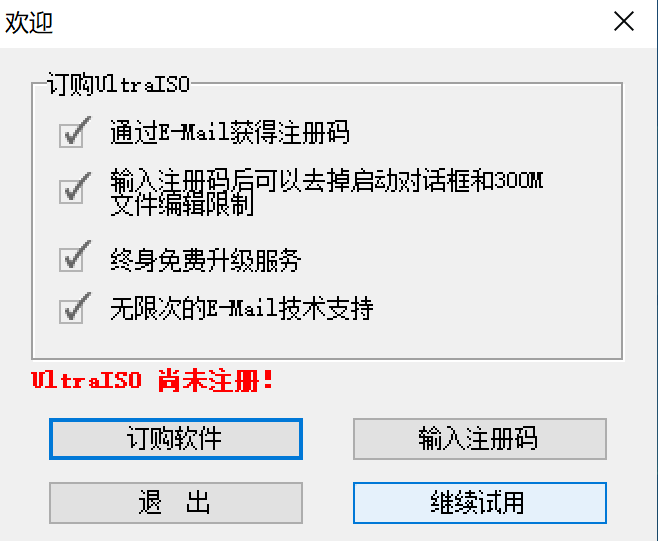
第 3 章 烧制镜像文件

将Clonezilla镜像文件烧制到移动硬盘的主分区，拷贝AGV平台系统文件到GHOST分区，完成服务器镜像文件制作。

3.1 刻录镜像文件

步骤1 双击打开UltraISO软件，在弹窗上点击“继续试用”。

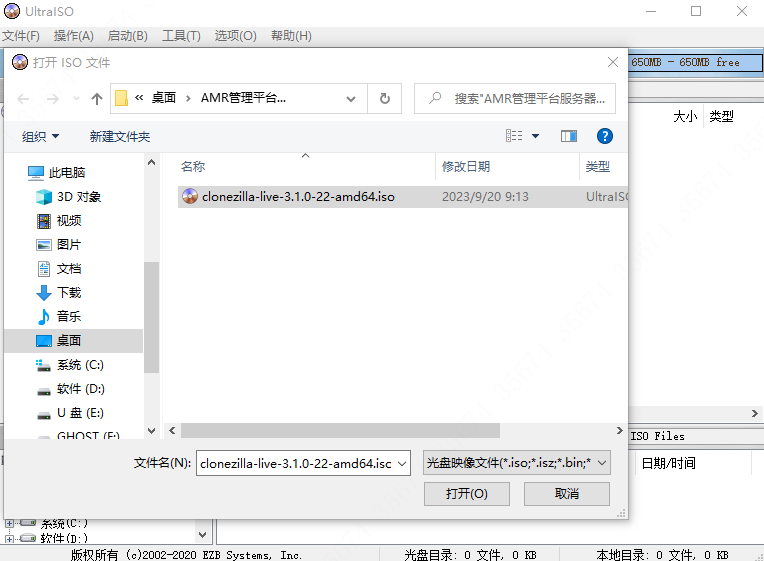
图3-1 ISO试用



步骤2 点击软件界面左上方“文件 > 打开”。

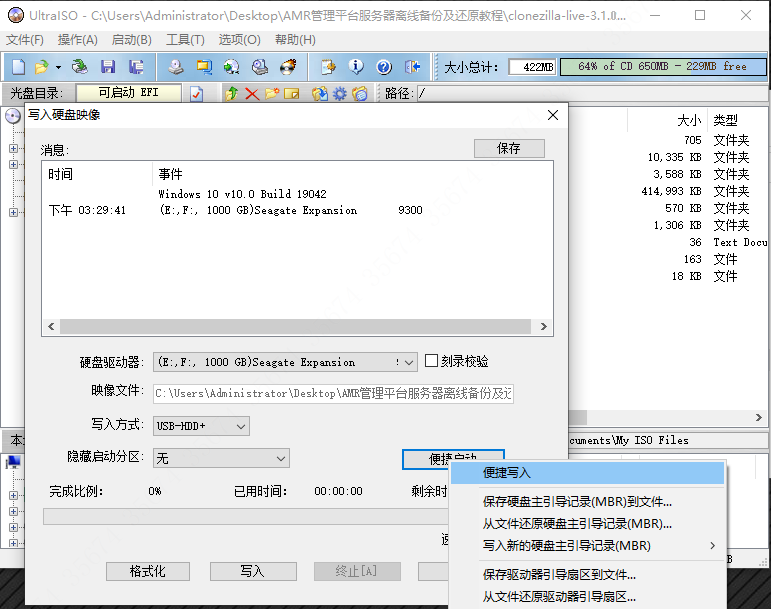
选择clonezilla镜像文件，并点击“打开”。

图3-2 镜像文件选择



步骤3 选择“启动 > 写入硬盘映像... > 便捷启动 > 便携写入”，开始刻录镜像文件到移动硬盘分区。

图3-3 便携写入



第 4 章 物理服务器的离线备份及还原

完成整个AMR管理平台服务器备份，需要准备以下工具：

● 服务器。

● 一个VGA接口的显示器。

● 一个USB接口的键盘。

● 一个不小于1T的制作好镜像的移动硬盘（移动硬盘大小取决于服务器硬盘使用的大小）。

前提条件

● 把显示器连接至服务器的VGA口。

● 把鼠标键盘接入服务器的USB口。

● 把移动硬盘接入服务器的USB口。

###### 第一部分：离线备份

步骤1 进入Boot。

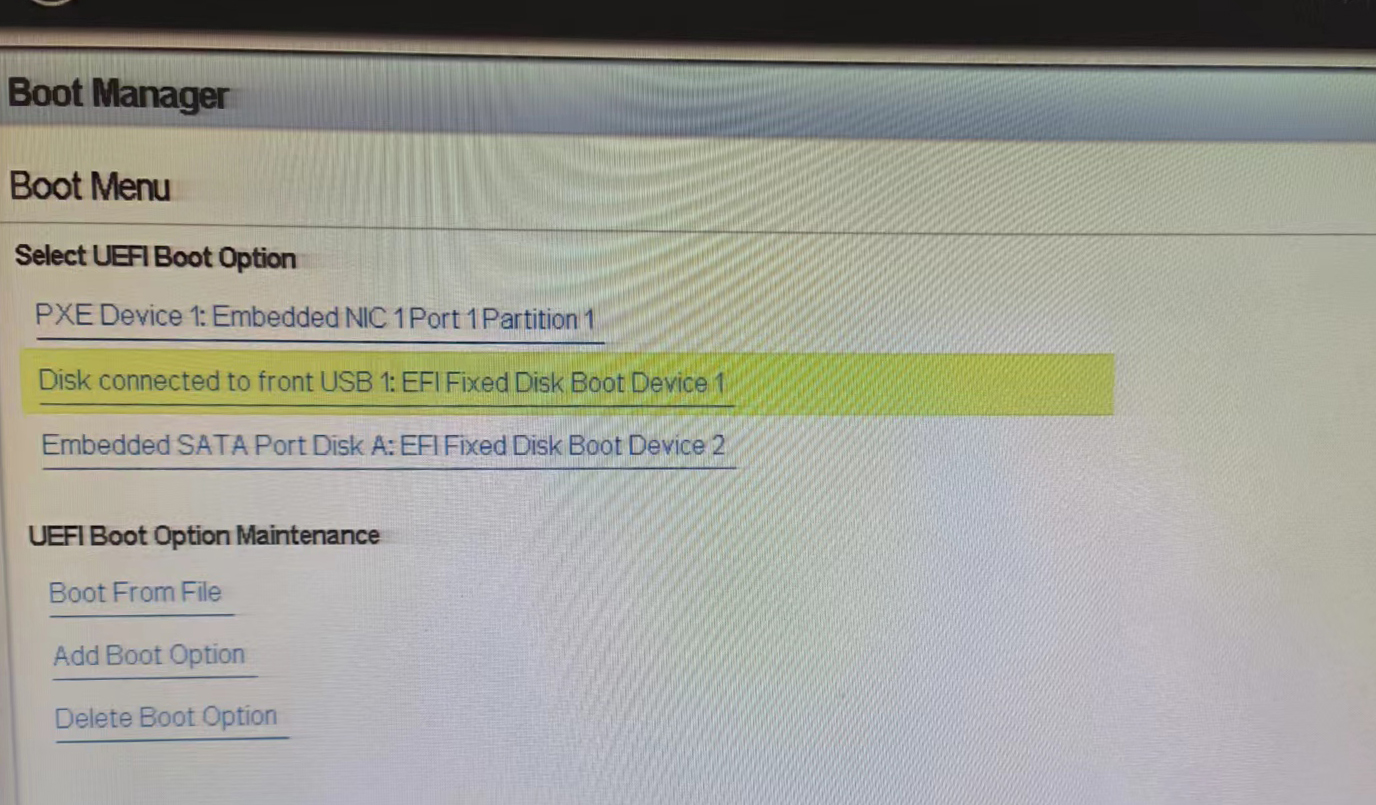
● DELL服务器为列，切换至USB硬盘启动

1. 按电源键开机后，按F11进入“Boot Manager”。

2. 选择“One-shot UEFI Boot Menu”，按回车。

3. 选择“带USB字样的移动硬盘”，按回车。

图2-1 DELL服务器



●

步骤2 Clonezilla界面弹出，选择“Clonezilla live”第一个选项，按回车。

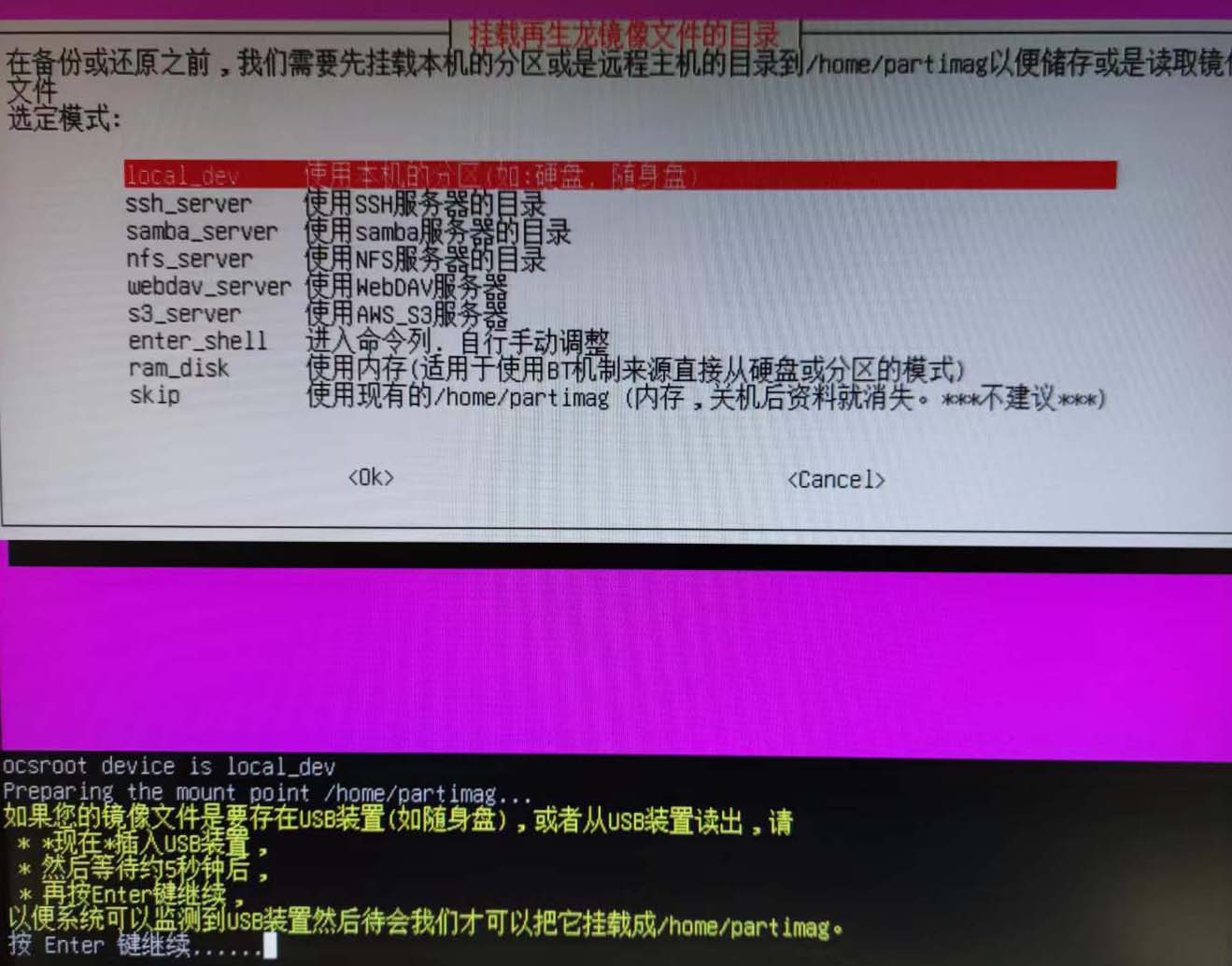
步骤3 界面跳转到语言选择，选择“简体中文”后按回车。

键盘选择“美式键盘”即可。

步骤4 按回车后，在弹出界面选择“使用再生龙”获取已烧制的服务器镜像文件。

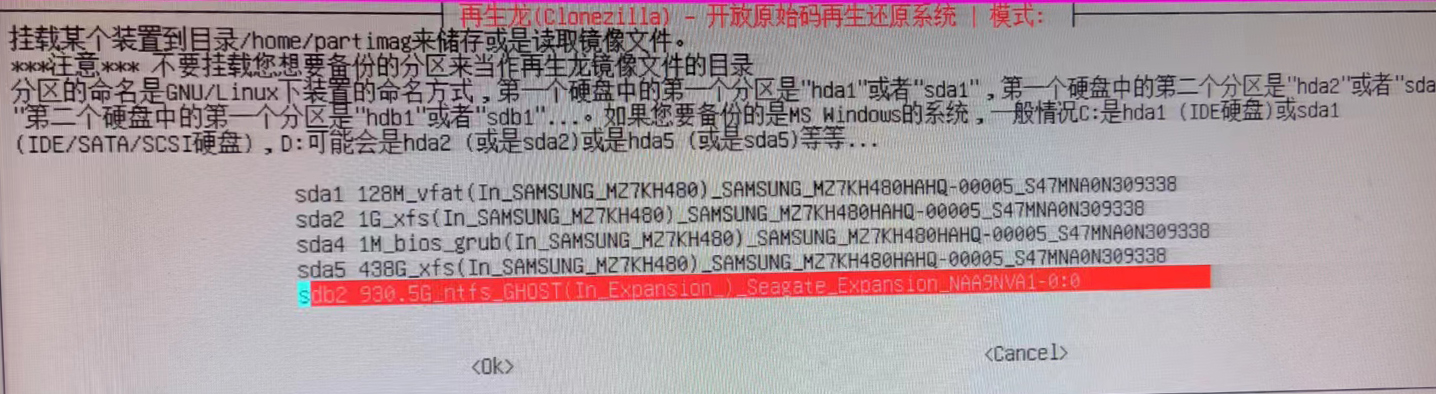
步骤5 选择“硬盘/分区[存到/来自]镜像文件”。按回车确认后，下一步选择“使用本机分区（如：硬盘，随身盘）”，再次按回车开始检测移动硬盘。

图2-3 检测移动硬盘



步骤6 检测到硬盘以后，同时按下键盘Ctrl+C键退出检测窗口。回到再生龙界面，选择存放AMR管理平台系统备份文件的磁盘分区。

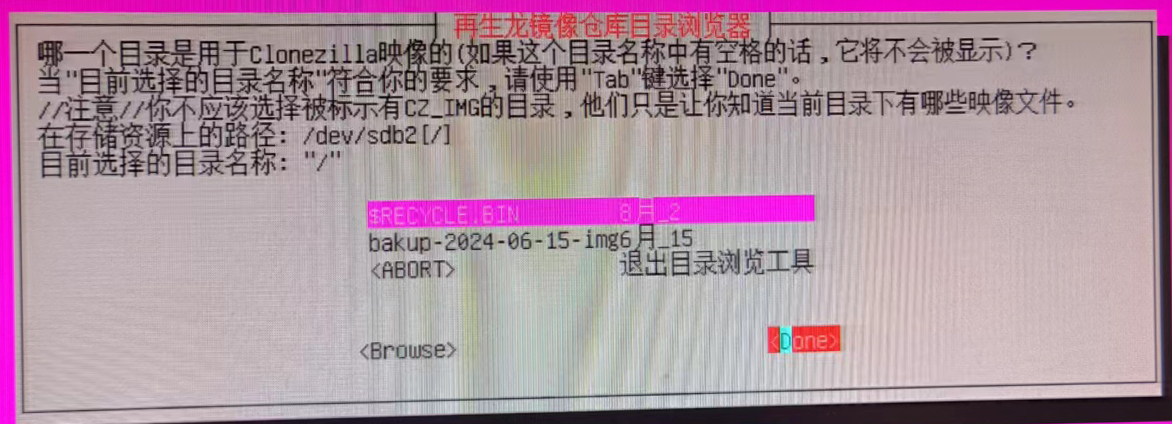
图2-4 系统备份文件存放区（打有GHOST标签）



步骤7 回车确认后选择“no-fsck”，再次按回车到下一步。

步骤8 按Tab键切换光标指向“Done”确认镜像文件的目录，如下图，没问题则按回车确认。

图2-5 切换光标

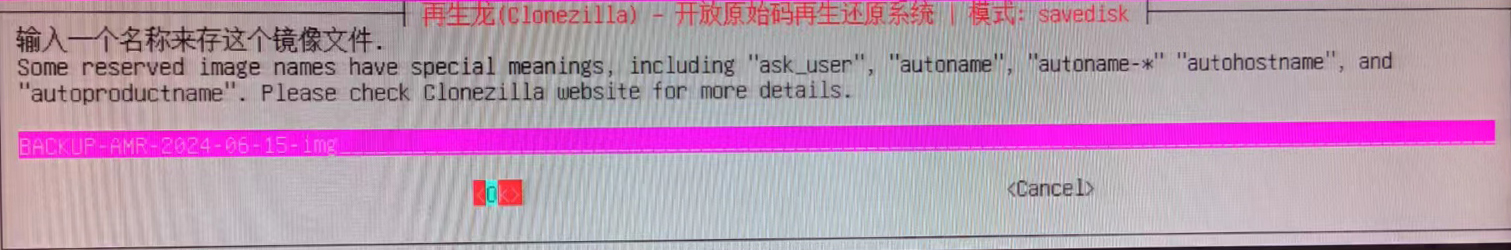


步骤9 继续按回车进入下一步，选择参数向导模式为“专家模式”。

步骤10 回车确认后，在弹出窗口选择“存储本机硬盘为镜像文件”。

步骤11 填写保存的备份镜像名称及时间。

图2-6 保存的备份镜像

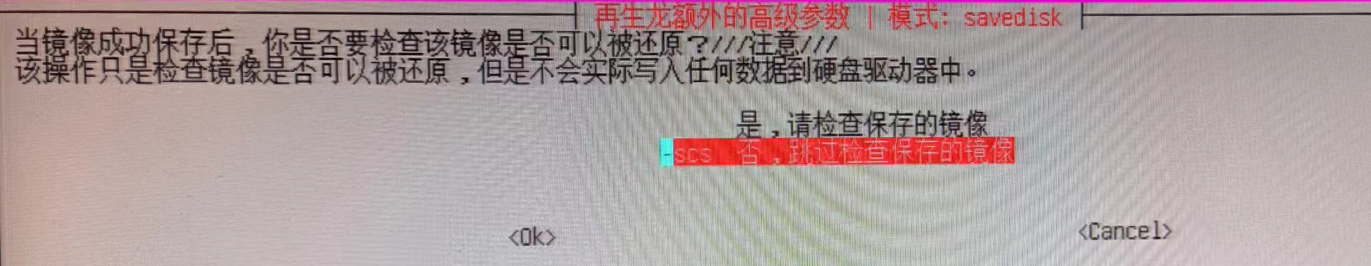


步骤12 填好名称后选择OK按回车继续。

步骤13 选择要备份的硬盘后选择OK按回车继续。

步骤14 连续默认回车至下图，选择否，跳过检查保存的镜像后回车继续。

图2-7 跳过检查保存的镜像



步骤15 默认回车后 > 选择关机 > 继续回车 > 再回车 > 至如下界面选择y后回车开始备份。

图2-8 跳过检查保存的镜像



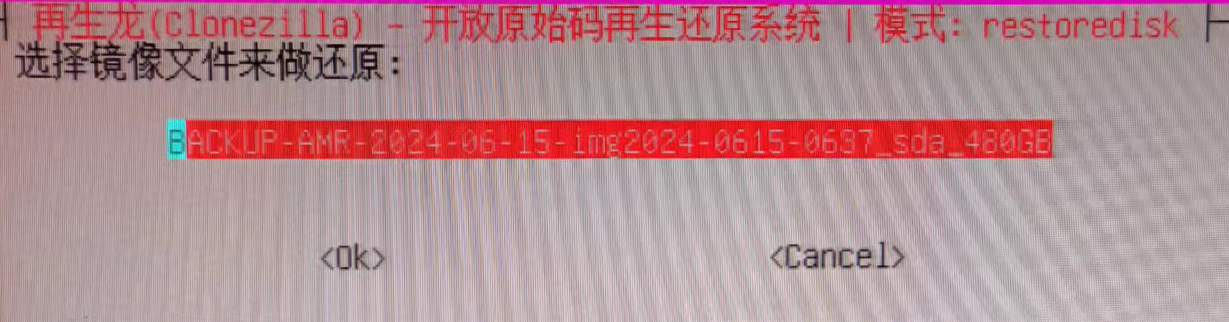
步骤16 备份过程中至进度结束后自动关机即可拔出移动硬盘

###### 第二部分：离线还原

重复离线备份前面1-9步后在弹出窗口选择“还原镜像文件到本机硬盘”。

步骤1 选择自己要还原的备份镜像文件后按回车开始还原镜像。

图2-2-1 选择要还原的镜像文件

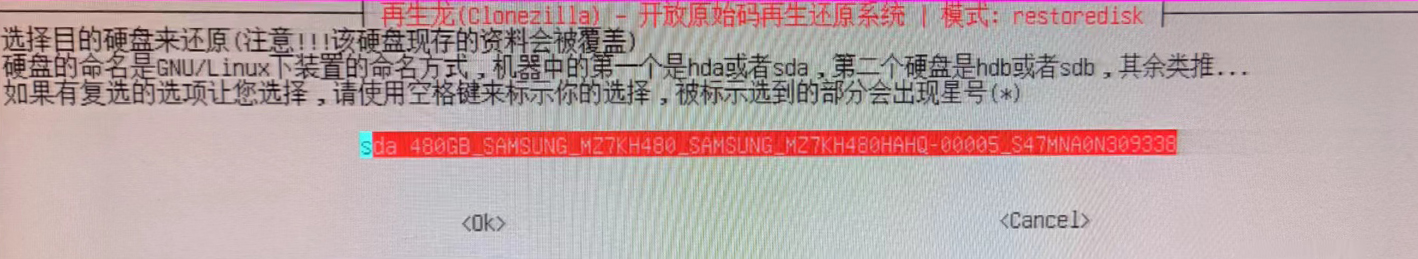


步骤2 选择要还原的硬盘后按回车继续。



还原后服务器系统将回到离线备份的那个点，之后的数据将无法找回，请慎用。

图2-2-2 选择要还原的镜像文件



步骤3 默认回车后，系统显示“设定高级参数”界面。选择“照比例放大产生硬盘分割表”后按回车确认。

步骤4 省略还原前检查，回车确认后，选择在完成所有操作后关机。

步骤5 根据界面提示，输入Y确认后按回车继续还原过程。

确认完成后，系统开始还原服务器镜像。完成后，系统会自动关机。



务必等系统还原完成关机之后，再拔下移动硬盘。

步骤6 （可选）若还原失败，长按服务器电源键至服务器关机，然后开机后重新还原即可。

# 附录1 法律声明

商标声明

● VGA是IBM公司的商标。

● Windows标识和Windows是微软公司的商标或注册商标。

● 在本文档中可能提及的其他商标或公司的名称，由其各自所有者拥有。

责任声明

● 在适用法律允许的范围内，在任何情况下，本公司都不对因本文档中相关内容及描述的产品而产生任何特殊的、附随的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉、文档丢失或预期节约的损失进行赔偿。

● 本文档中描述的产品均“按照现状”提供，除非适用法律要求，本公司对文档中的所有内容不提供任何明示或暗示的保证，包括但不限于适销性、质量满意度、适合特定目的、不侵犯第三方权利等保证。

隐私保护提醒

您安装了我们的产品，您可能会采集人脸、指纹、车牌、邮箱、电话、GPS等个人信息。在使用产品过程中，您需要遵守所在地区或国家的隐私保护法律法规要求，保障他人的合法权益。如，提供清晰、可见的标牌，告知相关权利人视频监控区域的存在，并提供相应的联系方式。

关于本文档

● 本文档供多个型号产品使用，产品外观和功能请以实物为准。

● 如果不按照本文档中的指导进行操作而造成的任何损失由使用方自己承担。

● 本文档会实时根据相关地区的法律法规更新内容，具体请参见产品的纸质、电子光盘、二维码或官网，如果纸质与电子档内容不一致，请以电子档为准。

● 本公司保留随时修改本文档中任何信息的权利，修改的内容将会在本文档的新版本中加入，恕不另行通知。

● 本文档可能包含技术上不准确的地方、或与产品功能及操作不相符的地方、或印刷错误，以公司最终解释为准。

● 如果获取到的PDF文档无法打开，请使用最新版本或最主流的阅读工具。

# 附录2 网络安全建议

**保障设备基本网络安全的必须措施：**

1. **使用复杂密码**

请参考如下建议进行密码设置：

● 长度不小于8个字符。

● 至少包含两种字符类型，字符类型包括大小写字母、数字和符号。

● 不包含账户名称或账户名称的倒序。

● 不要使用连续字符，如123、abc等。

● 不要使用重叠字符，如111、aaa等。

2. **及时更新固件和客户端软件**

● 按科技行业的标准作业规范，设备的固件需要及时更新至最新版本，以保证设备具有最新的功能和安全性。设备接入公网情况下，建议开启在线升级自动检测功能，便于及时获知厂商发布的固件更新信息。

● 建议您下载和使用最新版本客户端软件。

**增强设备网络安全的建议措施：**

1. **物理防护**

建议您对设备（尤其是存储类设备）进行物理防护，比如将设备放置在专用机房、机柜，并做好门禁权限和钥匙管理，防止未经授权的人员进行破坏硬件、外接设备（例如U盘、串口）等物理接触行为。

2. **定期修改密码**

建议您定期修改密码，以降低被猜测或破解的风险。

3. **及时设置、更新密码重置信息**

设备支持密码重置功能，为了降低该功能被攻击者利用的风险，请您及时设置密码重置相关信息，包含预留手机号/邮箱、密保问题，如有信息变更，请及时修改。设置密保问题时，建议不要使用容易猜测的答案。

4. **开启账户锁定**

出厂默认开启账户锁定功能，建议您保持开启状态，以保护账户安全。在攻击者多次密码尝试失败后，其对应账户及源IP将会被锁定。

5. **更改HTTP及其他服务默认端口**

建议您将HTTP及其他服务默认端口更改为1024～65535间的任意端口，以减小被攻击者猜测服务端口的风险。

6. **使能HTTPS**

建议您开启HTTPS，通过安全的通道访问Web服务。

7. **MAC地址绑定**

建议您在设备端将其网关设备的IP与MAC地址进行绑定，以降低ARP欺骗风险。

8. **合理分配账户及权限**

根据业务和管理需要，合理新增用户，并合理为其分配最小权限集合。

9. **关闭非必需服务，使用安全的模式**

● 如果没有需要，建议您关闭SNMP、SMTP、UPnP等功能，以降低设备面临的风险。

● 如果有需要，强烈建议您使用安全的模式，包括但不限于：

◇ SNMP：选择SNMP v3，并设置复杂的加密密码和鉴权密码。

◇ SMTP：选择TLS方式接入邮箱服务器。

◇ FTP：选择SFTP，并设置复杂密码。

◇ AP热点：选择WPA2-PSK加密模式，并设置复杂密码。

10. **音视频加密传输**

如果您的音视频数据包含重要或敏感内容，建议启用加密传输功能，以降低音视频数据传输过程中被窃取的风险。

11. **安全审计**

● 查看在线用户：建议您不定期查看在线用户，识别是否有非法用户登录。

● 查看设备日志：通过查看日志，可以获知尝试登录设备的IP信息，以及已登录用户的关键操作信息。

12. **网络日志**

由于设备存储容量限制，日志存储能力有限，如果您需要长期保存日志，建议您启用网络日志功能，确保关键日志同步至网络日志服务器，便于问题回溯。

13. **安全网络环境的搭建**

为了更好地保障设备的安全性，降低网络安全风险，建议您：

● 关闭路由器端口映射功能，避免外部网络直接访问路由器内网设备的服务。

● 根据实际网络需要，对网络进行划区隔离：若两个子网间没有通信需求，建议使用VLAN、网闸等方式对其进行网络分割，达到网络隔离效果。

● 建立802.1x接入认证体系，以降低非法终端接入专网的风险。

● 开启设备IP/MAC地址过滤功能，限制允许访问设备的主机范围。