

Acronis

acronis.com

Acronis Cyber Protect

Home Office



目录

1 简介	10
1.1 什么是 Acronis Cyber Protect Home Office?	10
1.2 在 Acronis True Image(2020 或 2021) 和 Acronis Cyber Protect Home Office 中创建的备份	10
1.2.1 备份文件命名	10
1.2.2 备份方案	11
1.2.3 清理 TIBX 格式备份	11
1.2.4 可以使用以下方案手动清理本地备份:	11
1.2.5 保留 TIB 格式的备份	11
1.3 系统要求与支持的媒体	12
1.3.1 最低系统要求	12
1.3.2 支持的操作系统	12
1.3.3 支持的文件系统	13
1.3.4 支持的 Internet 连接类型	13
1.3.5 支持的存储媒体	14
1.4 安装和删除 Acronis Cyber Protect Home Office	14
1.5 正在激活 Acronis Cyber Protect Home Office	15
1.5.1 正在激活 Acronis Cyber Protect Home Office	15
1.5.2 激活次数太多问题	16
1.5.3 手动管理您的订购许可	17
1.6 试用版信息	17
1.6.1 一般限制	17
1.6.2 同步	17
1.6.3 Acronis Cloud	17
1.6.4 购买完整版	17
1.7 升级 Acronis Cyber Protect Home Office	18
1.7.1 内置商店	18
1.8 技术支持	19
1.8.1 维护和支持计划	19
2 入门	20
2.1 用户界面语言	20
2.2 保护系统	20
2.2.1 备份计算机	20
2.2.2 创建 Acronis 可启动媒体	22
2.3 备份 PC 上的所有数据	22
2.4 创建 Acronis Survival Kit	24

2.5 备份您的文件	25
2.6 克隆硬盘驱动器	26
2.6.1 为何需要?	26
2.6.2 启动之前,	27
2.6.3 克隆磁盘	27
2.7 恢复计算机	28
2.8 Acronis 帐户	30
2.9 Acronis Cloud 快速入门	31
2.9.1 远程存储器	31
2.9.2 Web 应用程序	31
2.9.3 如何确保数据的安全性	32
2.9.4 订购许可信息	32
3 基本概念	33
3.1 文件备份与磁盘/分区映像之间的差别	34
3.1.1 磁盘/分区备份包含哪些内容?	34
3.1.2 磁盘备份中去除了哪些内容?	34
3.2 完整、增量和差异备份	35
3.2.1 完整方式	35
3.2.2 增量方式	36
3.2.3 差异方式	37
3.2.4 块修改跟踪器 (CBT)	38
3.3 决定存储备份的位置	38
3.3.1 为备份准备一个新磁盘	39
3.3.2 FTP 连接	40
3.3.3 验证设置	41
3.4 Acronis 不间断备份	41
3.4.1 不间断备份限制	41
3.4.2 工作方式	41
3.4.3 保留规则	42
3.4.4 Acronis 不间断备份数据存储	42
3.4.5 不间断备份 - 常见问题	43
3.5 备份文件命名	44
3.5.1 在 Acronis True Image(2020 或 2021) 和 Acronis Cyber Protect Home Office 中创建的备份文件的命名约定	44
3.5.2 Acronis True Image 2020 版本之前创建的备份文件的命名约定	44
3.6 与 Windows 集成	45
3.6.1 Windows“开始”菜单	45

3.6.2	任务栏上的 Acronis Cyber Protect Home Office 按钮	45
3.6.3	任务栏通知中心	45
3.6.4	快捷菜单命令	46
3.6.5	文件资源管理器中的文件级恢复	46
3.7	向导	46
3.8	备份、恢复和克隆的常见问题	47
4	备份数据	49
4.1	备份磁盘和分区	49
4.2	备份文件与文件夹	50
4.3	备份移动设备	51
4.3.1	Acronis Mobile	53
4.3.2	移动备份的本地目标位置	53
4.4	备份 Office 365 数据	53
4.4.1	为何备份 Office 365 数据?	53
4.4.2	备份 Office 365 数据	54
4.5	备份选项	54
4.5.1	计划	55
4.5.2	备份方案	58
4.5.3	备份操作的通知	63
4.5.4	从备份中排除项目	64
4.5.5	映像创建模式	66
4.5.6	备份保护	66
4.5.7	线上备份保护	67
4.5.8	备份前/后命令	67
4.5.9	备份分割	68
4.5.10	备份验证选项	69
4.5.11	备份保留副本	69
4.5.12	可移动媒体设置	70
4.5.13	错误处理	71
4.5.14	备份的文件级安全设置	72
4.5.15	计算机关机	72
4.5.16	备份操作的性能	73
4.5.17	选择用于备份的数据中心	74
4.5.18	笔记本电脑电源设置	75
4.5.19	使用 Wi-Fi 网络备份到 Acronis Cloud	75
4.6	使用备份执行的操作	76
4.6.1	备份操作菜单	76

4.6.2	备份活动和统计数据	77
4.6.3	在列表中对备份排序	79
4.6.4	将备份复制到 Acronis Cloud	79
4.6.5	验证备份	80
4.6.6	备份到不同位置	80
4.6.7	将现有备份添加至列表	81
4.6.8	公证备份	81
4.6.9	清理备份、备份版本和副本	85
4.6.10	清理 Acronis Cloud 上的空间	87
4.6.11	从 Acronis Cloud 中删除数据	87
5	恢复数据	90
5.1	恢复磁盘和分区	90
5.1.1	在崩溃后恢复系统	90
5.1.2	恢复分区和磁盘	101
5.1.3	关于恢复动态/GPT 磁盘和卷	113
5.1.4	在 BIOS 或 UEFI BIOS 中设置启动顺序	116
5.1.5	从云恢复磁盘	117
5.2	恢复文件和文件夹	121
5.3	搜索备份内容	123
5.4	恢复 Office 365 数据	123
5.4.1	可以恢复哪些项目?	124
5.4.2	恢复 Office 365 数据	124
5.5	恢复操作选择	124
5.5.1	磁盘恢复模式	125
5.5.2	恢复前/后命令	125
5.5.3	验证选项	125
5.5.4	计算机重新启动	126
5.5.5	文件恢复选项	126
5.5.6	覆盖文件选项	126
5.5.7	恢复操作的性能	127
5.5.8	恢复操作的通知	127
6	存档数据	129
6.1	什么是数据存档?	129
6.2	从存档中排除哪些数据?	129
6.3	云存档与在线备份	130
6.4	存档数据	130
6.4.1	数据存档选项	131

6.5 访问您的存档文件	132
7 共享数据	133
8 保护家庭数据	134
8.1 什么是家庭数据保护?	134
8.2 向在线控制面板添加新设备	134
8.3 远程备份数据	135
8.4 使用在线控制面板恢复数据	136
8.5 电子邮件通知	136
9 保护	138
9.1 “保护”仪表板	138
9.2 Active Protection	138
9.2.1 防勒索软件保护	139
9.2.2 实时保护	139
9.2.3 Web 过滤	140
9.2.4 配置 Active Protection	140
9.3 防病毒扫描	142
9.3.1 配置防病毒扫描	142
9.4 漏洞评估	143
9.5 管理检测到的问题	144
9.6 在隔离区中管理文件	144
9.7 配置保护排除项	145
9.8 针对 Zoom、Cisco Webex 和 Microsoft Teams 的保护	145
9.9 下载保护更新	146
10 同步数据	147
10.1 关于同步功能	147
10.2 可以和不可以同步的内容	147
10.2.1 存储类型	147
10.2.2 数据类型	147
10.3 同步图标	148
10.3.1 通知区域	148
10.3.2 文件资源管理器	148
10.4 创建同步	149
10.5 同步文件的版本	149
10.5.1 恢复到先前的文件版本	150
10.6 如何恢复删除的文件	150
10.7 删除同步	150
11 磁盘克隆和迁移	152

11.1 磁盘克隆实用工具	152
11.1.1 克隆磁盘向导	152
11.1.2 手动分区	154
11.1.3 从克隆中排除项目	155
11.1.4 迁移方法	156
11.2 将系统从 HDD 迁移至 SSD	162
11.2.1 SSD 大小	162
11.2.2 选择哪种迁移方法	163
11.2.3 Acronis Cyber Protect Home Office 无法识别 SSD 时的操作	163
11.2.4 使用备份与恢复方法迁移至 SSD	164
12 工具	166
12.1 Acronis 媒体生成器	166
12.1.1 创建 Acronis 可启动媒体	167
12.1.2 Acronis 可启动媒体启动参数	168
12.1.3 向现有 .wim 映像添加驱动程序	170
12.1.4 从 .wim 文件创建 .iso 文件	171
12.2 确保可启动媒体随时可用	172
12.2.1 要测试可启动媒体, 请执行以下操作:	172
12.2.2 如何进行恢复测试, 以及检查驱动器和网络适配器	173
12.2.3 在从可启动媒体启动时选择视频模式	175
12.3 Acronis 启动恢复管理器	177
12.3.1 其他信息	178
12.4 Try&Decide	179
12.4.1 在哪些情况下 Try&Decide 可以提供帮助	179
12.4.2 在计算机重新启动后, Try&Decide 如何工作	179
12.4.3 使用 Try&Decide 的限制	180
12.4.4 使用 Try&Decide	180
12.4.5 Try&Decide 选项和通知	182
12.4.6 Try&Decide: 典型使用案例	182
12.5 Acronis Secure Zone	184
12.5.1 Acronis Secure Zone 清理	184
12.5.2 创建和管理 Acronis Secure Zone	184
12.5.3 Acronis Secure Zone 位置	185
12.5.4 Acronis Secure Zone 的大小	186
12.5.5 Acronis Secure Zone 保护	186
12.5.6 正在删除 Acronis Secure Zone	187
12.6 添加新硬盘	188

12.6.1 选择硬盘	188
12.6.2 选择初始化方法	189
12.6.3 创建新分区	190
12.7 安全与隐私权工具	192
12.7.1 Acronis DriveCleanser	192
12.7.2 系统清理	197
12.7.3 硬盘抹除方式	204
12.8 加载映像	205
12.8.1 如何加载映像	206
12.9 卸载映像	206
12.10 使用 .vhd(x) 文件	207
12.10.1 .vhd(x) 文件的使用方法	207
12.10.2 限制和其他信息	207
12.10.3 转换 Acronis 备份	207
12.11 备份设置的导入及导出	208
12.12 Acronis 异机还原	209
12.12.1 它可以解决什么问题?	209
12.12.2 我如何使用?	209
12.12.3 创建 Acronis 异机启动媒体	209
12.12.4 使用 Acronis 异机还原	212
13 疑难解答	213
13.1 解决最常见的问题	213
13.2 Acronis 系统报告	213
13.3 Acronis 智能错误报告	214
13.3.1 如果您连接了互联网	214
13.3.2 如果您没有连接互联网	215
13.4 向 Acronis 发送反馈	215
13.5 如何收集崩溃转储	217
13.6 Acronis 客户体验计划	217
词汇表	218
索引	222

版权声明

© Acronis International GmbH, 2003-2021.保留所有权利。

引用的所有商标和版权均为其各自所有者的财产。

未经版权所有人的明确许可,禁止对本文档进行实质性修改并予以发布。

事先未征得版权所有人的许可,禁止出于商业目的,以任何标准(纸张)书籍形式,发布本作品及其衍生作品。

文档按“原样”提供,对于任何明示或暗示的条件、陈述和保证,包括任何对适销性、对特殊用途的适用性或不侵权的暗示保证,我方概不负责,除非上述免责声明被依法判定为无效。

第三方代码可由软件 and/或服务提供。此类第三方的许可证条款将在位于安装根目录中的 `license.txt` 文件中详细说明。您可以随时通过访问以下网址找到最新的第三方代码列表以及与软件和/或服务使用相关的许可证条款:<https://kb.acronis.com/content/7696>

Acronis 专利技术

本产品中使用的技术获得以下专利并受一个或多个美国专利号保护:7,047,380、7,246,211、7,275,139、7,281,104、7,318,135、7,353,355、7,366,859、7,383,327、7,475,282、7,603,533、7,636,824、7,650,473、7,721,138、7,779,221、7,831,789、7,836,053、7,886,120、7,895,403、7,934,064、7,937,612、7,941,510、7,949,635、7,953,948、7,979,690、8,005,797、8,051,044、8,069,320、8,073,815、8,074,035、8,074,276、8,145,607、8,180,984、8,225,133、8,261,035、8,296,264、8,312,259、8,347,137、8,484,427、8,645,748、8,732,121、8,850,060、8,856,927、8,996,830、9,213,697、9,400,886、9,424,678、9,436,558、9,471,441、9,501,234 及待定的专利申请。

1 简介

1.1 什么是 Acronis Cyber Protect Home Office?

Acronis Cyber Protect Home Office 是一款可确保您的所有信息安全无虞的全面网络保护解决方案。它可以备份文档、照片、电子邮件、所选分区,甚至整个硬盘驱动器,包括操作系统、应用程序、设置和您的所有数据。其主要优势之一在于数据保护和安全性功能。

通过这些备份,您可以在发生灾难时(例如,丢失数据、误删重要文件和文件夹或硬盘完全崩溃)恢复自己的计算机系统。

线上备份允许您在 Acronis Cloud 上存储文件和磁盘。即使您的计算机丢失、被盗或损坏,您的数据也会受到保护,而且您可以将数据完整恢复在新设备上(如果需要)。

主要功能:

- 到本地存储和到 Acronis Cloud 的磁盘备份
- 到本地存储和到 Acronis Cloud 的文件备份
- 防病毒和防恶意软件保护
- Acronis 可启动媒体
- 硬盘克隆
- 数据存档
- 家庭数据保护
- 文件同步
- 安全与隐私权工具

注意

您无法使用 Acronis Startup Recovery Manager 和 Acronis 可启动媒体创建到 Acronis Cloud 的备份。

了解如何通过两个简单的步骤来保护计算机:"[保护您的系统](#)"。

1.2 在 Acronis True Image(2020 或 2021) 和 Acronis Cyber Protect Home Office 中创建的备份

Acronis True Image 2020 引入了一种新的备份格式 TIBX, 这种格式更可靠便捷。TIBX 格式用于为内部驱动器、外部驱动器、网络共享创建的磁盘备份。

1.2.1 备份文件命名

使用 .tibx 扩展名的文件,其文件名中只包含备份名称和增量计数器。它不包含任何其他信息,例如 TIB 格式中使用的备份方法、备份链编号、备份版本号或卷号。

备份名称如下所示:

1. my_data.tibx
2. my_data_0001.tibx
3. my_data_0002.tibx
4. my_data_0003.tibx

1.2.2 备份方案

使用 TIBX 格式执行的备份支持所有备份方案。与 TIB 格式将每个备份版本保存为一个单独文件不同的是, TIBX 格式将完全备份和增量备份版本保存为单独的文件, 而增量备份版本会自动合并到其基础备份(完全备份或增量备份)中。

1.2.3 清理 TIBX 格式备份

如果要清理不再需要的备份版本, 可以使用自动和手动清理方式。

如果配置了自动或手动清理, 则清理后某些辅助文件可能仍留在存储中。Windows 显示的文件大小可能大于它们的实际大小。您可以通过检查 Windows 文件属性来查看实际大小。

注意

请勿手动删除任何文件!

1.2.4 可以使用以下方案手动清理本地备份:

- 完全备份只能与从属版本一起删除。
- 增量备份版本可以独立于任意其他备份版本删除。
- 增量备份:
 - 如果这是最后一个备份链, 则可以删除任意增量备份以释放空间。
 - 如果这不是最后一个备份链, 则只可以将任意增量备份版本以及同一链的所有其他增量版本一起删除。

1.2.5 保留 TIB 格式的备份

以下备份继续使用 TIB 格式:

- 文件级备份
- 不间断备份
- 公证备份
- 使用 CD/DVD/Blu-ray、FTP 或 Acronis Secure Zone 作为备份目标的备份

要详细比较以 .tibx 和 .tib 格式进行归档的区别, 请参阅[备份文件命名](#)。

有关清理的详细信息, 请参阅[清理备份、备份版本和副本](#)。

1.3 系统要求与支持的媒体

1.3.1 最低系统要求

Acronis Cyber Protect Home Office 对硬件的要求如下。

- 英特尔 CORE 2 Duo (2GHz) 处理器或同等性能的处理器。
CPU 必须支持 SSE 指令。
- 2 GB RAM
- 系统硬盘有 7 GB 的可用空间
- 创建可启动媒体的 CD-RW/DVD-RW 驱动器或 USB 驱动器
 - Linux 所需的可用空间大约为 660 MB。
 - Windows 所需的可用空间大约为 700 MB。
- 屏幕分辨率为 1024 x 768
- 鼠标或其它指针设备(推荐使用)

警告!

如果安装在虚拟机上则无法保证成功备份和恢复。

其他要求

- 产品激活、下载保护更新以及使用 Acronis Cloud 的所有功能都需要连接互联网。如果您的计算机未连接到互联网, 则可通过使用具有互联网连接的其他计算机来激活该产品。有关详细信息, 请参阅[激活 Acronis Cyber Protect Home Office](#)。
- 您需要具有管理员权限才能运行 Acronis Cyber Protect Home Office。

1.3.2 支持的操作系统

Acronis Cyber Protect Home Office 已在以下操作系统上进行测试。

- Windows 11
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1(所有版本)
- Windows Home Server 2011

注意

- Beta 版内部版本不受支持。请访问 <https://kb.acronis.com/content/60589>。
- Windows Embedded、IoT 版本、Windows 10 LTSC、Windows 10 LTSC 和 S 模式下的 Windows 10 不受支持。
- 若要在 Windows 7、Windows 8 和 Windows 8.1 上使用 Acronis Cyber Protect Home Office, 您需从 Microsoft 获得以下安全更新:KB4474419 和 KB4490628。请访问 <https://kb.acronis.com/content/69302>。

Acronis Cyber Protect Home Office 也可创建可启动 CD-R/DVD-R 或 USB 驱动器, 用于备份并恢复运行任何基于 Intel 或 AMD 的 PC 操作系统(包括 Linux®)的计算机上的磁盘/分区。请注意, 不支持基于 Intel 的 Apple Macintosh。

软件也许可以在其他 Windows 操作系统上运行, 但是我们不对此做出保证。

警告!

我们仅保证对受支持的操作系统实现成功的恢复。其他操作系统可以使用逐个扇区的方法进行备份, 但这些操作系统在恢复后可能无法启动。

1.3.3 支持的文件系统

- NTFS
- Ext2/Ext3/Ext4
- ReiserFS(3)*
- Linux SWAP *
- HFS+**/HFSX**
- FAT16/32/exFAT**

* 仅支持对文件系统进行磁盘或分区备份/恢复操作。

** 支持磁盘恢复、分区恢复和克隆操作, 而无需调整大小。

若文件系统不受支持或受到损坏, 则 Acronis Cyber Protect Home Office 可逐个扇区地复制数据。

1.3.4 支持的 Internet 连接类型

下表列出了产品功能所支持的 Internet 连接类型。

	Internet 连接类型				
	Windows 中的 Acronis 控制台		Acronis 可启动媒体		
	在 Windows 中建立的任意连接	代理服务器	以太网电缆	Wi-Fi	代理服务器
到 Acronis Cloud 的磁盘级和文件级备份	+	-	-	-	-

从 Acronis Cloud 执行磁盘级恢复	+	-	+	+	-
从 Acronis Cloud 执行文件级恢复	+	-	-	-	-
数据同步	+	-	-	-	-
产品激活	+	- *	-	-	-
产品更新	+	- **	-	-	-

* - 您可以使用激活码激活产品。有关详细信息，请参阅[激活 Acronis Cyber Protect Home Office](#) 中的[从其它计算机激活](#)一节。

** - 要更新产品，请从 Acronis 网站下载较新的产品版本，然后进行安装覆盖当前版本。

1.3.5 支持的存储媒体

- 硬盘驱动器 (HDD)
- 固态硬盘 (SSD)
- 网络存储设备
- FTP 服务器

注意

FTP 服务器必须允许被动模式文件传输。在 Acronis Cyber Protect Home Office 直接备份到 FTP 服务器时会将备份拆分为大小为 2 GB 的文件。

- CD-R/RW、DVD-R/RW、DVD+R(包括双面 DVD+R)、DVD+RW、DVD-RAM、BD-R、BD-RE
- USB 1.1/2.0/3.0、USB-C、eSATA、FireWire (IEEE-1394)、SCSI 和 PC 卡存储设备

动态磁盘的操作限制

- 不支持在动态磁盘上创建 Acronis Secure Zone。
- 不支持将动态卷恢复为可手动调节大小的动态卷。
- 无法使用 Try&Decide® 保护动态磁盘。
- 不支持动态磁盘的“克隆磁盘”操作。

源计算机的防火墙设置应该已为 TCP 和 UDP 协议打开端口 20 和 21，这样才可使其正常工作。**路由和远程访问**窗口服务应当被禁用。

1.4 安装和删除 Acronis Cyber Protect Home Office

安装 *Acronis Cyber Protect Home Office* 的方法

1. 访问 <https://go.acronis.com/home-office> 从 Acronis 网站下载 Acronis Cyber Protect Home Office 设置文件。
2. 运行安装文件。

在开始安装流程前, Acronis Cyber Protect Home Office 将从网站上查找较新的版本。若有, 则将安装较新的版本。

3. 单击 **安装**。

Acronis Cyber Protect Home Office 将安装到系统分区(通常是 C:) 上。

4. 安装完成后, 单击 **启动应用程序**。

5. 阅读并接受 Acronis Cyber Protect Home Office 和 Bonjour 许可证协议的条款。

Bonjour 软件将安装在您的计算机上以提供 NAS 设备的高级支持。您可以随时卸载该软件。

您也可以同意参与 [Acronis 客户体验计划](#)。您可以随时更改此设置。

6. 在 **激活** 窗口中, 您可以执行以下某项操作:

- 要激活 Acronis Cyber Protect Home Office, 请输入序列号, 然后单击 **激活**。将激活产品。
- 要登录您的 Acronis 帐户, 请单击 **登录**。有关详细信息, 请参阅 [Acronis 帐户](#)。
- 要使用试用版, 请单击 **开始试用**。

从 **Acronis Cyber Protect Home Office** 错误中恢复

若 Acronis Cyber Protect Home Office 停止运行或出现错误, 可能其文件已损坏。若要修复此问题, 必须先恢复程序。若要进行此操作, 请重新运行 Acronis Cyber Protect Home Office 安装程序。程序将对计算机上的 Acronis Cyber Protect Home Office 进行检测, 并询问是否要进行修复或删除。

删除 **Acronis Cyber Protect Home Office** 的方法

- 如果您使用的是 Windows 11, 请单击 **开始 > 设置 > 应用 > 应用和功能 > Acronis Cyber Protect Home Office > 卸载**。
- 如果您使用的是 Windows 10, 请单击 **开始 > 设置 > 系统 > 应用 > Acronis Cyber Protect Home Office > 卸载**。
- 如果您使用的是 Windows 8, 请单击 **设置** 图标, 然后选择 **控制面板 > 卸载程序 > Acronis Cyber Protect Home Office > 卸载**。
- 如果您使用的是 Windows 7, 请单击 **开始 > 控制面板 > 卸载程序 > Acronis Cyber Protect Home Office > 卸载**。

然后, 按照屏幕上的指示操作。此后, 可能必须重新启动计算机才能完成此任务。

注意

如果您使用过 "Acronis Secure Zone"(第 184 页) 或 "Acronis 不间断备份"(第 41 页), 请在出现的窗口中选择要如何处理安全区和不间断备份存储。

1.5 正在激活 Acronis Cyber Protect Home Office

要使用 Acronis Cyber Protect Home Office, 需要通过互联网将其激活。如果不激活, 这款功能完整的产品只能使用 30 天。如果在此期间不将其激活, 所有程序功能(除恢复外)都将不可用。

1.5.1 正在激活 Acronis Cyber Protect Home Office

您可以在自己的计算机上激活 Acronis Cyber Protect Home Office, 但如果您的计算机未连接到互联网, 则也可从其他计算机激活。

在连接到互联网的计算机上激活

如果您的计算机已连接到互联网,则会自动激活产品。

如果安装 Acronis Cyber Protect Home Office 的计算机未连接至互联网,或程序无法连接至 Acronis 激活服务器,请单击侧边栏上的**帐户**,然后选择以下其中一个操作:

- **再试一次** - 选择此选项可再次尝试连接至 Acronis 激活服务器。
- **离线激活** - 可从其他连接至互联网的计算机手动激活该程序(请参阅下文)。

从其他计算机激活

如果您的计算机未连接到互联网,则可通过使用连接到互联网的其他计算机来激活 Acronis Cyber Protect Home Office。

从其他计算机激活产品的方法

1. 在计算机上,安装并启动 Acronis Cyber Protect Home Office。
2. 在侧边栏上,单击**帐户**,然后单击**离线激活**。
3. 在 Acronis Cyber Protect Home Office 激活窗口中,执行 3 个简单步骤:
 - a. 通过单击**保存至文件**按钮将您的安装代码保存至文件,并指定可移动媒体作为文件位置(例如,USB 闪存驱动器)。您也可以在一张纸上写下此代码。
 - b. 在连接到互联网的其他计算机上,转至 <http://www.acronis.com.cn/activation/>。屏幕上的说明将帮助您通过使用安装代码来获取激活代码。将获取的激活代码保存至可移动媒体上的文件中,或写在纸上。
 - c. 在您的计算机上,单击**从文件加载**按钮并指定含有激活代码的文件的的路径;或将写在纸上的代码键入框中。
4. 单击**激活**。

此外,请观看位于 <https://goo.gl/DHd1h5> 的英语视频说明。

1.5.2 激活次数太多问题

“激活次数太多”问题的可能原因:

- **您超过了安装 Acronis Cyber Protect Home Office 的计算机的最大数目。**

例如,您拥有一个许可证或一台计算机的序列号,但却在第二台计算机上安装了 Acronis Cyber Protect Home Office。

解决方案:

- 输入新的序列号。如果您没有新的序列号,则可以在 Acronis 内建商店或 Acronis 网站购买。
- 将许可证从已激活产品的计算机中转移到新的计算机中。为此,请选择要从中移动许可证的计算机。请注意,在这台计算机上将停用 Acronis Cyber Protect Home Office。

- **您重新安装了 Windows, 或是更改了计算机的硬件。**

例如,您可能升级了计算机的主板或处理器。此时已丢失激活,因为 Acronis Cyber Protect Home Office 将您的计算机视为新计算机。

解决方案:

要在计算机上重新激活 Acronis Cyber Protect Home Office, 请从列表中按旧名称选择同一台计算机。

1.5.3 手动管理您的订购许可

如果您使用基于订购许可的 Acronis Cyber Protect Home Office 版本, 可以在 Acronis 网站手动管理许可。您可以执行以下操作:

- 在您的计算机之间移动许可
- 在您的帐户之间转移许可
- 从计算机中删除许可
- 解决产品激活冲突, 包括“激活次数太多”问题
- 购买新许可

管理许可的方法

1. 转至 <https://account.acronis.com/>, 然后使用您的 Acronis 帐户登录。
2. 在 **产品** 部分中, 找到 Acronis Cyber Protect Home Office, 然后单击 **管理**。

1.6 试用版信息

1.6.1 一般限制

试用版 Acronis Cyber Protect Home Office 仅在 30 天试用期内可用。其具有以下限制:

- 磁盘克隆已禁用。
- 从 Acronis 可启动媒体启动时, 只能执行恢复操作。

1.6.2 同步

数据同步的使用无限制, 但当试用期到期时:

- 您的计算机将从所有同步中排除。激活 Acronis Cyber Protect Home Office 的完整版后, 您将能够再次连接到同步。
- 所有同步文件版本都将从 [Acronis Cloud](#) 中永久删除。

1.6.3 Acronis Cloud

在试用期内, 您将获得云中 1,000 GB 的存储空间。您可以使用此空间存储在线备份、存档及同步文件版本。在试用期结束后, Acronis Cloud 只能在仅恢复模式下使用 30 天。在此期限之后, 您将无法再使用 Acronis Cloud 服务, 并且 Cloud 上的所有数据都将被删除。

1.6.4 购买完整版

您可以在 Acronis 网站上购买完整版, 或者使用应用程序内的购买功能。请参阅 [升级 Acronis Cyber Protect Home Office](#) 中的详细信息。

1.7 升级 Acronis Cyber Protect Home Office

当 Acronis 网站上发布 Acronis Cyber Protect Home Office 的更新时，您可以进行下载。如果您目前已安装 Acronis True Image(2017 或更高版本)，则新版本只需更新即可；无需删除旧版本并重新安装软件。如果您的当前版本较旧，我们建议您先删除当前版本。

使用先前版本的 Acronis Cyber Protect Home Office 创建的备份与较新的产品版本完全兼容。升级后，所有备份将自动添加到备份列表中。

较新版本的程序所创建的备份可能与之前版本的程序不兼容。若将 Acronis Cyber Protect Home Office 回滚至早期版本，则可能需要使用旧版本重新创建备份。强烈建议您在每次升级 Acronis Cyber Protect Home Office 后创建新的可启动媒体。

购买 Acronis Cyber Protect Home Office 的完整版

1. 启动 Acronis Cyber Protect Home Office。
2. 在工具条上，单击**帐户**，然后单击**购买完整版**。系统将会打开内置的商店。
3. 选择您要购买的许可证，然后单击**立即购买**。
4. 提供您的付款信息。

更新 Acronis Cyber Protect Home Office 的方法

1. 启动 Acronis Cyber Protect Home Office。
2. 在侧边栏上，单击**帐户**。
如果有可用的新版本，您将会在当前版本号旁边看到相应的消息。
3. 单击**下载并安装**。

注意

请确保您的防火墙不会阻止下载进程，然后再开始下载。

4. 新版本下载完成后，单击**立即安装**。

如需自动检查更新，请转至**设置**选项卡，然后选中**启动时自动检查更新**复选框。

1.7.1 内置商店

Acronis Cyber Protect Home Office 提供了应用程序内商店。通过该商店，您可以：

- 购买 Acronis Cyber Protect Home Office 的完整版。
- 购买 Acronis Cyber Protect Home Office 订购许可。
- 在 Acronis Cloud 上购买更多存储空间。

要访问应用程序内商店，请转至**帐户**选项卡，然后单击**Acronis 商店**。您将看到应用程序内商店以及所有可用的采购选项。

1.8 技术支持

1.8.1 维护和支持计划

如果需要关于 Acronis Cyber Protect Home Office 的帮助, 请访问 <http://www.acronis.com.cn/support/>。

2 入门

2.1 用户界面语言

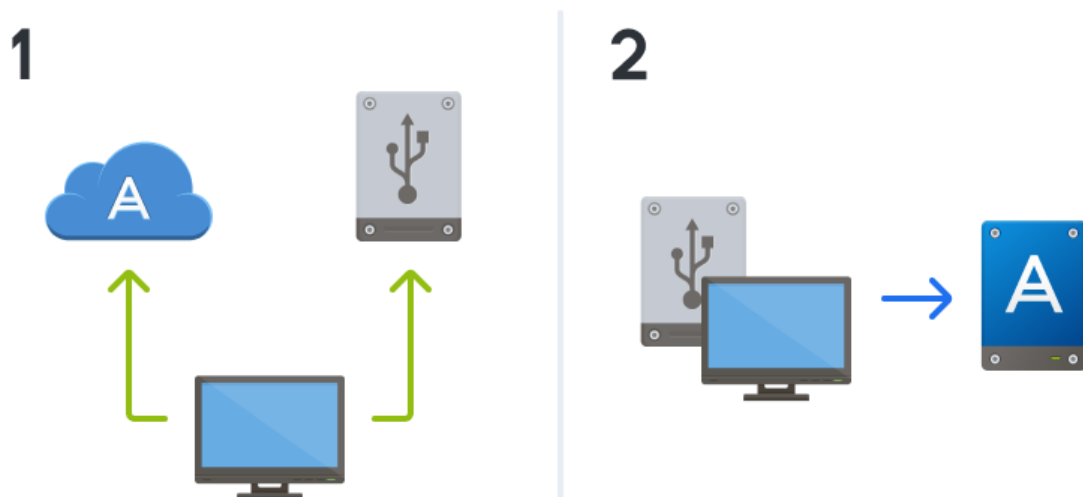
在开始之前，请为 Acronis Cyber Protect Home Office 用户界面选择首选语言。默认情况下，将根据您的 Windows 显示语言设置该语言。

更改用户界面语言

1. 启动 Acronis Cyber Protect Home Office。
2. 在**设置**部分中，从列表中选择首选语言。

2.2 保护系统

1. 备份计算机。
2. 创建 Acronis 可启动媒体。



- 建议按照[确保可启动媒体随时可用](#)所述的说明测试可启动媒体。

2.2.1 备份计算机

何时应该备份计算机？

系统中发生重大事件之后，都应该创建新的备份版本。

这些事件的示例包括：

- 购买新计算机。
- 在计算机上重新安装了 Windows。
- 在新计算机上配置了所有系统设置(例如：时间、日期、语言)并安装了所有必要的程序。
- 重要系统更新。

注意

为了确保您保存的是健康状态的磁盘,最好在备份它之前进行病毒扫描。请使用杀毒软件进行病毒扫描。请注意,此操作通常需要相当长的时间。

如何创建计算机备份?

您有两个用于保护系统的选项:

- **整个 PC 备份(建议)**

Acronis Cyber Protect Home Office 会以磁盘模式备份所有内部硬盘。备份包含操作系统、已安装的程序、系统设置以及所有个人数据(包括照片、音乐和文档)。有关详细信息,请参阅[备份 PC 上的所有数据](#)。

- **系统磁盘备份**

您可以选择备份系统分区或整个系统驱动器。有关详细信息,请参阅[备份磁盘和分区](#)。

我们不建议使用不间断备份作为系统的主要保护方式,因为该技术的主要目的是保护频繁更改的文件。要确保系统安全,请使用任何其他计划。在"自定义方案示例"(第 61 页)中查看示例。有关不间断备份功能的详细信息,请参阅"Acronis 不间断备份"(第 41 页)。

备份计算机

1. 启动 Acronis Cyber Protect Home Office。

2. 在侧栏上单击**备份**。

如果是第一次备份,则会显示备份配置屏幕。如果在备份列表中已具有一些备份,则单击**添加备份**。

3. 单击**备份源**图标,然后选择**整个 PC**。

如果要仅备份系统磁盘,则单击**磁盘和分区**,然后选择系统分区(通常是 C:)和系统保留分区(如果有)。

4. 单击**备份目标**图标,然后选择备份的存储位置(请参阅下面的建议)。

5. 单击**立即备份**。

因此,新备份框中将显示备份列表中。要在未来创建新的备份版本,请从列表中选择备份框,然后单击**立即备份**。

应该将磁盘备份存储在何处?

- **不错的选择** - 普通的内置硬盘。
- **更好的选择** - [Acronis 安全区](#)。这是本地硬盘上用于存储备份的特殊安全分区。
- **最好的选择** - [Acronis Cloud](#) 或外接硬盘。

有关详细信息,请参阅[决定存储备份的位置](#)。

需要多少个备份版本?

在大多数情况下,您需要整个 PC 内容或系统磁盘的 2 到 3 个**备份版本**,最多需要 4 到 6 个(有关何时创建备份的信息,请参阅上文)。您可以使用自动清除规则,控制备份版本的数量。有关详细信息,请参阅[自定义方案](#)。

请记住, 第一个备份版本(完整备份版本)最重要。它是最大的一个, 因为它包含存储在磁盘上的所有数据。后续备份版本(增量和差异备份版本)可用不同的方案组织。这些版本只包含数据更改。这就是它们为何依赖于完整版本以及完整版本为何如此重要的原因。

默认情况下, 会使用增量方案创建磁盘备份。在大多数情况下, 此方案是最佳的。

注意

对于高级用户: 最好创建 2 到 3 个完整备份版本并将它们存储在不同的存储设备上。此方法更加可靠。

2.2.2 创建 Acronis 可启动媒体

Acronis 可启动媒体是 CD、DVD、USB 闪存驱动器或其他可移动媒体, 在 Windows 无法启动时, 可以从该媒体运行 Acronis Cyber Protect Home Office。您可使用 Acronis 媒体生成器创建可启动媒体。

创建 Acronis 可启动媒体的方法

1. 放入 CD/DVD 或插入 USB 驱动器(USB 闪存驱动器或 HDD/SSD 外部驱动器)。
2. 启动 Acronis Cyber Protect Home Office。
3. 在侧边栏上, 单击工具, 然后单击**应急媒体生成器**。
4. 在第一个步骤中, 选择**简单**。
5. 选择用于创建可启动媒体的设备。
6. 单击**继续**。

使用 Acronis 可启动媒体

当 Windows 无法启动时, 可使用 Acronis 可启动媒体来恢复计算机。

1. 将可启动媒体连接至计算机(放入 CD/DVD 或插入 USB 驱动器)。
2. 在 BIOS 中设置启动顺序, 以便您的 Acronis 可启动媒体是要启动的第一个设备。
有关详细信息, 请参阅[设置 BIOS 启动顺序](#)。
3. 从可启动媒体启动您的计算机, 并选择 **Acronis Cyber Protect Home Office**。
加载 Acronis Cyber Protect Home Office 后, 就可以使用它来恢复计算机。

有关详细信息, 请参阅 [Acronis 媒体生成器](#)。

2.3 备份 PC 上的所有数据

什么是整个 PC 备份?

整个 PC 备份是备份计算机中所有内容的最简单方式。当您不确定要保护哪些数据时, 我们建议您选择该选项。如果只想备份系统分区, 请参阅[备份磁盘和分区](#)获取详情。

如果选择整个 PC 作为备份类型, Acronis Cyber Protect Home Office 会备份处于磁盘模式下的所有内部硬盘。备份包含操作系统、已安装的程序、系统设置以及所有个人数据(包括照片、音乐和文档)。

从整个 PC 备份的恢复过程也经过简化。您只需选择要将数据还原到的日期。Acronis Cyber Protect Home Office 会将备份中的所有数据恢复到原始位置。请注意，您无法选择特定磁盘或分区进行恢复，也无法更改默认的目标位置。如果需要避开这些限制，我们建议您使用普通磁盘级恢复方法备份您的数据。有关详细信息，请参阅[备份磁盘和分区](#)。

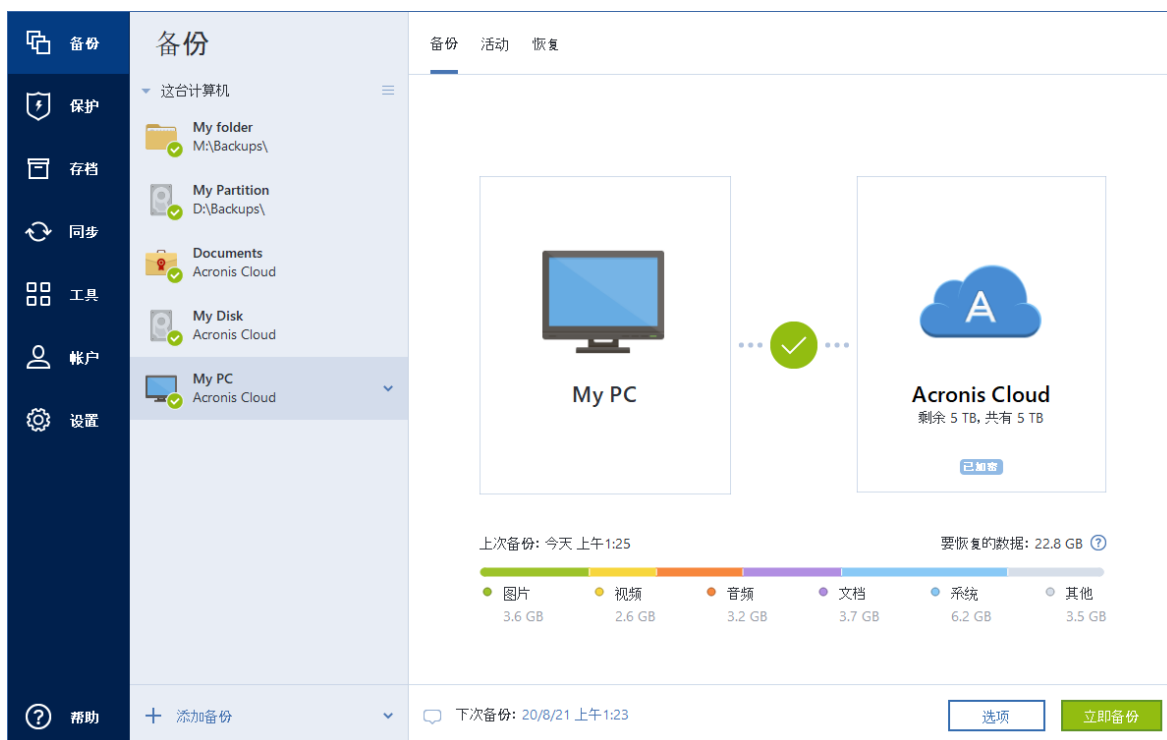
您也可以从整个 PC 备份恢复特定文件和文件夹。有关详细信息，请参阅[备份文件与文件夹](#)。

如果整个 PC 备份包含动态磁盘，您可以在分区模式下恢复数据。这意味着您可以选择要恢复的分区并更改恢复目标位置。有关详细信息，请参阅[关于恢复动态/GPT 磁盘和卷](#)。

创建整个 PC 备份

1. 启动 Acronis Cyber Protect Home Office。
2. 在侧栏上单击**备份**。
3. 单击备份列表底部的加号。
4. 单击**备份源**图标，然后选择**整个 PC**。
5. 单击**备份目标**图标，然后选择备份的目标位置。

建议您将计算机备份至 Acronis Cloud 或者备份至本地或网络存储。有关详细信息，请参阅[决定存储备份的位置](#)。



6. [可选步骤] 单击**选项**以设置备份选项。有关更多信息，请参阅[备份选项](#)。
7. 单击**立即备份**。

注意

当您把数据备份至 Acronis Cloud 时，第一个备份可能会花费大量时间才能完成。进一步的备份过程可能会快得多，因为届时将仅通过互联网传输对文件的更改。

此外，请观看位于 <https://goo.gl/KjW5sM> 的英语视频说明。

2.4 创建 Acronis Survival Kit

要在发生故障的情况下恢复您的计算机，您需要有两个关键的组件 — 系统磁盘的备份和 Acronis 可启动媒体。通常这些组件是分开的，例如，系统备份存储在外部驱动器或 Acronis Cloud 上，可启动媒体是一个小型 USB 闪存驱动器。Acronis Survival Kit 将两个组件结合在一起，这样您就可以拥有一个设备，可以让您在出现故障的情况下恢复计算机。它是一个外部硬盘，包含 Acronis 可启动媒体文件和系统分区、整个计算机或任何磁盘备份的备份。而且，数据的备份可用作正常备份：它可以包含您需要保护的任意数据，并且您可以设置计划以作为正常备份来更新它。甚至，外部硬盘不会被 Acronis Survival Kit 专门预订，其可启动媒体仅占用 2 GB 磁盘空间，而作为 Acronis Survival Kit 一部分的系统分区或整个计算机备份以及任何其他数据(包括其他备份、您的个人数据、照片等)都可以共享剩余空间。但是，请在一个外部硬盘上仅保留一个 Acronis Survival Kit。

无论在此外部硬盘上存储多少备份，仅需要使用一个 Acronis Survival Kit 来恢复计算机。如果任何系统分区或整个计算机备份是为同一计算机或具有相同配置的计算机而创建，则其可启动媒体组件可与它们配合使用。

您可以使用以下设备作为 Acronis Survival Kit 的设备：

- **外部硬盘驱动器**

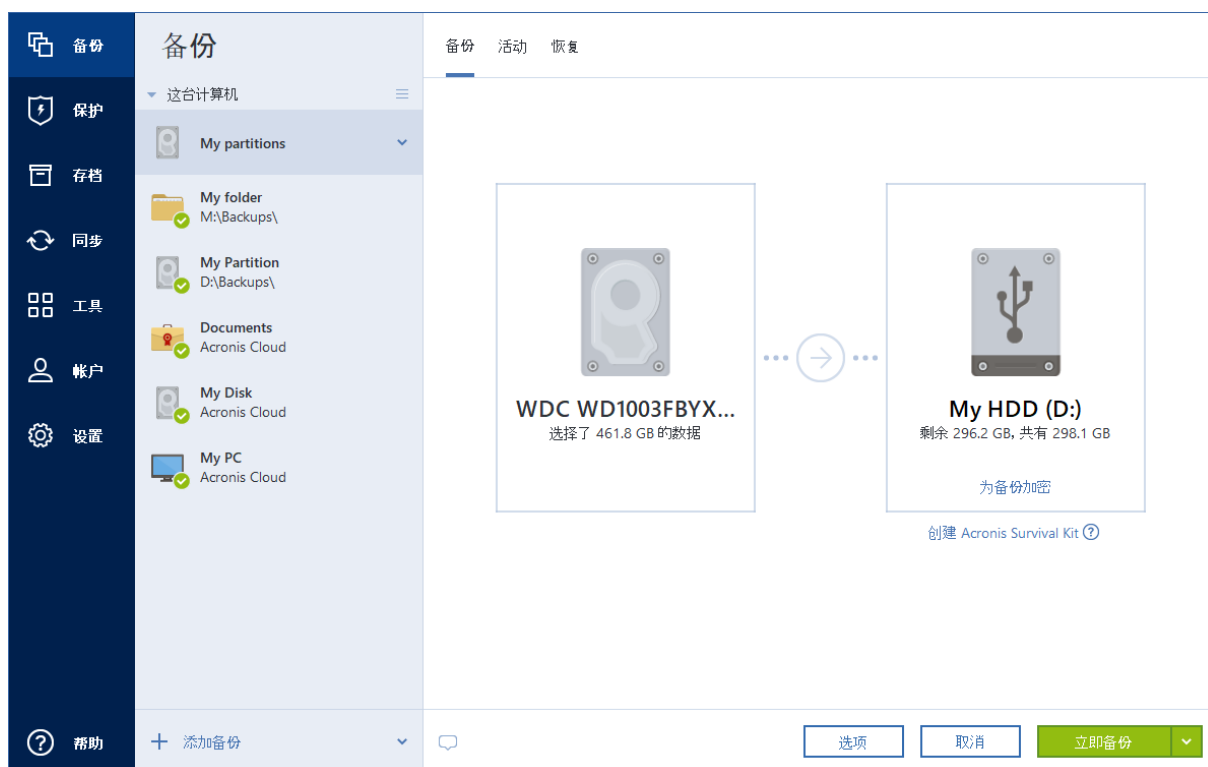
它必须大于 32 GB 并且具有 NTFS、FAT32 或 exFAT 文件系统。如果驱动器具有另一个文件系统，Acronis Cyber Protect Home Office 建议对驱动器进行格式化。

- **USB 闪存驱动器**

它必须是 MBR 闪存驱动器，最小为 32 GB。如果使用的是 GPT 闪存驱动器，Acronis Cyber Protect Home Office 建议将其格式化为 MBR。请注意，仅在 Windows 10(版本 1703 或更高版本)和 Windows 11 环境下支持闪存驱动器。

创建 Acronis Survival Kit 的方法

当您配置系统分区、整个计算机或任何磁盘备份的备份并选择一个外部硬盘作为目标位置时，Acronis Cyber Protect Home Office 将建议创建一个 Acronis Survival Kit。



1. 单击**立即备份或创建 Acronis Survival Kit**。

2. 在打开的窗口中，单击**创建**。

Acronis Cyber Protect Home Office 在选定的驱动器上创建一个小分区，并在其中写入启动文件。要创建该分区，现有卷的其中一个卷的大小将被调整。如果磁盘不是 GPT 并且具有不同于 NTFS、FAT32 或 exFAT 的文件系统，Acronis Cyber Protect Home Office 建议对磁盘进行格式化。注意，磁盘格式化将删除存储在磁盘上的所有数据。

3. 当启动文件被成功写入驱动器时，它就成为一个 Acronis 可启动媒体，您可以使用它来恢复计算机。若要完成 Acronis Survival Kit 创建，您需要将系统分区、整个计算机或任何磁盘备份的备份保存到该驱动器。为此，请单击**立即备份**。如果跳过此步骤，请不要忘记稍后在此驱动器上创建备份。有关详细信息，请参阅[备份磁盘和分区](#)。

当 Acronis Survival Kit 准备就绪后，您可以用它来恢复您的计算机。有关详细信息，请参阅[将系统恢复到同一磁盘](#)。

每当您将备份配置到带有 Survival Kit 的外部设备时，Acronis Cyber Protect Home Office 都将检查它的版本。如果 Survival Kit 的最新版本可用，Acronis Cyber Protect Home Office 将建议更新外部设备上的 Survival Kit。

2.5 备份您的文件

若要保护文档、照片、音乐文件和视频文件之类的文件，无需备份包含这些文件的整个分区。您可以备份特定文件和文件夹并将其保存到以下存储类型：

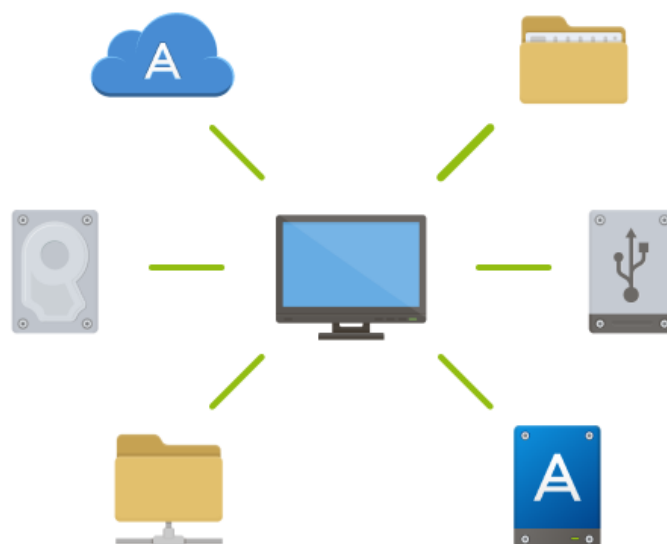
- **本地或网络存储**

该选项快速简单。使用它可保护极少更改的文件。

- **Acronis Cloud**

该选项非常可靠。使用它可保护重要的文件,以及要在设备之间共享或与其他人共享的文件。

要使用 Acronis Cloud, 您必须具有 Acronis 帐户和 Acronis Cloud 服务的订购许可。有关详细信息, 请参阅 "订购许可信息"(第 32 页)。



备份文件与文件夹

1. 启动 Acronis Cyber Protect Home Office。
2. 在侧栏上单击 **备份**。
3. 单击 **备份源** 图标, 然后选择 **文件与文件夹**。
4. 在打开的窗口中, 选中您要备份的文件及文件夹旁边的复选框, 然后单击 **确定**。
5. 单击 **备份目标位置** 图标, 然后选择一个备份目标位置:
 - **Acronis Cloud** - 登录您的帐户, 然后单击 **确定**。
 - **您的外接驱动器** - 当在计算机上插入外接驱动器时, 您可以从列表中选择该项。
 - **NAS** - 从找到的 NAS 设备列表选择一个 NAS。如果只有一个 NAS, 默认情况下, Acronis Cyber Protect Home Office 会建议将其用作备份目标位置。
 - **浏览** - 从文件夹树中选择一个目标位置。
6. 单击 **立即备份**。

有关详细信息, 请参阅 [备份文件与文件夹](#)。

此外, 请观看位于 <https://goo.gl/i4J1AN> 的英语视频说明。

2.6 克隆硬盘驱动器

2.6.1 为何需要?

当发现硬盘驱动器的可用空间不足以存储数据时, 您可能要购买新的更大的硬盘驱动器, 然后将数据转移到新驱动器。通常的复制操作无法使得新硬盘驱动器跟旧的驱动器完全一样。例如, 打开文

件资源管理器并将所有文件和文件夹复制到新硬盘驱动器后, Windows 不会从新硬盘驱动器启动。借助克隆磁盘实用工具, 您可以复制所有数据, 并且使得 Windows 可以从新硬盘驱动器进行启动。



2.6.2 启动之前,

我们建议您将目标(新)驱动器安装在计划要使用的位置上, 与源驱动器的放置位置分开, 例如外部 USB 盘。这点对笔记本电脑而言尤为重要。

注意

建议使用旧的和新的硬盘驱动器在相同的控制器模式(例如 IDE 或 AHCI)下工作。否则, 您的计算机不会从新的硬盘驱动器启动。

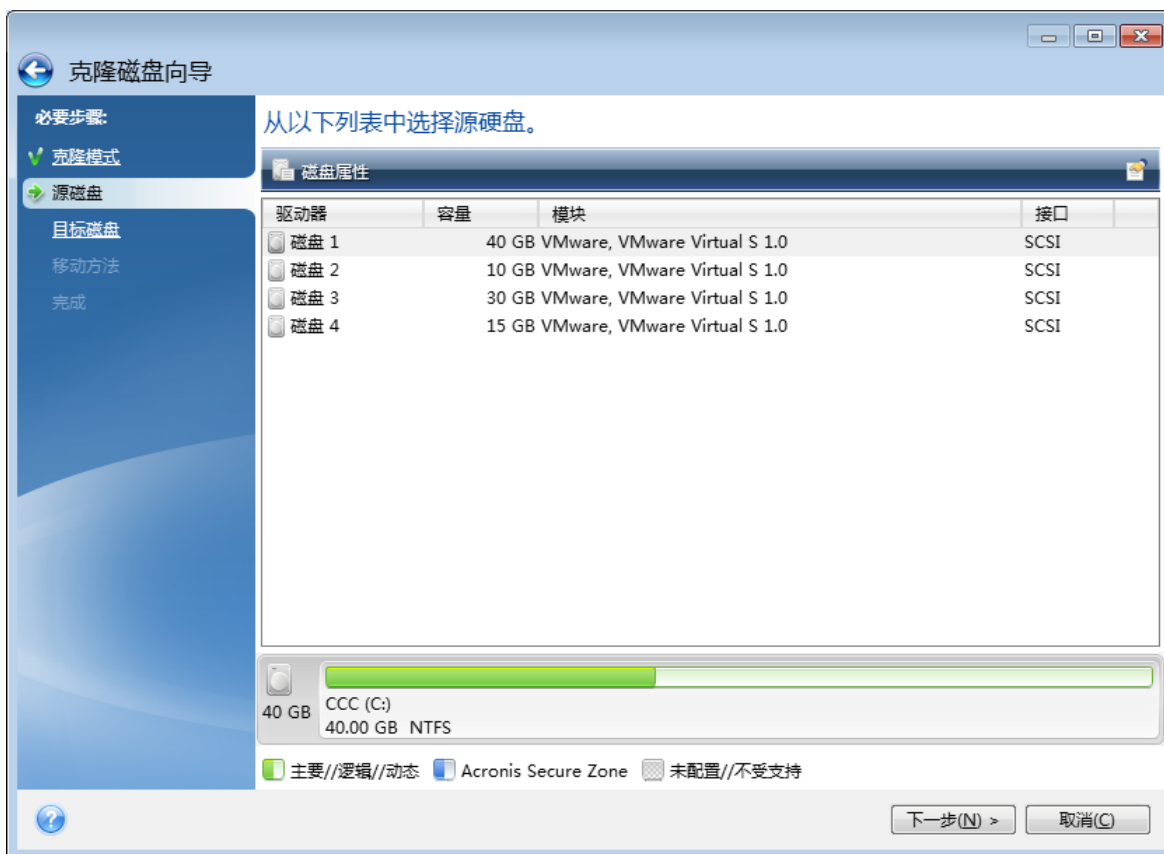
2.6.3 克隆磁盘

1. 单击工具条内的**工具**, 然后单击**克隆磁盘**。
2. 在**克隆模式**步骤中, 我们建议您选择**自动**转移模式。在这种情况下, 将按比例调整分区以适应新的硬盘驱动器。**手动**模式提供了更多的灵活性。有关手动模式的详细信息, 请参阅[克隆磁盘向导](#)。

注意

若程序找到两张磁盘, 其中一张已分区, 另一张尚未分区, 则系统会自动将已分区磁盘识别为源盘, 并将尚未分区的磁盘识别为目标磁盘。在这种情况下, 后面的步骤将被省略并转至克隆“摘要”屏幕。

3. 在**源磁盘**步骤中, 选择要克隆的磁盘。



4. 在**目标磁盘**步骤中，选择用于存储克隆数据的目标磁盘。

注意

若有未分区的磁盘，则程序会自动将其识别为目标磁盘，并略过该步骤。

5. 在**完成**步骤中，请确保配置的设置符合您的需求，然后单击**继续**。

默认情况下，Acronis Cyber Protect Home Office 会在克隆过程完成后关闭计算机。这可让您更改主控/从属跳线的位置并删除其中的一个硬盘。

此外，请观看位于 <https://goo.gl/bjWRLl> 的英语视频说明。

2.7 恢复计算机

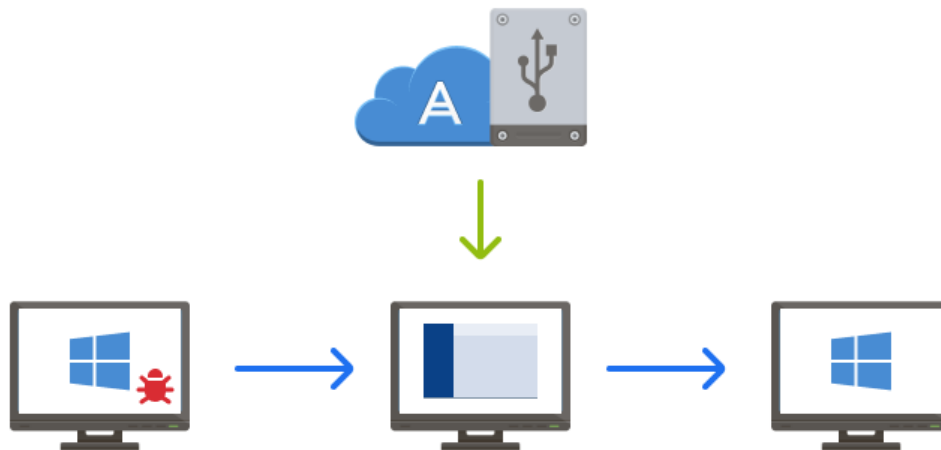
请注意，恢复系统磁盘是一项重要操作。开始执行此操作前，建议您阅读以下“帮助”主题中的详细说明：

- 尝试确定崩溃原因
- 准备恢复
- 将系统恢复到同一硬盘

让我们来看两个不同案例：

1. Windows 运行不正常，但您可以启动 Acronis Cyber Protect Home Office。
2. Windows 无法启动(例如，计算机可以启动，但屏幕显示异常内容)。

案例 1. 如何在 **Windows** 运行不正常的情况下恢复计算机？

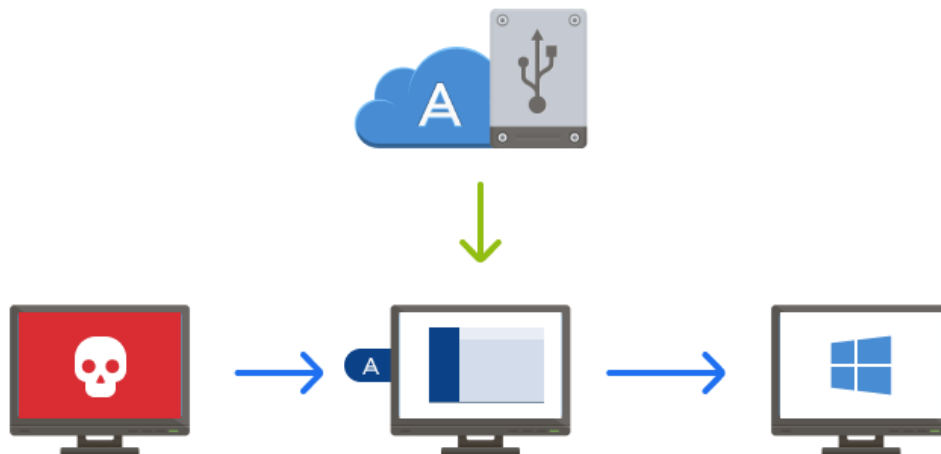


1. 启动 Acronis Cyber Protect Home Office。
2. 在侧栏上单击**备份**。
3. 从备份列表中, 选择包含系统磁盘的备份。备份可位于本地存储、网络存储或Acronis Cloud 上。
4. 在右侧面板中, 单击**恢复**。
5. 根据备份类型, 单击**恢复 PC** 或 **恢复磁盘**。
6. 在打开的窗口中, 选择备份版本(特定日期和时间的数据状态)。
7. 选择要恢复的系统分区和系统保留分区(如果有)。
8. 单击**立即恢复**。

注意

要完成操作, Acronis Cyber Protect Home Office 必须重新启动系统。

案例 2. 如何在 *Windows* 无法启动的情况下恢复计算机?



1. 将 Acronis 可启动媒体连接到计算机, 然后运行专用单机版 Acronis Cyber Protect Home Office。有关详细信息, 请参阅 [步骤 2 创建 Acronis 可启动媒体和设置 BIOS 启动顺序](#)。
2. 在“欢迎”屏幕上, 选择**恢复**下的**我的磁盘**。
3. 选择要用于恢复的系统磁盘备份。右键单击备份, 然后选择**恢复**。
如果未显示备份, 请单击**浏览**并手动指定备份路径。在同一窗口中, 可以连接到 Acronis Cloud 并选择线上备份。有关详细信息, 请参阅 [从 Acronis Cloud 恢复系统](#)。
4. 在**恢复方法**步骤中, 选择**恢复整个磁盘和分区**。
5. 在**恢复内容**屏幕中选择系统分区(通常是 C)。请注意, 可以通过 Pri、Act 标志辨别系统分区。选择系统保留分区(如果有)。
6. 您可以让分区的所有设置保持不变并单击**完成**。
7. 检查操作摘要, 然后单击**继续**。
8. 操作完成后, 退出单机版 Acronis Cyber Protect Home Office, 移除可启动媒体(如果有)并从恢复的系统分区启动。确保已将 Windows 恢复到需要的状态后, 请还原原始启动顺序。

2.8 Acronis 帐户

执行以下操作时需要 Acronis 帐户:

- 注册 Acronis 产品。
- 备份到 Acronis Cloud。
- 同步数据。
- 存档数据。

创建 Acronis 帐户的方法

1. 在侧边栏上, 单击**帐户**, 然后单击**登录或创建帐户**。
2. 单击**创建帐户**。

3. 填写注册表单。提供所需的数据，接受使用条款，并可选择订阅以接收偶尔发送的新闻和促销优惠。

注意

为保证您个人数据的安全，请为线上备份选择高强度密码、防止其落入坏人之手并不时更换密码。

4. 单击**创建帐户**。
5. 系统会将一封电子邮件发送到您指定的地址。打开该邮件并确认您想要创建帐户。

使用您的 **Acronis** 帐户登录

1. 在侧边栏上，单击**帐户**，然后单击**登录或创建帐户**。
2. 输入您的注册电子邮件地址和密码，然后单击**登录**。

要从您的 **Acronis** 帐户注销，请执行以下操作：

1. 在侧边栏上，单击**帐户**。
2. 单击您的电子邮件地址，然后选择**注销**。

2.9 Acronis Cloud 快速入门

注意

您所在的地区可能无法使用 Acronis Cloud。有关更多信息，请单击此处：<https://kb.acronis.com/content/4541>

2.9.1 远程存储器

一方面，Acronis Cloud 是可供您存储以下内容的应急远程存储：

- 您的文件和文件夹的备份
- 您的分区和磁盘的备份
- 同步版本的文件和文件夹

因为文件存储在远程存储器上，所以即使计算机被盗或是房子被烧毁，您的文件也会得到保护。若出现灾难或数据损坏，您可以恢复文件甚至计算机中的全部内容。

使用一个帐户，您可以保存来自多台计算机以及您所有运行 iOS 和 Android 操作系统的移动设备的数据。

要开始使用 Acronis Cloud，您需要订购此服务。有关详细信息，请参阅[订购许可信息](#)。

2.9.2 Web 应用程序

另一方面，Acronis Cloud 是供您恢复和管理存储在 Acronis Cloud 上的数据的 Web 应用程序。使用此应用程序，您可以使用所有连接到互联网的计算机。

要访问该应用程序，请转至 <https://www.acronis.com/my/online-backup/webrestore/>，然后登录到您的 Acronis 帐户。

2.9.3 如何确保数据的安全性

当您使用 Acronis Cloud 作为存储时,您可能想要确保个人文件不会落入他人之手。您可能尤其关心移动设备的安全性,因为所有数据都将通过 Internet 传输。

放心,我们会保证您数据的安全。首先,我们使用加密协议(SSL、TLS)同时通过 Internet 和 LAN 传输所有数据。要访问数据,需提供您帐户的电子邮件地址和密码进行登录。其次,您可以选择仅使用受保护的 Wi-Fi 网络来备份您的数据。在这种情况下,将您的数据传输到 Acronis Cloud 时将非常安全。在设置中选择安全的 **Wi-Fi 网络用于备份**。

2.9.4 订购许可信息

对于使用 Acronis Cloud 的 Acronis Cyber Protect Home Office 功能(例如线上备份、云存档和云同步),需要订阅 Acronis Cloud 存储。如需订购,请启动 Acronis Cyber Protect Home Office 并转至 **帐户** 选项卡,然后选择是要启动试用版订购许可还是购买完整版。

注意

请注意, Acronis Cloud 受我们的公平使用政策约束。有关详情,请访问 <https://kb.acronis.com/ati/fairusage>。

试用版

当您激活产品的试用版时,一个 1000 GB 的存储和 Acronis Cyber Protect Home Office 的 Acronis Cloud 试用期免费订阅将自动分配到您的帐户。有关详细信息,请参阅 [试用版信息](#)。

完整版

您可以在您的 Acronis Cyber Protect Home Office 版本的 **帐户** 部分或在 Acronis 网站购买完整 Acronis Cloud 订购许可。请参阅 [升级 Acronis Cyber Protect Home Office](#) 中的详细信息。

3 基本概念

本部分提供了有关基本概念的一般信息, 这些信息可能有助于了解程序的工作原理。

备份和恢复

备份指的是制作数据副本, 如果数据丢失, 这些附加副本即可用于**恢复**原始数据。

备份主要有两种用途:

- 在操作系统崩溃或无法启动时恢复操作系统(即灾难恢复)。有关保护您的计算机系统免受灾难损害的详细信息, 请参阅[保护系统](#)。
- 特定的文件和文件夹被误删或损坏之后对其进行恢复。

Acronis Cyber Protect Home Office 可通过分别创建磁盘(或分区)映像和文件级备份来实现备份。

恢复方法:

- 可以向原始位置或新位置执行**完整恢复**。
选择原始位置后, 该位置中的数据将完全被备份中的数据覆盖。如果选择一个新位置, 会将备份中的数据复制到该新位置。
- 仅向原始位置且仅从云备份执行**增量恢复**。在恢复开始之前, 将通过文件属性(如文件大小和上次修改日期)将原始位置中的文件与备份中的文件进行对比。那些不匹配的文件将标记为进行恢复, 在恢复期间将跳过其余文件。这样一来, 不同于完整恢复, Acronis Cyber Protect Home Office 只恢复更改的文件。在从 Acronis Cloud 恢复期间, 此方法显著缩短了恢复时间并节省了互联网流量。

备份版本

备份版本是指在每个备份操作中创建的文件。创建的版本数量与执行备份操作的次数相等。因此, 版本表示系统或数据可还原到的时间点。

备份版本可表示完整、增量和差异备份 - 请参阅[完整、增量和差异备份](#)。

备份版本与文件版本类似。对于使用 Windows 的一种称为“先前文件版本”功能的用户, 文件版本概念并不陌生。此功能允许您将文件还原到它在特定日期和时间下的存在状态。备份版本允许您以类似方式恢复数据。

磁盘克隆

此操作可以将一个磁盘驱动器上的整个内容复制到另一个磁盘驱动器。这可能是必需的, 例如, 当您想将操作系统、应用程序和数据克隆到一个新的更大容量的磁盘上时。您可以通过两种方式执行此操作:

- 使用克隆磁盘实用工具。
- 备份旧磁盘驱动器, 然后将其恢复到新的磁盘驱动器。

备份文件格式

Acronis Cyber Protect Home Office 通常以专有的 tib 压缩格式保存备份数据。 .tib 文件备份中的数据只能通过 Acronis Cyber Protect Home Office 在 Windows 或恢复环境中来恢复。

“Acronis 不间断备份”使用特殊的隐式存储器来存储数据和元数据。系统会对备份的数据进行压缩，然后将其拆分成大小约为 1 GB 的文件。这些文件同样具有专有格式，只有借助 Acronis Cyber Protect Home Office 才能恢复文件所包含的数据。

备份验证

备份验证功能允许您确定数据是否可以恢复。程序将校验和值添加至正在备份的数据块。在备份验证期间，Acronis Cyber Protect Home Office 将打开备份文件，重新计算校验和值，并将这些值与存储的值相比较。如果所有比较的值均匹配，则备份文件未破坏。

计划

为了真正发挥备份的作用，必须尽量确保其为“最新”。预定您的备份，使其自动定期运行。

删除备份

如果您想删除不再需要的备份和备份版本，请使用 Acronis Cyber Protect Home Office 提供的工具来完成此操作。有关详细信息，请参阅[删除备份和备份版本](#)。

Acronis Cyber Protect Home Office 将备份的信息存储在元数据信息数据库中。因此，在文件资源管理器中删除不需要的备份文件将不会从数据库中删除有关这些备份的信息。这将导致在程序对已不存在的备份执行操作时出错。

3.1 文件备份与磁盘/分区映像之间的差别

备份文件与文件夹时，仅压缩和存储文件与文件夹树。

磁盘/分区备份不同于文件和文件夹备份。Acronis Cyber Protect Home Office 会存储磁盘或分区的准确快照。此过程称为“创建磁盘映像”或“创建磁盘备份”，生成的备份则通常称为“磁盘/分区映像”或“磁盘/分区备份”。

3.1.1 磁盘/分区备份包含哪些内容？

磁盘/分区备份包含磁盘或分区上存储的所有数据：

1. 具有主启动记录 (MBR) 的硬盘的零磁道(仅适用于 MBR 磁盘备份)。
2. 一个或多个分区，包括：
 - a. 启动代码。
 - b. 文件系统元数据，包括服务文件、文件分配表 (FAT) 和分区启动记录。
 - c. 文件系统数据，包括操作系统(系统文件、注册表、驱动程序)、用户数据和软件应用程序。
3. 系统保留分区(如果有)。
4. EFI 系统分区(如果有，仅适用于 GPT 磁盘备份)。

3.1.2 磁盘备份中去除了哪些内容？

为了缩小映像的大小并提高映像创建速度，默认情况下，Acronis Cyber Protect Home Office 仅会存储包含数据的硬盘扇区。

Acronis Cyber Protect Home Office 会从磁盘备份中排除以下文件：

- pagefile.sys
- hiberfil.sys(计算机休眠时用于保存 RAM 内容的文件)

您可以通过打开逐个扇区模式更改此默认方法。在这种情况下, Acronis Cyber Protect Home Office 将复制所有硬盘扇区, 而不仅仅是包含数据的扇区。

另外, 当您将系统分区或磁盘备份到 Acronis Cloud 时, Acronis Cyber Protect Home Office 会排除以下数据:

- Temp 文件夹, 该文件夹通常位于:
 - C:\Windows\Temp\
 - C:\Users\\AppData\Local\Temp
- System Volume Information 文件夹(通常位于 C:\System Volume Information\ 下)
- 回收站
- 网络浏览器临时数据:
 - 临时互联网文件
 - Cookie
 - 历史记录
 - 缓存
- .tib 和 .tibx 文件
- .tmp 文件
- .~ 文件

3.2 完整、增量和差异备份

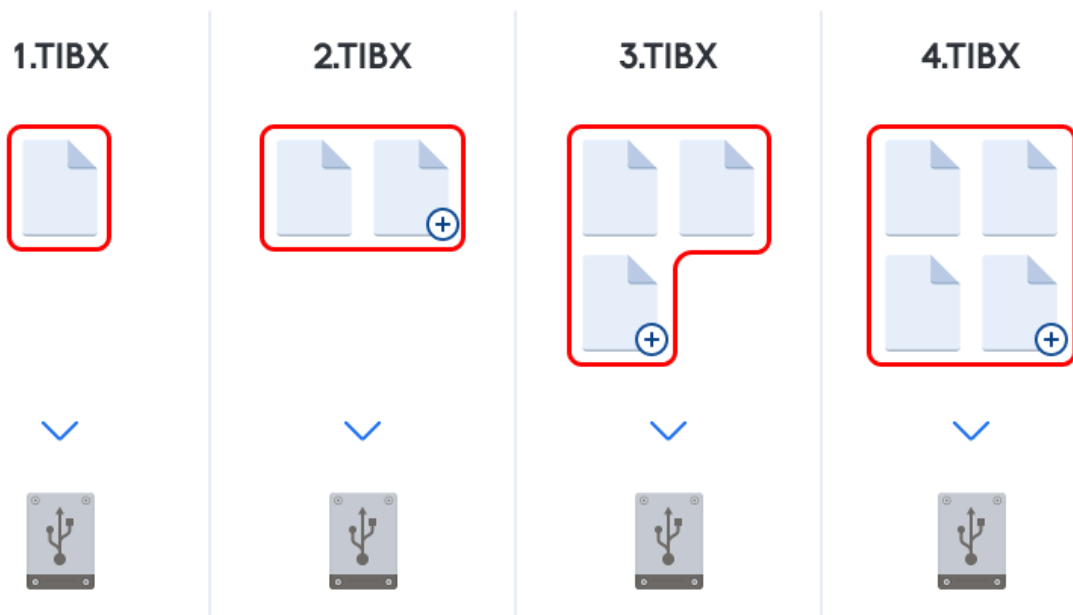
Acronis Cyber Protect Home Office 提供三种备份方法:完整、增量和差异。

3.2.1 完整方式

完整方式备份操作(也称为完整备份版本) 的结果包含创建备份时存在的所有数据。

示例:每天, 您编写一页文档并使用完整备份方法将其备份。每次您运行备份时, Acronis Cyber Protect Home Office 都会保存整个文档。

1.tibx、2.tibx、3.tibx、4.tibx — 完整备份版本的文件。



其他信息

完整备份版本可用作进一步增量或差异备份的基础。它也可用作独立备份。若经常将系统返回初始状态, 或者若您不喜欢管理多个备份版本, 建立独立的完整备份可能是最佳解决方案。

恢复: 在上面的示例中, 要从 4.tibx 文件恢复整个工作, 您只需要有一个备份版本 4.tib。

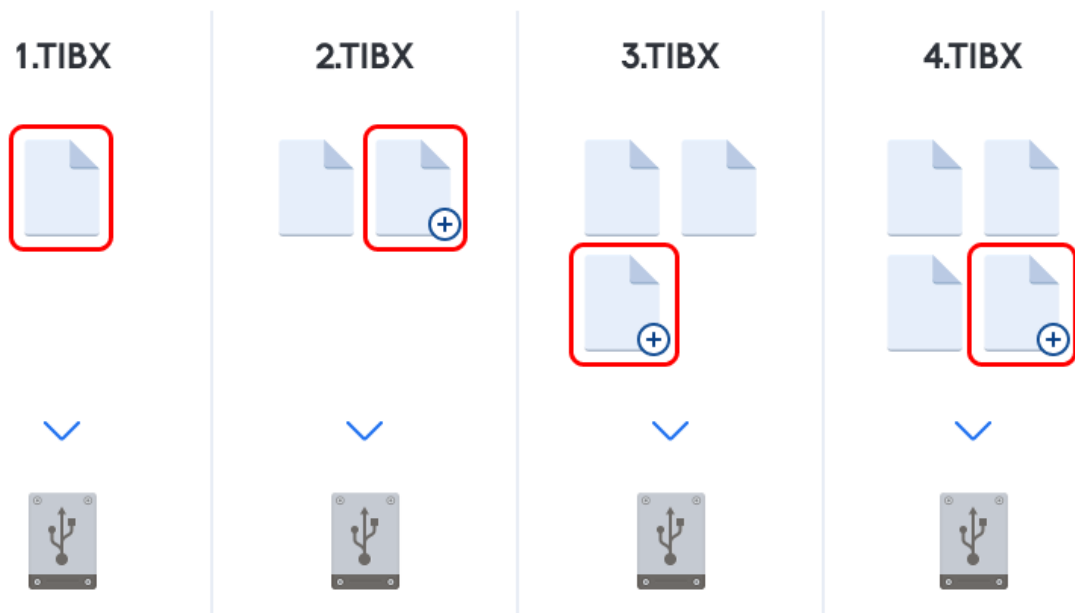
3.2.2 增量方式

增量方式备份操作(也称为增量备份版本)的结果仅包含自上次备份以来发生更改的所有文件。

示例: 每天, 您编写一页文档并使用增量备份方法将其备份。每次您运行备份时, Acronis Cyber Protect Home Office 都会保存该新页面。

注意: 您创建的第一个备份版本始终使用完整方式。

- 1.tibx — 完整备份版本的文件。
- 2.tibx、3.tibx、4.tibx — 增量备份版本的文件。



其他信息

如需多次备份的版本并要求能够及时返回到某个特定时间点，则增量方式最有用。通常，增量备份版本比完整备份或差异备份版本要小很多。另一方面，增量版本需要完成更多工作，程序才能提供恢复。

恢复: 在上面的示例中，要从 4.tibx 文件恢复整个工作，您要有所有备份版本 — 1.tibx、2.tibx、3.tibx 和 4.tibx。因此，如果某个增量备份版本丢失或损坏，之后的所有增量版本也将不可用。

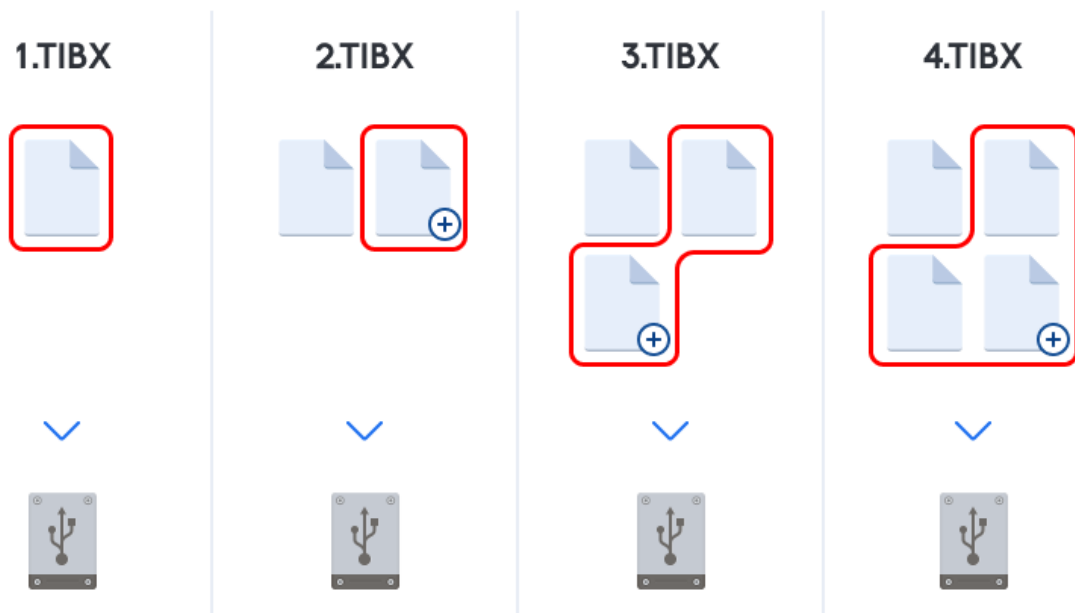
3.2.3 差异方式

差异方式备份操作(也称为差异备份版本)的结果仅包含自上次完整备份以来发生更改的所有文件。

示例: 每天，您编写一页文档并使用差异备份方法将其备份。Acronis Cyber Protect Home Office 会保存除完整备份版本中存储的第一页外的整个文档。

注意: 您创建的第一个备份版本始终使用完整方式。

- 1.tibx — 完整备份版本的文件。
- 2.tibx、3.tibx、4.tibx — 差异备份版本的文件。



其他信息

差异方式是介于两种方式之间的折中方式。它所需的时间和空间比“完整”备份少，但是比“增量”备份多。若要从差异备份版本恢复数据，Acronis Cyber Protect Home Office 只需要差异版本和上次完整版本。因此，从差异版本恢复比从增量版本恢复更简单、更可靠。

恢复: 在上面的示例中，要从 4.tibx 文件恢复整个工作，您需要有两个备份版本 — 1.tibx 和 4.tibx。若要选择所需备份方式，您通常需要配置自定义备份方案。如需更多信息，请参阅[自定义方案](#)。

注意

在磁盘进行碎片整理后创建的增量或差异备份，可能比正常情况大很多。这是因为碎片整理程序更改了磁盘上的文件位置，而备份会反映这些更改。因此，建议在磁盘碎片整理后重新创建完整备份。

3.2.4 块修改跟踪器 (CBT)

在创建本地增量或差异磁盘级备份版本时，CBT 技术可加快备份过程。系统会在块级别对磁盘内容进行的更改不断进行跟踪。当备份启动时，可以将更改立即保存到备份。

3.3 决定存储备份的位置

Acronis Cyber Protect Home Office 支持许多存储设备。有关详细信息，请参阅“支持的存储媒体”（第 14 页）。

下表显示了数据可能的备份目标位置。

	HDD*	SSD*	USB 闪存 驱动	Acronis Cloud	文件服务 器、NAS 或 NDAS	网 络 共	SMB	FTP	DVD	内 存 卡
--	-------------	-------------	--------------------------	--------------------------	----------------------------------	----------------------	------------	------------	------------	----------------------

			器			享				
MBR 分区或整个磁盘 (HDD、SSD)	+	+	+	+	+	+	+	+	+	+
GPT/动态卷或磁盘	+	+	+	+	+	+	+	+	+	+
文件与文件夹	+	+	+	+	+	+	+	+	+	+

*内部或外部。

虽然备份到本地硬盘驱动器是最简单的选项，但我们建议您异地存储备份，因为这可以增强数据安全性。

推荐的存储媒体：

1. Acronis Cloud

2. 外部驱动器

如果您想要将外置 USB 硬盘驱动器用于台式机，我们建议您使用一条短电缆将该驱动器连接至背面的连接口。

3. 家庭文件服务器、NAS 或 NDAS

在 Windows 中以及从可启动媒体启动时，请检查 Acronis Cyber Protect Home Office 是否检测到所选备份存储。

若要获取对已启动 NDAS 的存储设备的访问权限，在许多情况下，您需要指定 NDAS 设备 ID(20 个字符)和写入密钥(5 个字符)。写入密钥允许您以写入模式使用已启用 NDAS 的设备(例如，保存您的备份)。设备 ID 和写入密钥通常打印在标签上，该标签粘贴在 NDAS 设备的底部或位于外壳内侧。若未找到标签，您需要联系 NDAS 设备供应商以获取相关信息。

4. 网络共享

另请参阅：[验证设置](#)。

5. FTP 服务器

另请参阅：[FTP 连接](#)。

6. 可选光盘(CD、DVD 和 BD)

诸如 DVD-R 和 DVD+R 之类的空白光盘非常便宜，所以它们是您备份数据的最低成本解决方案，但速度也是最慢的。

当光盘数量超过三个时，需交换光盘，因此强烈建议避免备份到 DVD。若没有用于备份到 DVD 的备选方法，我们建议将所有 DVD 复制到硬盘上的文件夹中，然后从该文件夹恢复。

3.3.1 为备份准备一个新磁盘

Acronis Cyber Protect Home Office 可能无法识别一个新的内置或外接硬盘。如果出现这种情况，请使用操作系统工具将磁盘状态更改为**联机**，然后初始化磁盘。

将磁盘状态更改为“联机”

1. 打开**磁盘管理**。要进行此操作，请转到**控制面板 -> 系统和安全 -> 管理工具**，启动**计算机管理**，然后单击**磁盘管理**。
2. 找到标记为**脱机**的磁盘。右键单击磁盘，然后单击**联机**。
3. 磁盘状态将更改为**联机**。之后，您将能够初始化磁盘。

初始化磁盘

1. 打开**磁盘管理**。要进行此操作，请转到**控制面板 -> 系统和安全 -> 管理工具**，启动**计算机管理**，然后单击**磁盘管理**。
2. 找到标记为**未初始化的**的磁盘。右键单击磁盘，然后单击**初始化磁盘**。
3. 为磁盘选择一个分区表(MBR 或 GPT)，然后单击**确定**。
4. [可选步骤]要在磁盘上创建卷，请右键单击磁盘，单击**新建简单卷**，然后按照向导中的步骤配置新卷。要再创建一个卷，请重复此操作。

3.3.2 FTP 连接

Acronis Cyber Protect Home Office 允许您将备份存储在 FTP 服务器上。

要新建 FTP 连接，请在选定备份存储的同时单击**FTP 连接**，然后在打开的窗口中提供：

- FTP 服务器路径，例如：*my.server.com*
- 端口
- 用户名
- 密码

若要检查设置，请单击**测试连接**按钮。此时计算机将尝试连接到指定的 FTP 服务器。如果已建立测试连接，请单击**连接**按钮以添加 FTP 连接。

所创建的 FTP 连接将出现在文件夹树中。选择连接，浏览要使用的备份存储。

注意

请注意，仅打开 FTP 服务器的根文件夹是不会进入主目录的。

注意

对于直接从 FTP 服务器恢复的数据，备份所包含的每个文件的大小不得超过 2GB。

注意

因此，直接备份至 FTP 服务器时，Acronis Cyber Protect Home Office 会将备份分割为 2 GB 大小的文件。如果您备份至硬盘的目的在于稍后将备份传输至 FTP，则可在备份选项中设置所需文件大小，将备份分割为多个 2GB 大小的文件。

注意

FTP 服务器必须允许被动模式文件传输。

注意

源计算机的防火墙设置应该已为 TCP 和 UDP 协议打开端口 20 和 21, 这样才可使其正常工作。**路由和远程访问** 窗口服务应当被禁用。

3.3.3 验证设置

若正在连接至网络计算机, 在大多数情况下, 您必须提供访问网络共享所需的凭据。例如, 在您选择备份存储时就可能会出现这种情况。选择联网计算机的名称时, 将自动显示**验证设置**窗口。

如有必要, 请指定用户名和密码, 然后单击**测试连接**。成功通过测试后, 单击**连接**。

疑难解答

当您创建计划用作备份存储的网络共享时, 请确保至少满足以下条件之一:

- 在共享文件夹所在的计算机上, Windows 帐户有一个密码。
- 在 Windows 中关闭了密码保护的共享。

您可以在**控制面板** → **网络和 Internet** → **网络和共享中心** → **高级共享设置** → “关闭密码保护共享”中找到该设备。

否则, 您将无法连接到共享文件夹。

3.4 Acronis 不间断备份

Acronis 不间断备份让您可以轻松保护磁盘和文件。它允许您恢复整个磁盘、单个文件及其不同的版本。

Acronis 不间断备份的主要用途是提供连续的数据(文件、文件夹、联系人等)保护, 您也可以使用它保护分区。如果您选择保护整个分区, 则可以使用映像恢复程序恢复整个分区。

我们不建议使用不间断备份作为系统保护的主要方式。要确保系统安全, 请使用任何其他计划。有关范例和详细信息, 请参阅[自定义方案范例](#)。

3.4.1 不间断备份限制

- 您只能创建一个不间断备份。
- Acronis Cloud 不能用作磁盘级不间断备份的目标位置。
- 只能通过磁盘级不间断备份保护 Windows 库(文档、音乐等)。
- 您不能保护存储在外接硬盘上的数据。
- 不间断备份和 Try&Decide 不能同时工作。

3.4.2 工作方式

启动 Acronis 不间断备份时, 程序将对所选需要保护的数据执行初始完整备份。Acronis 不间断备份随后将不断监控受保护的文件(包括打开的文件)。一旦检测到修改, 便会备份更改的数据。增量备份操作的最短时间间隔为五分钟。这样允许您将系统恢复到精确的时间点。

Acronis 不间断备份在磁盘上检查文件更改,而非在内存中检查。例如,如果您在使用 Word 工作,并且很长时间未使用“保存”操作,那么将不会备份 Word 文档中的当前更改。

您可能会认为这样的备份速度会很快填满存储。不用担心,因为 Acronis Cyber Protect Home Office 将仅对被称作“增量”的数据备份。这表示系统只会备份旧版本与新版本之间的差异,而不会备份整个已更改的文件。例如,若您使用 Microsoft Outlook 或 Windows Mail,您的 pst 文件可能会非常大。此外,该文件会随着每次接收或发送邮件信息而更改。在每次更改之后备份整个 pst 文件将会对存储空间造成无法接受的浪费,因此 Acronis Cyber Protect Home Office 仅会备份在初始备份文件基础上所更改的部分。

3.4.3 保留规则

本地备份

Acronis 不间断备份将保留过去 24 小时内的所有备份。系统将对旧备份进行合并,方法是通过不间断备份保留过去 30 天的每日备份和每周备份,直至所有不间断备份数据目标位置空间占满。

合并将在每天午夜到凌晨 01:00 进行。首次合并将在不间断备份运行最少 24 小时之后开始。例如,您在 7 月 12 日上午 10:00 开启不间断备份。在这种情况下,首次合并将在 7 月 14 日的凌晨 00:00 到凌晨 01:00 进行,随后程序将在每天的同一时间合并数据。若计算机在凌晨 00:00 到凌晨 01:00 之间为关闭状态,合并将从计算机再次开启后启动。关闭不间断备份一段时间后,合并将在您再次开启后启动。

云备份

Acronis Cyber Protect Home Office 仅保留以下备份版本:

- 前一小时的所有版本
- 过去 24 小时内每一小时的第一个版本
- 前一周每一天的第一个版本
- 前一月每一周的第一个版本
- 每个月的第一个版本

系统会自动删除所有其他版本。保留规则已预先设置,无法更改。

3.4.4 Acronis 不间断备份数据存储

Acronis 不间断备份数据存储可在本地硬盘(内部和外接)或 Acronis Cloud 上创建。

在许多情况下,外接硬盘是不间断备份数据存储的最佳选择。您可以使用具有以下接口的外接磁盘:USB(包括 USB 3.0)、eSATA、FireWire 和 SCSI。

您还可以将 NAS 用作存储,但是有一个限制 — 必须使用 SMB 协议访问。要用于存储的 NAS 共享是否映射为本地磁盘并不重要。如果共享需要登录,则需要提供正确的用户名和密码。有关详细信息,请参见[身份验证设置](#)。Acronis Cyber Protect Home Office 会记住凭据且到共享的后续连接不需要登录。

如果没有外接硬盘或 NAS 可用,不间断备份的目标位置可能是内部磁盘(包括动态磁盘)。请注意,您不能将受保护的分区用作不间断备份存储。如果您的计算机只有一个包含一个分区的硬盘,但

您仍希望使用 Acronis 不间断备份,则可以创建 Acronis Secure Zone 并将其用作不间断备份数据存储。

在创建 Acronis 不间断备份数据存储之前,Acronis Cyber Protect Home Office 会检查选定目标位置是否有足够可用空间。它会将要保护的数据量乘以 1.2 并将计算出的值与可用空间进行比较。如果目标位置的可用空间满足此最低存储大小标准,则目标位置可用于存储不间断备份数据。

3.4.5 不间断备份 - 常见问题

为什么“Acronis 不间断备份”会自行暂停? - 这是为“Acronis 不间断备份”设计的行为。当系统负载升至临界水平时,“Acronis 不间断备份”将收到来自 Windows 的过载警报并自行暂停。此设计旨在帮助 Windows 减轻由其它应用程序带来的负载。运行占用大量资源的应用程序时(例如,用杀毒软件执行深度系统扫描时),可能会导致过载。

在这种情况下,“不间断备份”会自动暂停,并且无法重新启动。暂停后,“Acronis 不间断备份”会给系统 1 小时时间来减轻负载,然后尝试重新启动。

“Acronis 不间断备份”的自动重新启动计数为 6。这意味着,在首次尝试自动重新启动后,“Acronis 不间断备份”将继续再尝试重新启动 5 次,尝试之间的时间间隔为 1 小时。

在第 6 次尝试失败后,“Acronis 不间断备份”将等待下一个日历日。自动重新启动计数将在下一个日历日自动重置。如果没有干预,“Acronis 不间断备份”会每天尝试重新启动 6 次。

重新启动尝试计数可以通过以下任意方式重置:

- 重新启动“Acronis 不间断备份”服务
- 重新启动计算机。

重新启动“Acronis 不间断备份”服务仅会将重新启动计数重置为 0。如果系统仍然过载,“Acronis 不间断备份”将再次暂停。有关重新启动“Acronis 不间断备份”服务的信息,请访问 <https://kb.acronis.com/content/14708>。

重新启动计算机将重置负载和重新启动计数。如果系统再次过载,“Acronis 不间断备份”将暂停。

为何“Acronis 不间断备份”有时会导致 CPU 负载较高? - 这是“Acronis 不间断备份”的预期行为。如果大量受保护数据在暂停过程中被修改且重新启动了已暂停的“Acronis 不间断备份”,则会发生此种情况。

例如,如果您手动暂停用于保护系统分区的“Acronis 不间断备份”,然后安装一个新应用程序。当您重新启动“Acronis 不间断备份”时,它将在一段时间内占用大量 CPU 资源。但是,进程 (afcdpsrv.exe) 稍后将恢复正常。

之所以发生此种情况,是因为“Acronis 不间断备份”需要针对暂停过程中数据遭到修改的情况,检查已备份的数据,以确保保护的连续性。如果大量数据遭到修改,进程可能会在一段时间内占用大量 CPU 资源。待检查完成且备份所有已修改数据后,“Acronis 不间断备份”将恢复正常。

我可以在本地硬盘的 FAT32 分区上存储“Acronis 不间断备份”吗? - 可以, FAT32 和 NTFS 分区可用作存储。

我可以在网络共享或 NAS 上设置“Acronis 不间断备份”存储吗? - 可以,“Acronis 不间断备份”支持网络共享、映射驱动器、NAS 和其它网络附加设备,但是有一个限制,即它们必须使用 SMB 协议。

3.5 备份文件命名

根据创建备份的版本, 其名称将有所不同。

3.5.1 在 Acronis True Image(2020 或 2021) 和 Acronis Cyber Protect Home Office 中创建的备份文件的命名约定

备份文件名仅包含备份名称和一个增量计数器。它不包含任何其他信息, 例如备份方法、备份链编号、备份版本号或卷号。

备份名称如下所示:

1. my_documents.tibx
2. my_documents_0001.tibx
3. my_documents_0002.tibx
4. my_documents_0003.tibx

完整备份和差异备份存储在单独的文件中, 而增量备份将自动合并到完整备份中。

以下备份继续使用 TIB 格式和命名约定:

- 除 Acronis Cloud 外的所有目标位置的文件级备份。到 Acronis Cloud 的文件级备份采用 .tibx 格式。
- 不间断备份
- 公证备份
- 使用 CD/DVD/Blu-ray、FTP 或 "Acronis Secure Zone"(第 184 页) 作为备份目标位置的备份

3.5.2 Acronis True Image 2020 版本之前创建的备份文件的命名约定

TIB 备份文件名称具有以下属性:

- 备份名称
- 备份方法(full、inc、diff: 完整、增量、差异)
- 备份链¹数量(格式为 b#)
- 备份版本²数量(格式为 s#)
- 卷数量(格式为 v#)

例如, 当您将备份分割为若干个文件时, 此属性将会发生变化。有关详细信息, 请参阅[备份分割](#)。

¹最少两个备份版本序列, 包含第一个完整备份版本和后续的一个或多个增量或差异备份版本。备份版本链将持续到下一个完整备份版本(若有)。

²单次备份操作的结果。从物理角度看, 它是一份文件或文件集, 包含在特定日期与时间所备份数据的副本。由 Acronis Cyber Protect Home Office 创建的备份版本文件的文件扩展名为 .tibx。备份版本合并所生成的 TIBX 文件也称为备份版本。

因此, 备份名称可能如下所示:

1. my_documents_full_b1_s1_v1.tib
2. my_documents_full_b2_s1_v1.tib
3. my_documents_inc_b2_s2_v1.tib
4. my_documents_inc_b2_s3_v1.tib

如果您正在创建新备份, 且已有一个同名文件, 程序不会删除旧文件, 而是为新文件添加“数字”后缀, 例如 my_documents_inc_b2_s2_v1-2.tib。

3.6 与 Windows 集成

在安装过程中, Acronis Cyber Protect Home Office 提供与 Windows 的更紧密集成。这种合并使您能够充分利用您的计算机。

Acronis Cyber Protect Home Office 集成下列组件:

- Windows **开始**菜单上的 Acronis 项目
- 任务栏上的 Acronis Cyber Protect Home Office 按钮
- 快捷菜单命令

3.6.1 Windows“开始”菜单

开始菜单显示 Acronis 命令、工具和实用工具。您可以借此访问 Acronis Cyber Protect Home Office 功能, 而无需启动该应用程序。

3.6.2 任务栏上的 Acronis Cyber Protect Home Office 按钮

Windows 任务栏上的 Acronis Cyber Protect Home Office 按钮显示 Acronis Cyber Protect Home Office 操作的进度和结果。



3.6.3 任务栏通知中心

当 Acronis Cyber Protect Home Office 处于打开状态时, 您可以看到其中任何操作的状态。但是, 由于某些操作(例如备份)可能需要相当长一段时间, 因此无需让 Acronis Cyber Protect Home Office 来了解其结果。

任务栏通知中心将最新通知包含在一个位置, 让您可以看到重要的操作状态, 而无需在您需要查看时打开 Acronis Cyber Protect Home Office。以下通知会显示在 Acronis 任务栏通知中心: 有关备份操作结果的信息以及来自 Acronis Cyber Protect Home Office 的其他重要通知。任务栏通知中心处于最小化状态且隐藏在任务栏中的 Acronis Cyber Protect Home Office 下。

3.6.4 快捷菜单命令

要访问快捷菜单命令, 请打开文件资源管理器, 在选定的项目上单击鼠标右键, 指向 Acronis Cyber Protect Home Office, 然后选择命令。

- 要创建新的文件级备份, 请选择**新文件备份**。
- 要创建新的磁盘级备份, 请选择**新磁盘备份**。
- 要加载磁盘级备份(.tib 文件), 请选择**加载**。
- 要验证备份(.tib 文件), 请选择**验证**。

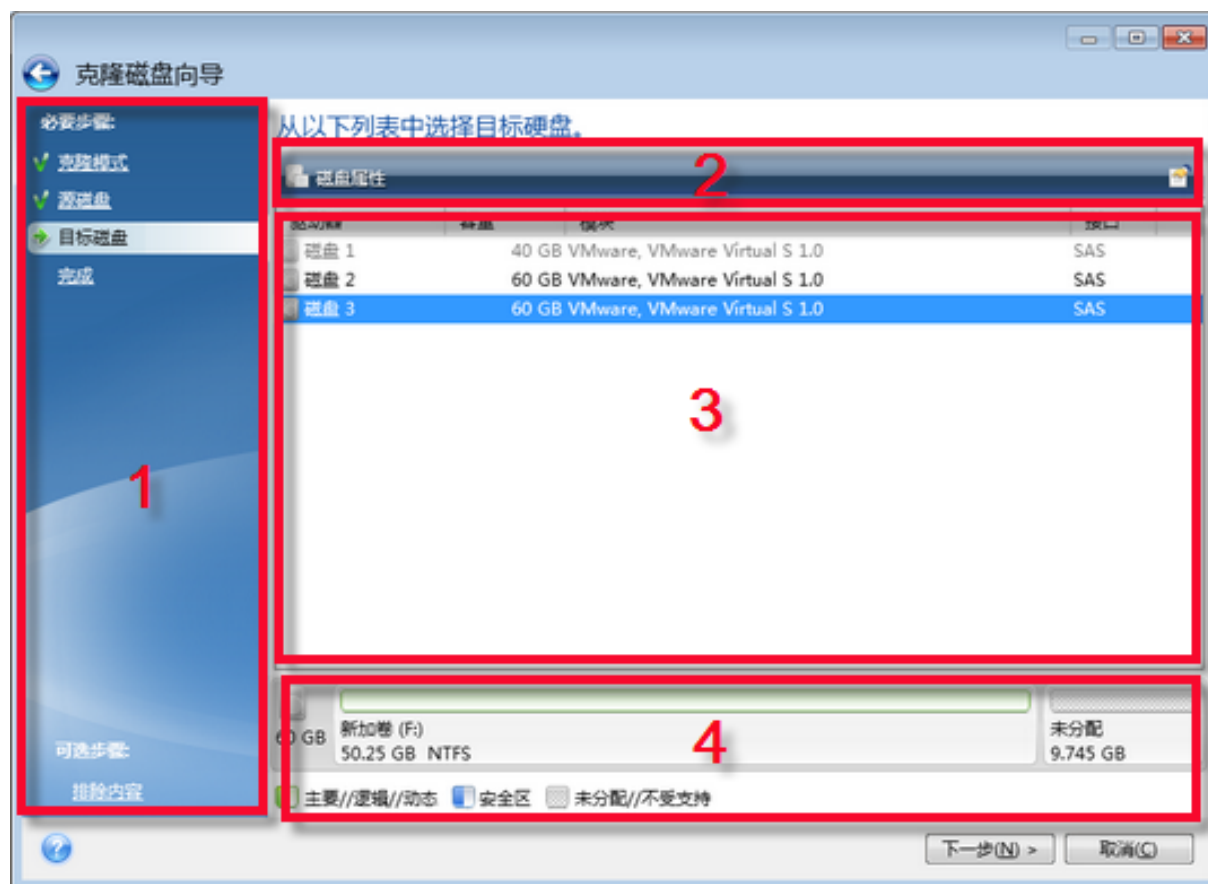
3.6.5 文件资源管理器中的文件级恢复

1. 在文件资源管理器中, 双击包含要恢复的数据的备份文件(.tib 文件)。
2. 将文件和文件夹复制或拖动到计算机上的任意位置, 就好像它们存储在普通磁盘上那样操作。





3.7 向导

使用可用的 Acronis Cyber Protect Home Office 工具与实用工具时, 在许多情况下, 程序将利用向导指导您完成所有操作。

例如, 参见以下屏幕截图。



向导窗口通常包含以下区域：

1. 这是完成操作所需的步骤列表。已完成的步骤旁边将显示绿色选中标记。绿色箭头指示当前步骤。当完成所有步骤后，程序将在**完成**步骤中显示“摘要”屏幕。检查摘要并单击**继续**以开始执行操作。
2. 该工具栏包含一些按钮，可用于管理区域 3 中所选择的对象。
例如：
 -  **详细信息** - 显示一个窗口，其中提供了关于所选备份的详细信息。
 -  **属性** - 显示一个窗口，其中包含所选项目的属性。
 -  **创建新分区** - 显示一个窗口，从中可以配置新的分区设置。
 -  **列** - 通过它可以选择要显示哪些表格列以及显示顺序。
3. 这是您可以在其中选择项目和更改设置的主区域。
4. 此区域将显示有关您在区域 3 中选择的项目的其他信息。

3.8 备份、恢复和克隆的常见问题

- **我有 150 GB 的系统分区，但该分区上占用的空间仅为 80 GB。Acronis Cyber Protect Home Office 会在备份中包含哪些内容？** - 默认情况下，Acronis Cyber Protect Home Office 仅复制包含数据的硬盘扇区，因此它只在备份中包含 80 GB 数据。您也可以选择逐个扇区模式。请注意，只有在特殊情况下才需要使用此备份模式。有关更多信息，请参阅[映像创建模式](#)。创建逐个扇区备份时，程序将同时复制已使用和未使用的硬盘扇区，备份文件通常大得多。
- **我的系统磁盘备份是否将包含驱动程序、文档和图片等？** - 是的，此备份将包含驱动程序，以及“我的文档”文件夹及其子文件夹的内容(如果您的默认位置保持为“我的文档”文件夹)。如果您的 PC 中仅有一个硬盘，此备份将包含所有操作系统、应用程序和数据。
- **我的笔记本电脑中的旧硬盘驱动器几乎已满。我买了一个容量更大的新 HDD。如何将 Windows、程序和数据传输到新硬盘？** - 您可在新硬盘上克隆旧硬盘，或备份旧硬盘然后将备份恢复到新硬盘。通常根据旧硬盘分区布局确定最适合您的方法。
- **我想要将旧系统硬盘迁移至 SSD。可以使用 Acronis Cyber Protect Home Office 完成这项操作吗？** - 可以，Acronis Cyber Protect Home Office 提供此项功能。有关步骤详细信息，请参阅[将系统从 HDD 迁移至 SSD](#)
- **将系统迁移至新磁盘的最佳方式：克隆还是备份与恢复？** - 备份与恢复方法的灵活性更强。在任何情况下，即使您决定使用克隆，我们都强烈建议对旧硬盘进行备份。如果克隆过程中原始硬盘出错，此备份将是您的数据保护程序。例如，用户选择了错误的磁盘作为其目标磁盘而擦除了系统磁盘。此外，您可创建多个备份，以实现冗余并提高安全性。
- **我应备份什么：分区还是整个磁盘？** - 在大多数情况下，最好备份整个磁盘。但在有些情况下建议备份分区。例如，您的笔记本电脑只有一个硬盘，而该硬盘有两个分区：系统(磁盘代号 C)和数据(磁盘代号 D)。系统分区将您的工作文档存储在“我的文档”文件夹及其子文件夹中。数据分区存储视频、图片和音乐文件。这些文件已被压缩，使用 Acronis Cyber Protect Home Office 备份这些文件不会显著减少备份文件的大小。但如果您的备份存储有足够的空间，我们建议创建至少一个完整磁盘备份。
- **是否可以告诉我如何克隆：在 Windows 中还是从 Acronis 可启动媒体启动后？** 即使您开始在 Windows 中执行克隆操作，计算机将和从 Acronis 可启动媒体启动一样重新启动进入 Linux 环境。因此，最好在 Acronis 可启动媒体下进行克隆。例如，有些情况下，在 Windows 中检测到的

硬盘驱动器在 Linux 中检测不到。如果这样，重启后克隆操作将会失败。从可启动媒体启动时，可确保在 Acronis Cyber Protect Home Office 检测到来源和目标磁盘后才开始执行克隆操作。

- **我能否克隆或备份并恢复双启动计算机？** 能，当两个操作系统均为 Windows 时可以这样做。如果您的系统安装在同一物理硬盘驱动器的不同分区，克隆或恢复操作通常不会出现任何问题。如果系统安装在不同的物理硬盘驱动器上，则恢复后启动时可能会出现一些问题。
- **Acronis Cyber Protect Home Office 是否支持 RAID？** - Acronis Cyber Protect Home Office 支持所有常见类型的硬件 RAID 阵列。还提供对动态磁盘上软件 RAID 配置的支持。Acronis 可启动媒体支持大多数常见硬件 RAID 控制器。如果标准 Acronis 可启动媒体未将 RAID“视作”单个卷，则表明该媒体没有相应的驱动程序。在这种情况下，您可以尝试创建基于 WinPE 的媒体。此媒体可能会提供必要的驱动程序。

4 备份数据

4.1 备份磁盘和分区

与文件备份相反，磁盘和分区备份包含磁盘或分区上存储的所有数据。此备份类型通常用于创建整个系统磁盘的系统分区的精确副本。此类备份允许您在 Windows 工作异常或无法启动时恢复计算机。

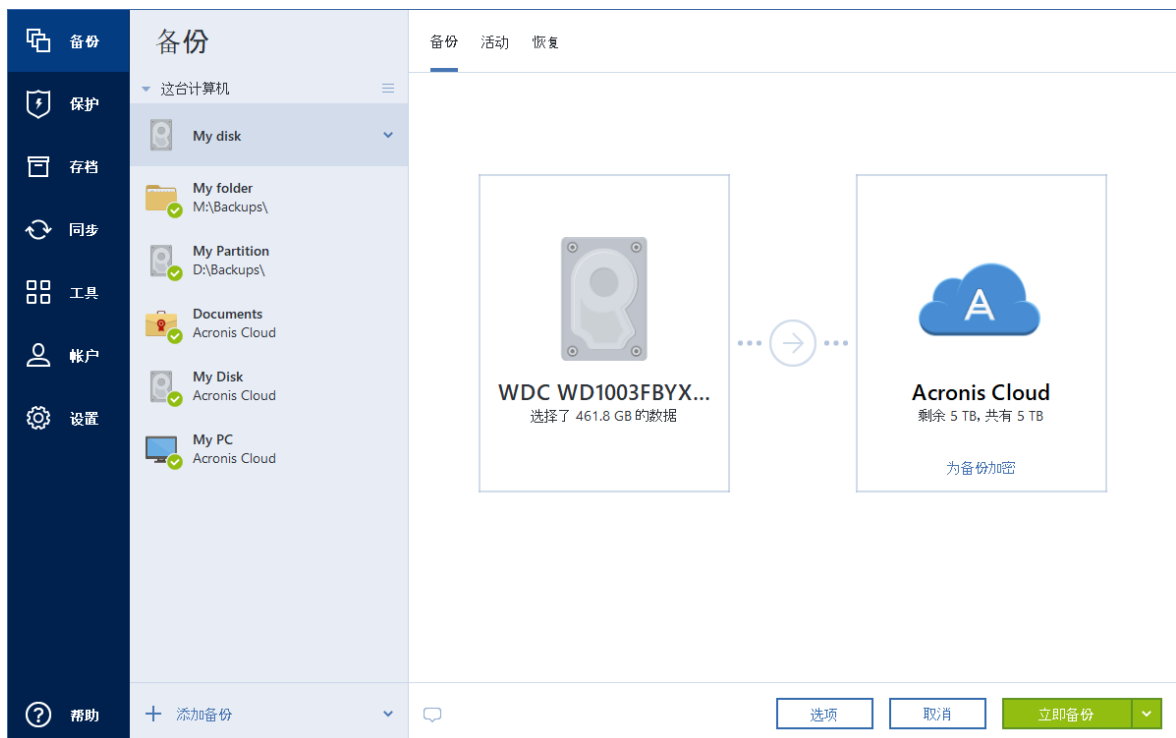
备份分区或磁盘

1. 启动 Acronis Cyber Protect Home Office。
2. 在侧栏上单击**备份**。
3. 单击**添加备份**。
4. [可选] 要重命名备份，请单击备份名称旁边的箭头，再单击**重命名**，然后输入新名称。
5. 单击**备份源区域**，然后选择**磁盘与分区**。
6. 在打开的窗口中，选中您要备份的分区和磁盘旁边的复选框，然后单击**确定**。

要查看隐藏的分区，请单击**完整分区列表**。

注意

若要备份动态磁盘，您只能使用分区模式。



7. 单击**备份目标位置区域**，然后选择一个备份目标位置：

- **Acronis Cloud** - 登录您的帐户，然后单击**确定**。

如果您没有 Acronis 帐户，请单击**创建帐户**，键入您的电子邮件地址、密码，然后单击**创建帐户**按钮。有关详细信息，请参阅 [Acronis 帐户](#)。

- **您的外接驱动器** - 当在计算机上插入外接驱动器时,您可以从列表中选择该项。
- **NAS** - 从找到的 NAS 设备列表选择一个 NAS。如果只有一个 NAS,默认情况下,Acronis Cyber Protect Home Office 会建议将其用作备份目标位置。
- **浏览** - 从文件夹树中选择一个目标位置。

注意

应尽量避免将系统分区备份存储在动态磁盘中,因为系统分区在 Linux 环境中恢复。Linux 和 Windows 使用动态磁盘的方式不同。这可能会导致在恢复过程中出现问题。

8. [可选步骤]单击**选项**以设置备份选项。有关更多信息,请参阅[备份选项](#)。
9. [可选步骤]单击**添加注释**图标,然后键入有关备份版本的注释。日后在恢复数据时,备份注释将有助于您找到所需版本。
10. 请执行以下任一操作:
 - 要立即运行备份,请单击**立即备份**。
 - 要稍后运行或定时运行备份,请单击**立即备份**按钮右侧的箭头,然后单击**稍后**。

注意

当您将数据备份至 Acronis Cloud 时,第一个备份可能会花费大量时间才能完成。进一步的备份过程可能会快得多,因为届时将仅通过互联网传输对文件的更改。

注意

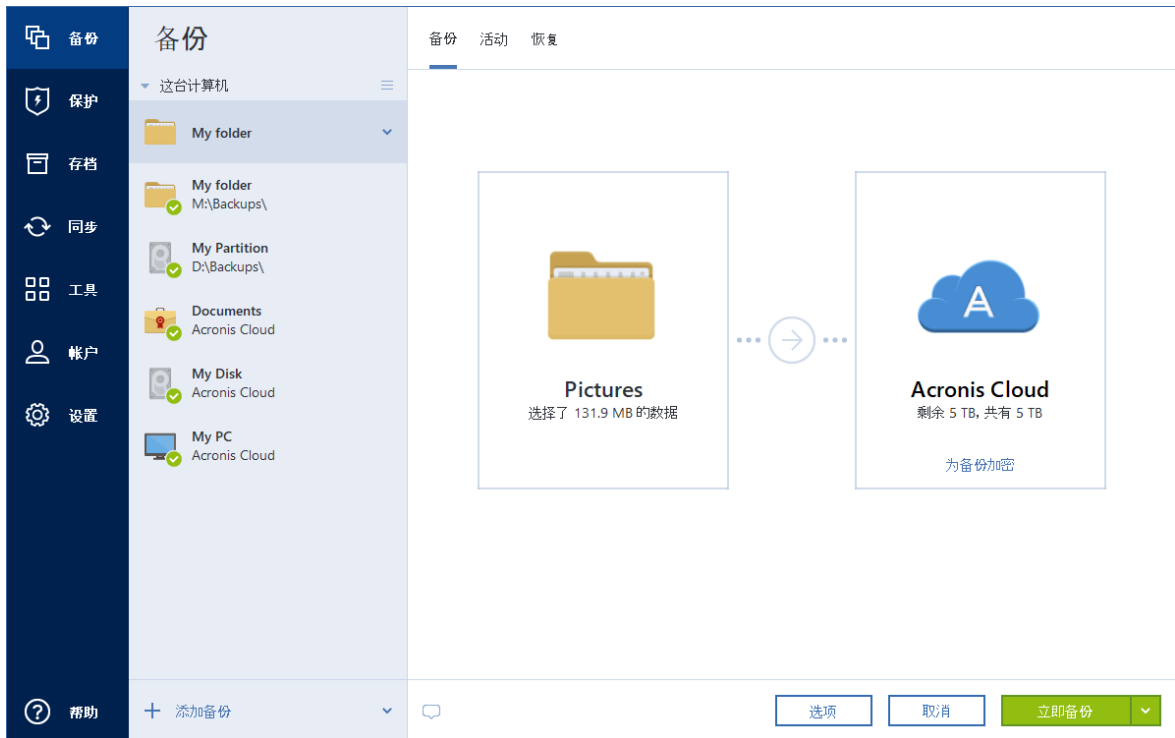
一旦启动线上备份,您便可以随意关闭 Acronis Cyber Protect Home Office。备份进程将在后台模式下继续进行。如果您暂停备份、关闭计算机或断开其与互联网的连接,当您单击“立即备份”或当互联网连接恢复时,备份将会继续。备份中断不会导致上载数据两次。

4.2 备份文件与文件夹

若要保护文档、照片、音乐文件和视频文件之类的文件,无需备份包含这些文件的整个分区。您可以备份特定文件和文件夹。

备份文件与文件夹

1. 启动 Acronis Cyber Protect Home Office。
2. 在侧栏上单击**备份**。
3. 单击**添加备份**。
4. [可选]要重命名备份,请单击备份名称旁边的箭头,再单击**重命名**,然后输入新名称。
5. 单击**备份源**区域,然后选择**文件与文件夹**。
6. 在打开的窗口中,选中您要备份的文件及文件夹旁边的复选框,然后单击**确定**。



7. 单击**备份目标位置**区域，然后选择一个备份目标位置：

- **Acronis Cloud** - 登录您的帐户，然后单击**确定**。
如果您没有 Acronis 帐户，请单击**创建帐户**，键入您的电子邮件地址、密码，然后单击**创建帐户**按钮。有关详细信息，请参阅 [Acronis 帐户](#)。
- **您的外接驱动器** - 当在计算机上插入外接驱动器时，您可以从列表中选择该项。
- **NAS** - 从找到的 NAS 设备列表选择一个 NAS。如果只有一个 NAS，默认情况下，Acronis Cyber Protect Home Office 会建议将其用作备份目标位置。
- **浏览** - 从文件夹树中选择一个目标位置。

8. [可选步骤] 单击**选项**以设置备份选项。有关更多信息，请参阅 [备份选项](#)。

9. [可选步骤] 单击**添加注释**图标，然后键入有关备份版本的注释。日后在恢复数据时，备份注释将有助于您找到所需版本。

10. 请执行以下任一操作：

- 要立即运行备份，请单击**立即备份**。
- 要稍后运行或定时运行备份，请单击**立即备份**按钮右侧的向下箭头，然后单击**稍后**。

注意

当您将数据备份至 Acronis Cloud 时，第一个备份可能会花费大量时间才能完成。进一步的备份过程可能会快得多，因为届时将仅通过互联网传输对文件的更改。

此外，请观看位于 <https://goo.gl/i4J1AN> 的英语视频说明。

4.3 备份移动设备

如果您拥有 iOS 或 Android 智能手机，可以使用 Acronis Cyber Protect Home Office 保护移动数据，例如照片、视频文件、联系人和日历。有关详细信息，请参阅 [Acronis Mobile](#)。

在开始备份之前，选择要将备份存储到的位置：Acronis Cloud 或您计算机上的本地存储。您可以稍后更改目标，但是不能同时备份至两个目标。要将数据备份到 Acronis Cloud，请使用 Acronis Mobile 应用程序。有关详细信息，请参阅“将移动设备备份至 Acronis Cloud”。

将移动数据备份至计算机上本地存储的方法

1. 确保：
 - 已在您的计算机上安装 Acronis True Image(2017 或更高版本) 或者 Acronis Cyber Protect Home Office。
 - 已在您的移动设备上安装 Acronis Mobile 应用程序。
 - 您的移动设备和计算机已连接到相同的 Wi-Fi 网络。
2. 在您的计算机上：
 - a. 启动 Acronis True Image(2017 或更高版本) 或者 Acronis Cyber Protect Home Office。
 - b. 在侧边栏上，单击**备份**，然后单击**添加备份**。
 - c. 单击**备份源**区域，然后选择**移动设备**。
此时将显示二维码。请勿关闭此窗口。
3. 在您的移动设备上：
 - a. 启动 Acronis Mobile。
 - b. 键入加号图标创建备份。请注意，在您第一次备份移动设备时不会出现此操作。
 - c. 选择计算机作为备份目标位置。
 - d. 轻击**扫描 QR 代码**，使摄像头对准计算机屏幕上的 QR 代码，然后等到移动设备连接到计算机。
 - e. 选择要备份的数据类别，或如果要备份所有数据，则点击**确认**。
 - f. 允许 Acronis Mobile 访问您的个人数据。
 - g. [可选步骤]您还可以通过密码加密备份并予以保护。否则，点击**跳过加密**。
 - h. 点击**开始备份**。

备份开始后，您可以在任意应用程序中(在计算机或移动设备上)跟踪进度，但是错误和警告消息仅显示在移动应用程序中。

您可以将计算机上的 Acronis Cyber Protect Home Office 和 Acronis Mobile 应用程序都关闭。备份将在后台模式下继续进行。

如果您希望自动备份数据更改(如新照片)，请确保打开**连续备份**设置。如果此设置处于关闭状态，则仅当您轻击**备份**时才会备份新数据。有关详细信息，请参阅[移动应用程序设置](#)。

在将移动备份目标位置从本地存储更改为 Acronis Cloud 时，移动设备与计算机之间的连接将会丢失，并且 Acronis Cyber Protect Home Office 会停止将列表中的移动备份与移动设备相关联。之后，如果您想要将目标位置更改回本地存储，则需要恢复此连接。由于发生错误，连接也可能丢失。要恢复连接，请在 Acronis Cyber Protect Home Office 的备份列表中选择移动备份，点击**重新连接**，然后使用您的移动设备扫描二维码。完成该操作后，备份将使用相同的设置正常继续。

4.3.1 Acronis Mobile

注意

您所在的地区可能无法使用 Acronis Cloud。有关更多信息，请单击此处：<https://kb.acronis.com/content/4541>

Acronis Mobile 支持您将数据备份到 Acronis Cloud、备份到您计算机上的本地存储，那么在丢失或损坏的情况下即可恢复数据。请注意，备份到云存储需要 Acronis 帐户和 Acronis Cloud 订购许可。

有关 Acronis Mobile 主要功能和支持的设备的详细信息，请参阅 [Acronis Mobile 文档](#)。

可在何处获取这些应用程序？

您可以查看其他信息并从 Apple App Store 或 Google Play 下载 Acronis Mobile：

- 适用于 iOS 设备的 Acronis Mobile：<https://go.acronis.com/atimobile/download/iOS>
- 适用于 Android 设备的 Acronis Mobile：<https://go.acronis.com/atimobile/download/Android>

4.3.2 移动备份的本地目标位置

将移动数据备份到计算机时，Acronis Mobile 会将备份存储到默认文件夹 `C:\ProgramData\Acronis Mobile Backup Data\acronis-local-data\` 中。更改默认文件夹时，`acronis-local-data` 文件夹将移至您选择的位置。所有新的移动数据都将备份到新的位置。

注意

所有移动备份将始终存储到相同的文件夹并且无法单独存储。

更改移动备份的本地目标位置

1. 在侧边栏上单击 **设置**，找到 **移动备份位置** 选项。
2. 在 **移动备份位置** 部分中，单击 **更改**。此时将显示 **更改位置** 窗口。
3. 单击 **选择位置**，然后为备份选择新位置。请注意，您只可以选择内置硬盘上的位置。

要将新位置更改为初始位置，请单击 **重置为默认值**。

4.4 备份 Office 365 数据

4.4.1 为何备份 Office 365 数据？

尽管 Microsoft Office 365 for Home 是一组云服务，常规备份可以提供更深层次的保护以免受用户错误和恶意软件行为的侵害。通过将 Microsoft Outlook 邮箱和 Microsoft OneDrive 数据备份到安全的 Acronis Cloud，Acronis Cyber Protect Home Office 可以对它们进行保护。在将内容上传到 Acronis Cloud 后，可以随时从任何设备访问所有内容。即使 Office 365 保留时期已过，仍可以从备份中恢复删除的项目。

4.4.2 备份 Office 365 数据

Outlook 邮箱中可以备份的数据包括：

- 所有文件夹
- 电子邮件
- 附件

注意

您无法备份共享邮箱或分组邮箱。

OneDrive 中可以备份的数据包括：

- 所有文件与文件夹

备份 Office 365 数据的步骤：

1. 通过执行以下操作之一，打开在线控制面板：
 - 访问以下链接：<https://cloud.acronis.com>。
 - 在 Acronis Cyber Protect Home Office 的侧栏上，单击**备份**，接着单击**添加备份**，再单击**备份源**区域，然后选择**云服务**。
2. 登录您的 Acronis 帐户。
3. 在侧边栏上，单击**资源**，再单击**添加**，然后选择 **Microsoft Office 365 for Home**。
4. 登录您的 Microsoft 帐户(如果出现提示)。
5. 在**备份源**区域，选择要备份的项目：
 - 整个帐户
 - Outlook
 - OneDrive
6. 单击**完成**。
7. 可以通过**清理**窗格为备份配置清理规则。您还可以通过密码加密备份并予以保护。完成后，单击**应用**。
8. 要启动备份，请单击**立即运行**。

4.5 备份选项

创建备份时，您可以更改其他选项并微调备份流程。要打开选项窗口，请选择备份的源位置和目标位置，然后单击**选项**。

注意，每种备份类型(磁盘级备份、文件级备份、线上备份、不间断备份)的选项是完全独立的，您应分别对其进行配置。

安装应用程序后，所有选项均设置为初始值。您只能更改当前备份操作或今后创建的所有备份的初始值。选择**另存为默认设置**复选框，以在默认情况下将修改的设置应用于所有后续备份操作。



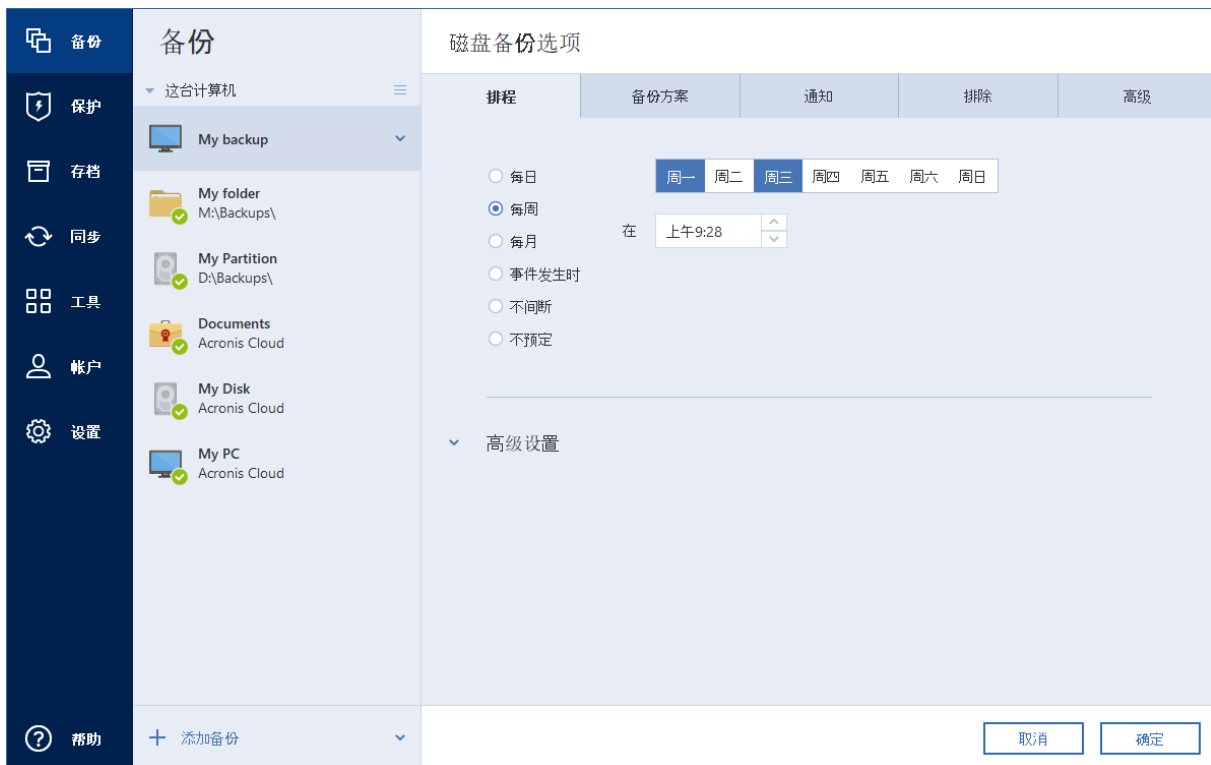
若要将所有修改的选项重置为安装产品之后初次设置的值，请单击**重置为初始设置**按钮。注意，这将仅针对当前备份重置设置。要针对以后所有的备份重置设置，请单击**重置为初始设置**，选中**将设置保存为默认设置**复选框，然后单击**确定**。

此外，请观看位于 <https://goo.gl/bKZyaG> 的英语视频说明。

4.5.1 计划

位置：**选项 > 计划**

计划选项卡允许您指定备份和验证计划设置。



您可以为定期创建或验证的备份指定预定：

- **每日** - 每天执行一次操作或更频繁。
- **每周** - 每周一次或在选定的多个日期每周多次执行操作。
- **每月** - 每月一次或在选定的多个日期每月多次执行操作。
- **事件发生时** - 事件发生时执行操作。
- **不间断** - 每五分钟运行一次操作。
- **不预定** - 系统将会针对当前操作关闭预定程序。在此情况下，仅当分别单击主窗口中的**立即备份**或**验证备份**时，才会运行备份或验证。

高级设置

单击**高级设置**允许您为备份和验证指定以下附加设置：

- **仅当计算机被锁定或屏幕保护程序正在运行时备份** — 选择此复选框以推迟预定操作，直到下次计算机未在使用中时(屏幕保护程序显示或计算机已被锁定)。对于验证预定，此复选框将更改为**仅当计算机空闲时运行验证**。
- **唤醒处于睡眠/休眠状态的计算机** — 选中此复选框以唤醒处于睡眠/休眠状态的计算机，从而执行预定操作。
- **防止计算机进入睡眠/休眠状态** — 选中此复选框以消除当计算机进入睡眠或休眠模式时耗时的备份被中断的情况。
- **系统启动时延迟运行错过的操作(分钟)** — 选中此复选框以便当计算机在预定时间关闭而使操作未执行时，强制计算机在下次系统启动时运行错过的操作。

此外，还可以设置系统启动后开始备份的延迟时间。例如，若要在系统启动 20 分钟后开始备份，请在相应的方框中输入 20。

- **当连接外部设备时运行错过的操作** [可选, 如果您预定备份到 USB 闪存驱动器或验证位于 USB 闪存驱动器上的备份] — 选中此复选框以便当系统在预定时间断开连接时, 在连接 USB 闪存驱动器后运行错过的操作。

每日备份参数

您可以为每日创建或验证的备份设置以下参数:

- **每隔** - 从下拉列表中选择每日周期(例如, 每隔 2 小时)。
- **一天一次** - 操作在一天的指定时间启动一次。
- **一天两次** - 操作一天启动两次。为两项操作的每一项选择时间。

有关**高级设置**的介绍, 请参阅[预定](#)。

每周备份参数

您可以为每周创建或验证的备份设置以下参数:

- **星期几** - 选择星期几来运行操作。
- **几时** - 选择操作开始时间。

有关**高级设置**的介绍, 请参阅[预定](#)。

每月备份参数

您可以为每月创建或验证的备份设置以下参数:

- **每** - 从下拉列表中选择数字和星期几。例如, 选择**每个月的第一个星期一**可在每个月的第一个星期一运行操作。
- **在每月选定的第几天** - 选择备份日期。例如, 您可能想在每月的第 10 天和最后一天运行操作。
- **几时** - 选择操作开始时间。

有关**高级设置**的介绍, 请参阅[预定](#)。

发生事件时执行操作参数

您可以为在发生某个事件时创建或验证的备份设置以下参数:

- **一天仅一次** - 若要仅在当天首次发生事件时运行操作, 请选中该复选框。
- 指定触发备份创建或验证的事件:
 - **连接外部设备时** - 每次将您以前用作备份目标位置的相同外部设备(USB 闪存驱动器或外部硬盘)插入计算机时, 该操作都将启动。注意, Windows 应该将此设备识别为外部设备。
 - **用户登录时** - 每次当前用户登录到操作系统时, 该操作都将启动。
 - **用户注销时** - 每次当前用户从操作系统注销时, 该操作都将启动。
 - **系统关闭或重新启动时** - 每次计算机关闭或重新启动时, 该操作都将启动。
 - **系统启动时延迟(分钟)** - 每个操作系统按照您指定的延迟时间启动时, 该操作都将启动。

有关**高级设置**的介绍, 请参阅[预定](#)。

4.5.2 备份方案

位置: **选项 > 备份方案**

备份方案和预定程序可帮助您设置备份策略。该方案可让您优化备份存储空间的使用、提高数据存储的可靠性并自动删除过时的备份版本。

注意

对于在线备份, 备份方案是预设的, 不可更改。进行初始完整备份后, 仅会创建增量版本。

备份方案定义了下列参数:

- 用于创建备份版本的**备份方式**(完整、差异或增量)
- 使用不同方法创建备份版本的顺序
- 版本清理规则



Acronis Cyber Protect Home Office 可让您选择以下备份方案:

- **单个版本方案** - 若要使用最小备份存储, 则选择此方案。
- **版本链方案** - 在多数情况下, 这可能是最佳方案。
- **增量方案** - 选择该项可在每五个增量版本后创建一个完整版本。该项为默认方案。
- **差异方案** - 选择该项可在创建原始完整备份后只创建差异备份。
- **自定义方案** - 选择该项可手动设置备份方案。

您可以轻松地为己存在的备份更改备份方案。这不会影响备份链的完整性, 所以您将能够从以前的任何备份版本恢复数据。

注意

备份至 DVD/BD 等光学媒体时,无法更改备份方案。在这种情况下,Acronis Cyber Protect Home Office 默认仅对完整备份使用自定义方案。这是因为该程序无法对光学媒体上存储的备份进行合并。

单一版本方案

该备份方案对于磁盘备份和文件备份类型相同(预定程序设置除外)。

每当根据指定计划或者当您手动运行备份时,程序都会创建一个完整的备份版本并将其覆盖。在此过程中,只有在创建新版本后才会删除旧版本。

注意

第一个文件将用于辅助目的,里面不包含数据。请不要删除它!

磁盘备份的备份预定程序设置:每月一次。

文件备份的备份预定程序设置:每日。

结果:您拥有单个最新的完整备份版本。

所需存储空间:最小。

版本链方案

该备份方案不同于磁盘备份和文件备份类型。

磁盘备份版本链

首先,程序会创建第一个完整备份版本。该版本将一直保留到您手动将其删除。之后,根据指定预定(或者当手动运行备份时)程序会创建:1个完整备份版本和5个差异备份版本,然后再创建1个完整备份版本和5个差异备份版本等依此类推。这些版本将会保存6个月。其后,程序将分析是否可以删除最旧的备份版本(第一个完整版本除外)。这取决于版本的最小数量(8)和版本链的一致性。使用同一备份方式创建新版本后,程序会依次删除最旧版本(例如,创建最新的差异版本后将删除最旧的差异版本)。首先将删除最旧的差异版本,然后删除最旧的完整版本。

备份预定程序设置:每月一次。

结果:您会拥有最近6个月的每月备份版本以及可能保留更长时间的初始完整备份版本。

所需存储空间:取决于版本数量及其大小。

文件备份版本链

根据指定计划(或当您手动运行备份时),程序将创建:1个完整备份版本和6个增量备份版本,然后再创建1个完整备份版本和6个增量备份版本等依此类推。这些版本将会保存1个月。其后,程序将分析是否删除最旧的备份版本。这取决于版本链的一致性。为保持一致性,程序会在创建新的类似版本链后按照“1个完整版本+6个增量备份版本”的形式删除最旧版本。

备份预定程序设置:每日。

结果:上个月里您每天都有备份版本。

所需存储空间:取决于版本数量及其大小。

自定义方案

您还可以使用 Acronis Cyber Protect Home Office 创建自己的备份方案。方案可基于预定义的备份方案。您可以更改选定的预定义方案以满足您的需求,然后将更改的方案另存为新方案。

注意

您不能覆盖现有的预定义备份方案。

此外,您还可以重新创建基于完整、差异或增量备份版本的自定义方案。

因此,首先请在相应的方框内选择一种备份方式。

- **完整**

如果只创建完整备份版本,则选择此方式。

- **增量**

如果要创建只包含完整备份版本和增量备份版本的备份链,则选择此方式。

可使用下列选项之一配置方案:

- **在初始完整版本之后只创建增量版本** - 选择此选项可只创建一个备份版本链。此选项不提供自动清理。
- **在每 [n] 个增量版本后创建完整版本** - 选择此选项可创建多个备份版本链。这是一个比较可靠但占用空间较大的备份方案。

- **差异**

如果要创建只包含完整备份版本和差异备份版本的备份链,则选择此方式。

可使用下列选项之一配置方案:

- **在初始完整版本之后只创建差异版本** - 选择此选项可只创建一个备份版本链。此选项不提供自动清理。
- **在每 [n] 个差异版本后创建完整版本** - 选择此选项可创建多个备份版本链。这是一个比较可靠但占用空间较大的备份方案。

打开自动清理

- **旧版本清理规则** - 若要自动删除过时的备份版本,您可设置下列清理规则之一:

- **删除 [n] 天之前的版本** [只适用于完整方式] - 选择此选项可限制备份版本的期限。指定时间段之前的所有版本将自动删除。
- **删除 [n] 天之前的版本链** [只适用于增量和差异方式] - 选择此选项可限制备份版本链的期限。仅当最旧版本链的最新备份版本早于指定的期间时,才会删除最旧版本链。
- **仅存储最近的 [n] 个版本** [仅适用于完整方式] - 选择此选项可限制备份版本的最大数量。当版本的数量超过指定值时,最旧的备份版本将会自动被删除。
- **仅存储最近的 [n] 个版本链** [仅适用于增量和差异方式] - 选择此选项可限制备份版本链的最大数量。当版本链的数量超过指定值时,最旧的备份版本链将会自动删除。
- **保持备份大小不超过 [定义大小]** [不适用于本地备份] - 选择此选项可限制备份的最大大小。创建新备份版本后,程序将检查总备份大小是否超过了指定值。如果超过,则会删除最旧的备份版本。

- **不删除备份的第一个版本** - 选中此复选框以保留初始数据状态。程序将创建两个初始完整备份版本。第一个版本将从自动清理中排除，一直存储到您手动删除它。如果选择增量或差异方式，第一个备份链将从第二个完整备份版本开始。且只有第三个备份版本才是增量或差异备份版本。请注意，如果为完整方式选中此复选框，**仅存储最近的 [n] 个版本**复选框将更改为**仅存储最近的 1+[n] 个版本**。

管理自定义备份方案

如果更改现有备份方案的任何内容，则可以将更改的方案另存为一个新方案。在此情况下，您需要为该备份方案指定一个新名称。

- 您可以覆盖现有的自定义方案。
- 您不能覆盖现有的预定义备份方案。
- 方案名称可使用操作系统允许的用于命名文件的任何符号。备份方案名称的最大长度为 255 个符号。
- 最多可创建 16 个自定义备份方案。

创建自定义备份方案后，配置备份时您可以将其用作任何其它现有的备份方案。

您还可以使用自定义备份方案而不保存它。在此情况下，该方案将只适用于创建它的备份，并且您无法将其用于其它备份。

如果不再需要自定义备份方案，可将其删除。要删除方案，请在备份方案列表中选择该方案，单击**删除**，然后在**删除方案**窗口中确认删除。

注意

预定义备份方案无法删除。

自定义方案示例

1. 整个 PC 备份“两个完整版本”

案例：您要使用两个完整版本保护计算机上的所有数据，并且要每月更新一次备份。现在我们看一下，如何使用自定义备份方案实现此目的。

1. 开始配置整个 PC 备份。有关详细信息，请参阅[备份 PC 上的所有数据](#)。
2. 确保选择“整个 PC”作为备份源。
3. 单击**选项**，打开**计划**选项卡，单击**每月**，然后指定每月几号（例如 20 号）。这样一来，每月将在您指定的日期创建一个备份版本。然后，指定备份操作的开始时间。
4. 打开**备份方案**选项卡，然后选择**自定义方案**而不是**增量方案**。
5. 在**备份方式**框中，从下拉列表中选择**完整**。
6. 要限制版本数量，请单击**存储不超过最近的 [n] 个版本**，键入或选择“2”，然后单击**确定**。
在这种情况下，程序将在每月 20 号创建一个新的完整版本。创建第三个版本后，将自动删除最旧的版本。
7. 检查所有设置是否正确，然后单击**立即备份**。如果要仅在预定程序中指定的时间运行首次备份，请单击**立即备份**按钮右侧的向下箭头，然后在下拉列表中选择**稍后**。

2. 文件备份“每日增量版本 + 每周完整版本”

案例:您有每天要处理的文件和/或文件夹。您需要保存每天的工作结果,并且希望能够将数据恢复到前三周中某一天的状态。现在我们看一下,如何使用自定义备份方案实现此目的。

1. 开始配置文件备份。有关详细信息,请参阅“备份文件与文件夹”。
2. 单击**选项**,打开**计划**选项卡,单击**每日**,然后指定备份操作的开始时间。例如,如果您晚上 8:00 完成日常工作,请指定以此时间或稍晚的时间(晚上 8:05)作为开始时间。
3. 打开**备份方案**选项卡,然后选择**自定义方案**而不是**增量方案**。
4. 在**备份方式**框中,从下拉列表中选择**增量**。
5. 单击**在每 [n] 个增量版本后创建一个完整版本**,然后键入或选择“6”。
在这种情况下,程序将首先创建初始完整备份版本(无论备份过程如何设置,首次备份版本将始终是完整版本),然后会逐日创建六个增量版本。然后,程序将再次创建一个完整版本和六个增量版本,以此类推。所以每周将创建一个新的完整版本。
6. 要限制版本的存储时间,请单击**开启自动清理**。
7. 单击**删除 [n] 天前的版本链**,键入或选择“21”,然后单击**确定**。
8. 检查所有设置是否正确,然后单击**立即备份**。如果要仅在预定程序中指定的时间运行首次备份,请单击**立即备份**按钮右侧的向下箭头,然后在下拉列表中选择**稍后**。

3. 磁盘备份“每两个月创建一次完整版本 + 每个月创建两个差异版本”

案例:您需要一个月中备份两次系统分区,并且每两个月创建一个完整备份版本。此外,您想使用不超过 100GB 的磁盘空间存储备份版本。现在我们看一下,如何使用自定义备份方案实现此目的。

1. 开始配置磁盘备份。请参阅 [备份磁盘和分区](#)。
2. 选择系统分区(通常是 C:)作为备份源。
3. 单击**选项**,打开**计划**选项卡,单击**每月**,然后指定比如每月 1 号和 15 号。这样一来,大约每两周创建一个备份版本。然后,指定备份操作的开始时间。
4. 打开**备份方案**选项卡,然后选择**自定义方案**而不是**增量方案**。
5. 在**备份方式**框中,从下拉列表中选择**差异**。
6. 单击**在每 [n] 个差异版本后创建一个完整版本**,然后键入或选择“3”。
在这种情况下,程序将首先创建初始完整备份版本(无论备份过程如何设置,首次备份版本将始终是完整版本),然后会创建三个差异版本,大约每两周创建一个。然后,会再次创建一个完整版本和三个差异版本,以此类推。这样,每两个月将创建一个新完整版本。
7. 要限制版本的存储时间,请单击**开启自动清理**。
8. 单击**保持备份大小不超过 [定义的大小]**,键入或选择“100 GB”,然后单击**确定**。

注意

当总备份大小超过 100 GB 时,Acronis Cyber Protect Home Office 将清理现有备份版本,以使剩余版本符合大小限制。程序将删除由一个完整备份版本和三个差异备份版本组成的最旧备份链。

9. 检查所有设置是否正确,然后单击**立即备份**。如果要仅在预定程序中指定的时间运行首次备份,请单击**立即备份**按钮右侧的向下箭头,然后在下拉列表中选择**稍后**。

4.5.3 备份操作的通知

位置: **选项 > 通知**

有时备份或恢复过程可能持续一小时或更长时间。当该过程完成时, Acronis Cyber Protect Home Office 可以通过电子邮件通知您。在操作过程中, 程序还可复制已发布的消息, 或在操作完成后发送完整的操作日志。

所有通知默认禁用。

可用磁盘空间阈值

您可能希望系统在备份存储上的可用空间小于指定阈值时向您发送通知。若在启动备份后, Acronis Cyber Protect Home Office 发现所选备份位置中的可用空间小于指定值, 程序将不会启动实际的备份进程, 并会立即显示相应的消息通知您这一情况。消息中将向您提供三种选择 - 忽略这一情况并继续备份操作、为备份浏览另一位置, 或取消备份。

若在备份运行时, 出现可用空间小于指定值的情况, 程序将显示相同的消息, 请您再次作出决定。

Acronis Cyber Protect Home Office 可对以下存储设备的可用空间进行监控: 本地硬盘、USB 卡和驱动器以及网络共享 (SMB)。对于 FTP 服务器和 CD/DVD 驱动器, 此选项将无法启用。

设置可用磁盘空间阈值

1. 选中**可用磁盘空间不足时显示通知消息**复选框。
2. 在**可用磁盘空间少于以下限值时通知我**框中输入阈值。

注意

若已在**错误处理**设置中勾选了**处理时不显示消息和对话框(无消息模式)**复选框, 则将不会显示此消息。

电子邮件通知

1. 选中**发送有关操作状态的电子邮件通知**复选框。
2. 配置电子邮件设置:
 - 在**收件人**字段中输入电子邮件地址。您可以输入多个地址, 并以分号隔开。
 - 在**服务器设置**字段中输入邮件发送服务器 (SMTP)。
 - 设置发送邮件服务器的端口。默认情况下, 端口设为 25。
 - 为电子邮件选择所需的加密。
 - 如果需要, 请选中 **SMTP 身份验证**复选框, 然后在相应的字段中输入用户名和密码。
3. 若要检查设置是否正确, 请单击**发送测试消息**按钮。

如果测试消息发送失败

1. 单击**显示扩展设置**。
2. 配置其他电子邮件设置:

- 在**发件人**字段中输入发件人的电子邮件地址。如果您不确定要指定哪个地址，请以标准格式键入所需的任何地址，例如 *aaa@bbb.com*。
- 视需要更改**主题**字段中的邮件主题。
要简化对备份状态的监控，您可以将最重要的信息添加到电子邮件的主题中。您可以键入以下文本标签：
 - %BACKUP_NAME% - 备份名称
 - %COMPUTER_NAME% - 在其中启动备份的计算机的名称
 - %OPERATION_STATUS% - 备份或其他操作的结果
 例如，您可以键入：*%BACKUP_NAME% 的备份状态:%OPERATION_STATUS% (%COMPUTER_NAME%)*
- 选中**登录传入邮件服务器**复选框并在其下输入传入邮件服务器 (POP3)。
- 设置接收邮件服务器的端口。默认情况下，端口设为 110。

3. 再次单击**发送测试邮件**按钮。

其它通知设置

- **操作成功完成时发送通知** - 选中此复选框以发送有关进程完成的通知。
- **操作无法完成时发送通知** - 选择此复选框以发送有关进程识别的通知。
- **需要用户互动时发送通知** - 选中此复选框以发送包含操作消息的通知。
- **添加完整日志至通知** - 选中此复选框以发送包含完整操作日志的通知。

注意

您将仅获得有关特定备份的电子邮件通知。如果要接收有关所有备份的通知，可以在在线控制面板中设置电子邮件通知。有关详细信息，请参阅[电子邮件通知](#)。两种方法彼此独立地工作，并且可以同时使用。

4.5.4 从备份中排除项目

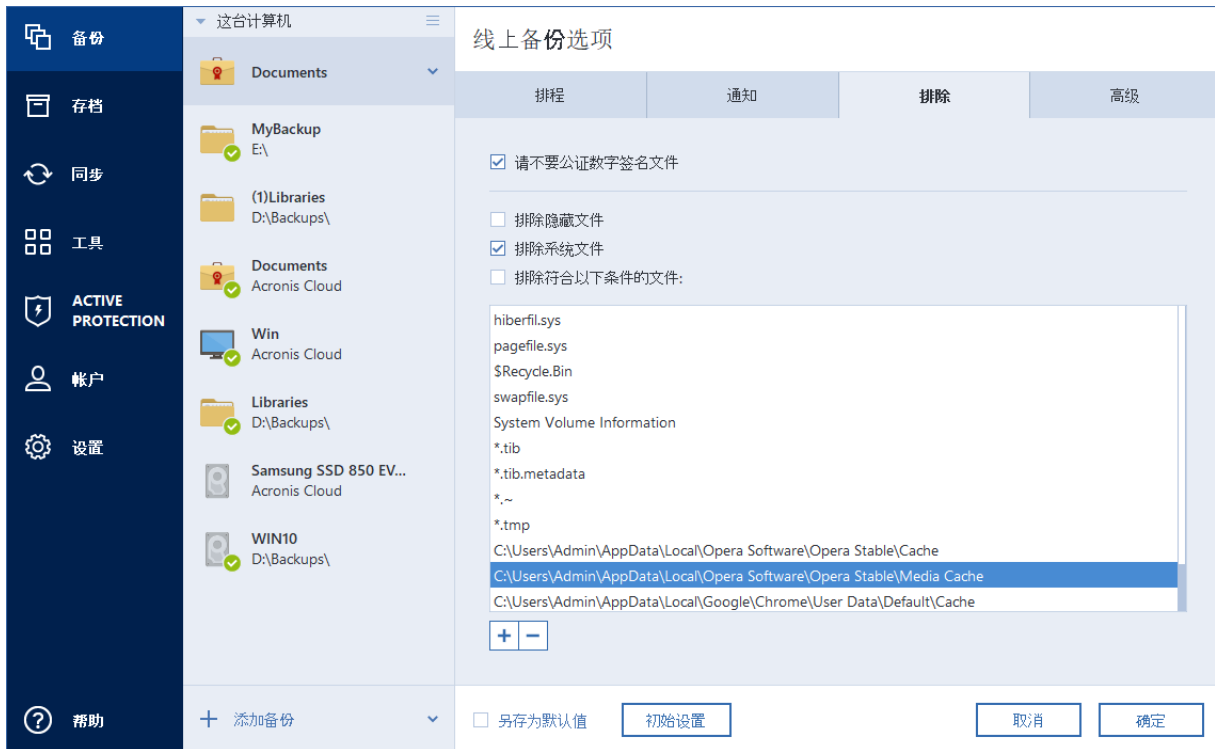
位置：**选项 > 排除**

若要从备份中排除不需要的文件，请在备份选项的**排除**选项卡上指定相应的文件类型。您可以指定磁盘备份、文件备份或者线上备份类型的排除。

如果为备份选择特定文件，则无法使用排除设置将其排除。排除设置仅适用于位于为备份选定的分区、磁盘或文件夹中的文件。

如何使用默认排除设置

安装应用程序后，所有排除设置均设置为初始值。您只能更改当前备份操作或今后创建的所有备份的初始值。选择**另存为默认设置**复选框，以在默认情况下将修改的设置应用于所有后续备份操作。若要将所有修改的设置重置为安装产品之后初次设置的值，请单击**重置为初始设置**按钮。



排除内容与方式

您可以通过以下选项从备份中排除文件：

- **请勿公证数字签名的文件** (仅适用于公证的备份) — 公证备份的主要目的是保护您的个人文件。因此，您无需备份系统文件、应用程序文件以及具有数字签名的其他文件。要排除这些文件，请选择相应的复选框。
- **排除隐藏文件** — 选择此复选框，可以从文件级备份中排除隐藏文件和文件夹。
- **排除系统文件** — 选择此复选框，可以从文件级备份中排除系统文件和文件夹。

您可以排除符合您指定标准的文件。若要执行此操作，请勾选**排除符合以下标准的文件**复选框，单击加号，然后输入排除标准。

注意

不建议从系统分区的备份中排除隐藏文件和系统文件。

添加排除标准

- 您可输入从备份中排除的显式文件名：
 - *file.ext* - 所有此类文件均会从备份中排除。
 - *C:\file.ext* - C 上的 *file.ext* 文件：排除磁盘。
- 您可以使用通配符 (*** 和 *?*)：
 - **.ext* - 将排除扩展名为 *.ext* 的所有文件。
 - *??name.ext* - 将排除扩展名为 *.ext*，且文件名(以任何两个符号 *??* 开头并以 *name* 结尾)为六个字母的所有文件。

- 要从磁盘级备份中排除某个文件夹, 请依次单击加号和省略号按钮, 转到目录树并选择您想要排除的文件夹, 最后单击**确定**。

要删除错误添加的标准, 请选择该标准, 然后单击减号。

4.5.5 映像创建模式

位置: **选项 > 高级 > 映像创建模式**

此选项不适用于使用 Acronis Cloud 作为备份目标位置的备份。

可使用这些参数创建整个分区或硬盘的精确副本, 而不仅是包含数据的扇区。例如, 这在您想备份包含 Acronis Cyber Protect Home Office 不支持的操作系统的分区或磁盘时会非常有用。请注意, 此模式会增加处理时间且通常会产生较大的映像文件。

- 要逐个扇区创建映像, 请选中**逐个扇区备份**复选框。
- 要将所有未分配的磁盘空间包括在备份中, 请选中**备份未分配空间**复选框。
此复选框仅在选中**逐个扇区备份**复选框时才可用。

4.5.6 备份保护

位置: “备份”仪表板 > **选项 > 高级 > 备份保护**

注意

本主题适用于本地和网络备份。有关保护云备份的信息, 请参阅[在线备份保护](#)。

默认情况下, 没有针对备份的密码保护, 但您可以配置密码以保护您的备份文件。

注意

您不能为现有的备份更改备份保护选项。

保护备份

1. 在相应的字段中输入备份的密码。建议您使用超过七个字符的密码, 可包含字母(最好是大小写相结合)和数字, 这样才不容易被猜中。

注意

密码不可检索。请记住您指定于备份保护的密码。

2. 要确认先前输入的密码, 请在相应的字段中重新键入该密码。
3. [可选步骤] 若要提升机密数据的安全性, 可以用强大的行业标准 AES(高级加密标准)加密算法对备份进行加密。AES 目前有三种密钥长度 - 128、192 和 256 位, 可根据需要来平衡性能和保护等级。

128 位加密密钥足以满足大多数应用程序的需要。密钥越长, 数据安全性越高。不过, 192 和 256 位长密钥会显著降低备份的速度。

若要使用 AES 进行加密, 请选择以下其中一种密钥:

- **AES 128** - 使用 128 位加密密钥
- **AES 192** - 使用 192 位加密密钥
- **AES 256** - 使用 256 位加密密钥

如果不想加密备份, 而只想使用密码保护备份, 请选择**无**。

4. 指定警告设置后, 单击**确定**。

如何访问受密码保护的备份

每次尝试修改备份时, Acronis Cyber Protect Home Office 都会要求提供密码:

- 从备份恢复数据
- 编辑设置
- 加载
- 移动

若要访问备份, 您必须指定正确的密码。出于安全原因, 无法恢复丢失的密码。

4.5.7 线上备份保护

位置: **选项 > 高级 > 备份保护**

为避免 Acronis Cloud 上的数据遭到未经授权的访问, 您可以使用加密。在这种情况下, 当您备份数据时, 将使用 AES-256 算法对数据进行加密, 然后保存到 Acronis Cloud。要对数据加密和解密, 程序需要您应该在配置线上备份时指定的密码。您可按照自己的意愿指定任意一组字符。请注意, 密码区分大小写。

警告!

线上备份的密码无法检索。请记住您为备份保护指定的密码。

试图访问加密数据时, 程序会要求您输入密码。

注意

请注意, 您不能为已存在的线上备份设置或更改密码。

4.5.8 备份前/后命令

位置: **选项 > 高级 > 事前/事后命令**

此选项不适用于使用 Acronis Cloud 作为备份目标位置的备份。

您可以指定要在备份前和之后将自动执行的命令(甚至批处理文件)。

例如, 您可能希望在开始备份前启动/停止某些 Windows 程序或检查数据。

指定命令(批处理文件)

- 选中**使用自定义命令**复选框。
- 在**命令前**字段中, 选择将要在备份程序开始前执行的命令。若要创建新命令或选择新的批处理文件, 请单击**编辑**按钮。

- 在**命令后**字段中,选择将要在备份程序结束后执行的命令。若要创建新命令或选择新的批处理文件,请单击**编辑**按钮。

请勿尝试执行交互命令,即要求用户输入的命令(例如,“暂停”)。系统不支持这些命令。

编辑用于备份的用户命令

您可以指定要在备份程序前后执行的用户命令:

- 在**命令**字段中键入命令,或从列表中选择命令。单击 **...**,以选择批处理文件。
- 在**工作目录**字段中键入执行命令的路径,或从先前输入的路径列表中选择路径。
- 在**参数**字段中输入命令执行参数,或从列表中选择。

禁用**命令执行完成后方执行操作**参数(默认为执行命令之前启用),将允许在执行命令的同时运行备份程序。

若**用户命令执行失败即中止操作**(默认为启用)参数会在命令执行出错时中止操作。

单击**测试命令**按钮测试您所输入的命令。

4.5.9 备份分割

位置:**选项 > 高级 > 备份拆分**

注意

Acronis Cyber Protect Home Office 不能拆分已存在的备份。仅可在创建时拆分备份。

此选项不适用于使用 Acronis Cloud 作为备份目标位置的备份。

大备份可拆分成几个文件,它们一起组成原始备份。单个备份也可以拆分,以便于刻录至可移动媒体。

默认设置 - **自动**。设置后,Acronis Cyber Protect Home Office 将进行以下操作:

备份至硬盘时:

- 若选定的硬盘拥有足够空间,并且其文件系统支持估计的文件大小,则该程序将创建一个单一备份文件。
- 若存储盘拥有足够空间,但其文件系统不支持预计的文件大小,则程序会自动将映像分割为几个文件。
- 若硬盘上没有足够的空间来存储映像,则程序会向您发出警告,并等待您做出如何处理此问题的决定。您可尝试释放一些多余空间,然后继续或另选一个磁盘。

备份到 CD-R/RW、DVD-R/RW、DVD+R/RW、BD-R/RE 上时:

- 会在上一个磁盘满后,Acronis Cyber Protect Home Office 会要求您插入新磁盘。

或者,您可以从下拉列表中选择所需文件大小。备份将拆分为指定大小的多个文件。这在将备份存储到硬盘,以便稍后将备份刻录到 CD-R/RW、DVD-R/RW、DVD+R/RW 或 BD-R/RE 上时,十分方便。

注意

在 CD-R/RW、DVD-R/RW、DVD+R/RW、BD-R/RE 上直接创建映像可能比在硬盘上创建映像慢得多。

4.5.10 备份验证选项

位置: **选项 > 高级 > 验证**

此选项不适用于使用 Acronis Cloud 作为备份目标位置的备份。

您可以指定以下设置：

- **每次完成备份后验证备份** - 选择该项可在备份后立即检查备份版本的完整性。我们建议您在备份关键数据或系统磁盘时启用此选项。
 - **仅验证最新相异备份版本** - 快速验证最新备份片断。
 - **验证整个备份**
- **按计划验证备份** - 选择该项可预定备份验证，以确保它们仍然“健康”。
 - **完成备份后的最新相异备份版本**
 - **完成备份后的整个备份**

默认设置如下：

- **频率** - 每月一次。
- **日期** - 备份开始的日期。
- **时间** - 备份开始时间加上 15 分钟。

您还可以从备份上下文菜单手动配置验证的启动。

要执行此操作，请在备份上单击鼠标右键，然后选择：

- **验证所有版本**
- **验证最新版本**

示例:您于 7 月 15 日 12:00 开始备份操作。备份版本创建于 12:05。如果您的计算机在此时处于“屏幕保护程序”状态，则验证将于 12:15 运行。如果不是，则验证不会运行。一个月之后的 8 月 15 日 12:15，验证将再次开始。跟以前一样，您的计算机必须处于“屏幕保护程序”状态。同样的操作将发生在 9 月 15 日，以后依此类推。

您可以更改默认设置并指定自己的方案。如需更多信息，请参阅[预定](#)。

4.5.11 备份保留副本

位置: **选项 > 高级 > 备份保留副本**

此选项不适用于使用 Acronis Cloud 作为备份目标位置的备份，适用于在 Acronis True Image(2020 或 2021) 和 Acronis Cyber Protect Home Office 中创建的本地备份。

备份保留副本是正常备份后系统立即创建的一个独立完整的备份版本。即使在您创建仅包含数据变化的增量或差异备份版时，保留副本也会包含正常备份的所有选择数据。您将可以把备份的保留副本存储在文件系统、网络驱动器或 USB 闪存驱动器上。

注意

请注意, CD/DVD 不可用作保留副本的位置。

创建保留副本

1. 选择**创建我的备份保留副本**复选框。
2. 指定备份副本的位置。
3. 选择保留副本格式。您可以将其创建为 Acronis 备份(.tib 文件),也可以将源文件复制到原来的选定位置,而不进行任何修改。
4. [可选步骤]使用密码保护保留副本。
该副本将会继承源备份的所有其他备份选项。

4.5.12 可移动媒体设置

位置: **选项 > 高级 > 可移动媒体设置**

备份到可移动媒体时,将其他组件写入该媒体便可使其成为可启动媒体。因此,不需要单独的可启动磁盘。

警告!

如果闪存驱动器格式化为 NTFS 或 exFAT,则 Acronis Cyber Protect Home Office 不支持创建可启动媒体。该驱动器必须具有 FAT16 或 FAT32 文件系统。

可使用下列设置:

- **在媒体上放置 Acronis Cyber Protect Home Office** - 我们强烈建议选择此选项以支持 USB、PC 卡(以前称为 PCMCIA)和 SCSI 接口以及通过它们连接的存储设备。
- **在媒体上放置 Acronis Cyber Protect Home Office(64 位)** - 适用于 64 位系统的相同选项。
- **在媒体上放置 Acronis 系统报告** - 选择该选项后,可在程序出现任何问题时,生成用于收集系统相关信息的系统报告。在从可启动媒体启动 Acronis Cyber Protect Home Office 前,可生成报告。生成的系统报告可保存至 USB 闪存驱动器。
- **在媒体上放置 Acronis 系统报告(64 位)** - 适用于 64 位系统的相同选项。
- **在可移动媒体上创建备份时要求使用第一个媒体** - 选择该选项后,在备份到可移动媒体时将会显示**插入第一个媒体**提示。使用默认设置(选项处于选中状态)时,由于程序须等待用户单击提示框中的**确定**,因此,用户不在时,将无法备份至可移动媒体。因此,在执行定时备份以备份到可移动媒体时,应禁用提示。接着,若有可用的可移动媒体(例如已插入 CD-R/RW),此备份即可在无需用户介入的情况下自动运行。

若您的计算机上已安装了其他 Acronis 产品,则这些程序组件的可启动版本也会提供。

32 位或 64 位组件

请注意哪些 Acronis Cyber Protect Home Office 和 Acronis 系统报告版本与您的计算机兼容。

	32 位组件	64 位组件
--	---------------	---------------

基于 BIOS 的 32 位计算机	+	-
基于 BIOS 的 64 位计算机	+	+
基于 EFI 的 32 位计算机	+	-
基于 EFI 的 64 位计算机	-	+

4.5.13 错误处理

若 Acronis Cyber Protect Home Office 在执行备份的过程中发生错误，它会停止备份进程并显示相关消息，等待做出如何处理错误的响应。您可以配置错误处理策略，以便 Acronis Cyber Protect Home Office 不会停止备份进程，而是会依据已设置的规则处理错误，然后继续操作。

注意

此主题适用于使用本地或网络备份目标位置的备份。对于使用 Acronis Cloud 作为备份目标位置的备份的错误处理选项，请参阅 [Cloud 备份和副本的错误处理](#)。

要设置错误处理策略，请执行以下操作：

1. 在“备份”仪表板 > 选项 > 高级 > 错误处理上
2. 设置错误处理策略：

- **处理时不显示消息和对话框(无消息模式)**- 启用此设置，可在创建备份时忽略错误。这在您无法控制备份流程时非常有用。
- **忽略损坏的扇区**- 此选项只对磁盘和分区备份可用。选择此选项即可成功完成备份，即使硬盘上有损坏的扇区。
在硬盘功能出现问题时，建议您选中此复选框，例如：
 - 在操作中，硬盘发出滴答声或研磨声。
 - S.M.A.R.T. 系统检测到硬盘驱动器问题，并建议您尽快备份该硬盘驱动器。
 如果您未选中此复选框，备份可能会由于硬盘上可能的损坏扇区而失败。
- **ASZ 空间不足时将删除最旧的备份**(默认情况下处于启用状态) — 在计划将无人参与的预定备份保存到 Acronis Secure Zone 中时，建议选中此复选框。否则，如果在备份操作期间 Acronis Secure Zone 已满，则 Acronis Cyber Protect Home Office 会暂停备份并要求您采取措施。该对话框在已启用 **处理时不显示消息和对话框(无消息模式)** 设置的情况下仍将会显示。
- **如果备份失败则重复尝试** - 此选项允许您在由于某种原因备份失败时自动重复备份尝试。您可以指定尝试次数和尝试时间间隔。注意，如果中断备份的错误持续出现，将不会创建备份。

注意

直到完成所有尝试，才会启动预定的备份操作。

3. 单击**确定**。

Cloud 备份和副本的错误处理

您可以配置 Acronis Cyber Protect Home Office，以便在向 Cloud 执行备份和复制失败时重新尝试该操作。

要配置重试尝试次数以及两次尝试之间的时间间隔，请执行以下操作：

1. 在**备份**仪表板上，单击到 Cloud 的备份，再单击**选项**，然后转到**高级**选项卡。
2. 在**错误处理**下，选中**如果备份失败则重复尝试**复选框，然后选择尝试次数(1 到 99) 以及两次尝试之间的时间间隔。
3. 单击**确定**。

新设置将应用于选定备份对象向 Cloud 执行的所有后续备份和复制操作。

注意

直到完成重复备份的所有尝试，才会启动预定的备份操作。

4.5.14 备份的文件级安全设置

位置: **选项 > 高级 > 文件级别安全设置**

注意

此选项仅对文件级备份可用。

此选项不适用于使用 Acronis Cloud 作为备份目标位置的备份。

您可以指定备份文件的安全性设置：

- **在备份中保留文件的安全设置** - 选择此选项可保留备份文件的所有安全属性(分配给组或用户的权限)，以便进一步予以恢复。
默认情况下，文件和文件夹将连同它们的 Windows 初始安全设置(即，在文件**属性** -> **安全**中设置的各用户或用户群组的读取、写入、执行等权限)一并保存到备份。若在计算机上恢复安全文件/文件夹时未在权限中指定用户，您可能将无法读取或修改此文件。
若要消除此类问题，可禁用“在备份中保留文件的安全设置”。这样，经恢复的文件/文件夹将始终从其恢复到的文件夹继承权限(若恢复至根目录，则为父文件夹或磁盘)。
或者，也可以在恢复时禁用文件安全设置，即使这些设置在备份中可用。结果一样。
- **将加密文件以解密状态存储于备份中(预设禁用)** - 若备份中有加密文件，且您希望其在恢复后可供任何用户访问，则请选择此选项。否则，只有加密此文件/文件夹的用户方可读取。若要恢复另一计算机上的加密文件，解密也可能很有用。
若不使用 Windows XP 及更高版本操作系统提供的加密功能，忽略此选项即可。(文件/文件夹加密可在**属性** -> **常规** -> **高级属性** -> **加密内容以保护数据**中进行设置)。

4.5.15 计算机关机

位置: **选项 > 高级 > 计算机关机**

您可以配置以下选项：

- **关闭计算机时停止所有当前操作** - 如果在 Acronis Cyber Protect Home Office 长时间执行一项操作(例如磁盘备份到云)时关闭计算机，此操作会阻止计算机关闭。如果选中此复选框，Acronis Cyber Protect Home Office 会自动在关机之前停止所有当前操作。这可能需要大约两分钟时间。下次您运行 Acronis Cyber Protect Home Office 时，它将重新开始已停止的备份。

- **备份完成后关闭计算机** - 如果您配置的备份进程可能需要很长时间, 请选择该选项。这样您就不必一直等到操作完成。程序将执行备份并在完成后自动关闭计算机。

此选项在预定备份时同样有用。例如, 您可能希望在工作日的晚上执行备份以保存所有工作。预定备份并选中该复选框。当您完成工作后可以离开, 因为您知道计算机将备份关键数据并在完成后关闭。

4.5.16 备份操作的性能

到本地目标位置的备份的位置: **选项 > 高级 > 性能**

到 Acronis Cloud 的备份的位置: **选项 > 高级 > 性能和网络**

压缩级别

可选择的备份压缩级别:

- **无** — 不压缩数据而直接复制, 这会大大增大备份文件大小。
- **一般** — 建议使用此数据压缩级别(默认设置)。
- **高** — 较高的备份文件压缩级别, 创建备份需要更长时间。
- **最高** — 最高的备份压缩级别, 创建备份需要很长时间。

注意

最佳数据压缩级别视备份中的文件类型而定。例如, 若备份中包含已压缩的文件, 如 .jpg、.pdf 或 .mp3, 则即使采用最高压缩级别也无法明显减小备份的大小。

注意

您不能为已存在的备份设置或更改压缩级别。

操作优先级

更改备份或恢复进程的优先级会加快或减慢运行速度(视您提升还是降低优先级而定), 但也会对其他运行中的程序的性能产生负面影响。系统中运行的任何进程的优先级可决定分配给该进程的 CPU 使用量和系统资源。降低操作优先级, 可释放更多资源给其他 CPU 任务。提高备份或恢复优先级可加快进程, 因为系统会从当前运行的其他程序中获取资源。实际效果依 CPU 使用总量和其他因素而定。

您可设置操作优先级:

- **低**(默认为启用) — 备份或恢复速度较慢, 但是会提升其他程序的性能。
- **一般** — 备份或恢复进程与其他进程拥有同等优先级。
- **高** — 备份或恢复进程速度较快, 但是会降低其他程序的性能。请注意, 选择此选项可能导致 Acronis Cyber Protect Home Office 的 CPU 占用率达到 100%。

网络连接传输速率

将数据备份至 Acronis Cloud 时, 您可以更改 Acronis Cyber Protect Home Office 使用的连接速度。设置的连接速度要允许您使用互联网和网络资源而不会发生烦人的减速。

要设置连接速度，请在**网络连接传输速率**下选择以下选项之一：

- **最大值**
在系统配置中，数据传输速率是最大值。
- **将上载速度限制为**
您可以为数据上载速度指定一个最大值。

备份快照

警告！

此选项仅供高级用户使用。如果您不确定选择哪个选项，请勿更改默认设置。

在磁盘或分区备份过程(通常花费很长时间)中，一些备份文件可能正在使用中、处于锁定状态或者正在修改(无论方式如何)。例如，您可能正在处理一个文档并不时进行保存。如果 Acronis Cyber Protect Home Office 逐一备份文件，那么打开的文件自备份开始以来可能经过更改，然后在备份中保存为另一个时间点。因此，备份中的数据会不一致。为了消除这种情况，Acronis Cyber Protect Home Office 创建了快照，可以将要备份的数据固定到某个特定时间点。在备份开始之前进行此操作并保证数据处于一致状态。

从**备份快照**列表中选择选项：

- **无快照** — 不会创建快照。与普通复制操作一样，将逐一备份文件。
- **VSS** — 对于磁盘级备份和整个 PC 备份，此选项为默认设置并且保证备份中的数据一致性。

警告！

对于备份系统，这是唯一推荐的选项。从使用不同快照类型创建的备份进行恢复后，系统可能不会启动。

- **Acronis 快照** — 将使用在早期版本的 Acronis Cyber Protect Home Office 中使用的 Acronis 驱动程序创建快照。
- **不带编写器的 VSS** — 对于文件级备份，此选项为默认设置。VSS 编写器是用于通知应用程序将要创建快照的特殊 VSS 组件，以便于应用程序准备好用于快照的数据。对于执行大量文件操作并且要求数据一致性的应用程序(如数据库)，需要编写器。因为此类应用程序不安装在家用计算机上，因此无需使用编写器。此外，这样可减少文件级备份所需的时间。

4.5.17 选择用于备份的数据中心

位置：**选项 > 高级 > 数据中心**

注意

此选项仅适用于线上备份。

创建 Acronis Cloud 备份时，您的数据将上传到位于不同国家/地区的 Acronis 数据中心之一。最初，该数据中心将定义为在创建 Acronis 帐户时离您的所在地最近的数据中心。之后，您的在线备份和同步文件将默认存储到同一数据中心内。

当您位于不同的国家/地区并且默认的数据中心不是离您当前的所在地最近的数据中心时，建议您将该数据中心设置为手动备份。这样可以显著提升数据的上传速度。

注意

您不能更改预先存在的备份的数据中心。

4.5.18 笔记本电脑电源设置

位置: **设置 > 电池省电程序**

注意

该设置仅适用于带电池的计算机(笔记本电脑、带 UPS 的计算机)。

长期备份可能会非常快速地消耗电池电量。当您使用笔记本电脑且您身边没有电源时，或者当您的计算机在断电后已切换到 UPS 时，节省电池电量是合理的做法。

节省电池电量的方法

- 在侧边栏上，单击 **设置 > 电池省电程序**，选中 **当电池电量低于以下值时不备份** 复选框，然后使用滑块设置确切的电池剩余电量以启动省电模式。

当启用此设置时，如果您拔下笔记本电脑电源适配器或者在断电后您使用 UPS 为计算机供电，并且剩余电池电量等于或低于滑块中的级别，则所有当前备份将暂停且计划的备份将不会启动。当您重新插入电源适配器或者恢复电源后，暂停的备份将继续进行。由于此设置而错过的预定备份也将启动。

此设置不会完全禁止备份功能。您始终可以手动启动备份。

本地移动备份不取决于此设置。您的移动数据将照常备份到计算机上的本地存储。

4.5.19 使用 Wi-Fi 网络备份到 Acronis Cloud

位置: **设置 > 用于备份的 Wi-Fi 网络**

当您备份数据到 Acronis Cloud 时，如果您的个人数据通过未受保护的 Wi-Fi 网络进行传输，您可能会关心这些数据的安全性。为了避免个人数据被窃取的风险，我们强烈建议您仅使用受保护的 Wi-Fi 网络。

保护数据的方法

1. 在侧边栏上，单击 **设置 > 用于备份的 Wi-Fi 网络**，然后单击 **设置网络**。
2. 在 **用于备份的 Wi-Fi 网络** 窗口(其中包含所有当前可用以及已保存的不可用 Wi-Fi 网络)中，选中您要用于备份数据的网络旁边的复选框。

当选择了网络时，如果您的计算机丢失任何网络连接，所有当前备份均会暂停并且不会启动计划的备份。在计算机连接到其中的任何网络后，暂停的备份将会继续。由于此设置而错过的预定备份也将启动。

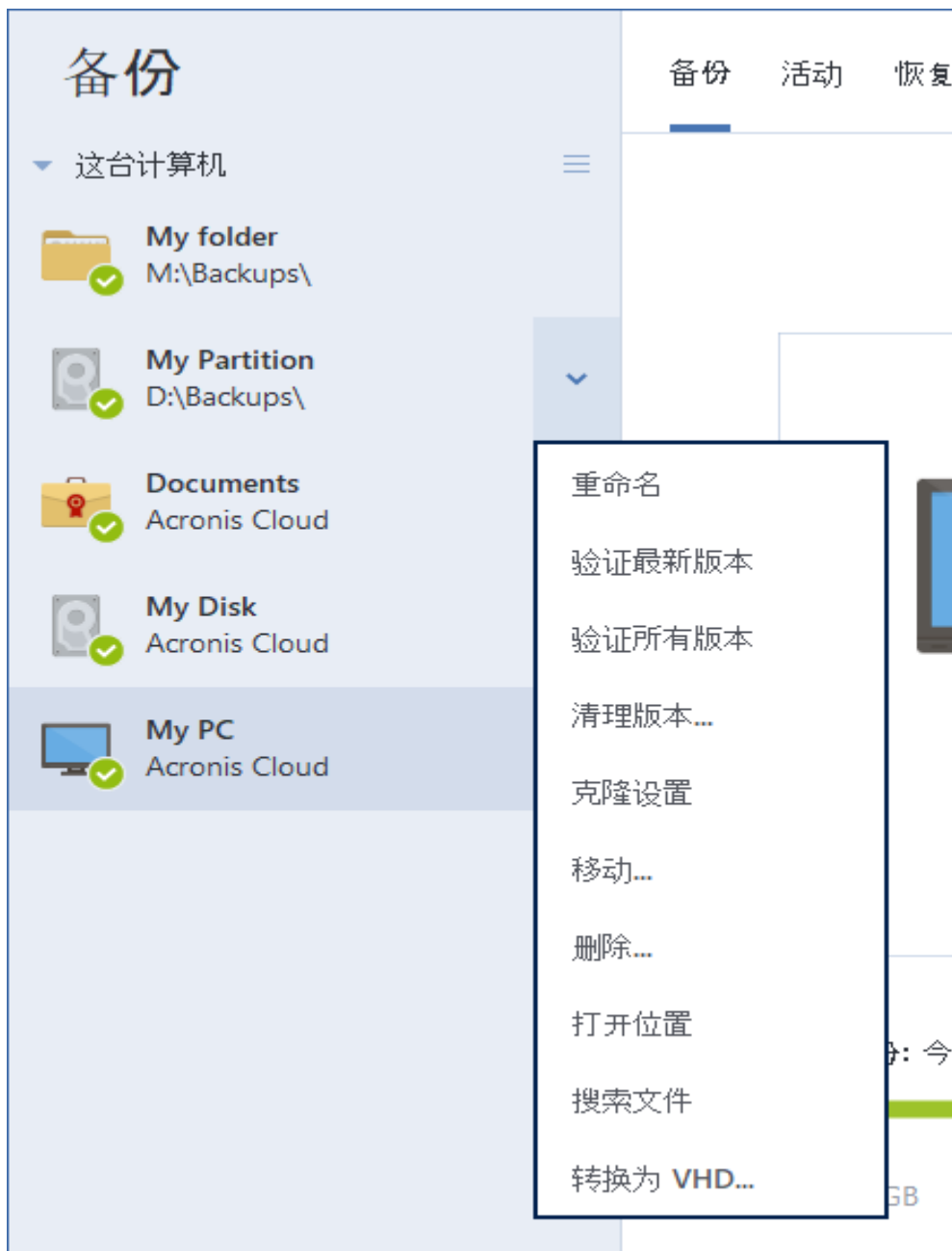
要使用新的 Wi-Fi 网络备份您的数据，只需在 **用于备份的 Wi-Fi 网络** 窗口中选择该网络即可。只要您需要使用新网络，便可以执行该操作。

本地移动备份不取决于此设置。您的移动数据将照常备份到计算机上的本地存储。

4.6 使用备份执行的操作

4.6.1 备份操作菜单

通过备份操作菜单，可快速完成可针对所选备份执行的操作。



备份操作菜单可包含下列各项：

- **重命名**(不适用于到 Acronis Cloud 的备份)- 使您可以为列表中的备份设置新名称。备份文件不会被重命名。

- **重新配置**(针对手动添加到备份列表中的备份)- 允许配置由以前的 Acronis Cyber Protect Home Office 版本创建的备份的设置。此项目也适用于在另一台计算机上创建且添加到备份列表但未导入其设置的备份。

如果没有备份设置,您不能通过单击**立即备份**来刷新备份。此外,您也不能编辑和克隆备份设置。

- **重新配置**(针对线上备份)- 允许您将选定的线上备份绑定到当前计算机。若要执行此操作,请单击此项目并重新配置备份的设置。请注意,一个线上备份只能在一台计算机上激活。
- **验证所有版本** - 启动所有备份片断验证。
- **验证最新版本** - 启动最新备份片断的快速验证。
- **清理版本** - 使您可以删除不再需要的备份版本。
- **克隆设置** - 使用初始备份的设置创建一个新的空备份框并将其命名为 **(1) [初始备份名称]**。更改设置并保存,然后在克隆的备份框中单击**立即备份**。
- **移动** - 单击此选项可将全部备份文件移到其它位置。之后的备份版本将被保存到新位置。如果您通过编辑备份设置来更改备份目标位置,则只有新备份版本才会被保存到新位置。之前的备份版本仍将留在原位置。
- **删除** - 根据备份类型,此命令将从备份位置完全删除备份,或者允许您选择要完全删除备份还是仅删除备份框。当您删除备份框时,备份文件将保留在位置中,并且以后您可以将备份添加至列表。请注意,如果您完全删除备份,则无法撤消删除操作。
- **打开位置** - 打开包含备份文件的文件夹。
- **搜索文件** - 使您可以通过在搜索字段中输入特定文件或文件夹的名称,在备份中查找该文件或文件夹。
- **转换为 VHD**(对于磁盘级备份) - 使您可以将选定的 Acronis 备份版本(.tibx 文件)转换为虚拟硬盘(.vhd(x) 文件)。将不会修改初始备份版本。

4.6.2 备份活动和统计数据

在**活动**选项卡和**备份**选项卡上,您可以查看有关备份的其他信息,例如备份包含的备份历史记录和文件类型。**活动**选项卡包含从备份创建之时开始对所选备份执行的操作列表、操作状态和统计数据。如果您需要弄清楚在后台模式中备份的相关信息(例如,预定备份操作的数量和状态、备份数据的大小、备份验证的结果等),则该选项卡会派上用场。

当您创建备份的第一个版本时,**备份**选项卡将按文件类型显示备份内容的图形表示。

“活动”选项卡

注意

不间断备份和移动备份不具有活动源。

查看备份活动的方法

1. 在侧栏上单击**备份**。
2. 在备份列表中,选择备份,以及您要查看的内容的历史记录。
3. 在右侧窗格中,单击**活动**。

✓ 已成功于今天的 下午3:31 完成备份

已备份	速度	已用时间	要恢复的数据	方法
1.6 GB	111.0 Mbps	3 分钟 54 秒	1.6 GB	完整

您可查看和分析的内容包括：

- 备份操作及其状态(成功、失败、已取消、已中断等)
- 对备份执行的操作及其状态
- 错误消息
- 备份注释
- 备份操作详细信息, 包括:
 - **已备份** — 最后一个备份版本包含的数据的大小。
对于文件级备份, Acronis Cyber Protect Home Office 计算了要备份的文件大小。该参数的值等于要为完整备份版本恢复的数据的值。对于差异和增量版本, 通常小于要恢复的数据, 因为在这种情况下 Acronis Cyber Protect Home Office 另外使用了以前版本的数据进行恢复。
对于磁盘级备份, Acronis Cyber Protect Home Office 会计算包含要备份的数据的硬盘扇区的大小。因为扇区可能包含到文件的硬链接, 即使对于完整的磁盘级备份版本, 该参数的值也可以小于“要恢复的数据”参数的值。
 - **速度** — 备份操作的速度。
 - **已用时间** — 备份操作所用的时间。
 - **要恢复的数据** — 可以从最后一个备份版本恢复的数据的大小。
 - **方法** — 备份操作的方法(完整、增量或差异)。

有关详情, 请参阅知识库文章: <https://kb.acronis.com/content/60104>。

“备份”选项卡

当创建备份后, 您可以查看有关最后一个备份版本所包含的备份文件的类型的统计数据:



指向颜色段可查看文件的数量和每个数据类别的总大小:

- 图片
- 视频文件
- 音频文件
- 文档
- 系统文件
- 其他文件类型, 包括隐藏的系统文件

待恢复数据 显示您所选的原始备份数据的大小。

4.6.3 在列表中对备份排序

默认情况下, 备份按创建日期(从最新到最旧)排序。要更改顺序, 请在备份列表的上部选择适当的排序类型。选项如下:

命令		说明
排序方式	名称	此命令将所有备份按照字母顺序排序。 要颠倒顺序, 请选择 Z → A 。
	创建日期	此命令将所有备份按照新旧顺序排序。 要颠倒顺序, 请选择 最旧的在顶部 。
	更新日期	此命令将所有备份按照最后一个版本的日期排序。最后一个备份版本越新, 备份在列表中的排位越高。 要颠倒顺序, 请选择 最早的在顶部 。
	大小	此命令将所有备份按照大小顺序(从最大到最小)排序。 要颠倒顺序, 请选择 最小的在顶部 。
	源类型	此命令将所有备份按照源类型排序。
	目标类型	此命令将所有备份按照目标类型排序。

4.6.4 将备份复制到 Acronis Cloud

为什么要复制?

即使通过备份数据来提供保护, 我们也建议您将所有本地备份复制到 Acronis Cloud 以防计算机意外损坏。当然, 您可以创建两个备份计划, 一个用于备份到您的本地计算机, 另一个用于备份到 Acronis Cloud。但是, 如果设置备份计划并创建副本快于创建另一个备份, 则自动复制会节省时间。副本是另一份备份, 可用作一种保护措施并且可从任何位置访问。

复制激活

默认情况下, 复制不处于激活状态。您可以为使用在 Acronis True Image(2020 或 2021) 或者 Acronis Cyber Protect Home Office 中配置的本地目标位置(复制到外部或内部磁盘)的磁盘、分区或整台机器的任何本地备份激活复制。您可以在某个备份计划的特定选项卡下归档复制。

激活到 Acronis Cloud 的备份复制:

1. 从备份列表中, 选择要复制的备份, 然后打开 **副本** 选项卡。
2. 单击 **复制**。现在, 复制已处于激活状态并在创建正常备份后启动。您随时可以关闭 Acronis Cyber Protect Home Office。备份和复制进程将在后台模式下继续。

3. [可选步骤] 单击 **选项 > 高级 > 到 Acronis Cloud 的复制** 以查看存储您的备份复制的数据中心并为 **配置清理设置** 以优化其空间使用。

已复制数据的保护

通过使用安全套接字层 (SSL) 将已复制的数据上传到 Acronis Cloud。

在 Cloud 中, 将根据您的加密设置存储数据。如果未设置加密密码, 则已复制的数据将以未加密方式存储。否则, 将使用 AES-256 对数据进行加密。

4.6.5 验证备份

验证程序会检查您是否可从备份恢复数据。

例如, 在恢复系统之前必须先验证备份。如果您从已损坏的备份开始恢复, 该过程将失败并且计算机将无法启动。我们建议您在可启动媒体中验证系统分区备份。其他备份可以在 Windows 中验证。另请参见 **准备恢复** 和 **基本概念**。

在 Windows 中验证整个备份

1. 启动 Acronis Cyber Protect Home Office, 然后单击侧边栏中的 **备份**。
2. 在备份列表中, 单击要验证的备份旁边的下箭头, 然后单击 **验证**。

在单机版 Acronis Cyber Protect Home Office(可启动媒体) 中验证特定备份版本或整个备份

1. 在 **恢复** 选项卡上, 查找包含要验证的的版本的备份。如果未列出该备份, 请单击 **浏览备份**, 然后指定该备份的路径。Acronis Cyber Protect Home Office 会将此备份添加到列表中。
2. 右键单击备份或特定版本, 然后单击 **验证存档**。此时将打开 **验证向导**。
3. 单击 **继续**。

4.6.6 备份到不同位置

通过在编辑备份设置时更改备份目标位置, 您可以将备份的不同版本保存到不同的目标位置。例如, 将初始完整备份保存到外接 USB 硬盘驱动器后, 您可以通过编辑备份设置, 将备份目标位置更改为 USB 闪存盘。

后续的增量或差异备份将写入到该 USB 闪存盘。

注意

您无法继续备份到一个可选光盘。

注意

Acronis Secure Zone 和 FTP 服务器仅可包含整个备份。

动态分割备份

当目标存储(CD-R/RW 或 DVD-R/RW) 上的可用空间不足以完成当前备份操作时, 程序将会显示警告消息。

要完成备份, 请执行以下任一操作:

- 在磁盘上释放一些空间, 然后单击**重试**。
- 单击**浏览**, 然后选择另一个存储设备。
- 单击**格式化**以擦除磁盘上的所有数据, 然后继续执行备份。

如果备份的不同版本存储在不同的位置, 您可能需要在恢复期间指定这些位置。

4.6.7 将现有备份添加至列表

您可能从以前的产品版本创建或从另一台计算机复制的 Acronis Cyber Protect Home Office 备份。每次启动 Acronis Cyber Protect Home Office 时, 它都会扫描计算机中的此类备份, 并自动将它们添加到备份列表中。

如果列表中未显示您的备份, 您可以手动添加。

手动添加备份的方法

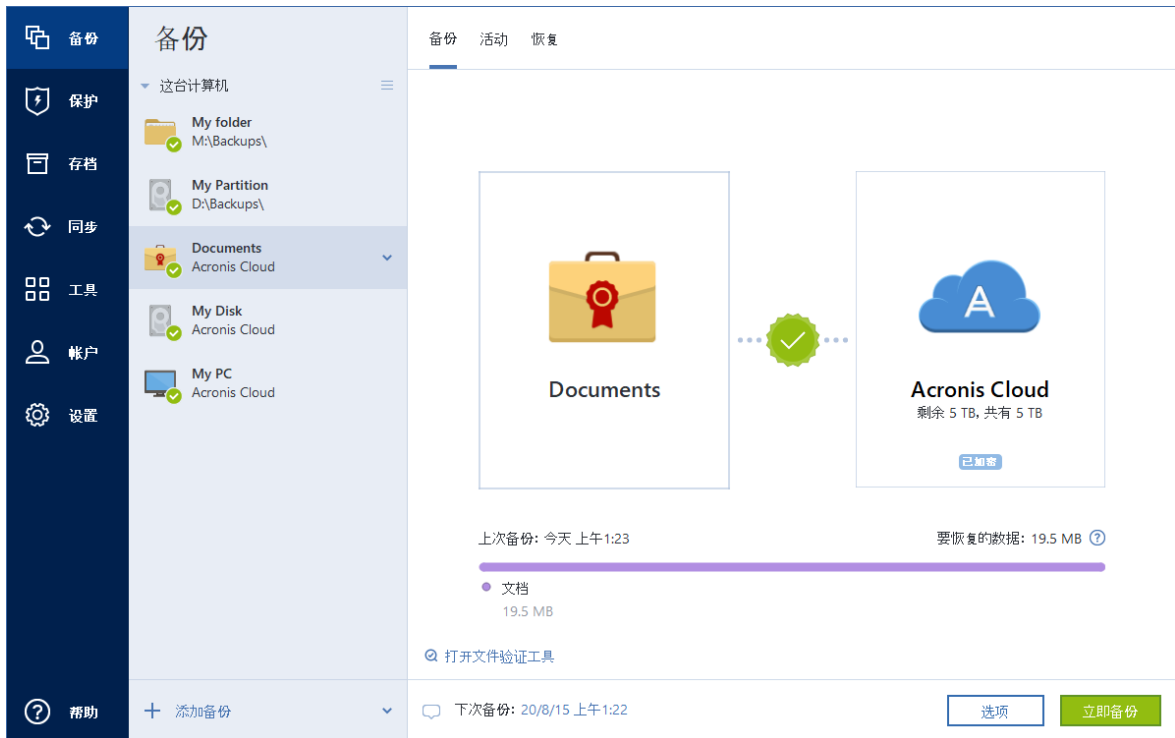
1. 在**备份**部分中, 从备份列表的底部单击箭头图标, 然后单击**添加现有备份**。程序将打开一个窗口, 从中可浏览计算机上的备份。
2. 选择备份版本(.tib 文件), 然后单击**添加**。
整个备份都将添加到列表中。

4.6.8 公证备份

通过使用区块链技术, Acronis Cyber Protect Home Office 可以保护文件免遭未经授权的修改。这可以保证您从备份的相同文件恢复数据。我们建议您使用这种备份类型, 以保护法律文件或者需要证明可信性的任何其他文件。有关详细信息, 请参阅[使用区块链技术](#)。

如需创建文件和文件夹的公证备份, 请执行以下操作:

1. 启动 Acronis Cyber Protect Home Office。
2. 在侧栏上单击**备份**。
3. 单击**添加备份**。
4. [可选] 要重命名备份, 请单击备份名称旁边的箭头, 再单击**重命名**, 然后输入新名称。
5. 单击**备份源**区域, 然后选择**要公证的文件**。
6. 在打开的窗口中, 选中您要备份的文件及文件夹旁边的复选框, 然后单击**确定**。



7. 单击**备份目标位置**区域，然后选择一个备份目标位置：

- **Acronis Cloud** - 登录您的 Acronis 帐户，然后单击**确定**。

如果您没有 Acronis 帐户，请单击**创建帐户**，键入您的电子邮件地址、密码，然后单击**创建帐户**按钮。有关详细信息，请参阅 [Acronis 帐户](#)。

- **您的外接驱动器** - 当在计算机上插入外接驱动器时，您可以从列表中选择该项。
- **NAS** - 从找到的 NAS 设备列表选择一个 NAS。如果只有一个 NAS，默认情况下，Acronis Cyber Protect Home Office 会建议将其用作备份目标位置。
- **浏览** - 从文件夹树中选择一个目标位置。

8. [可选步骤] 单击**选项**以设置备份选项。有关更多信息，请参阅 [备份选项](#)。

要从备份中排除具有电子签名的文件，请勾选**排除项**选项卡下**请勿公证数字签名的文件**复选框。有关详细信息，请参阅 [从备份中排除项目](#)。

9. [可选步骤] 单击**添加注释**图标，然后键入有关备份版本的注释。日后在恢复数据时，备份注释将有助于您找到所需版本。

10. 请执行以下任一操作：

- 要立即运行备份，请单击**立即备份**。
- 要稍后运行或定时运行备份，请单击**立即备份**按钮右侧的向下箭头，然后单击**稍后**。

注意

当您将数据备份至 Acronis Cloud 时，第一个备份可能会花费大量时间才能完成。进一步的备份过程可能会快得多，因为届时将仅通过互联网传输对文件的更改。

此外，请观看位于 <https://goo.gl/WjUoPZ> 的英语视频说明。

使用区块链技术

Acronis Cyber Protect Home Office 使用区块链技术, 为您的备份文件提供顶级保护。此技术可保证您的文件未被欺诈软件修改, 并且在需要恢复时, 您将从备份的相同文件中恢复数据。

什么是区块链?

区块链是包含关于交易及顺序信息的数据库。通常, 交易代表事件, 例如, 财务运作或者其他资产运作。交易统一在区块中, 然后区块一个一个写入到数据库中形成区块链。每一个交易和每一个区块都拥有自己的唯一识别码。非常重要的一点是, 每一个区块中都存储了关于所有之前区块链的信息。一旦写入数据库中, 关于交易的信息将无法以任何方式或被任何人更改, 并且交易顺序无法修改。任何更改数据库中任何信息片段的尝试都可以由数据库的任何用户轻松发现, 因为在所有后续的区块中都没有关于虚假交易或虚假区块的信息。此技术可保证数据库中存储的数据有效、属于某个特定人员并且未被任何人修改。有关区块链的详细信息, 请访问 [https://en.wikipedia.org/wiki/Blockchain_\(database\)](https://en.wikipedia.org/wiki/Blockchain_(database))。

Acronis Cyber Protect Home Office 使用区块链技术的方式

为了保护您的文件免遭未经授权修改, Acronis Cyber Protect Home Office 采用了 Acronis Notary 技术。这款通用解决方案适用于对任何数据对象和流进行时间戳标记和指纹识别。因为在区块链数据库中存储大量数据不切实际, 所以 Acronis Cyber Protect Home Office 仅向 Acronis Notary 服务发送文件哈希代码。

哈希代码是哈希函数产生的固定大小的唯一编号。该代码可精确定义数据的任意集合, 例如, 备份文件。备份文件的任意更改都会导致哈希代码更改。因此, 要检查文件是否被更改, 只需要比较文件的初始状态和当前状态中产生的哈希代码。如果代码相符, 则可以保证文件未被任何人修改。


当 Acronis Notary 收到文件的哈希代码时, 它会计算一个新的哈希代码并将其发送到基于 Ethereum 区块链的数据库。有关 Ethereum 的详细信息, 请访问 <https://www.ethereum.org/>。

当哈希代码到达数据库后, 用于计算此哈希代码的文件将由 Acronis Notary 进行公证。通过使用 [验证文件可信性](#) 中所述的流程, 您可以随时轻松验证文件的可信性。每一个经过公证的文件都具有公证证书, 作为文件受区块链技术保护的文件证明。证书中包含关于文件的一般信息和技术详细信息, 让您能够手动验证文件的可信性。有关详细信息, 请参阅 [手动验证文件的可信性](#)。

验证文件的可信性

通过使用区块链技术, Acronis Cyber Protect Home Office 可以保护备份文件免遭未经授权的修改。这可以保证您从备份的相同文件恢复数据。

在 Acronis Cyber Protect Home Office 中验证文件可信性的方法

1. 启动 Acronis Cyber Protect Home Office。
2. 在侧栏上单击 **备份**。
3. 从备份列表中选择包含您要验证的文件的公证备份。
4. 在右侧面板中, 打开 **恢复** 选项卡。
5. 浏览到所需的文件, 单击“菜单”图标 (), 然后单击以下选项之一:

- **查看证书** — 网络浏览器中将打开包含关于文件安全性详细信息的证书。
- **验证** - Acronis Cyber Protect Home Office 将检查文件的可信性。

在文件验证工具中验证文件的可信性

1. 使用以下方法之一打开文件验证工具：
 - 在网络浏览器中，打开 <https://notary.acronis.com/verify>。
 - 在 Acronis Cyber Protect Home Office 的侧边栏中，单击**备份**，选择公证备份，然后单击右侧面板中的**打开文件验证工具**。
2. 在文件资源管理器中，浏览到您想要验证的文件，然后将该文件拖到网络浏览器窗口中。

如果在 Acronis Cloud 上存储了公证备份，也可以在 Acronis Cloud Web 应用程序中验证所备份文件的可信性。

在 Acronis Cloud 中验证文件可信性的方法

1. 转到 <https://www.acronis.com/my/online-backup/webrestore/>，然后登录您的 Acronis 帐户。
2. 在侧栏上单击**备份**。
3. 从备份列表中选择包含您要验证的文件的公证备份。
4. 浏览到所需的文件，然后通过复选标记将其选中。然后，在右侧的侧栏上，单击**验证**。

手动验证文件的可信性

验证文件可信性的最简单方法是使用 Acronis Cyber Protect Home Office 或 Acronis Cloud Web 应用程序中的**验证**命令。有关详细信息，请参阅[验证文件可信性](#)。除了这种简单的方法，您还可以按步骤自行执行验证流程。

手动验证文件可信性的的方法

第 1 步. 计算文件的 MD5 哈希

1. 启动 Windows PowerShell。
2. 例如，要计算位于 C:\Users\picture.png 的 picture.png 文件的 md5 哈希，请键入：

```
$(CertUtil -hashfile "C:\Users\picture.png" MD5)[1] -replace " ", ""
```

md5 哈希的范例：eea16ade1edf2750a46bb6bffb2e45a2

3. 检查所计算的 md5 哈希是否等于公证证书“数据”字段中的 eTag。有关获取文件证书的详细信息，请参阅[验证文件可信性](#)。

第 2 步. 检查 ROOT 是否存储在区块链中

1. 打开区块链管理器，例如 <https://etherscan.io/>。
2. 在搜索字段中输入证书中的交易 ID。
3. 检查“事件日志”选项卡中的“数据”字段是否与证书中的 ROOT 值相同。

第 3 步. 检查树中是否包括哈希

1. 从 GitHub 库中下载命令行实用程序：<https://github.com/acronis/notary-verifyhash/releases>。
2. 按照以下网址的说明进行操作：<https://github.com/acronis/notary-verifyhash>。

Acronis ASign

什么是 Acronis ASign?

Acronis ASign 是一项允许多人以电子方式签署文件的在线服务。一开始, 应该通过备份、存档或同步将文件上传到 Acronis Cloud。为了进一步保护已签署的文件, 将通过 Acronis Notary 对其进行公证和保护。

ASign 解决方案可用于签署任何电子文档, 包括不同类型的合同、协议、证书、财务文档和公函。

签署文件

在 *Acronis Cloud* 上签署文件

1. 转到 <https://www.acronis.com/my/online-backup/webrestore/>, 然后登录您的 Acronis 帐户。
2. 浏览到所需的文件, 单击文件名, 然后在打开的菜单中选择 **发送以进行签名**。
3. 键入您希望签署该文件的人员的电子邮件地址, 然后向他们发送邀请函。

在所有签字者签署该文件之后, Acronis Notary 会对该文件进行公证并生成一个签名证书。

有关该功能的完整说明, 请参阅英语版 Acronis ASign Web 帮助, 网址

为: <https://www.acronis.com/en-us/support/documentation/ATI2017ASign/>。

4.6.9 清理备份、备份版本和副本

要删除您不再需要的备份和备份版本, 请使用 Acronis Cyber Protect Home Office 提供的工具。

Acronis Cyber Protect Home Office 将备份的信息存储在元数据信息数据库中。因此, 在文件资源管理器中删除不需要的备份文件将不会从数据库中删除有关这些备份的信息。这将导致在程序对已不存在的备份执行操作时出错。

删除整个备份及其副本

在 **备份** 部分中, 单击要删除的备份旁边的下箭头, 然后单击 **删除**。

根据备份类型, 此命令将从备份位置完全删除备份, 或者允许您选择要完全删除备份还是仅删除备份框。当您仅删除备份框时, 备份文件将保留在位置中, 并且以后您可以将备份添加至列表。请注意, 如果您完全删除备份, 则无法撤消删除操作。

当您删除备份时, 将连同其副本一起自动删除。无法删除本地备份并且仍然保存其副本。但是, 您可以仅删除副本并且保留本地备份。

删除整个备份副本

您可以删除副本及其原始备份, 或者单独删除副本。要删除副本及备份, 请使用上面介绍的方式来删除备份。

要删除副本而不删除备份, 请在 **备份** 部分中, 单击要删除的备份及副本旁边的下箭头图标, 然后单击 **删除副本**。

自动清理备份版本

1. 转至**备份**部分。
2. 从备份列表中, 选择您要为其清理副本版本的备份, 然后单击**选项**。
3. 在**备份方案**选项卡上, 选择**自定义方案**, 选择一种备份方法, 然后单击**开启自动清理**。
4. 配置备份的清理规则。

有关详细信息, 请参阅[自定义方案](#)。

注意

在执行清理后, 一些辅助文件可能保存在存储中。请不要删除它们!

自动清理副本版本

1. 转至**备份**部分。
2. 从备份列表中, 选择您要为其清理副本版本的备份, 然后单击**选项**。
3. 在**高级**选项卡上, 打开**Acronis Cloud 清理**选项卡。
 - 请使用**仅存储最近备份版本**选项, 输入副本版本的最大存储数量限制值。
 - 请选中**删除旧于此时间的备份版本**复选框, 并输入先前版本的最早时间限制值。系统将保留最新版本并自动删除所有其他版本。

手动清理备份和副本版本

当您想要删除不再需要的备份版本时, 请使用应用程序中提供的工具。如果您在 **Acronis Cyber Protect Home Office** 之外(例如, 在 **File Explorer** 中)删除备份版本文件, 这将导致在执行备份操作期间出现错误。

以下备份版本无法手动删除:

- 存储在 CD、DVD、BD 或 Acronis Secure Zone 上的备份。
- 不间断备份。
- 公证备份。

清理特定备份版本

1. 启动 **Acronis Cyber Protect Home Office**。
2. 在**备份**部分中, 单击要清理的备份旁边的下箭头, 然后单击**清理版本**。
将打开**清理备份版本**窗口。
3. 选择所需版本, 然后单击**删除**。
4. 在确认请求中单击**删除**。

请等待清理操作完成。在执行清理后, 一些辅助文件可能保存在存储中。请不要删除它们。

清理有从属版本的版本

当您选择要删除的备份版本时, 请记住此版本可能有从属版本。在此情况下, 还会选择要删除的从属版本, 因为不可能再从这些版本执行数据恢复。

- **如果选择一个完整版本** - 程序还会选择所有后续增量版本及差异版本，直到下一个完整版本。换句话说，整个备份版本链将被删除。
- **如果选择一个差异版本** - 程序还会选择备份版本链中的所有从属增量版本。
- **如果选择一个增量版本** - 程序还会选择备份版本链中的所有从属增量版本。

另请参阅

[完整、增量和差异备份。](#)

[从 Acronis Cloud 中删除数据。](#)

4.6.10 清理 Acronis Cloud 上的空间

1. 转到 <https://www.acronis.com/my/online-backup/webrestore/>，然后登录您的 Acronis 帐户。系统会打开 Acronis Cloud Web 应用程序。
2. 在 Web 应用程序的左侧侧栏上，单击 **帐户**。
3. 在 **Acronis Cloud** 行上，单击 **清理**。
4. 选择您想删除的版本：
 - 早于特定时间的版本。
 - 除某些最近版本之外的所有旧版本。

警告！

请小心！已删除的版本无法还原。

另一种清理方式是删除您不再需要的云备份。在这种情况下，会从 Acronis Cloud 中删除备份的所有版本历史记录。

4.6.11 从 Acronis Cloud 中删除数据

由于 Acronis Cloud 的可用空间有限，因此您需要对云空间进行管理，清理过时的数据或不再需要的数据。可以在 Acronis Cyber Protect Home Office 中执行清理，也可以通过 Acronis Cloud Web 应用程序执行清理。

删除整个备份

最“极端”的选项是从 Acronis Cloud 上删除整个备份。当删除备份时，将永久擦除其所有数据。无法恢复删除的数据。

在 **Acronis Cyber Protect Home Office** 中：

单击要删除的备份旁边的下箭头，然后单击 **删除**。该备份及其所有版本、设置和计划都将被删除。

在 **Acronis Cloud Web** 应用程序中：

1. 转到 <https://www.acronis.com/my/online-backup/webrestore/>，然后登录您的 Acronis 帐户。
2. 在 **备份** 选项卡上，将光标移到您要删除的备份上。
3. 单击备份大小，然后将显示详细视图。
4. 在详细视图中单击 **删除**。

请注意，该备份将从 Acronis Cloud 中删除，但是其所有设置和预定会保留在 Acronis Cyber Protect Home Office 应用程序中。

删除复制到云的备份版本

在 **Acronis Cyber Protect Home Office** 中：

1. 单击要删除版本的备份旁边的向下箭头图标，然后单击**清理版本**。
备份版本列表将会打开。
2. 选择要删除的版本，然后单击**删除**。

注意

Acronis Cloud 中的配额可能需要一天时间来更新。

在 **Acronis Cloud Web** 应用程序中：

1. 转到 <https://www.acronis.com/my/online-backup/webrestore/>，然后登录您的 Acronis 帐户。
2. 在**备份**选项卡上，单击要删除版本的备份大小。
备份的详细信息视图将会打开。
3. 在详细信息视图中，单击**清理**。
您可以选择删除比您选择的期间更早的版本，也可以清理除许多最新版本外的所有版本。
4. 配置要删除的内容，然后单击**立即清理**。
5. 在确认对话框中，单击**删除**。

在操作完成后，将会显示清理过程的状态。

删除复制到云的备份副本的版本

在 **Acronis Cyber Protect Home Office** 中：

1. 在**备份**部分中，找到复制云的本地备份，单击向下箭头，然后选择**清理版本**。
“清理备份版本”对话框将会打开。
2. 在**从以下位置删除版本**下，选择 **Acronis Cloud**。
备份副本版本列表将会显示。
3. 选择要删除的副本版本，然后单击**删除**。
4. 在确认对话框中，单击**删除**。

注意

Acronis Cloud 中的配额可能需要一天时间来更新。

在 **Acronis Cloud Web** 应用程序中：

1. 转到 <https://www.acronis.com/my/online-backup/webrestore/>，然后登录您的 Acronis 帐户。
2. 在**备份**选项卡上，单击要删除版本的备份副本的大小。
备份副本的详细信息视图将会打开。
3. 在详细信息视图中，单击**清理**。

您可以选择删除比您选择的期间更早的版本，也可以清理除许多最新版本外的所有版本。

4. 配置要删除的内容，然后单击**立即清理**。
5. 在确认对话框中，单击**删除**。

在操作完成后，将会显示清理过程的状态。

一次性清理

当您的 Acronis Cloud 已满或即将用完空间时，我们建议您使用 Acronis Cloud Web 应用程序中的清理工具。该工具使您可以方便快捷地释放云上的大量空间。

注意

您可以逐一地单独清理备份，甚至可以清理加密的备份。此时会请求您提供密码。

1. 转到 <https://www.acronis.com/my/online-backup/webrestore/>，然后登录您的 Acronis 帐户。
2. 在**备份**选项卡上，将光标移到您要删除的备份上。
3. 单击**清理**按钮。
4. 在打开的窗口中，配置清理设置，然后单击**立即清理**。

要对所有未加密的备份执行一次性清理，请使用以下选项：

1. 转到**帐户**选项卡。
2. 单击**清理**按钮。

5 恢复数据

5.1 恢复磁盘和分区

5.1.1 在崩溃后恢复系统

当计算机无法启动时，建议您首先尝试用[尝试确定崩溃原因](#)中给出的建议查找原因。如果崩溃是由操作系统损坏造成，则使用备份恢复系统。完成[准备恢复](#)中描述的准备工作时，继续恢复您的系统。

尝试确定崩溃原因

系统崩溃可能由两个基本因素造成：

- **硬件故障**

在这种情形下，最好让服务中心来完成相应的修复服务。然而，您可能希望执行一些常规测试。检查外部设备的电缆、连接器和电源等，然后重新启动计算机。如有硬件问题，开机自检 (POST) 会告知您此故障。

如果 POST 未发现硬件故障，请进入 BIOS 并检查它是否能够识别系统硬盘驱动器。若要进入 BIOS，请在 POST 顺序中按所需的组合键(**Del**、**F1**、**Ctrl+Alt+Esc**、**Ctrl+Esc** 或其它键，具体取决于 BIOS)。通常情况下，启动测试时会显示这一必须使用的组合键。按此组合键将进入设置菜单。找到硬盘自动检测实用工具，它通常位于“标准 CMOS 设置”或“高级 CMOS 设置”中。如果实用工具未检测到系统硬盘，则表明检测失败且需要更换驱动器。

- **操作系统损坏(Windows 无法启动)**

如果 POST 正确地检测到系统硬盘，则导致崩溃的原因可能是病毒、恶意软件或启动所需的系统文件损坏。在这种情况下，请使用系统盘备份或系统分区备份来恢复系统。有关详细信息，请参阅[恢复系统](#)。

准备恢复

我们建议您在恢复之前先执行以下操作：

- 如果您怀疑崩溃是由病毒或恶意软件攻击造成的，扫描计算机是否有病毒。
- 在可启动媒体下，尝试进行恢复空闲的硬盘驱动器(如果有)测试。
- 在可启动媒体下验证映像。在 Windows 验证过程中可读取的备份，在 **Linux** 环境中不一定可读。

在可启动媒体下，有两种方式可以验证备份：

- 若要手动激活备份，请在[恢复](#)选项卡上，右键单击备份并选择[验证存档](#)。
- 若要在恢复之前自动激活备份，请在[恢复向导](#)的[选项](#)步骤中，选择[恢复前验证备份存档复选](#)

框。



- 为硬盘驱动器上的所有分区分配唯一的名称(标签)。这将使您可更轻松地查找包含备份的磁盘。

当您使用 Acronis 可启动媒体时,它创建的磁盘驱动器号可能会与 Windows 标识驱动器的方式不同。例如,在单机版可启动媒体中识别的 D 盘可能与 Windows 中的 E 盘对应。

将系统恢复到同一硬盘

我们建议您在开始操作之前先完成[准备恢复](#)中介绍的程序。

恢复系统

1. 附加包含将要用于恢复的备份的外部驱动器,并确保已启动该驱动器。
2. 设置 BIOS 启动顺序,从而将您的应急媒体设备(CD、DVD 或 USB 驱动器)设置为第一启动设备。请参阅在[BIOS 或 UEFI BIOS 中设置启动顺序](#)。

如果您使用 UEFI 计算机,请注意 UEFI BIOS 中可启动媒体的启动模式。建议启动模式与备份中的系统类型相匹配。如果备份包含 BIOS 系统,那么将在 BIOS 模式下启动可启动媒体;如果系统为 UEFI,请确保已设置 UEFI 模式。

3. 从可启动媒体启动,并选择 **Acronis Cyber Protect Home Office**。
4. 在主页屏幕上,选择**恢复**下方的**我的磁盘**。

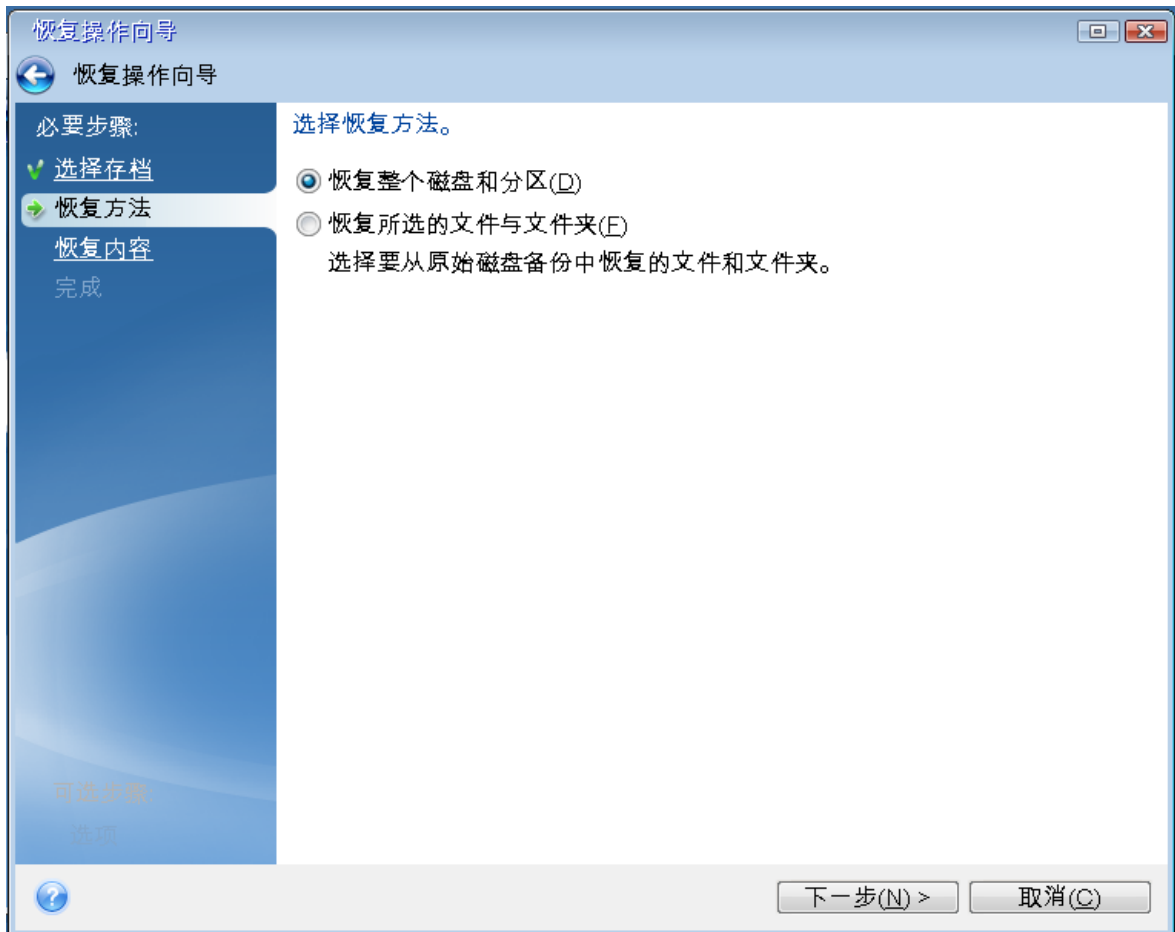


5. 选择要用于恢复的系统磁盘或分区备份。
如果未显示备份, 请单击**浏览**并手动指定备份路径。

注意

如果备份位于 USB 驱动器上并且驱动器未能正确识别, 请检查 USB 端口版本。如果为 USB 3.0 或 USB 3.1, 请尝试将驱动器连接到 USB 2.0 端口。

6. 在**恢复方法**步骤中选择**恢复整个磁盘和分区**。



7. [可选] 在 **恢复点** 步骤, 选择要将您的系统恢复到的日期和时间。
8. 在 **恢复内容** 屏幕中选择系统分区(通常是 C)。如果系统分区有不同的代号, 则使用 **标志** 列来选择分区。它必须有 **Pri**、**Act** 标志。如果您具有系统保留分区, 请也选择该分区。



9. 在“分区 C 的设置”(如果分区不同,则为系统分区的代号)步骤中检查默认设置,如果正确则单击**下一步**。否则,在单击**下一步**之前根据需要更改设置。恢复到不同容量的新硬盘时,需要更改设置。
10. 在**完成**步骤中仔细阅读操作摘要。如果没有重新调整分区的大小,那么**删除分区**和**恢复分区**项目中的大小必需匹配。查看完摘要后,单击**继续**。



11. 在完成操作后, 退出单机版 Acronis Cyber Protect Home Office, 移除应急媒体并从恢复的系统分区启动。确保已将 Windows 恢复到需要的状态后, 请还原原始启动顺序。

在可启动媒体下将系统恢复到新磁盘

在开始之前, 我们建议您先完成[准备恢复](#)中所描述的准备工作。您无需格式化新磁盘, 因为格式化会在恢复过程中完成。

注意

建议使用旧的和新的硬盘驱动器在相同的控制器模式(例如 IDE 或 AHCI)下工作。否则, 您的计算机不会从新的硬盘驱动器启动。

将系统恢复到新磁盘

1. 将新硬盘安装到计算机的原来位置, 并与原驱动器使用相同的电缆和连接器。如果这不可能实现, 就要将新的驱动器安装在需要使用它的地方。
2. 附加包含将要用于恢复的备份的外部驱动器, 并确保已启动该驱动器。
3. 设置 BIOS 启动顺序, 从而将您的可启动媒体(CD、DVD 或 USB 闪存盘)设置为第一启动设备。请参阅在[BIOS 或 UEFI BIOS 中设置启动顺序](#)。

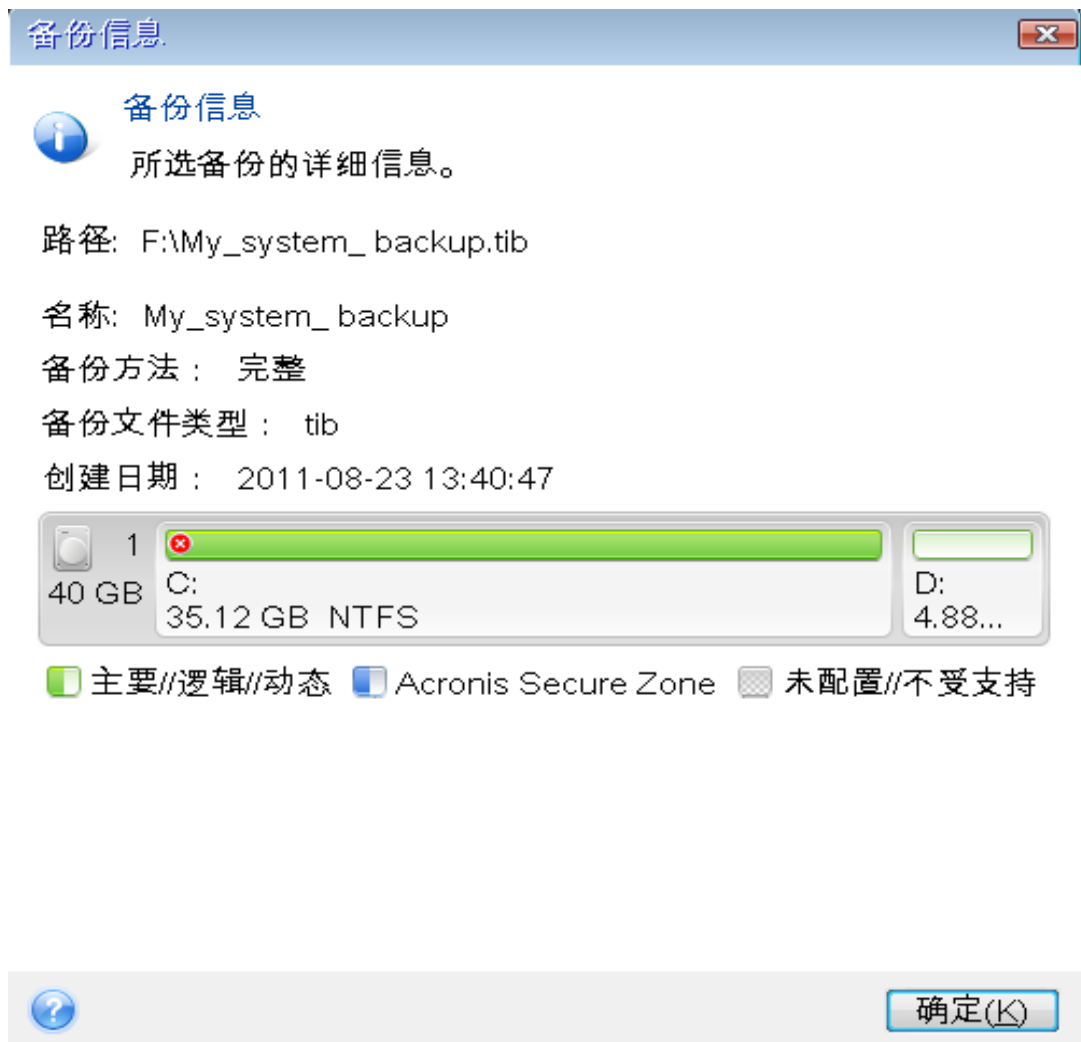
如果您使用 UEFI 计算机, 请注意 UEFI BIOS 中可启动媒体的启动模式。建议启动模式与备份中的系统类型相匹配。如果备份包含 BIOS 系统, 那么将在 BIOS 模式下启动可启动媒体; 如果系统为 UEFI, 请确保已设置 UEFI 模式。

4. 从可启动媒体启动, 并选择 **Acronis Cyber Protect Home Office**。
5. 在主页屏幕上, 选择**恢复**下方的**我的磁盘**。
6. 选择要用于恢复的系统磁盘或分区备份。如果未显示备份, 请单击**浏览**并手动指定备份路径。

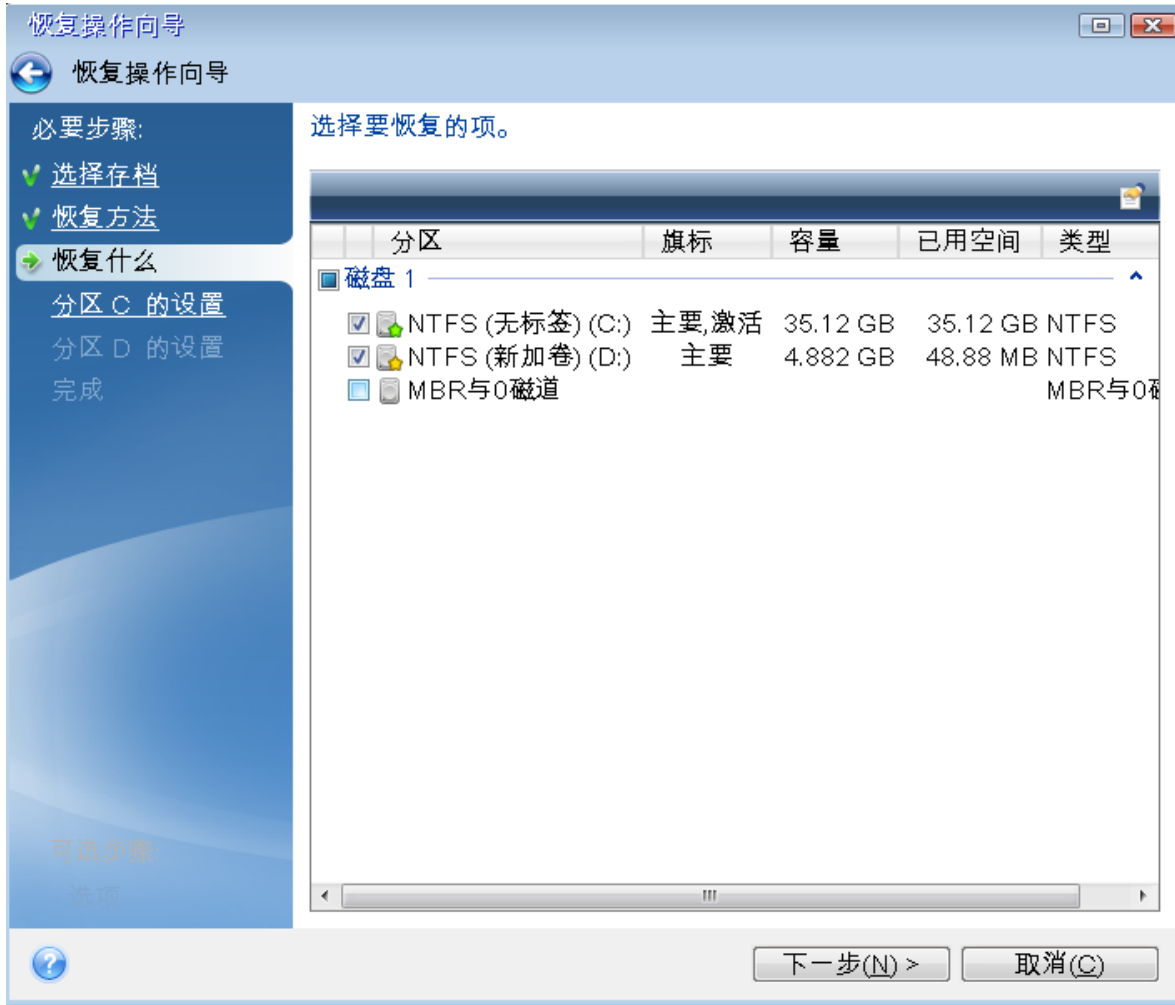
注意

如果备份位于 USB 驱动器上并且驱动器未能正确识别, 请检查 USB 端口版本。如果为 USB 3.0 或 USB 3.1, 请尝试将驱动器连接到 USB 2.0 端口。

7. 如果您有隐藏的分区(例如, 系统保留分区或计算机制造商创建的分区), 请在向导工具栏中单击**详细信息**。请记住隐藏分区的位置和大小, 因为您的新磁盘需要使用与这些参数相同的参数。



8. 在**恢复方法**步骤中选择**恢复整个磁盘和分区**。
9. 在**恢复内容**步骤中, 选择要进行恢复的分区旁边的方框。
如果您选择整个磁盘, 也将恢复磁盘的 MBR 和 0 磁道。



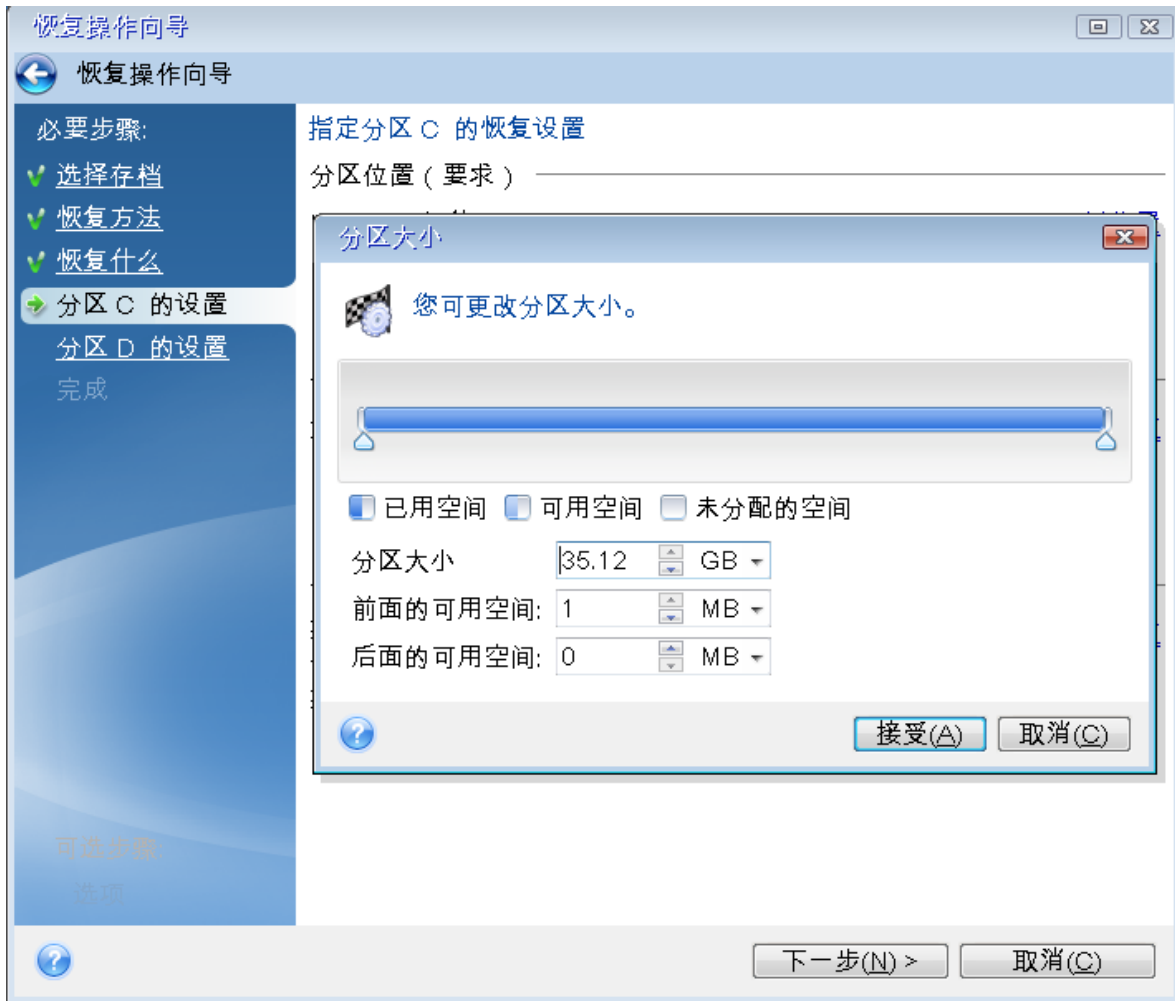
选择分区后, 将显示相关步骤“分区设置...”。请注意, 这些步骤将从不具有指定磁盘代号的分区开始(通常从具有隐藏分区的磁盘开始)。这些分区的分区磁盘代号将按照升序指定。不可更改此顺序。此顺序可能与硬盘上分区的物理顺序不同。

10. 在隐藏分区的“设置”步骤(通常称为“分区 1-1 的设置”)中指定以下设置:

- **位置** - 单击**新建位置**, 根据指定名称或容量选择新磁盘, 然后单击**接受**。



- **类型** - 检查分区类型, 如有必要, 作出更改。确保系统保留分区(如果有)是主分区且标记为活动状态。
- **大小** - 在分区大小区域中单击**更改默认值**。默认情况下,分区会占据整个新磁盘。在“分区大小”字段中输入正确的大小(您可以在**恢复内容**步骤中看到此值)。然后,将此分区拖动到您在“备份信息”窗口中看到的相同的位置(如果需要)。单击**接受**。



11. 在分区 C 的设置步骤中, 指定第二个分区(在此示例中是您的系统分区)的设置。

- 单击**新建位置**，然后在将收到第二个分区的目标磁盘上选择未分配空间。



- 更改分区类型(如果需要)。系统分区必须是主分区。
- 指定分区大小, 其默认为原始大小。通常, 在进行分区之后将没有可用空间, 所以请将新磁盘上的所有未分配空间分配给第二个分区。单击**接受**, 然后单击**下一步**。



12. 仔细阅读要执行的操作的摘要，然后单击**继续**。

完成恢复之后

启动计算机之前，请断开旧驱动器的连接(如果有)。如果 Windows 在启动期间能够同时“看到”新旧驱动器，则会导致在启动 Windows 时出现问题。如果将旧驱动器升级为具有更大容量的新驱动器，请在第一次启动之前断开旧驱动器的连接。

移除可启动媒体并在计算机中启动 Windows。系统可能会报告发现新硬件(硬盘驱动器)，需要重新启动 Windows。确保系统运行正常后，还原原始启动顺序。

Acronis异机还原

当您将系统恢复到不同硬件时，目标计算机可能无法启动。这是因为新硬件与映像中包含的关键驱动程序不兼容。Acronis 异机还原将帮助您使目标计算机可启动。有关详细信息，请参阅 [Acronis 异机还原](#)。

5.1.2 恢复分区和磁盘

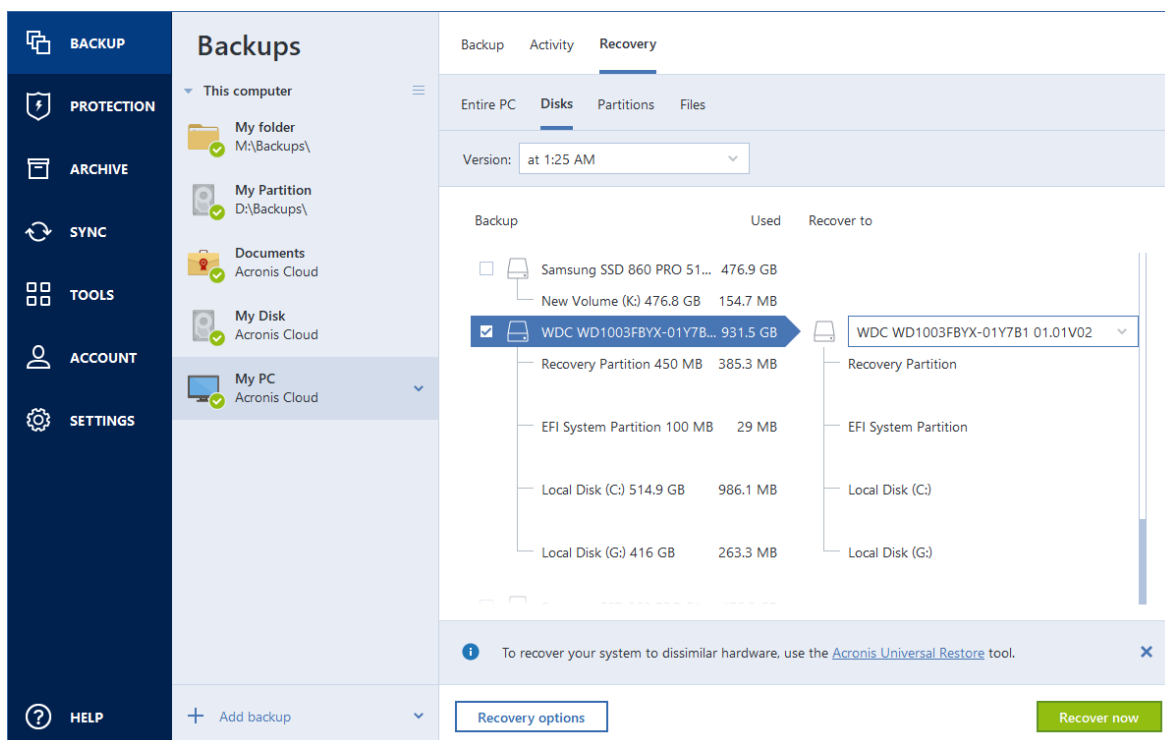
您可以从位于本地存储或 Acronis Cloud 中的备份恢复磁盘。

注意

根据您的互联网连接速度，从 Acronis Cloud 恢复磁盘可能需要较长的时间。

恢复分区或磁盘

1. 启动 Acronis Cyber Protect Home Office。
2. 如果您想从 Acronis Cloud 恢复数据，请确保您已登录自己的 Acronis 帐户。
3. 在**备份**部分中，选择包含您要恢复的分区或磁盘的备份，打开**恢复**选项卡，然后单击**恢复磁盘**。
4. 在**备份版本**列表中，根据备份日期和时间选择要恢复的备份版本。



5. 选择**磁盘**选项卡以恢复磁盘，或者选择**分区**选项卡以恢复特定分区。选择您要恢复的对象。
6. 在分区名称下方的“恢复目标”字段中，选择目标分区。不适合的分区名称用红色边框表示。请注意，目标分区上的所有数据都会丢失，因为恢复的数据和文件系统将替换它们。

注意

要恢复到原始分区，此分区必须至少有 5% 的可用空间。否则，**立即恢复**按钮将不可用。

7. [可选] 若要为磁盘恢复过程设置其他参数，请单击**恢复选项**。
8. 完成选择之后，请单击**立即恢复**以开始恢复。

分区属性

将分区恢复到基本磁盘时，您可以更改这些分区的属性。要打开**分区属性**窗口，请单击选定目标分区旁边的**属性**。

管理分区
✕

代号	标识	类型
<input type="text" value=""/>	<input type="text" value="New Volume"/>	<input type="text" value="主分区"/>

已使用: **1.2 GB** 分区大小:

未分配的空间

在分区后放置

▼

7.0

↑
↓

GB

i 您可以使用 Acronis Disk Director 在未分配的空间上创建分区。
[了解更多有关 Acronis Disk Director 的信息](#)

您可以更改以下分区属性：

- 代号
- 标识
- 类型

您可以将分区设为主分区、活动主分区或逻辑分区。

- 大小

通过在屏幕的水平栏上用鼠标拖动右边框，您可以调整分区的大小。要为分区指定特定大小，请在分区大小字段中输入相应数值。您还可以在分区前后选择未分配空间的位置。

统一扩展固件接口 (UEFI)

使用 Acronis Cyber Protect Home Office 还可以将 **BIOS** 转换为 **UEFI** 系统。

UEFI 是什么？

统一扩展固件接口 (UEFI) 是通过设置启动和运行时服务的标准语法，以提供更好的软件互操作性的规格。有关 UEFI 的更多信息，请访问 <http://www.uefi.org>。

以下操作系统支持 UEFI 技术：

- Windows 8 (x86) 及更高版本的 x86 版 Windows。
- Windows Vista SP1 (x64) 及更高版本的 x64 版 Windows。

为什么使用 UEFI?

- **与 BIOS 兼容** - 由于兼容支持模块 (CSM), 基于 UEFI 的系统还可以启动基于 BIOS 的操作系统。
- **从大型磁盘启动** - 基于 UEFI 的系统支持 GPT 分区布局, 该分区布局允许超过 2^{32} 个扇区的磁盘。
- **独立 CPU 体系结构** - 所有处理器体系结构的 UEFI 都很相似。
- **独立 CPU 驱动程序** - UEFI 规格包括 EFI 字节码 (EBC) 并允许创建可在任何系统上运行的 EBC 映像(驱动程序)。
- **灵活的前操作系统环境** - 基于 UEFI 的系统可在任何硬件上启动。
- **模块化设计** - UEFI 允许单个组件升级而不影响其他组件。

注意

因为 UEFI 是一项新技术, 并非所有系统都支持。请向您的硬件生产商咨询您的计算机是否支持 UEFI。

如何在 BIOS 中启用 UEFI?

以下描述了在 BIOS 中开启/关闭 UEFI 的典型方法:

1. 启动过程中, 屏幕上将会显示一条信息, 告知您进入 BIOS 设置程序所需的按键。通常该键为 [Del] 或 [F2]。
2. 使用方向键调用 **启动选项** 菜单。
3. 进入 **UEFI 启动** 项并选择 **启用**(或请选择 **禁用**, 条件是要在系统中 **关闭 UEFI**)。
4. 导航至 **保存并退出设置** 然后按 **Enter** 键以保存更改并启动系统。

如果在启用 UEFI 过程中需要帮助, 请联系硬件生产商。

如何将初始系统迁移至更大的硬盘驱动器?

Acronis Cyber Protect Home Office 现在可从原先创建的存档中将系统迁移或还原至超过 2^{32} 字节的硬盘驱动器(磁盘容量为 2 TB, 带标准 512 字节逻辑扇区或磁盘容量为 16 TB, 带 4 KB [4096 字节] 逻辑扇区)。

这可以通过使用 Acronis 媒体或启动至安装了 Acronis Cyber Protect Home Office 的基于 UEFI 的操作系统来实现:

使用 **Acronis** 媒体迁移系统

1. 从 Acronis 媒体启动系统。
2. 在启动菜单中选择 **Acronis Cyber Protect Home Office(完整版)** 以继续从媒体启动。
3. 导航至所需的向导(**还原**或**克隆**)并按照指示进行操作。

将系统迁移至基于 **UEFI** 的操作系统

1. 启动至支持 UEFI 的 Windows 操作系统。
2. 运行 Acronis Cyber Protect Home Office, 转至 **备份与恢复** 选项卡, 单击工具栏上的 **恢复** 并按照说明进行操作。

分区布局

分区布局定义了操作系统组织硬盘驱动器的方法：

- **MBR(主引导记录)**- 一个 512 字节的引导扇区，是硬盘的第一个扇区，用于放置磁盘的主分区表。

MBR 是标准的分区方案，用于多数硬盘驱动器中。MBR 的主要限制是最多仅支持 2 TB 的硬盘大小，因此无法使用现代大型硬盘驱动器 - 用户无法访问超过 2 TB 的空间。

- **GPT(GUID 分区表)**- 用于硬盘分区表布局的新标准。

GPT 允许磁盘/分区的最大容量为 9.4 ZB(9.4 x 10²¹ 字节)。

下表显示了支持读取 GPT 磁盘和/或从该类磁盘启动的操作系统：

	支持读取 GPT 磁盘的操作系统	可从 GPT 磁盘启动的操作系统
Windows XP x32	否	否
Windows XP x64	是	否
Windows Vista x32	是	否
Windows Vista x64	是	否
Windows Vista x64 SP1 或更高版本	是	是
Windows 7 x32	是	否
Windows 7 x64	是	是
Windows 8 x32	是	是
Windows 8 x64	是	是
Windows 8.1 x32	是	是
Windows 8.1 x64	是	是
Windows 10 x32	是	是
Windows 10 x64	是	是
Windows 11	是	是

表 1. 超过 2 TB 的目标磁盘

下表显示了将源磁盘迁移至大型硬盘(超过 2 TB)的所有可用选项。

如果源磁盘为 MBR，需要选择将目标磁盘保留为 MBR，还是使用 Acronis Cyber Protect Home Office 将其转换为 GPT。

根据系统参数的不同，每个选项都各有利弊。主要表现在目标磁盘的可启动性和使用大型磁盘的所有空间的能力上。

	我的系统从 BIOS 启动(Windows 或 Acronis 可启动媒体)	我的系统从 UEFI 启动(Windows 或 Acronis 可启动媒体)
源磁盘为 MBR 且操作系统不支持 UEFI	分区样式在克隆后将保留为 MBR, Acronis 总线驱动程序将安装至克隆的操作系统中。同时,由于 MBR 不支持超过 2TB 的硬盘驱动器,您将无法使用超过 2TB 的磁盘空间。要使用整个磁盘空间,需要将分区样式更改为 GPT,或在操作完成后重新启动 Acronis Cyber Protect Home Office 并使用 Acronis Extended Capacity Manager,让添加新磁盘工具识别超过 2TB 的磁盘空间。	<p>您可以选择以下所需的迁移方法之一:</p> <ul style="list-style-type: none"> 按原样复制源分区 <p>分区样式将保留为 MBR,但在操作完成后,操作系统将无法从 UEFI 启动。Acronis 总线驱动程序将安装至克隆的操作系统中。同时,由于 MBR 不支持超过 2TB 的硬盘驱动器,您将无法使用超过 2TB 的磁盘空间。要使用整个磁盘空间,需要将分区样式更改为 GPT,或在操作完成后重新启动 Acronis Cyber Protect Home Office 并使用 Acronis Extended Capacity Manager,让添加新磁盘工具识别超过 2TB 的磁盘空间。</p> <ul style="list-style-type: none"> 将分区样式转换为 GPT <p>目标分区将转换为 GPT 样式。该方法可用于非系统磁盘,因为操作系统不支持 UEFI。整个磁盘空间都将可用。</p>
源磁盘为 MBR 且操作系统支持 UEFI	迁移后,分区样式将保留为 MBR。Acronis 总线驱动程序将安装至克隆的操作系统中。由于 MBR 不支持超过 2TB 的硬盘驱动器,您将无法使用超过 2TB 的磁盘空间。要使用整个磁盘空间,需要将分区样式更改为 GPT,或在操作完成后重新启动 Acronis Cyber Protect Home Office 并使用 Acronis Extended Capacity Manager,让添加新磁盘工具识别超过 2TB 的磁盘空间。	目标磁盘的分区样式将自动转换为 GPT。该磁盘可用于在 UEFI 中启动。同时,整个磁盘空间都将可用。
源磁盘为 MBR 且操作系统为非 Windows 或无操作系统	<p>您可以选择以下所需的迁移方法之一:</p> <ul style="list-style-type: none"> 按原样复制源分区 <p>分区样式将保留为 MBR,但由于 MBR 不支持超过 2TB 的硬盘驱动器,您将无法使用超过 2TB 的磁盘空间。要使用整个磁盘空间,需要将分区样式更改为 GPT,或在操作完成后重新启动 Acronis Cyber Protect Home Office 并使用 Acronis Extended Capacity Manager,让添加新磁盘工具识别超过 2TB 的磁盘空间。</p> <ul style="list-style-type: none"> 将分区样式转换为 GPT <p>操作完成后,分区样式将转换为 GPT。由于源磁盘上未安装 Windows 操作系统,目标磁盘将无法用于启动。整个磁盘空间</p>	<p>您可以选择以下所需的迁移方法之一:</p> <ul style="list-style-type: none"> 按原样复制源分区 <p>分区样式将保留为 MBR,但由于 MBR 不支持超过 2TB 的硬盘驱动器,您将无法使用超过 2TB 的磁盘空间。要使用整个磁盘空间,需要将分区样式更改为 GPT,或在操作完成后重新启动 Acronis Cyber Protect Home Office 并使用 Acronis Extended Capacity Manager,让添加新磁盘工具识别超过 2TB 的磁盘空间。</p> <ul style="list-style-type: none"> 将分区样式转换为 GPT <p>目标分区将转换为 GPT 样式。由于源磁盘上未安装 Windows 操作系统,目标磁盘将无法用于启动。同时,整个磁盘空间都将可用。</p>

	都将可用。	
源磁盘为 GPT 且操作系统支持 UEFI	迁移后，分区样式将保留为 GPT。由于操作系统不支持从 BIOS 的 GPT 上启动，在操作完成后，系统将无法从 BIOS 启动。整个磁盘空间都将可用。	该操作不会影响分区布局或磁盘的可启动性：分区形式将保留为 GPT，目标磁盘可在 UEFI 中启动。整个磁盘空间都将可用。
源磁盘为 GPT 且操作系统为非 Windows 或无操作系统	该操作不会影响分区布局或磁盘的可启动性：分区形式将保留为 GPT，目标磁盘将不可启动。整个磁盘空间都将可用。	该操作不会影响分区布局或磁盘的可启动性：分区形式将保留为 GPT，目标磁盘不可在 UEFI 中启动。整个磁盘空间都将可用。

表 2. 小于 2 TB 的目标磁盘

下表显示了将源磁盘迁移至小于 2TB 的硬盘的可用选项。

如果源磁盘为 MBR，需要选择将目标磁盘保留为 MBR，还是使用 Acronis Cyber Protect Home Office 将其转换为 GPT。

根据系统参数的不同，每个选项都各有利弊。主要表现在目标磁盘的可启动性上。

	我的系统从 BIOS 启动 (Windows 或 Acronis 可启动媒体)	我的系统从 UEFI 启动 (Windows 或 Acronis 可启动媒体)
源磁盘为 MBR 且操作系统不支持 UEFI	该操作不会影响分区布局或磁盘的可启动性：分区样式将保留为 MBR，目标磁盘可在 BIOS 启动。整个磁盘空间都将可用。	操作完成后，分区样式将保留为 MBR，但操作系统将无法从 UEFI 启动，因为操作系统不支持。
源磁盘为 MBR 且操作系统支持 UEFI	该操作不会影响分区布局或磁盘的可启动性：分区样式将保留为 MBR，目标磁盘可在 BIOS 启动。整个磁盘空间都将可用。	目标分区将转换为 GPT 样式，这样，目标磁盘就可在 UEFI 中启动。整个磁盘空间都将可用。
源磁盘为 MBR 且操作系统为非 Windows 或无操作系统	<p>您可以选择以下所需的迁移方法之一：</p> <ul style="list-style-type: none"> • 按原样复制源分区 <p>分区样式将保留为 MBR。目标磁盘将不可启动，因为系统中未检测到 Windows 操作系统。</p> <ul style="list-style-type: none"> • 将分区样式转换为 GPT <p>目标磁盘将转换为 GPT 样式并作为非系统磁盘使用，因为操作系统不支持在 BIOS 上从 GPT 启动。</p>	<p>您可以选择以下所需的迁移方法之一：</p> <ul style="list-style-type: none"> • 按原样复制源分区 <p>分区样式将保留为 MBR。目标磁盘将不可启动，因为系统中未检测到 Windows 操作系统。</p> <ul style="list-style-type: none"> • 将分区样式转换为 GPT <p>目标分区将转换为 GPT 样式并作为非系统磁盘使用，因为系统中未检测到 Windows 操作系统。</p>
源磁盘为 GPT 且操作系统支持 UEFI	操作完成后，分区样式将保留为 GPT，但系统将无法在 BIOS 上启动，因为操作系统不支持在 BIOS 上从 GPT 启动。	操作完成后，分区样式将保留为 GPT，操作系统可在 UEFI 上启动。

源磁盘为 GPT 且操作系统为非 Windows 或无操作系统	操作完成后,分区样式将保留为 GPT,但系统将无法从 BIOS 启动,因为操作系统不支持在 BIOS 上从 GPT 启动。	操作完成后,分区样式将保留为 GPT,系统将无法启动,因为系统中未检测到 Windows 操作系统。
---------------------------------	---	--

迁移方法

Acronis Cyber Protect Home Office 允许您在恢复操作完成后为目标磁盘选择分区布局:

- **MBR(主引导扇区)**- 一个 512 字节的引导扇区,是硬盘的第一个扇区,用于放置磁盘的主分区表。
- **GPT(GUID 分区表)**- 用于硬盘分区表布局的标准。GPT 允许磁盘/分区的最大容量为 9.4 ZB(9.4 x 10²¹ 字节)。

使用该向导可在恢复操作的同时转换分区布局,或保持源布局:

- **按原样复制分区** - 选择该选项,迁移系统而不更改分区布局。注意,在这种情况下超过 2TB 的磁盘空间将无法访问。若要分配超过 2TB 的磁盘空间,必须使用 Acronis Extended Capacity Manager。
- **复制分区,将磁盘作为非系统磁盘使用,保留 GPT 样式** - 选择此选项将分区转换为 GPT 布局。

使用 Acronis Cyber Protect Home Office 还可以将 **BIOS** 转换为 **UEFI** 系统。

BIOS 启动系统、MBR、不支持 UEFI

请在向导的本步骤选择目标硬盘。

当前系统包括:

系统: BIOS 启动

源分区样式: MBR

源磁盘的操作系统: Windows, 不支持在 UEFI 启动

目标磁盘大小: 小于 2 TB

如果将系统迁移到选定的磁盘:

系统: BIOS 启动

分区样式: MBR

操作系统: Windows, 不支持在 UEFI 启动

磁盘大小: 整个磁盘空间可用

有关迁移步骤的更多信息,请查阅[迁移方法](#)部分。

BIOS 启动的系统、MBR、支持 UEFI

请在向导的本步骤选择目标硬盘。

当前系统包括：

系统：BIOS 启动

源分区样式：MBR

源磁盘的操作系统：Windows, 支持在 UEFI 启动

目标磁盘大小：小于 2 TB

如果将系统迁移到选定的磁盘：

系统：BIOS 启动

分区样式：MBR

操作系统：Windows, 支持在 UEFI 启动

磁盘大小：整个磁盘空间可用

有关迁移步骤的更多信息，请查阅[迁移方法](#)部分。

BIOS 启动系统、MBR、非 Windows

Acronis Cyber Protect Home Office 允许您在操作完成后为目标磁盘选择分区布局。

当前系统包括：

系统：BIOS 启动

源分区样式：MBR

源磁盘的操作系统：非 Windows 或无 OS

目标磁盘大小：小于 2 TB

使用这些系统参数可以选择以下一项：

1. 按原样复制分区

在目标磁盘上保留 MBR 分区样式。

迁移后的目标磁盘：

系统：BIOS 启动

分区样式：MBR

操作系统：非 Windows 或无 OS

磁盘大小：整个磁盘空间可用

2. 复制分区并将磁盘用作非系统的 GPT 样式

可将分区样式转换为 GPT。

迁移后的目标磁盘：

系统：在 BIOS 中不可启动

分区样式:GPT

操作系统:非 Windows 或无 OS

磁盘大小:整个磁盘空间可用

警告!

迁移完成后,目标磁盘仅可作为非系统磁盘使用。如果 Acronis Cyber Protect Home Office 在 Windows XP x32 操作系统中运行,则该选项不可用。

有关迁移步骤的更多信息,请查阅[迁移方法](#)部分。

BIOS 启动系统、GPT、支持 UEFI

请在向导的本步骤选择目标硬盘。

当前系统包括:

系统:BIOS 启动

源分区样式:GPT

源磁盘的操作系统:Windows, 支持在 UEFI 启动

如果将系统迁移到选定的磁盘:

系统:在 BIOS 中不可启动

分区样式:GPT

操作系统:Windows, 支持在 UEFI 启动

磁盘大小:整个磁盘空间可用

警告!

迁移完成后,操作系统将无法从目标磁盘在 BIOS 中启动。如果想在迁移后从目标磁盘启动,则需要要在系统中启用 UEFI 启动(请参阅“统一扩展固件接口”部分),然后重新启动操作。

有关迁移步骤的更多信息,请查阅[迁移方法](#)部分。

BIOS 启动系统、GPT、非 Windows

请在向导的本步骤选择目标硬盘。

当前系统包括:

系统:BIOS 启动

源分区样式:GPT

源磁盘的操作系统:非 Windows 或无 OS

如果将系统迁移到选定的磁盘:

系统:BIOS 启动

分区样式:GPT

操作系统:非 Windows 或无 OS

磁盘大小:整个磁盘空间可用

有关迁移步骤的更多信息,请查阅[迁移方法](#)部分。

UEFI 启动系统、MBR、不支持 UEFI

请在向导的本步骤选择目标硬盘。

当前系统包括:

系统:UEFI 启动

源分区样式:MBR

源磁盘的操作系统:Windows, 不支持在 UEFI 启动

目标磁盘大小:小于 2 TB

如果将系统迁移到选定的磁盘:

系统:在 UEFI 中不可启动

分区样式:MBR

操作系统:Windows, 不支持在 UEFI 启动

磁盘大小:整个磁盘空间可用

警告!

操作系统可能无法从目标磁盘在 UEFI 中启动。

有关迁移步骤的更多信息,请查阅[迁移方法](#)部分。

UEFI 启动的系统、MBR、支持 UEFI

请在向导的本步骤选择目标硬盘。

当前系统包括:

系统:UEFI 启动

源分区样式:MBR

源磁盘的操作系统:Windows, 支持在 UEFI 启动

如果将系统迁移到选定的磁盘:

迁移完成后,目标分区样式将转换为 GPT 并从此处启动。

迁移后的目标磁盘:

系统:UEFI 启动

分区样式:GPT

操作系统:Windows, 支持在 UEFI 启动

磁盘大小:整个磁盘空间可用

有关迁移步骤的更多信息, 请查阅[迁移方法](#)部分。

UEFI 启动系统、MBR、非 Windows

Acronis Cyber Protect Home Office 允许您在操作完成后为目标磁盘选择分区布局。

当前系统包括:

系统:UEFI 启动

源分区样式:MBR

源磁盘的操作系统:非 Windows 或无 OS

目标磁盘大小:小于 2 TB

使用这些系统参数可以选择以下一项:

1. 按原样复制分区

在目标磁盘上保留 MBR 分区样式。

迁移后的目标磁盘:

系统:UEFI 启动

分区样式:MBR

操作系统:非 Windows 或无 OS

磁盘大小:整个磁盘空间可用

2. 复制分区并将磁盘用作非系统的 GPT 样式

可将分区样式转换为 GPT。

迁移后的目标磁盘:

系统:在 UEFI 中不可启动

分区样式:GPT

操作系统:非 Windows 或无 OS

磁盘大小:整个磁盘空间可用

警告!

迁移完成后, 目标磁盘仅可作为非系统磁盘使用。

有关迁移步骤的更多信息, 请查阅[迁移方法](#)部分。

UEFI 启动系统、GPT、支持 UEFI

请在向导的本步骤选择目标硬盘。

当前系统包括：

系统：UEFI 启动

源分区样式：GPT

操作系统：Windows, 支持在 UEFI 启动

如果将系统迁移到选定的磁盘：

系统：UEFI 启动

分区样式：GPT

磁盘大小：整个磁盘空间可用

有关迁移步骤的更多信息，请查阅[迁移方法](#)部分。

UEFI 启动系统、GPT、非 Windows

请在向导的本步骤选择目标硬盘。

当前系统包括：

系统：UEFI 启动

源分区样式：GPT

操作系统：非 Windows 或无 OS

如果将系统迁移到选定的磁盘：

系统：UEFI 启动

分区样式：GPT

磁盘大小：整个磁盘空间可用

有关迁移步骤的更多信息，请查阅[迁移方法](#)部分。

5.1.3 关于恢复动态/GPT 磁盘和卷

恢复动态卷

您可以将动态卷恢复至本地硬盘的以下位置：

- 动态卷。

注意

不支持在恢复至动态磁盘时手动调节动态卷的大小。若需在恢复操作时调节动态卷的大小，应将其恢复至基本磁盘。

- 原位置(同一动态卷)。

目标卷类型不变。

- **另一动态磁盘或卷。**
目标卷类型不变。例如，在动态跨区卷上恢复动态带区卷时，目标卷仍将为跨区卷。
- **动态组的未分配空间。**
恢复的卷类型将与它原来在备份中的卷类型相同。
- **基本卷或磁盘。**
目标卷保持为基本卷。
- **裸机恢复。**
若要将动态卷“裸机恢复”至尚未格式化的新磁盘上，恢复后的卷将变为基本卷。如果希望恢复后的卷保持动态状态，则目标磁盘应预处理成动态状态(已分区和格式化)。这可以通过使用第三方工具来完成，例如 Windows 的“磁盘管理”管理单元。

恢复基本卷和磁盘

- 在将基本卷恢复至动态组的未分配空间时，恢复后的卷将变为动态卷。
- 在将基本磁盘恢复至包含两个磁盘的动态组的动态磁盘时，恢复后的磁盘仍将是基本磁盘。执行了恢复操作的动态磁盘将“丢失”，而第二个磁盘上的跨区/带区动态卷将“失败”。

恢复后的分区样式

目标磁盘的分区样式取决于您的计算机是否支持 UEFI，还取决于您的系统是由 BIOS 启动还是由 UEFI 启动。参见下表：

	我的系统从 BIOS 启动(Windows 或 Acronis 可启动媒体)	我的系统从 UEFI 启动(Windows 或 Acronis 可启动媒体)
源磁盘为 MBR 且操作系统不支持 UEFI	该操作不会影响分区布局或磁盘的可启动性：分区样式将保留为 MBR，目标磁盘可在 BIOS 启动。	操作完成后，分区样式将转换成 GPT 样式，但操作系统将无法从 UEFI 启动，因为操作系统不支持。
源磁盘为 MBR 且操作系统支持 UEFI	该操作不会影响分区布局或磁盘的可启动性：分区样式将保留为 MBR，目标磁盘可在 BIOS 启动。	目标分区将转换为 GPT 样式，这样，目标磁盘就可在 UEFI 中启动。请参阅 恢复至 UEFI 系统的示例
源磁盘为 GPT 且操作系统支持 UEFI	操作完成后，分区样式将保留为 GPT，但系统将无法在 BIOS 上启动，因为操作系统不支持在 BIOS 上从 GPT 启动。	操作完成后，分区样式将保留为 GPT，操作系统可在 UEFI 上启动。

恢复过程的示例

请参阅[恢复至 UEFI 系统的示例](#)

恢复至 UEFI 系统的示例

下面的示例说明如何传输条件如下的系统：

- 源磁盘为 MBR 且操作系统支持 UEFI。
- 目标系统是由 UEFI 启动。

- 旧的和新的硬盘驱动器必须在相同的控制器模式(例如 IDE 或 AHCI)下工作。

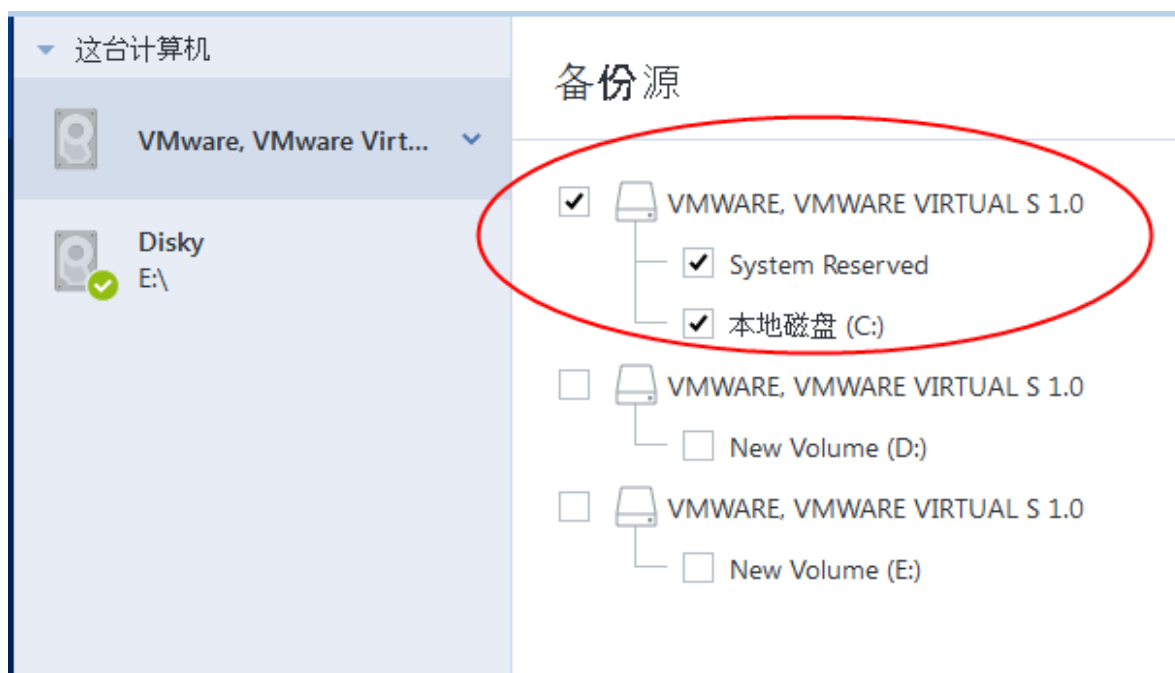
在开始该过程之前,请确保您具有:

- **Acronis 可启动媒体。**

有关详细信息,请参阅[创建 Acronis 可启动媒体](#)。

- **系统磁盘的备份以磁盘模式创建。**

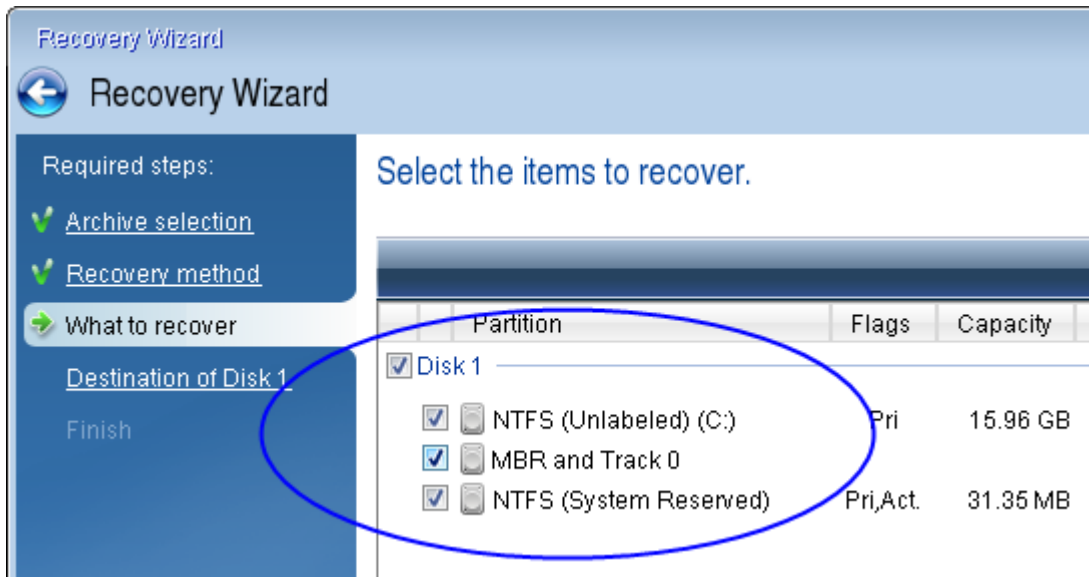
若要创建此备份,请切换至磁盘模式,然后选择包含系统分区的硬盘。有关详细信息,请参阅[备份磁盘和分区](#)。



将系统从 MBR 磁盘传输到由 UEFI 启动的计算机

1. 在 UEFI 模式下,从 Acronis 可启动媒体启动,并选择 Acronis Cyber Protect Home Office。
2. 运行[恢复向导](#)并按照[恢复系统](#)中所述的说明操作。
3. 在[恢复内容](#)步骤上,选中磁盘名称旁边的复选框以选择整个系统磁盘。

在下面的示例中,您需要选中**磁盘 1**复选框:



4. 在**完成**步骤上, 单击**继续**。

操作完成后, 便会将目标磁盘转换为 GPT 样式, 以使它能够以 UEFI 模式启动。

恢复之后, 请确保以 UEFI 模式启动计算机。您可能需要在 UEFI 启动管理器的用户界面中更改系统磁盘的启动模式。

5.1.4 在 BIOS 或 UEFI BIOS 中设置启动顺序

若要从 Acronis 可启动媒体启动您的计算机, 您需要设置启动顺序, 以便将该媒体设置为第一启动设备。在 BIOS 或 UEFI BIOS 中更改启动顺序, 具体取决于您的计算机固件界面。在 BIOS 或 UEFI BIOS 中更改启动顺序的步骤非常类似。

从 Acronis 可启动媒体启动

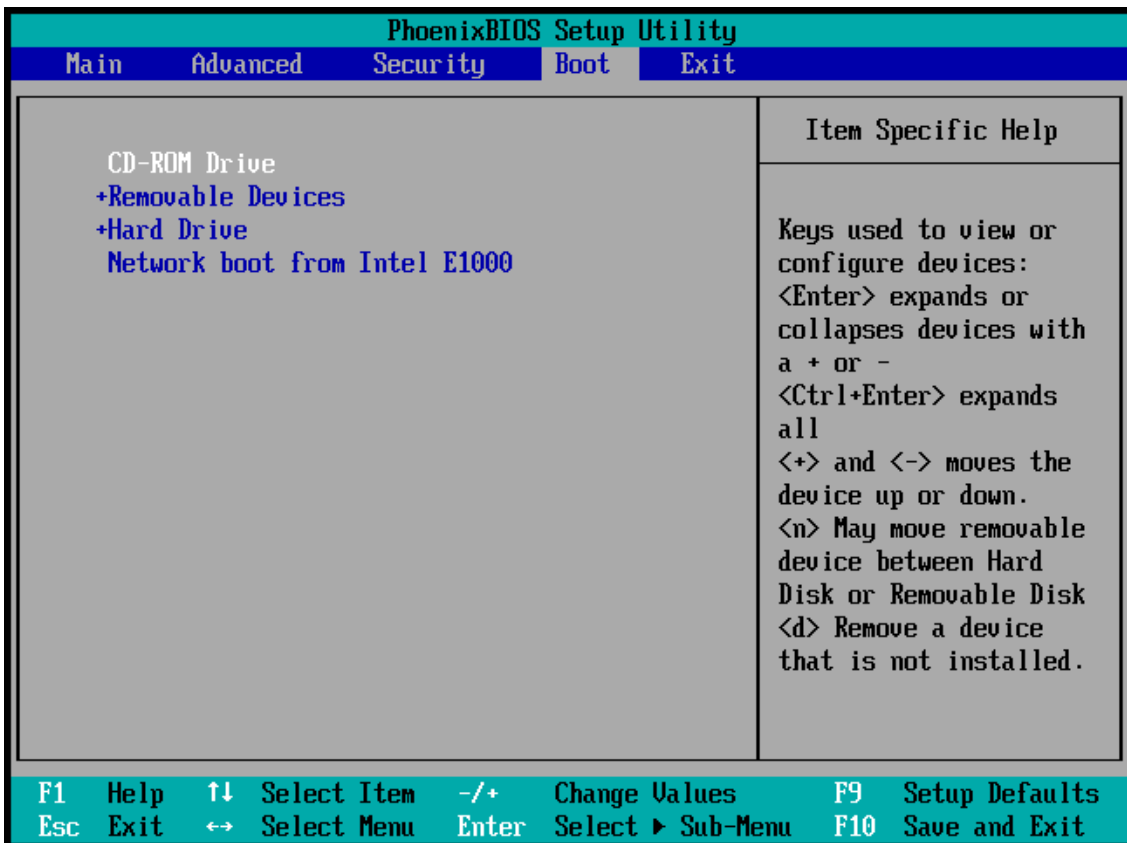
1. 如果您使用 USB 闪存驱动器或外部驱动器作为可启动媒体, 请将其插入 USB 端口。
2. 打开计算机。在开机自检 (POST) 过程中, 您将看到进入 BIOS 或 UEFI BIOS 需要按的组合键。
3. 按下组合键(例如 **Del**、**F1**、**Ctrl+Alt+Esc**、**Ctrl+Esc**)。BIOS 或 UEFI BIOS 设置实用工具将会打开。请注意, 实用工具的外观、项目集及其名称等可能不尽相同。

注意

某些主板具有所谓的启动菜单, 可通过按特定键或组合键(例如 **F12**) 将其打开。启动菜单允许您从可启动设备列表中选择启动设备, 而无需更改 BIOS 或 UEFI BIOS 设置。

4. 如果您使用 CD 或 DVD 作为可启动媒体, 请将其插入 CD 或 DVD 驱动器。
5. 将您的可启动媒体(CD、DVD 或 USB 驱动器) 设备设置为第一启动设备:
 - a. 使用键盘上的箭头键导航至“启动顺序”设置。
 - b. 将指针置于您的启动媒体设备上, 然后将其设置为列表中的第一项。您通常可以使用“加号”

或“减号”键更改顺序。



6. 退出 BIOS 或 UEFI BIOS 并保存您所做的更改。计算机将从 Acronis 可启动媒体启动。

注意

如果计算机从第一设备启动失败，则会尝试从第二设备启动，以此类推。

5.1.5 从云恢复磁盘

从 Acronis Cloud 恢复磁盘与从普通硬盘驱动器进行恢复非常相似。

- 如果您可以启动 Windows 和 Acronis Cyber Protect Home Office，请参阅 [恢复分区和磁盘](#)。
- 如果 Windows 无法启动，请参阅 [从 Acronis Cloud 恢复系统](#)。

工作方式

您的计算机应通过互联网线缆或通过 Wi-Fi 连接到互联网。Acronis Cyber Protect Home Office 支持几种无线安全协议，包括 WPA-Personal、WPA2-Personal 和 WPA2-Enterprise。

恢复到原始位置

如果将磁盘恢复到原始位置，Acronis Cyber Protect Home Office 不会将整个磁盘空间下载到您的计算机。它将扫描您的磁盘，搜索数据更改并仅恢复与图像中的文件不同的文件。此技术可显著减少下载量以便恢复磁盘所需的数据量。

恢复到新位置

将磁盘恢复到其他位置或未分配的空间时，过程与从本地存储进行恢复非常相似。唯一的区别在于数据写入方法。Acronis Cyber Protect Home Office 会按单独的块下载和写入数据，而不是持续下载和写入。此技术可提高恢复速度以及整个过程的可靠性。

恢复中断时的操作

由于从 Acronis Cloud 恢复磁盘需要使用互联网连接并且通常需要较长的时间，因此与从普通硬盘进行恢复相比，恢复中断的可能性更高。

恢复中断的可能原因：

- Internet 连接已丢失。
- 到 Acronis Cloud 的连接已丢失。
- 您故意或意外地取消了恢复。
- 供电问题。

如果恢复因连接问题而未完成，Acronis Cyber Protect Home Office 将自动尝试重新连接到 Acronis Cloud 并继续恢复过程。在这种情况下，建议检查您的 Internet 连接设置。如果所有自动尝试均告失败，当连接恢复时，请再次手动运行恢复。

在其他情况下，请再次手动运行恢复并确保恢复已完成。

无论中断原因如何，Acronis Cyber Protect Home Office 都不会从头开始恢复。它将继续该过程并仅下载未恢复的数据。

从 Acronis Cloud 恢复您的系统

注意

根据您的互联网连接速度，从 Acronis Cloud 恢复磁盘可能需要较长的时间。

在开始之前，我们建议您先完成[准备恢复](#)中所描述的准备工作。如果将您的系统恢复到新的磁盘中，您无需格式化新磁盘，因为在恢复过程中会执行格式化。

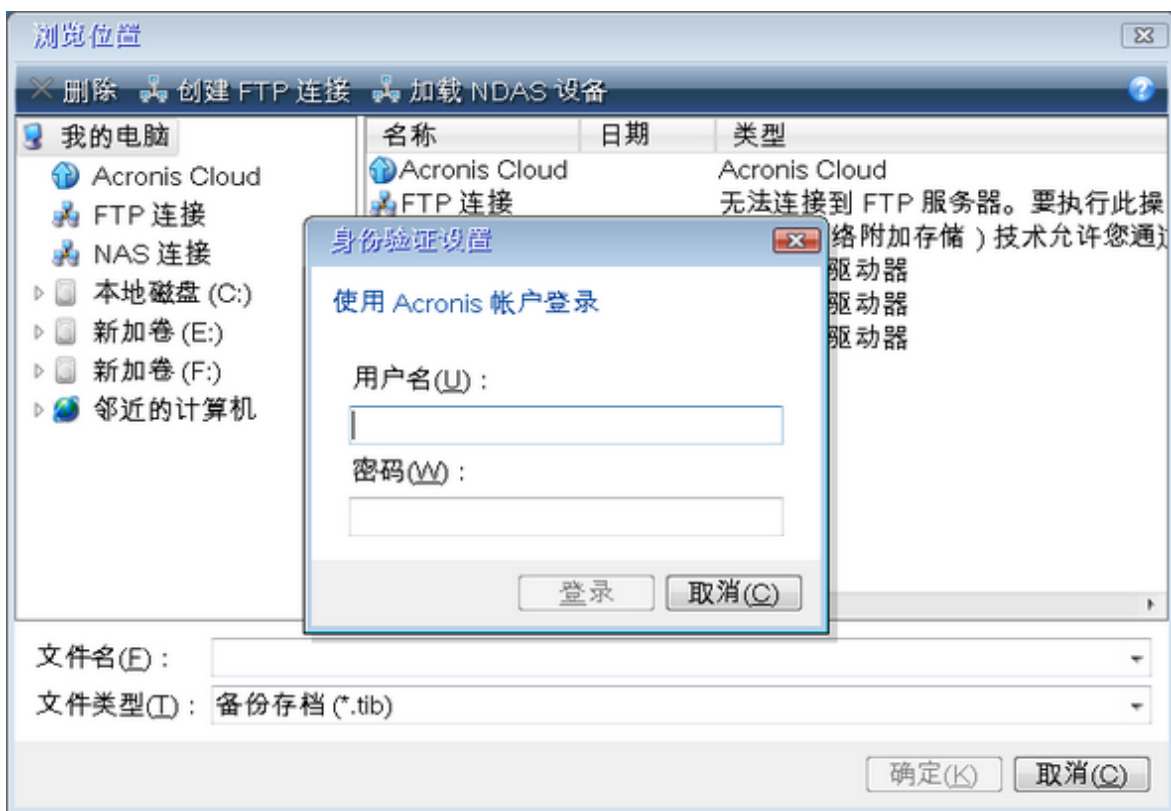
在开始此过程之前，请确保您的计算机已通过以太网电缆或 Wi-Fi 连接到 Internet。

从 **Acronis Cloud** 恢复系统磁盘

1. 设置 BIOS 启动顺序，从而将您的 Acronis 可启动媒体 (CD、DVD 或 USB 闪存盘) 设置为第一启动设备。请参阅[设置 BIOS 启动顺序](#)。
2. 从可启动媒体启动，并选择 **Acronis Cyber Protect Home Office**。
3. 在主页屏幕上，选择**恢复**下方的**我的磁盘**。



4. 若要将系统磁盘或系统分区的线上备份添加到可用备份列表, 请单击**浏览**。
5. 在已打开窗口的目录树中, 选择 Acronis Cloud 并输入您的 Acronis 帐户的凭据。



6. 选择要用于恢复的备份, 然后单击**确定**。
7. 在**选择存档**步骤中, 选择线上备份并单击**下一步**。



8. 在**恢复方法**步骤中, 选择恢复整个磁盘和分区。
9. 在**恢复内容**步骤中, 选择系统分区(一般为 C)以及系统保留分区(如果有)。您也可以通过 **Pri**、**Act** 标志识别分区。



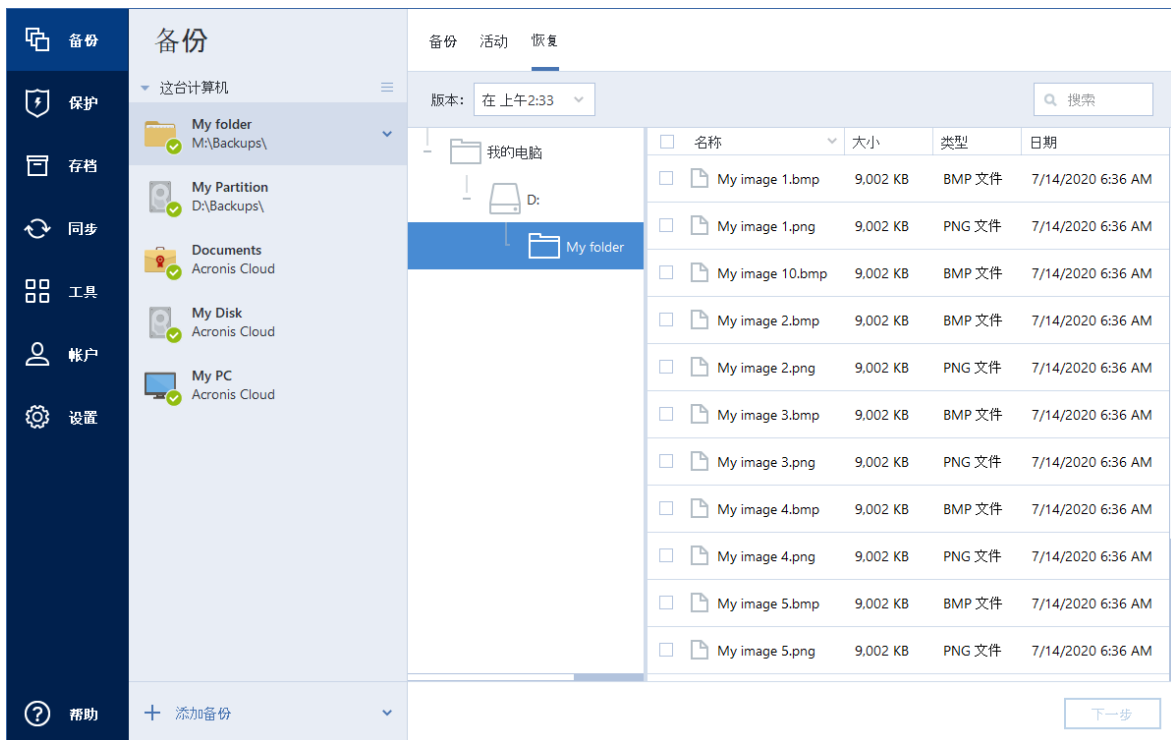
10. 在“分区 C 的设置”(如果分区不同,则为系统分区的代号)步骤中,根据需要更改设置。例如,恢复到不同容量的新硬盘时,您需要更改设置。
11. 在**完成**步骤中仔细阅读操作摘要。如果没有重新调整分区的大小,那么**删除分区**和**恢复分区**项目中的大小必需匹配。单击**继续**。
12. 当恢复完成时,退出单机版 Acronis Cyber Protect Home Office, 移除可启动媒体。从恢复的系统分区启动。确保已将 Windows 恢复到需要的状态后, **还原原始启动顺序**。

5.2 恢复文件和文件夹

您可以在 Acronis Cyber Protect Home Office、文件资源管理器或 Acronis Cloud 中浏览和恢复备份的文件与文件夹。您可以从文件级和磁盘级备份中恢复文件和文件夹。

在 Acronis Cyber Protect Home Office 中恢复数据的方法

1. 在侧栏上单击**备份**。
2. 从备份列表中,选择包含您要恢复的文件或文件夹的备份,然后打开**恢复**选项卡。
3. [可选]在工具栏的**版本**下拉列表中,选择所需日期和时间的备份。默认情况下,将恢复最新的备份。
4. 选中您要恢复的相应文件或文件夹的复选框,然后单击**下一步**。



5. [可选] 默认情况下, 将在原始位置恢复数据。要更改该位置, 请单击工具栏上的**浏览**, 然后选择所需的文件夹。
6. [可选] 设置恢复进程的选项(恢复进程优先级、文件级安全设置等)。要设置选项, 请单击**恢复选项**。您在此设置的选项将只应用于当前恢复操作。
7. 要开始恢复, 请单击**立即恢复**按钮。
选定的文件版本将下载到指定的目标。
您可以通过单击**取消**停止恢复。请记住, 中途放弃的恢复仍可能导致目标文件夹被更改。

在文件资源管理器中恢复数据

1. 双击对应的 .tib 文件, 然后浏览到您要恢复的文件或文件夹。
2. 将该文件或文件夹复制到硬盘上。

注意

复制的文件将丢失“已压缩”和“已加密”属性。如需保留这些属性, 建议对备份进行恢复操作。

在 Acronis Cloud 中恢复数据的方法

1. 在左侧的侧栏上, 单击**备份**。
2. 从备份列表中选择包含您要恢复的文件或文件夹的云备份。
3. 从文件和文件夹列表中, 选择您要恢复的文件和文件夹。
4. [可选] 您可以恢复特定版本的文件(不是文件夹)。要进行此操作, 请单击右侧侧栏上的**版本**, 然后单击所需版本行上的下载图标。
5. 要开始恢复, 请单击右侧侧栏上的**下载**。
系统会将选定的数据复制到默认的下​​载文件夹。

注意

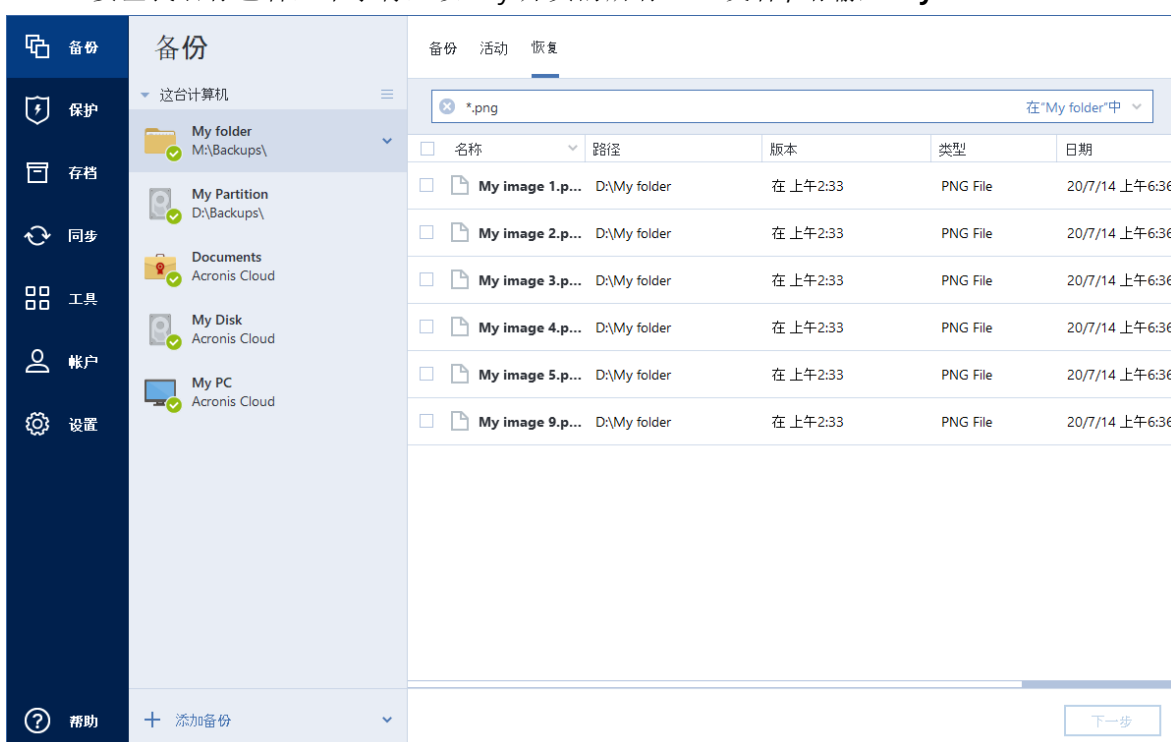
如果您选择了多个文件和文件夹，系统会将它们放入 zip 存档。

5.3 搜索备份内容

从本地备份恢复数据时，您可以搜索存储在选定备份中的特定文件和文件夹。

搜索文件和文件夹的方法

1. 按恢复分区和磁盘或恢复文件和文件夹中所述开始恢复数据。
2. 选择要恢复的文件和文件夹时，在搜索字段中输入文件或文件夹的名称。程序将显示搜索结果。您也可以使用常见的 Windows 通配符：* 和 ?。例如，要查找扩展名为 .exe 的所有文件，请输入 *.exe。要查找名称包含五个字符且以“my”开头的文件，请输入 My????.exe。



3. 默认情况下，Acronis Cyber Protect Home Office 将搜索在上一步中选择的文件夹。要在搜索中包括整个备份，请单击向下箭头，然后单击**整个备份**。
要返回上一步，请删除搜索文本，然后单击十字形图标。
4. 搜索完成后，选择要恢复的文件，然后单击**下一步**。

注意

请注意“版本”列。不能同时恢复属于不同备份版本的文件和文件夹。

5.4 恢复 Office 365 数据

通过 Acronis Cyber Protect Home Office，可以保护您的个人 Office 365 帐户，以免丢失电子邮件、文件和文件夹、个人资料信息和其他数据。如果您具有帐户数据的云备份，则可以浏览它以及恢复

特定项目。

5.4.1 可以恢复哪些项目？

可从邮箱备份中恢复以下项目：

- 整个邮箱
- 电子邮件
- 附件

可从 **OneDrive** 备份中恢复以下项目：

- 整个 OneDrive
- 备份的所有文件和文件夹

5.4.2 恢复 Office 365 数据

浏览并恢复数据的方法

1. 通过执行以下操作之一，打开在线控制面板：
 - 访问以下链接：<https://cloud.acronis.com>。
 - 在 Acronis Cyber Protect Home Office 的侧栏上，单击 **帐户**，然后单击 **打开在线控制面板**。
2. 登录您的 Acronis 帐户。
3. 在侧边栏上，单击 **资源**，找到 Office 365 备份框，然后单击 **恢复**。
4. 浏览备份列表。如有必要，使用过滤器按内容查找备份。
5. 选择备份后，单击 **恢复...**，然后选择要恢复的数据：
 - 整个 OneDrive 或特定文件和文件夹。
 - 整个邮箱或特定电子邮件。

当选择备份特定项目时，在线控制面板会打开已备份项目的列表。您可以浏览这些项目，查看其内容，以及使用搜索查找特定项目（不适用于某些数据类型）。

选择项目后，您可以选择要执行的操作（根据数据类型，某些操作可能不可用）：

- **显示内容** — 单击可查看项目详细信息或者以全尺寸将其打开。
 - **作为电子邮件发送** — 单击以将电子邮件发送给选定的收件人。
 - **显示版本** — 单击以查看项目的版本。
 - **恢复** — 单击以指定所恢复项目的位置。您也可以恢复某些项目的共享权限。
 - **下载** — 单击以下载选定的文件。
6. 单击 **开始恢复**。

5.5 恢复操作选择

您可以配置磁盘/分区及文件恢复流程的选项。在安装应用程序后，所有选项均被设为初始值。您可以只为当前恢复操作更改这些值，也可以为所有后续恢复操作更改这些值。选择 **将设置保存为默认值** 复选框以在默认情况下将修改的设置应用到所有后续恢复操作。

注意，磁盘恢复选项和文件恢复选项完全独立，应单独进行配置。

若要将所有修改的选项重置为安装产品之后设置的初始值，请单击**重置为初始设置**按钮。

5.5.1 磁盘恢复模式

位置：**恢复选项 > 高级 > 磁盘恢复模式**

使用此选项，您可选择适用于映像备份的磁盘恢复模式。

- **逐个扇区恢复** - 若要恢复磁盘或分区上已使用和未使用的扇区，请选中此复选框。此选项仅在您选择恢复逐个扇区的备份时才有效。

5.5.2 恢复前/后命令

位置：**恢复选项 > 高级 > 事前/事后命令**

您可以指定要在恢复程序之前和之后自动执行的命令(甚至批处理文件)。

例如，您可能想要开始/停止某个 Windows 进程，或在恢复前检查数据是否带有病毒。

若要指定命令(批处理文件)：

- 在**命令前**字段中，选择将要在恢复程序开始前执行的命令。若要创建新命令或选择新的批处理文件，请单击**编辑**按钮。
- 在**命令后**字段中，选择将要在恢复程序结束后执行的命令。若要创建新命令或选择新的批处理文件，请单击**编辑**按钮。

请勿尝试执行交互命令，即要求用户输入的命令(例如，“暂停”)。系统不支持这些命令。

编辑用于恢复的用户命令

您可以指定还原前后要进行的用户命令：

- 在**命令**字段中键入命令，或从列表中选择命令。单击 **...**，以选择批处理文件。
- 在**工作目录**字段中，输入执行命令的路径，或从先前输入的路径列表中选择路径。
- 在**参数**字段中输入命令执行参数，或从列表中选择。

禁用**命令执行完成后方进行操作**参数(默认为启用)，将允许在执行命令的同时运行恢复进程。

若**用户命令执行失败即中止操作**(默认为启用)参数会在命令执行出错时中止操作。

单击**测试命令**按钮可测试您所输入的命令。

5.5.3 验证选项

位置：**恢复选项 > 高级 > 验证**

- **恢复之前验证备份** - 启用此选项可在恢复之前检查备份的完整性。
- **恢复之后检查文件系统** - 启用此选项可检查已恢复分区上的文件系统的完整性。

注意

只有在 FAT16/32 和 NTFS 下才可进行文件系统检查。

注意

若恢复时要求重新启动(例如,将系统分区恢复至原始位置时),将不对文件系统进行检查。

5.5.4 计算机重新启动

位置: **恢复选项 > 高级 > 计算机重新启动**

如果希望计算机在恢复需要时自动重新启动,请选中**恢复需要时自动重新启动计算机**复选框。当操作系统锁定的分区必须恢复时,可能会使用此选项。

5.5.5 文件恢复选项

位置: **恢复选项 > 高级 > 文件恢复选项**

您可以选择以下文件恢复选项:

- **恢复文件及其原始安全性设置** — 如果在备份期间保留了文件安全性设置(请参见[备份的文件级安全性设置](#)),则可以选择是否要恢复它们,或者让这些文件继承它们将要恢复到的文件夹的安全性设置。此选项只在通过文件/文件夹备份恢复文件时才有效。
- **设置已恢复文件的当前日期和时间** - 您可以选择从备份恢复文件日期和时间,也可以选择为文件指定当前日期和时间。在默认情况下,系统将指定为备份内的文件日期和时间。

5.5.6 覆盖文件选项

位置: **恢复选项 > 高级 > 覆盖文件选项**

选择当程序在目标文件夹中找到与备份中名称相同的文件时要执行的操作。

注意

只有在恢复文件和文件夹(非磁盘和分区)时才可以此选项。

如果需要使用备份中的文件覆盖硬盘上的文件,请选择**覆盖现有文件**复选框。如果已取消勾选该复选框,那么较新的文件和文件夹将保留在磁盘上。

若不需要覆盖某些文件:

- 勾选**隐藏的文件和文件夹**复选框,以禁止覆盖所有隐藏的文件和文件夹。向本地目标和网络共享执行文件级别备份时可以使用此选项。
- 勾选**系统文件和文件夹**复选框,以禁止覆盖所有系统文件和文件夹。向本地目标和网络共享执行文件级别备份时可以使用此选项。
- 勾选**较新的文件和文件夹**复选框,以禁止覆盖新的文件和文件夹。
- 单击**添加特定文件和文件夹**,以管理不想覆盖的自定义文件和文件夹列表。向本地目标和网络共享执行文件级别备份时可以使用此选项。
 - 若要禁用覆盖特定文件,请单击加号,以创建排除标准。
 - 在指定标准时,可使用常用的 Windows 通配符。例如,若要保留所有以 **.exe** 为扩展名的文件,请添加 ***.exe**。添加 **My???.exe** 将保留名称含 5 个字符且以“my”开头的所有 .exe 文件。

若要删除某个标准,请在列表中进行选择,然后单击减号。

5.5.7 恢复操作的性能

位置: **恢复选项** > **高级** > **性能**

您可以配置以下设置:

操作优先级

更改备份或恢复进程的优先级会加快或减慢运行速度(视您提升还是降低优先级而定),但也会对其他运行中的程序的性能产生负面影响。系统中运行的任何进程的优先级可决定分配给该进程的 CPU 使用量和系统资源。降低操作优先级,可释放更多资源给其他 CPU 任务。提高备份或恢复优先级可加快进程,因为系统会从当前运行的其他程序中获取资源。实际效果依 CPU 使用总量和其他因素而定。

您可设置操作优先级:

- **低**(默认为启用) — 备份或恢复速度较慢,但是会提升其他程序的性能。
- **一般** — 备份或恢复进程与其他进程拥有同等优先级。
- **高** — 备份或恢复进程速度较快,但是会降低其他程序的性能。请注意,选择此选项可能导致 Acronis Cyber Protect Home Office 的 CPU 占用率达到 100%。

5.5.8 恢复操作的通知

位置: **恢复选项** > **通知**

有时备份或恢复过程可能持续一小时或更长时间。当该过程完成时, Acronis Cyber Protect Home Office 可以通过电子邮件通知您。在操作过程中,程序还可复制已发布的消息,或在操作完成后发送完整的操作日志。

所有通知默认禁用。

可用磁盘空间阈值

您可能希望系统在恢复存储上的可用空间小于指定阈值时向您发送通知。若在启动备份后, Acronis Cyber Protect Home Office 发现所选备份位置中的可用空间小于指定值,程序将不会启动实际的恢复进程,并会立即显示相应的消息通知您这一情况。消息将向您提供三种选择 — 忽略这一情况并继续恢复操作、浏览另一恢复位置,或取消恢复。

若在运行恢复时,出现可用空间小于指定值的情况,程序将显示相同的消息,请您再次做出决定。

设置可用磁盘空间阈值

- 选中**可用磁盘空间不足时显示通知消息**复选框。
- 在**大小**方框中键入或选择一个阈值,并选择度量单位。

Acronis Cyber Protect Home Office 可对以下存储设备的可用空间进行监控:

- 本地硬盘
- USB 卡和驱动器

- 网络共享 (SMB)

注意

若已在**错误处理**设置中勾选了**处理时不显示消息和对话框(无消息模式)**复选框,则将不会显示此消息。

注意

对于 CD/DVD 驱动器,此选项将无法启用。

电子邮件通知

1. 选中**发送有关操作状态的电子邮件通知**复选框。
2. 配置电子邮件设置:
 - 在**收件人**字段中输入电子邮件地址。您可输入多个电子邮件地址,并以分号隔开。
 - 在**服务器设置**字段中输入邮件发送服务器 (SMTP)。
 - 设置发送邮件服务器的端口。默认情况下,端口设为 25。
 - 如果需要,请选中 **SMTP 身份验证**复选框,然后在相应的字段中输入用户名和密码。
3. 若要检查设置是否正确,请单击**发送测试消息**按钮。

如果测试消息发送失败

1. 单击**显示扩展设置**。
2. 配置其他电子邮件设置:
 - 在**发件人**字段中输入发件人的电子邮件地址。如果您不确定要指定哪个地址,请以标准格式键入所需的任何地址,例如 *aaa@bbb.com*。
 - 视需要更改**主题**字段中的邮件主题。
 - 选择**登录接收邮件服务器**复选框。
 - 在 **POP3 服务器**字段中输入接收邮件服务器 (POP3)。
 - 设置接收邮件服务器的端口。默认情况下,端口设为 110。
3. 再次单击**发送测试邮件**按钮。

其它通知设置

- 若要发送有关进程完成的通知,请选中**操作成功完成时发送通知**复选框。
- 若要发送有关进程失败的通知,请选中**操作失败时发送通知**复选框。
- 若要发送带有操作消息的通知,请选中**需要用户交互时发送通知**复选框。
- 若要发送带有完整操作日志的通知,请选中**在通知中添加完整日志**复选框。

6 存档数据

6.1 什么是数据存档？

数据存档是一款工具，支持您将大型文件或不常用文件移至 Acronis Cloud、NAS、外部硬盘或 USB 闪存驱动器。每次您运行此工具时，它都会分析选定文件夹中的数据，并建议将找到的文件上传到 Acronis Cloud 或将其移至本地存储。您可以选择要存档的文件和文件夹。移至存档后，将删除这些文件的本地副本。文件的链接存储在一个称为 Acronis Drive 的特殊位置。您可以在文件资源管理器中将此位置作为普通文件夹进行访问。双击文件链接将打开文件，就像文件存储在本地文件夹中一样。如果文件存档至 Acronis Cloud，首先要将其重新下载到您的计算机上。您也可以直接在 Acronis Cloud 中对其进行访问和管理。

数据存档具有以下主要特点：

- **节省可用存储空间：**

通常，现代化大容量硬盘驱动器的存储空间大多被用户数据所占用（如照片和文档），而不是操作系统或应用程序。由于大多数数据只是偶尔使用，因此无需将它们保留在本地驱动器上。数据存档可帮助您腾出存储空间，用于存放常用文件。

- **云存档和本地存档**

您可以选择存档的目标类型：Acronis Cloud 或本地存储，例如内部硬盘、外部硬盘、NAS 或 USB 闪存驱动器。每次您选择 Acronis Cloud 作为目标时，选定的数据都将存储在相同的云存档中。本地存档相互独立，可能具有不同的名称、目标、加密设置等等，不过您可以选择现有的存档作为目标而不是创建一个新的存档。本地存档的数量没有限制。

- **从任何设备轻松访问云存档**

将文件存档到 Acronis Cloud 之后，您可以从任何运行 Windows、macOS、iOS 和 Android 的设备（包括平板电脑和智能手机），通过 Acronis Cyber Protect Home Office、Acronis Cyber Protect Home Office 移动应用程序和 Acronis Cloud Web 应用程序进行访问。

- **云存档中的数据保护**

存储在 Acronis Cloud 中的数据不会受到损坏或灾难的影响。例如，当您的本地硬盘驱动器发生故障时，您可以将文件下载到新硬盘驱动器。此外，您的数据会以加密状态存储。除您之外的任何人都无法访问您的数据，您完全可以放心。

- **文件共享**

将文件上传到 Acronis Cloud 之后，您可以创建公共链接，与您的朋友共享文件或者将文件发布到论坛和社交网络上。

- **文件版本**

对于已经多次更改并上传到 Acronis Cloud 的文件，Acronis Cyber Protect Home Office 可在不同的文件版本中保留所有更改。您可以选择以前的文件版本并下载到设备中。

6.2 从存档中排除哪些数据？

为了缩小存档规模并消除损坏系统的可能性，默认情况下，Acronis Cyber Protect Home Office 会从存档中排除以下数据：

- pagefile.sys
- swapfile.sys
- Temp 文件夹
- System Volume Information 文件夹
- 回收站
- 网络浏览器临时数据：
 - 临时互联网文件
 - 缓存
- .tib 文件
- .tib.metadata 文件
- .tmp 文件
- .~ 文件

有关完整文件列表, 请参见知识库文章: <https://kb.acronis.com/content/58297>。

6.3 云存档与在线备份

将数据存档到 Acronis Cloud 类似于在线备份, 但是存在很多差异。

	线上备份	云存档
功能用途	保护数据不会受到操作系统损坏、硬件故障和丢失单独文件的影响。	清理本地存储设备并将数据移到 Acronis Cloud。
数据保护	<ul style="list-style-type: none"> • 全面保护计算机上的所有数据, 尤其是操作系统。 • 保护常用文件。 	保护不常用文件和旧文件, 主要是您的个人文档、照片等。
源数据选择	手动选择。	手动选择自动找到的文件。
源数据处理	源数据保留在原始位置。	从原始位置删除源数据。如果您的硬盘驱动器或笔记本电脑被盗, 这样可保证您的数据不会被别有用心的人所利用。
数据更改频率	备份的数据经常被更改。通常一个备份具有许多不时更新的版本。	存档的数据很少被更改。文件版本很少。

6.4 存档数据

数据存档通过将旧文件或不常用文件移至 Acronis Cloud 或本地存储, 可帮助您腾出存储空间。有关详细信息, 请参阅[什么是数据存档](#)。

存档数据的方法

1. 启动 Acronis Cyber Protect Home Office, 然后转到**存档**部分。
 2. [可选步骤]若要了解数据存档功能的基本知识, 请查看“入门”幻灯片。
 3. 请执行以下任一操作:
 - 若要分析默认 Windows 用户文件夹中的文件(通常位于 C:\Users\[用户名]), 请单击**分析主文件夹**。
 - 若要分析自定义文件夹中的文件, 请单击向下箭头, 单击**选择其它文件夹**, 然后选择要分析的文件夹。
- Acronis Cyber Protect Home Office 将分析计算机上的文件。请注意, 该过程可能需要几分钟时间。
4. 在左侧区域中, 选择数据类别。然后, 在右侧区域中选择要存档的文件和文件夹。
选择找到的文件时, 可以对它们进行排序, 例如按大小或按时间(上次修改日期)排序。要对文件进行排序, 请单击相应的列标题。
 5. 单击**选择目标位置**, 然后为存档的文件选择 Acronis Cloud 或自定义本地目标位置。
 6. [可选步骤]单击**选项**以设置存档的选项, 包括**数据中心**和**加密**。有关详细信息, 请参阅**数据存档选项**。
 7. 单击**存档**。
 8. 确认您要将文件移至存档并自动从计算机中删除它们。

此外, 请观看位于 <https://goo.gl/eEkNj2> 的英语视频说明。

6.4.1 数据存档选项

数据中心

将文件存档至 Acronis Cloud 时, 文件将上传到位于不同国家/地区的 Acronis 数据中心之一。最初, 该数据中心将定义为在创建 Acronis 帐户时离您的所在地最近的数据中心。之后, 您的存档文件将默认存储到同一数据中心。

当您位于其他国家/地区并且默认的数据中心不是离您当前的所在地最近的数据中心时, 建议您手动设置用于存档的数据中心。这样可以显著提升数据的上传速度。

注意

开始存档过程后不可更改数据中心。

选择数据中心的方法

1. 配置首次存档过程时, 单击**选项**。
2. 选择离您当前的所在地最近的国家/地区。

加密

要保护存档的数据以防止未经授权的访问, 您可以使用行业标准 AES(高级加密标准)加密算法(采用 256 位长密钥)对存档进行加密。

注意

您不能为已存在的存档设置或更改存档加密选项。

要对存档进行加密,请执行以下操作:

1. 配置首次存档过程时,单击**选项**。
2. 选中**使用 AES-256 算法对存档进行加密**复选框。
3. 在相应的字段中输入存档的密码。建议您使用超过七个字符的密码,可包含字母(最好是大小写相结合)和数字,这样才不容易被猜中。

注意

密码不可检索。请记住您为存档保护指定的密码。

每次尝试修改存档时,Acronis Cyber Protect Home Office 都会要求提供密码。要访问存档,您必须指定正确的密码。

6.5 访问您的存档文件

成功存档您的文件后,可以在以下位置访问它们:

- **文件资源管理器**

启动文件资源管理器,然后单击收藏夹下的 **Acronis Drive**。

您能够以只读模式使用文件。如需修改文件,请先将文件复制到其他文件夹。

- **Acronis Cloud**(仅适用于云存档)

通过以下方式之一打开 Acronis Cloud Web 应用程序:

- 启动 Acronis Cyber Protect Home Office,单击**存档**,然后单击在 **Web 浏览器中查看**。
- 转到 <https://www.acronis.com/my/online-backup/webrestore/>,然后登录您的帐户。

7 共享数据

您可以共享在 Acronis Cloud 的备份和存档中存储的文件与文件夹。

1. 在 Acronis Cyber Protect Home Office 侧栏上, 单击**帐户**。
2. 在 **Acronis Cloud Storage** 部分中, 单击**浏览我的数据**。
系统会将您重定向至 Acronis Cloud 浏览器页面。
3. 根据您要共享的内容, 执行以下操作:
 - 如果您要从备份共享文件或文件夹, 请在左侧的侧栏上, 单击**备份**。通过复选标记选择所需的文件或文件夹。
 - 如果您要从存档共享文件或文件夹, 请在左侧的侧栏上, 单击**存档**。通过复选标记选择所需的文件或文件夹。
4. 在右侧的侧栏上, 单击**共享链接**。
5. [可选] 您可以配置共享选项。要进行此操作, 请在链接窗口中, 单击**链接设置**。您可以应用密码, 设置到期日期, 并限制下载量。
6. 在链接窗口中, 单击**复制链接**, 然后将其关闭。

现在, 您可以共享此链接。要查看共享文件, 请在左侧的侧栏中, 单击**共享**。您可以在此处选择任何文件, 然后在右侧的侧栏中复制其链接, 配置链接设置, 或者将其删除。

8 保护家庭数据

8.1 什么是家庭数据保护？

家庭数据保护是一个统一的跨平台解决方案，支持您跟踪并控制共享同一个帐户的所有计算机、智能手机和平板电脑的保护状态。由于这些设备的用户必须登录同一个帐户，因此通常他们是同一个家庭的成员。一般来说，他们每个人都可以使用该功能，但是经常是一个家庭成员比其他人拥有更多技术经验。因此，让这个人来负责保护家庭数据是一种合理的做法。

若要跟踪并控制家庭设备的保护状态，请使用基于 Web 的在线控制面板(可以从连接到互联网的任何计算机进行访问)。有了这款 Web 应用程序，您的家庭 IT 管理员可以：

- 控制运行 Windows、macOS、iOS 和 Android 的所有家庭设备上的所有备份的当前状态。
- 向列表添加新设备。
- 在任何计算机上手动启动任何备份。
- 在 PC 和 Mac 上创建任意类型(整个计算机、文件级、磁盘级)的新备份。
- 更改现有备份的设置。
- 从位于 Acronis Cloud 中的任何备份恢复数据，包括来自 PC、Mac 以及运行 iOS 和 Android 的设备上的备份。
- 解决某些与产品相关的问题。

8.2 向在线控制面板添加新设备

要利用在线控制面板的所有优势，包括远程管理您的备份，首先需要将您的设备添加到设备列表。

添加新设备

1. 在您的设备上安装 Acronis Cyber Protect Home Office。
 - 您可以在 Acronis 网站上下载适用于 Windows 和 macOS 的安装文件。
 - 要将 Acronis Cyber Protect Home Office 安装在 iOS 和 Android 设备上，请遵循“安装适用于移动设备的 Acronis Cyber Protect Home Office”中的说明。
2. 启动 Acronis Cyber Protect Home Office 并登录您的帐户。

或者，也可以通过在线控制面板界面来添加设备。

通过在线控制面板添加新设备

1. 在要添加的设备上，打开在线控制面板，网址为：<https://cloud.acronis.com>。
2. 使用您的帐户登录。
3. 在**资源**选项卡上，单击**添加**。
4. 下载并安装 Acronis Cyber Protect Home Office。
5. 启动 Acronis Cyber Protect Home Office 并登录同一个 Acronis 帐户。

8.3 远程备份数据

借助基于 Web 的在线控制面板,您可以在共享相同帐户的任何计算机(PC或Mac)上配置和运行备份。

备份之前,请确保您对计算机具有访问权限

1. 打开在线控制面板,网址为:<https://cloud.acronis.com>。
2. 使用您的帐户登录。
3. 在**资源**选项卡上,查找您要备份的计算机。
 - 如果您未找到该计算机,则首先需要将其添加到列表中。要执行此操作,请将 Acronis Cyber Protect Home Office 安装在该计算机上,启动应用程序,然后使用您的帐户登录。有关详细信息,请参阅**添加新设备**。
 - 如果计算机离线,请务必打开计算机并连接到互联网。

在计算机上创建第一个备份

1. 打开在线控制面板,然后查找包含您要备份的数据的计算机。
2. 单击**启用备份**,然后为新备份配置设置,包括:
 - 备份类型(整个计算机、磁盘级或文件级)
 - 要备份的数据
 - 备份目标位置
 - 计划
 - 保留规则
 - 数据加密
3. 在配置备份时,单击**应用**,然后单击**立即运行**。

创建现有备份的新版本

1. 打开在线控制面板,然后查找包含您要备份的数据的计算机。
2. 单击**立即备份**,然后选择您要更新的备份。

更改现有备份的设置

1. 打开在线控制面板,然后查找作为备份来源的计算机。
2. 单击齿轮图标,再单击**备份**,然后查找您要重新配置的备份。
3. 单击备份名称旁边的齿轮图标,然后单击以下选项之一:
 - 要更改主设置,请单击**编辑**。
 - 要更改其他选项,请单击**备份选项**。
4. 单击**保存更改**。

创建新备份

1. 打开在线控制面板,然后查找包含您要备份的数据的计算机。
2. 单击齿轮图标,然后单击**备份**。
3. 单击**添加备份计划**。

- 要使用预定义的设置创建备份，请单击**应用**。整个计算机将备份到 Acronis Cloud。
 - 要使用自定义设置创建备份，请单击**创建新备份**，更改设置，然后单击**应用**。
4. 要启动备份，请单击**立即运行**。

8.4 使用在线控制面板恢复数据

通过基于 Web 的在线控制面板，您可以从上传自家庭设备(包括 PC、Mac、智能手机和平板电脑)的任何在线备份中恢复数据。

通过在线备份恢复数据的方法

1. 打开在线控制面板，网址为：<https://cloud.acronis.com>。
2. 使用您的帐户登录。
3. 在**资源**选项卡上，查找要作为从中恢复数据的来源的设备。如果设备离线，请务必打开设备并连接到互联网。
4. 如果您从以下位置恢复数据：
 - 计算机 — 单击**恢复**。Acronis Cloud Web 应用程序将打开，您可以在其中浏览和恢复您的数据。有关详细信息，请参阅“从线上备份中恢复数据”。
 - 移动设备 — 单击**恢复**。在左侧面板中，按备份日期和时间选择备份版本。然后，在右侧面板中，选择要恢复的项目，再单击**下载**。

8.5 电子邮件通知

有时，备份操作会持续很长时间。要跟踪备份的状态以及它们何时完成，您可以通过在线控制面板配置电子邮件通知。

配置电子邮件通知的方法

1. 在在线控制面板上打开电子邮件通知。您可以通过以下两种方式执行此操作：
 - 在在线控制面板上，单击右上角的帐户图标，然后选择**电子邮件通知**。
 - 在 Acronis Cyber Protect Home Office 应用程序中，单击**设置**，然后单击**更改电子邮件通知设置**。
2. 在**发送的通知关于**中，选择您感兴趣的信息。
 - 错误
 - 警告
 - 成功备份
3. 在**收件人电子邮件地址**字段中，键入目标电子邮件地址。您可以输入多个地址，并以分号隔开。
4. [可选步骤]在**主题**中，更改电子邮件通知主题。

您可以使用以下变量：

 - [computer_name] — 计算机的名称
 - [operation_status] — 已完成操作的状态
 - [backup_name] — 备份的名称

默认主题为 [computer_name] - [operation_status] - [backup_name]。

保存设置后,您将从 Acronis 服务器收到有关运行 Windows 和 macOS 的所有家庭设备上所有备份的信息。

9 保护

Acronis Cyber Protect Home Office 为数据提供以下保护：

- Active Protection 在后台不断运行，会在您照常工作的情况下实时保护您的计算机。
- 防病毒扫描可按需运行，以在整个系统中深度搜索恶意软件。
- 漏洞评估是在后台运行的每日扫描，可检测系统和应用程序中的漏洞，然后评估其严重性。

注意

您只能在 Acronis Cyber Protect Home Office 用户界面中启用或禁用保护。无法通过任务管理器或任何其他外部工具手动停止该进程。

9.1 “保护”仪表板

“保护”仪表板包含有关 **Active Protection**、**防病毒扫描**和**漏洞评估**进程的统计数据，并提供对保护状态的控制和对保护设置的访问。

要访问“保护”仪表板，请单击侧边栏上的**保护**。

在仪表板的**概述**选项卡上，您可以：

- 查看有关 Active Protection 状态的统计信息。
- 查看检测到的问题、已隔离的项目和保护排除项的数量。
- 查看**防病毒扫描**的最新报告。若要查看此报告，请单击**扫描报告**。
- 查看下次预定扫描时间。
- 手动运行完整或快速**防病毒扫描**。要执行此操作，请单击**运行完整扫描**或**运行快速扫描**。
- 查看检测到的漏洞的最新报告，然后从其运行新扫描。若要查看此报告，请单击**检测到的漏洞**。
- 将整个保护停止预定义的时间段(30分钟、1小时、4小时、直到重启)。要执行此操作，请单击**关闭保护**，然后选择时间段。

注意

通过关闭保护可以取消激活 Active Protection。预定的按需扫描将不会启动。

在仪表板的**活动**选项卡上，您可以查看对您的保护状态和设置应用的更改的日志。

9.2 Active Protection

为了实时保护您的计算机免遭恶意软件侵害，Acronis Cyber Protect Home Office 采用了 Acronis Active Protection 技术。

Active Protection 会在您照常工作的情况下，不断检查您的计算机。除了您的文件，Acronis Active Protection 还会保护 Acronis Cyber Protect Home Office 应用程序文件、您的备份和硬盘的主引导记录。

Active Protection 包含几个保护级别，这几个保护级别可以相互独立启用：

- 防勒索软件保护
- 实时保护
- Web 过滤

9.2.1 防勒索软件保护

勒索软件会对文件进行加密，需要交付赎金来换取加密密钥。加密货币挖矿恶意软件会在后台执行数学计算，从而窃取您的计算机的处理能力和网络流量。

当启用**防勒索软件保护**服务后，该服务会实时监控正在计算机上运行的进程。当检测到第三方进程尝试加密您的文件或加密货币进行挖矿时，该服务会向您发送通知并询问您是要允许该进程继续运行还是阻止该进程。

要允许进程继续运行，请单击**信任**。如果无法确定该进程是否安全合法，我们建议您单击**隔离**。执行此操作后，会将该进程添加到**隔离区**并阻止它执行任何活动。

阻止进程后，我们建议您检查文件是否被加密或以任何方式被损坏。如果是，请单击**恢复修改的文件**。Acronis Cyber Protect Home Office 将在以下位置搜索要恢复的最新文件版本。

- 在进程验证过程中初步创建的临时文件副本
- 本地备份
- 云备份

如果 Acronis Cyber Protect Home Office 找到合适的临时副本，则将从该副本还原文件。如果临时文件副本不适合还原，Acronis Cyber Protect Home Office 会在本地和云中搜索备份副本，比较在这两个位置找到的副本的创建日期，并从最新的可用未损坏副本还原您的文件。

注意

Acronis Cyber Protect Home Office 不支持从受密码保护的备份恢复文件。

要将 Acronis Cyber Protect Home Office 配置为在阻止进程后自动恢复文件，请选中 Active Protection 设置中的**阻止进程后自动恢复文件**复选框。请参阅[配置 Active Protection](#)。

9.2.2 实时保护

当启用**实时保护**后，该服务会不断检查您交互的文件，以实时保护您的计算机，使其免遭可疑活动、病毒及其他恶意威胁的侵害。

实时保护附带以下其他保护选项：

- 行为分析 — 用于识别恶意进程，Active Protection 使用行为启发式方法。该功能可将某一进程执行的操作链与在恶意行为模式数据库中记录的事件链进行比较。这一方法使 Active Protection 能够依据典型行为检测新恶意软件。
- 利用攻击防护 — Active Protection 会分析在计算机上运行的进程的行为并检测异常活动。该服务会阻止受感染的进程蔓延并利用在系统上安装的其他软件的漏洞。Active Protection 采用几种利用攻击防御方法：
 - 内存保护可检测并阻止执行权限对内存页的可疑修改。恶意进程会对页属性应用此类修改，以便允许从堆栈和堆等不可执行的内存区域执行 ShellCode。

- 权限升级防护可检测并阻止未获授权的代码或应用程序进行权限升级的尝试。恶意代码会使用权限升级来获取受攻击计算机的完整权限，然后执行重要的敏感任务。未获授权的代码不得访问重要系统资源或修改系统设置。
- 代码注入防护可检测并阻止恶意代码注入到远程进程中。代码注入用于将某个应用程序的恶意意图隐藏于干净或善意进程之后，以便避开防恶意软件产品的检测。

您可以选择以下扫描类型之一：

- **访问时智能保护**检测是指程序在后台运行，它会在系统整个开机期间主动且持续地扫描您的计算机系统以查找病毒及其他恶意威胁。在执行文件时以及在执行打开文件以进行读取/编辑等各种操作时，将会检测恶意软件。
- **执行时**检测是指将仅在可执行文件运行的时刻扫描这些文件，以确保它们是干净的，不会导致对您的计算机或数据造成任何损害。复制受感染文件的行为将被忽略。

您可以在“保护”仪表板的**活动**选项卡中查看实时保护检查的结果。

9.2.3 Web 过滤

恶意软件通常由恶意或受感染的站点分发，并使用所谓的“路过式下载”感染方法。

Web 过滤会在您尝试打开可能有害的网站和不可信 Web 资源时阻止访问，帮助保护您免遭它们的侵害。为了确定哪些网站可能有害，Web 过滤使用保护更新数据库。Web 过滤数据库还包括有关包含欺诈和网络钓鱼 URL 的网站的信息。您可以通过配置 Web 过滤列表的例外，修改在数据库中定义的规则。

Web 过滤具有两种操作模式：

- **完全阻止** — 将完全阻止对网站的访问。
- **仅通知** — 将显示通知，但用户能够访问网站。

9.2.4 配置 Active Protection

要访问 Active Protection 设置，请单击侧栏上的**保护**，然后单击**设置**并转到**Active Protection**选项卡。

若要配置防勒索软件保护，请执行以下操作：

1. 开启**防勒索软件保护**开关以启用防勒索软件保护。
当启用该功能后，该服务将保护您计算机免遭在后台运行的可能有害应用程序和进程的侵害。
2. 选择您要启用的选项。
 - **阻止进程后自动恢复文件** — 尽管进程被阻止，但文件仍然可能已被修改。如果选中此复选框，Acronis Cyber Protect Home Office 会按如下所述恢复文件。
Acronis Cyber Protect Home Office 将在以下位置搜索要恢复的最新文件版本。
 - 在进程验证过程中初步创建的临时文件副本
 - 本地备份
 - 云备份

如果 Acronis Cyber Protect Home Office 找到合适的临时副本，则将从该副本还原文件。如果临时文件副本不适合还原，Acronis Cyber Protect Home Office 会在本地和云中搜索备份副本，比较在这两个位置找到的副本的创建日期，并从最新可用的未修改副本还原您的文件。

注意

Acronis Cyber Protect Home Office 不支持从受密码保护的备份恢复文件。

- **保护备份文件免遭勒索软件侵害** — Acronis Cyber Protect Home Office 将保护自己的进程以及您的备份免遭勒索软件侵害。您的存档也将受到保护。
- **保护网络共享和 NAS** — Acronis Cyber Protect Home Office 将监控并保护您可以访问的网络共享和 NAS 设备。您还可以为受勒索软件攻击影响的文件指定恢复位置。
- **保护您的计算机免遭非法加密货币挖矿的攻击** — 选择此复选框以保护计算机免遭加密货币挖矿恶意软件的攻击。

3. 单击**确定**。

要配置实时保护，请执行以下操作：

1. 开启**实时保护**开关以启用实时保护。

当启用实时保护后，该服务将检查您交互的所有文件以查找有无恶意软件。

2. 选择何时应检查这些文件。

- **访问时智能保护** — 所有系统活动都受到监控，在您访问文件时会扫描这些文件。
- **执行时** — 仅在启动可执行文件时扫描这些文件，以确保它们不会损坏您的计算机。

3. 从下拉列表中选择要对检测到的对象执行的操作。

- **阻止并通知** — 将会阻止疑似恶意软件活动的进程，您将收到通知。
- **隔离** — 将会阻止疑似恶意软件活动的进程并将可执行文件移到隔离区文件夹。

4. 启用其他保护选项。

- **检测进程中的恶意行为** — 使 Active Protection 能够依据典型行为检测新恶意软件并将其阻止。
- **检测并阻止恶意进程利用系统上的软件漏洞 (试验)** — 使 Active Protection 能够检测并阻止尝试利用系统上其他进程的错误和漏洞的进程。

注意

将立即阻止所有检测到的对象。这些对象将不会被移到隔离区，也不会被添加到检测到的问题列表。

要配置 Web 过滤，请执行以下操作：

1. 开启 **Web 过滤**开关以保护您免遭可能有害的网站和不可信 Web 资源的侵害。

2. 从**检测到恶意 URL 时采取的操作**下拉菜单中，选择要对检测到的恶意 URL 采取的操作。

- **完全阻止** — 将完全阻止对网站的访问。
- **阻止并通知** — 网站将被阻止，而用户可以继续访问。

3. 要配置可信或已阻止网站的列表，请单击**管理例外**。

- a. 要将新 URL 添加到列表，请单击**添加 URL**。
- b. 输入有效 URL 名称。其域将添加到例外。

注意

您输入的域中的所有地址将被视为可信或已阻止。例如,如果您输入了 xyz.com 作为可信域,则 xyz.com 下的所有路径或子域将被视为可信。

- c. 从下拉菜单中,选择 **已允许**或**已阻止**。系统将不对已允许的网站扫描威胁。系统将不会打开已阻止的网站,或者在尝试打开时通知您。
- d. 单击**添加 URL**。
- e. 单击**应用**。

9.3 防病毒扫描

防病毒扫描是 Acronis Cyber Protect Home Office 防病毒和防恶意软件保护的组件之一。该组件通过按需(手动检查或者按照您可配置的预定义时间间隔)检查恶意软件来保护您的计算机。

可以选择两种扫描类型之一。

- **完整**扫描可检查整台计算机有无病毒。完整扫描通过检查除您在排除列表中定义的已排除文件或文件夹外的所有文件和进程(或文件和进程的子集)来检测恶意软件。
- **快速**扫描仅检查特定文件和文件夹。快速扫描通过检查被视为最可能蕴藏病毒的特定文件夹来检测恶意软件。

您还可以选择要扫描的内容:存档文件、外部驱动器或者仅新文件和更改的文件。

注意

您可以将 Acronis Cyber Protect Home Office 配置为当扫描操作正在运行时禁止您的计算机进入睡眠或休眠模式。请注意,默认情况下此选项处于选中状态。

默认情况下,当 CPU 负载过重时,将会降低防病毒扫描的优先级,以便让其他应用程序正常运行。这将导致降低扫描速度。您可以禁用该选项以加快扫描。

若要查看**扫描详细信息报告**窗口,包括防病毒扫描详细信息,请单击**扫描报告**按钮。

9.3.1 配置防病毒扫描

防病毒设置

在此处,您可以配置主要**防病毒**功能。例如,可以选择**检测时采取的操作**,定义**扫描类型**,设置**预定**,以及选择要扫描的内容等。

要访问**防病毒**设置,请单击侧边栏上的**保护**,然后单击**设置**并转到**防病毒**选项卡。

要配置检测时采取的操作,请执行以下操作:

选择您要启用的选项。

- **隔离** - 默认设置此选项。当 Acronis Cyber Protect Home Office 检测到潜在的恶意软件威胁时,它会停止该进程并将可疑文件移到隔离区文件夹。

- **仅通知** - 当检测到可疑进程时，您将收到有关潜在恶意软件威胁的通知。

要配置扫描类型，请执行以下操作：

选择要执行的扫描类型。

- **完整** — 默认设置此选项。Acronis Cyber Protect Home Office 将检查整个 PC。
- **快速** - Acronis Cyber Protect Home Office 将仅检查被视为最可能蕴藏威胁的特定文件夹。

要预定防病毒扫描，请执行以下操作：

选中一个复选框以配置扫描进程将启动的时间。

- **每日** — 将在每天的特定时间运行扫描。
- **每周** — 将在每周的特定一天运行扫描。设置星期几和时间。
- **每月** — 将在每月的特定一天运行扫描。
- **系统启动时** — 每次启动您的操作系统时运行扫描。
- **不预定** — 不计划运行特定时间的扫描。

要配置要扫描的内容，请执行以下操作：

选中以下复选框：

- **扫描的存档文件大小不得大于**。使用箭头选择值。
- **扫描外部驱动器**
- **扫描网络共享和 NAS**
- **仅扫描新文件和更改的文件**

要配置执行防病毒扫描期间的系统行为，请执行以下操作：

有时，系统可能会在防病毒扫描完成之前关机。对于此类情况，请选中**启动时运行错失的任务**复选框，通过进行该选择，将 Acronis Cyber Protect Home Office 配置为在系统重新启动时继续执行扫描。

而且，您还可以启用**禁止睡眠或休眠模式**选项，以便在扫描操作正在运行时，禁止您的计算机关机。

如果 CPU 过载，可以降低防病毒扫描的优先级，以便让其他应用程序正常运行。该选项默认情况下处于启用状态，这可能会降低扫描速度。要加快扫描，请清除**将优先级让与其他应用程序**复选框。

配置防病毒扫描后，单击**确定**。

9.4 漏洞评估

漏洞评估是 Acronis Cyber Protect Home Office 防病毒和防恶意软件保护的组件之一。它是在后台运行的每日扫描，可检测系统和应用程序中的漏洞，然后评估其严重性。您还可以在需要时手动运行扫描。

注意

要更新漏洞数据库，需要稳定的 Internet 连接。

若要查看漏洞，请执行以下操作：

1. 在左侧的侧栏上，单击**保护**。
2. 在**概述**选项卡上的**漏洞评估**下，单击**检测到的漏洞**。系统将显示报告。
3. 要运行新扫描，请单击**运行扫描**。
4. [可选] 若要显示**详细信息**窗口，请单击漏洞名称旁边的信息图标。
5. [可选] 若要查看有关漏洞的详细信息，请单击其名称旁边的箭头。此时将显示包含此信息的网页。
6. 要解决检测到的问题，请安装受影响应用程序的最新更新。然后，再次进行扫描以确保漏洞得到修复。如果漏洞仍然存在，则意味着某些应用程序可能仍使系统面临风险。为了完全保护您的数据，请备份操作系统，并启用防恶意软件保护。

要配置漏洞评估，请执行以下操作：

1. 在左侧的侧栏上，单击**保护**，然后单击**设置**。
2. 转至**漏洞评估**选项卡，然后打开或关闭漏洞扫描以将其启用或禁用。

9.5 管理检测到的问题

如果将防病毒扫描配置为在检测到恶意对象时采取**阻止并通知**操作，则会填充检测到的问题列表。您应查看该列表并确定是信任还是移到隔离区。

要检查并管理检测到的问题，请执行以下操作：

1. 在**保护**仪表板上，单击**检测到的问题**。
2. 选中列表中问题的相应复选框，并选择如何处理它。
 - 要将该文件或进程添加到保护排除项列表，请单击**信任**。

注意

如果选择信任某文件或进程，则该文件或进程将从未来的防病毒扫描中排除。

- 要将某文件或进程移到隔离区，请单击**隔离**。
3. 单击**关闭**。

如果您单击 Acronis Cyber Protect Home Office 侧边栏上的**保护**，然后单击**设置**，再转至**高级**选项卡，还可以管理检测到的问题。在**检测到的问题**下，单击**管理**。

9.6 在隔离区中管理文件

根据您的设置，Active Protection 和防病毒扫描可以将已阻止的文件移到隔离区。隔离区是一个用于将受感染的文件和可疑文件与您的计算机和数据相隔离的特殊存储。在将应用程序文件放置在隔离区中后，将最大程度地降低遭受被阻止应用程序的潜在有害行为损害的风险。

默认情况下，这些文件会在隔离区中保留 30 天，然后会从您的 PC 中删除。您可以查看隔离区中的这些文件，决定在该期限到期之前是保留还是删除它们。也可以更改默认期限以将文件保留在隔离区中。

要从隔离区中还原或删除文件，请执行以下操作：

1. 在**保护**仪表板上, 单击**隔离区**。
2. 在“隔离区”列表中, 选择项目。
 - 要将该项目恢复到其原始位置, 请单击**还原**。
 - 要删除项目, 请单击**从 PC 中删除**。
3. 单击**关闭**。

要设置从隔离区中自动删除文件的期限, 请执行以下操作:

1. 在**保护**仪表板上, 单击**设置**, 然后单击**高级**选项卡。
2. 在**隔离区**部分中, 选择要将隔离的项目保留的天数。
3. 单击**确定**。

9.7 配置保护排除项

Active Protection 和防病毒扫描使用保护数据库中的定义来确定潜在威胁。如果您信任某些可执行文件和文件夹, 可以将其添加到保护排除项列表, 以便 Acronis Cyber Protect Home Office 在扫描时跳过它们。

将文件或文件夹添加到保护排除项列表

1. 在**保护**仪表板上, 单击**保护排除项**。
2. 从**添加排除项**菜单中, 选择要排除的项目。
 - **添加文件** — 用于从扫描中排除可执行文件或其他文件。
 - **添加文件夹** — 用于从扫描中排除文件夹。
3. 浏览您要排除的项目, 然后单击**打开**。
4. 添加其他要排除的项目, 或者单击**保存**以更新列表。

从保护排除项列表中删除文件或文件夹

1. 在**保护**仪表板上, 单击**保护排除项**。
2. 在保护排除项列表中, 选中要删除项目的相应复选框, 然后单击**删除**。
3. 单击**保存**以更新列表。

要配置 Web 过滤的保护排除项, 请参阅[配置 Active Protection](#)。

9.8 针对 Zoom、Cisco Webex 和 Microsoft Teams 的保护

Zoom、Cisco Webex Meetings 和 Microsoft Teams 被广泛用于 Web 会议和通信。Acronis Cyber Protect Home Office 的防勒索软件功能默认情况下按如下所述保护这些协作应用程序。

- 保护应用程序进程免遭代码注入
- 禁止应用程序进程的可疑操作

9.9 下载保护更新

默认情况下, Acronis Cyber Protect Home Office 会自动下载保护更新。您可以检查保护数据库和组件的状态, 或者禁用保护更新自动下载。

要检查保护更新的状态, 请执行以下操作:

1. 在**保护**仪表板上, 单击**设置**, 然后单击**高级**选项卡。
2. 在底部找到**保护更新**部分。

最新的数据库版本和下载日期将显示在该部分的底部。

要禁用保护更新自动下载, 请执行以下操作:

注意

要确保获得最大保护, 建议不要禁用自动保护更新。

1. 在**保护**仪表板上, 单击**设置**, 然后单击**高级**选项卡。
2. 在底部找到**保护更新**部分。
3. 清除**自动下载保护更新**复选框。

要下载最新保护更新, 请执行以下操作:

如果已禁用自动下载保护更新, 您可以手动检查更新并进行下载。

1. 在**保护**仪表板上, 单击**设置**, 然后单击**高级**选项卡。
2. 在底部找到**保护更新**部分。
3. 单击**检查更新**。只有在未选中**自动下载保护更新**复选框时, 此选项才可用。
4. 如果保护更新不是最新的, 请单击**更新**。

10 同步数据

10.1 关于同步功能

同步功能的主要优势在于：

- 您可以在所有计算机上拥有相同的数据 - 文档、照片、视频等等。您可随时随地轻松访问这些数据。无需再将文件通过电子邮件发送给自己或一直携带 USB 驱动器。
- 您可以根据需要创建尽可能多的同步。
- Acronis Cloud 会保留您同步的文件以及这些文件的不同版本。这样，您可在需要时回滚到以前的文件版本。

注意

需要 Acronis Cloud 存储订购许可才能使用此功能。有关详细信息，请参阅订购许可信息。

- 您还可以使用 Web 浏览器访问 Cloud，而不必安装我们的应用程序。
- 当您在两台或更多台计算机之间直接创建同步时，不需要 Acronis Cloud 订购许可。

10.2 可以和不可以同步的内容

您可以同步在两个或多个文件夹中存储的数据。下面我们将探讨这些文件夹可能的所在位置以及可能包含的数据。

10.2.1 存储类型

可在以下项目之间建立同步过程：

- 两台或多台计算机上的两个或多个文件夹。
- 一个或多个计算机和 Acronis Cloud。

Acronis Cloud 始终包含同步文件的最新版本。同时，您不能选择 Acronis Cloud 中的文件夹参与同步，此类文件夹将自动创建。

在一个同步过程中，您可能在每台计算机上仅分配一个同步文件夹。

注意

您不能选择同步单个文件。若要同步该文件，请选择同步包含该文件的文件夹。

10.2.2 数据类型

可以同步以下数据：

- 文件(照片、音乐、视频、文档等), 以下列出的文件除外

注意

仅本机 FAT32 和 NTFS 文件属性被同步。如果同步的文件夹属于不同的文件系统, 程序将只同步这两个文件系统都支持的属性。

- 同步文件夹内的其它文件夹(即同步子文件夹)及其内容

不能同步以下数据:

- 磁盘与分区
- 系统文件与文件夹
- 隐藏文件与文件夹
- 临时文件与文件夹
- 系统注册表
- 数据库
- 电子邮件程序(包括 Microsoft Outlook 及其它程序)的数据
- 不能表示单独文件或文件夹的其它数据(例如, 通讯簿中的联系人)
- Windows 库(文档、音乐等)




10.3 同步图标

使用同步时, 您将看到特殊图标。这些图标为您提供以下信息:

- 同步的类型和当前状态(图标显示在通知区域中)。
- 同步文件和文件夹的当前状态(图标显示在文件资源管理器中)。

10.3.1 通知区域

同步状态图标:

图标	说明
	同步正在正常模式下工作。
	同步已暂停。
	上次同步过程中发生错误。



10.3.2 文件资源管理器

文件和文件夹的同步状态图标:

图标	说明
	文件或文件夹已同步。

图标	说明
	文件或文件夹此时正在同步。
	由于发生错误, 文件或文件夹尚未同步。

同步文件夹的同步类型图标:

图标	说明
	与 Acronis Cloud 同步。
	通过局域网在计算机之间同步。

10.4 创建同步

开始创建新同步之前, 请确保满足以下条件:

- 您具有一个 Acronis 帐户。
- 如果您计划在同步中包含 Acronis Cloud, 则必须订阅 Acronis Cloud 存储。请参阅 "订购许可信息"(第 32 页), 了解详细信息。
- 已在每台计算机上安装 Acronis Cyber Protect Home Office 或 Acronis True Image(2012 或更高版本)。
- 如果通过局域网连接计算机, 请确保已建立本地连接。
- 每台计算机均已联网。

同步文件和文件夹

1. 在侧栏上单击**同步**。
2. 如果您未登录, 请输入您的 Acronis 帐户凭据。
3. 单击**添加同步**。
4. 确定是否要在新同步中包含 Acronis Cloud, 然后选择适当的同步类型。
5. 选择要同步的文件夹, 然后单击**确定**。
6. 要加入此同步, 请在另外一台计算机上启动 Acronis Cyber Protect Home Office, 在“同步”部分选择此同步, 单击**加入同步**, 然后选择要同步的文件夹。

10.5 同步文件的版本

Acronis Cyber Protect Home Office 允许您撤消由于同步对文件所做的更改。如果发现其中一个文件包含不合乎需要的更改, 您可以查看此文件的先前版本, 然后选择并回滚至其正确版本。详情请参阅[恢复到先前的文件版本](#)。

所有版本都存储在可通过互联网访问的 Acronis Cloud 上。要使用 Acronis Cloud, 您必须具有 Acronis Cloud 服务的订购许可。有关详细信息, 请参阅订购许可信息。

要删除过时的版本, 请在 Acronis Cloud Web 应用程序中运行清理操作。有关详细信息, 请参阅[如何清理 Acronis Cloud 上的空间](#)。

警告!

如果使用 Acronis Cyber Protect Home Office 的试用版, 试用期到期时, 包括最新版本在内的所有存储版本都将从云中删除。

10.5.1 恢复到先前的文件版本

如果在 Acronis Cloud 中存储同步历史记录, 则可以将同步文件的当前版本恢复到其先前版本。要撤消一些不合乎需要的同步操作时, 此操作非常有用。

恢复到先前的文件版本

1. 在**同步**部分中找到带有所需文件的同步框。然后单击 **Acronis Cloud** 链接。
2. 在 Web 浏览器中打开同步项目列表后, 选择要恢复到先前版本的文件。然后单击右侧的齿轮图标。在打开的菜单中选择**查看版本**。
3. 选择要回滚至的版本。系统将显示版本的准确日期和时间。您的当前版本将恢复到它在该时间点时的状态。
4. 单击**恢复**以继续。选定的版本将成为 Cloud 上的最新版本。然后, 系统会将该版本下载到拥有相应同步的计算机上。

10.6 如何恢复删除的文件

有时, 您可能会误删同步中的文件。那么, 您需要恢复删除的文件。对于在 Acronis Cloud 上保留五个版本的同步, 可以恢复删除的文件。

但有一个条件 - 已删除的文件必须未在 Cloud 清理期间移除。

要恢复删除的文件, 请执行以下操作:

1. 启动 Acronis Cyber Protect Home Office。
2. 在侧边栏上单击**同步**, 选择包含要恢复的文件的同步, 然后单击 **Acronis Cloud** 链接。
3. 单击**文件**选项卡, 然后选择从中删除了该文件的同步。
4. 选择同步后, 将显示文件和文件夹列表。
5. 选中**显示删除文件**复选框, 然后选择要恢复的已删除文件。
6. 单击**恢复**按钮, 将删除的文件恢复到其文件夹。

10.7 删除同步

1. 在侧栏上单击**同步**。
2. 如果您未登录, 请输入您的 Acronis 帐户凭据。
3. 从同步列表中选择要删除的同步, 单击箭头图标, 然后单击**删除**。

此操作仅会中断同步文件夹之间的连接。同步文件将保留在位置中, 并且无法以任何方式修改。

11 磁盘克隆和迁移

此操作可以将一个磁盘驱动器上的整个内容复制到另一个磁盘驱动器。这种操作很有必要，例如，要将操作系统、应用程序和数据克隆到新的更大容量的磁盘时。您可以通过两种方式执行此操作：

- 使用克隆磁盘实用工具。
- 备份旧的硬盘驱动器，然后恢复到新的硬盘驱动器。

11.1 磁盘克隆实用工具

“克隆磁盘”实用工具可允许您通过将分区复制到另一个硬盘来克隆硬盘驱动器。

开始之前请阅读以下内容：

- 如果您想将系统克隆到容量更高的硬盘，我们建议您将目标(新)驱动器安装在计划要使用的位置上，而将源驱动器安装在另一个位置(例如，外部 USB 盘)。这点对笔记本电脑而言尤为重要。

注意

建议使用旧的和新的硬盘驱动器在相同的控制器模式(例如 IDE 或 AHCI)下工作。否则，您的计算机不会从新的硬盘驱动器启动。

注意

如果您将含有 Windows 的磁盘克隆到外部 USB 硬盘，将无法从该硬盘启动。我们建议改为克隆到内部 SSD 或 HDD。

- 克隆磁盘实用工具不支持多启动系统。
- 在程序屏幕上，已损坏的分区的左上角有一个带白色十字的红色圆圈标志。开始克隆前，应使用适当的操作系统工具对此类磁盘进行错误检查并更正错误。
- 为安全起见，强烈建议您创建整个原始磁盘的备份。如果克隆过程中原始硬盘出错，此备份将是您的数据保护程序。有关如何创建此类备份的信息，请参阅[备份分区和磁盘](#)。创建备份后，请确保对其进行验证。

11.1.1 克隆磁盘向导

开始之前，我们建议您阅读关于[磁盘克隆实用工具](#)的常规信息。如果您使用 UEFI 计算机并决定在可启动媒体下启动克隆步骤，请注意 UEFI BIOS 中可启动媒体的启动模式。建议启动模式与备份中的系统类型相匹配。如果备份包含 BIOS 系统，那么将在 BIOS 模式下启动可启动媒体；如果系统为 UEFI，请确保已设置 UEFI 模式。

克隆磁盘的方法

1. 启动 Acronis Cyber Protect Home Office。
2. 单击工具条内的工具，然后单击**克隆磁盘**。
3. 在**克隆模式**步骤中，选择转移模式。

- **自动**—建议大部分情况下使用。
- **手动**—在手动模式下,可更灵活地传输数据。手动模式在您需要更改磁盘分区配置时相当有用。

注意

若程序找到两张磁盘,其中一张已分区,另一张尚未分区,则系统会自动将已分区磁盘识别为源盘,并将尚未分区的磁盘识别为目标磁盘。在这种情况下,后面的步骤将被省略并转至**摘要**屏幕。

4. 在**源磁盘**步骤中,选择要克隆的磁盘。

注意

Acronis Cyber Protect Home Office 不支持动态磁盘克隆。

5. 在**目标磁盘**步骤中,选择用于存储克隆数据的目标磁盘。
如果选定的目标磁盘包含分区,您需要确认删除分区。请注意,只有在向导的最后一步中单击**继续**时才会执行实时数据销毁。

注意

若有未分区的磁盘,则程序会自动将其识别为目标磁盘,并略过该步骤。

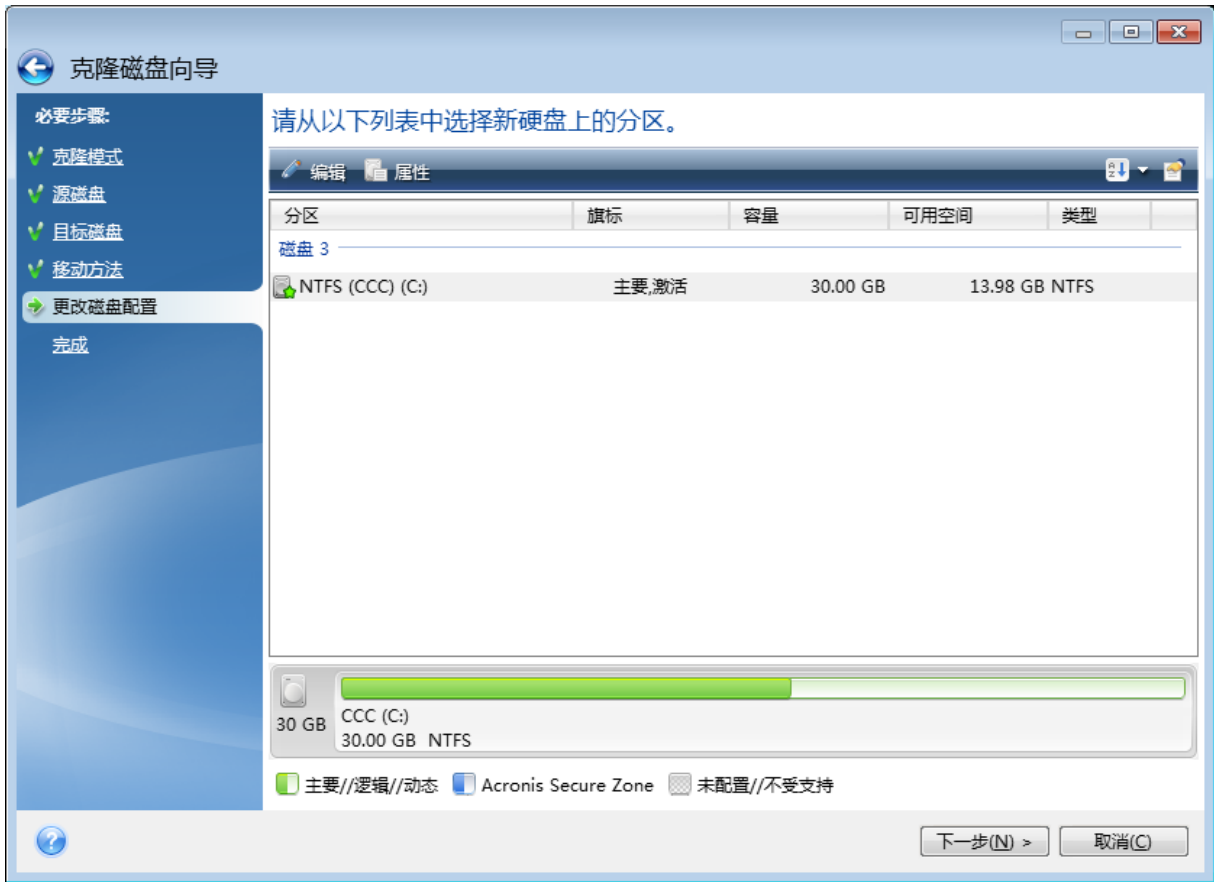
6. [仅在源磁盘已安装操作系统的情况下,此步骤才可用]。在**磁盘使用**步骤中,选择您要使用克隆的方式。
 - **替换此计算机上的磁盘**—将复制系统磁盘数据,并且克隆将可启动。使用此克隆将系统磁盘替换为此 PC 上的新磁盘。
 - **在另一计算机上使用**—将复制系统磁盘数据,并且克隆将可启动。使用此克隆将所有数据传输到另一 PC 上的可启动磁盘。
 - **用作数据磁盘**—将复制磁盘数据。将此克隆用作非可启动数据驱动器。
7. [只有在手动克隆模式下才会有该步骤]。在**移动方式**步骤中,选择数据移动方式。
 - **保持原样**—使用相同大小和类型、文件系统和标卷,为每个旧分区创建新分区。未使用的空间将变成未分配的空间。
 - **按比例**—将新磁盘空间按比例分配给克隆的分区。
 - **手动**—您可以自行指定新的大小和其它参数。
8. [只有在手动克隆模式下才会有该步骤]。在**更改磁盘配置**步骤中,您可以编辑将要在目标磁盘创建的分区设置。有关详细信息,请参阅[手动分区](#)。
9. [可选步骤]在**排除内容**步骤中,您可以指定不打算克隆的文件和文件夹。有关详细信息,请参阅[从克隆中排除项目](#)。
10. 在**完成**步骤中,请确保配置的设置符合您的需求,然后单击**继续**。

如果由于某些原因克隆操作停止,您将需要进行配置并再次启动克隆过程。您不会丢失数据,因为 Acronis Cyber Protect Home Office 在克隆过程中不会更改所存储的原始磁盘和数据。

默认情况下,Acronis Cyber Protect Home Office 会在克隆过程完成后关闭计算机。这可让您更改主控/从属跳线的位置并删除其中的一个硬盘。

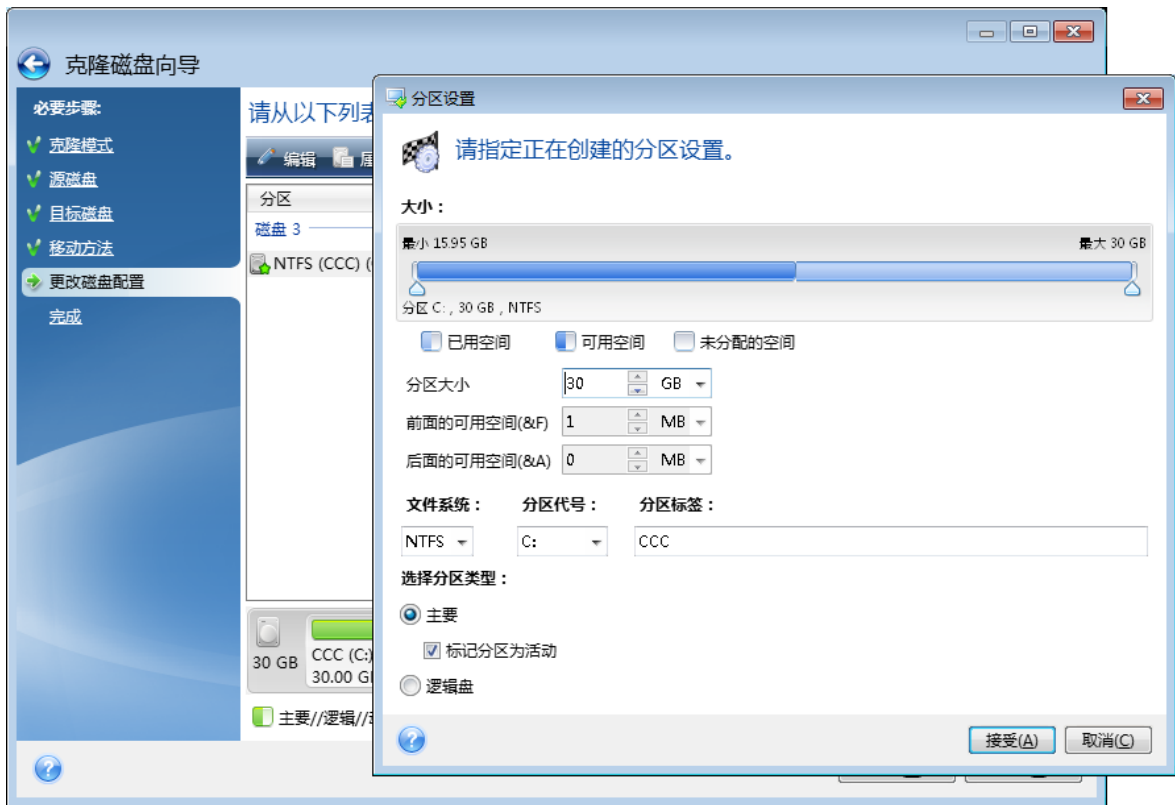
11.1.2 手动分区

您可用手动传输方法调整新磁盘上分区的大小。默认情况下，程序会按比例调整分区的大小。



编辑分区

1. 选择相应分区，然后单击**编辑**。此时将打开“分区设置”窗口。



2. 为此分区指定以下设置：

- 大小及位置
- 文件系统
- 分区类型(仅适用于 MBR 磁盘)
- 分区代号与标签

有关详细信息，请参阅[分区设置](#)。

3. 单击**接受**。

警告！

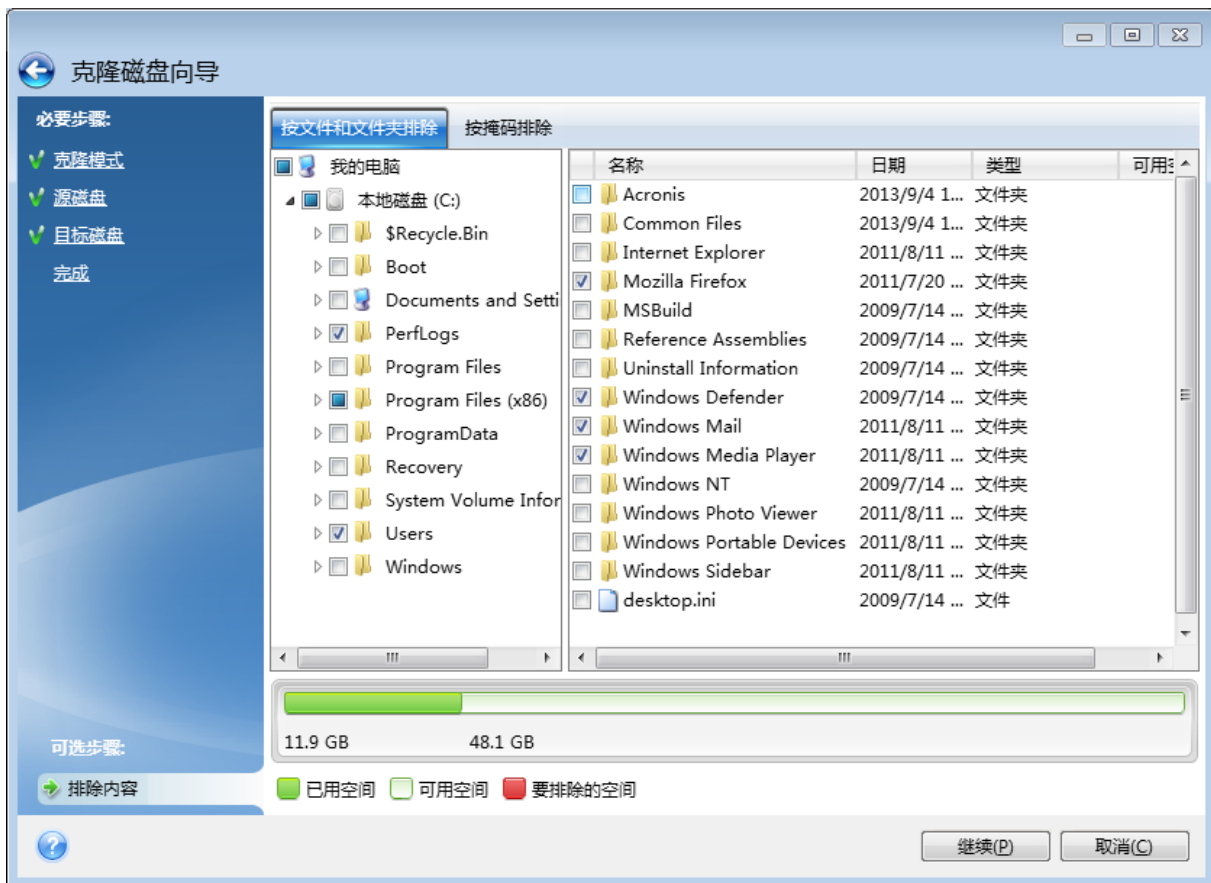
单击此窗口侧边栏上任何之前的向导步骤时，将重置已选定的所有大小和位置更改，因而您必须重新进行指定。

11.1.3 从克隆中排除项目

如果您不希望克隆源磁盘中的特定文件(例如，当您的目标磁盘小于源磁盘时)，您可以选择在**排除内容**步骤中排除它们。

注意

当克隆系统分区时，不建议排除隐藏文件和系统文件。



您可以通过以下两种方式排除文件和文件夹：

- **按文件和文件夹排除** — 此选项卡允许您从文件夹树中选择特定文件和文件夹。
- **按掩码排除** — 此选项卡允许您按掩码排除一组文件，或按名称或路径排除单个文件。
若要添加排除标准，请单击**添加**，键入文件名、路径或掩码，然后单击**确定**。您可以根据需要添加任何数量的文件和掩码。

排除标准的示例：

- 您可以输入显式的文件名：
 - *file.ext* — 将从克隆中排除所有此类文件。
 - *C:\file.ext* - C 上的 file.ext 文件：排除磁盘。
- 您可以使用通配符 (* 和 ?)：
 - **.ext* - 将排除扩展名为 .ext 的所有文件。
 - *??name.ext* - 将排除扩展名为 .ext，且文件名(以任何两个符号(??)开头并以 name 结尾)为六个字母的所有文件。
- 您可以输入文件夹的路径：
 - *C:\my pictures* — C: 盘上的我的图片文件夹。排除磁盘。

使用右侧窗格上的相应按钮编辑和删除排除标准。

11.1.4 迁移方法

Acronis Cyber Protect Home Office 允许您在克隆操作完成后为目标磁盘选择分区布局：

- **MBR(主引导扇区)**- 一个 512 字节的引导扇区, 是硬盘的第一个扇区, 用于放置磁盘的主分区表。
- **GPT(GUID 分区表)**- 用于硬盘分区表布局的标准。GPT 允许磁盘/分区的最大容量为 9.4 ZB(9.4 x 10²¹ 字节)。

使用该向导可在克隆操作的同时转换分区布局, 或保持源布局:

- **按原样复制分区** - 选择该选项, 迁移系统而不更改分区布局。注意, 在这种情况下超过 2TB 的磁盘空间将无法访问。若要分配超过 2TB 的磁盘空间, 必须使用 Acronis Extended Capacity Manager。
- **复制分区, 将磁盘作为非系统磁盘使用, 保留 GPT 样式** - 选择此选项将分区转换为 GPT 布局。

使用 Acronis Cyber Protect Home Office 还可以将 **BIOS** 转换为 **UEFI** 系统。有关更多信息, 请参阅 [统一扩展固件接口](#)。

BIOS 启动系统、MBR、不支持 UEFI

请在向导的本步骤选择目标硬盘。

当前系统包括:

系统: BIOS 启动

源分区样式: MBR

源磁盘的操作系统: Windows, 不支持在 UEFI 启动

目标磁盘大小: 小于 2 TB

如果将系统迁移到选定的磁盘:

系统: BIOS 启动

分区样式: MBR

操作系统: Windows, 不支持在 UEFI 启动

磁盘大小: 整个磁盘空间可用

有关迁移步骤的更多信息, 请查阅 [迁移方法](#) 部分。

BIOS 启动的系统、MBR、支持 UEFI

请在向导的本步骤选择目标硬盘。

当前系统包括:

系统: BIOS 启动

源分区样式: MBR

源磁盘的操作系统: Windows, 支持在 UEFI 启动

目标磁盘大小: 小于 2 TB

如果将系统迁移到选定的磁盘：

系统：BIOS 启动

分区样式：MBR

操作系统：Windows, 支持在 UEFI 启动

磁盘大小：整个磁盘空间可用

有关迁移步骤的更多信息，请查阅[迁移方法](#)部分。

BIOS 启动系统、MBR、非 Windows

Acronis Cyber Protect Home Office 允许您在操作完成后为目标磁盘选择分区布局。

当前系统包括：

系统：BIOS 启动

源分区样式：MBR

源磁盘的操作系统：非 Windows 或无 OS

目标磁盘大小：小于 2 TB

使用这些系统参数可以选择以下一项：

1. 按原样复制分区

在目标磁盘上保留 MBR 分区样式。

迁移后的目标磁盘：

系统：BIOS 启动

分区样式：MBR

操作系统：非 Windows 或无 OS

磁盘大小：整个磁盘空间可用

2. 复制分区并将磁盘用作非系统的 GPT 样式

可将分区样式转换为 GPT。

迁移后的目标磁盘：

系统：在 BIOS 中不可启动

分区样式：GPT

操作系统：非 Windows 或无 OS

磁盘大小：整个磁盘空间可用

警告！

迁移完成后，目标磁盘仅可作为非系统磁盘使用。如果 Acronis Cyber Protect Home Office 在 Windows XP x32 操作系统中运行，则该选项不可用。

有关迁移步骤的更多信息，请查阅[迁移方法](#)部分。

BIOS 启动系统、GPT、支持 UEFI

请在向导的本步骤选择目标硬盘。

当前系统包括：

系统：BIOS 启动

源分区样式：GPT

源磁盘的操作系统：Windows，支持在 UEFI 启动

如果将系统迁移到选定的磁盘：

系统：在 BIOS 中不可启动

分区样式：GPT

操作系统：Windows，支持在 UEFI 启动

磁盘大小：整个磁盘空间可用

警告！

迁移完成后，操作系统将无法从目标磁盘在 BIOS 中启动。如果想在迁移后从目标磁盘启动，则需要在系统中启用 UEFI 启动(请参阅“统一扩展固件接口”部分)，然后重新启动操作。

有关迁移步骤的更多信息，请查阅[迁移方法](#)部分。

BIOS 启动系统、GPT、非 Windows

请在向导的本步骤选择目标硬盘。

当前系统包括：

系统：BIOS 启动

源分区样式：GPT

源磁盘的操作系统：非 Windows 或无 OS

如果将系统迁移到选定的磁盘：

系统：BIOS 启动

分区样式：GPT

操作系统：非 Windows 或无 OS

磁盘大小：整个磁盘空间可用

有关迁移步骤的更多信息，请查阅[迁移方法](#)部分。

UEFI 启动系统、MBR、不支持 UEFI

请在向导的本步骤选择目标硬盘。

当前系统包括：

系统：UEFI 启动

源分区样式：MBR

源磁盘的操作系统：Windows, 不支持在 UEFI 启动

目标磁盘大小：小于 2 TB

如果将系统迁移到选定的磁盘：

系统：在 UEFI 中不可启动

分区样式：MBR

操作系统：Windows, 不支持在 UEFI 启动

磁盘大小：整个磁盘空间可用

警告！

操作系统可能无法从目标磁盘在 UEFI 中启动。

有关迁移步骤的更多信息，请查阅[迁移方法](#)部分。

UEFI 启动的系统、MBR、支持 UEFI

请在向导的本步骤选择目标硬盘。

当前系统包括：

系统：UEFI 启动

源分区样式：MBR

源磁盘的操作系统：Windows, 支持在 UEFI 启动

如果将系统迁移到选定的磁盘：

迁移完成后，目标分区样式将转换为 GPT 并从此处启动。

迁移后的目标磁盘：

系统：UEFI 启动

分区样式：GPT

操作系统：Windows, 支持在 UEFI 启动

磁盘大小：整个磁盘空间可用

有关迁移步骤的更多信息，请查阅[迁移方法](#)部分。

UEFI 启动系统、MBR、非 Windows

Acronis Cyber Protect Home Office 允许您在操作完成后为目标磁盘选择分区布局。

当前系统包括：

- 系统：UEFI 启动
- 源分区样式：MBR
- 源磁盘的操作系统：非 Windows 或无 OS
- 目标磁盘大小：小于 2 TB

使用这些系统参数可以选择以下一项：

1. 按原样复制分区

在目标磁盘上保留 MBR 分区样式。

迁移后的目标磁盘：

- 系统：UEFI 启动
- 分区样式：MBR
- 操作系统：非 Windows 或无 OS
- 磁盘大小：整个磁盘空间可用

2. 复制分区并将磁盘用作非系统的 GPT 样式

可将分区样式转换为 GPT。

迁移后的目标磁盘：

- 系统：在 UEFI 中不可启动
- 分区样式：GPT
- 操作系统：非 Windows 或无 OS
- 磁盘大小：整个磁盘空间可用

警告！

迁移完成后，目标磁盘仅可作为非系统磁盘使用。

有关迁移步骤的更多信息，请查阅[迁移方法](#)部分。

UEFI 启动系统、GPT、支持 UEFI

请在向导的本步骤选择目标硬盘。

当前系统包括：

- 系统：UEFI 启动

源分区样式:GPT

操作系统:Windows, 支持在 UEFI 启动

如果将系统迁移到选定的磁盘:

系统:UEFI 启动

分区样式:GPT

磁盘大小:整个磁盘空间可用

有关迁移步骤的更多信息, 请查阅[迁移方法](#)部分。

UEFI 启动系统、GPT、非 Windows

请在向导的本步骤选择目标硬盘。

当前系统包括:

系统:UEFI 启动

源分区样式:GPT

操作系统:非 Windows 或无 OS

如果将系统迁移到选定的磁盘:

系统:UEFI 启动

分区样式:GPT

磁盘大小:整个磁盘空间可用

有关迁移步骤的更多信息, 请查阅[迁移方法](#)部分。

11.2 将系统从 HDD 迁移至 SSD

首先, 确保 Acronis Cyber Protect Home Office 能在 Windows 中和 Acronis 可启动媒体下检测到新的 SSD。如有问题, 请参阅 [Acronis Cyber Protect Home Office 无法识别 SSD 时的操作](#)。

11.2.1 SSD 大小

由于通常 SSD 的容量比 HDD 的容量要小, 因此旧硬盘上占用的空间可能会超过您 SSD 的大小。如果出现这种情况, 则无法进行迁移。

要减少系统盘上的数据量, 请尝试以下操作:

- 将旧硬盘中的数据文件移动到另一个位置, 例如移动到另一个内置或外接硬盘驱动器上。
- 创建 .zip 格式的数据文件(例如文档、图片、音频文件等等)存档, 然后删除原始文件。
- 使用 Windows 磁盘清理实用工具清理硬盘。

请注意, 为实现稳定的操作, Windows 需要在系统分区上拥有数 GB 的可用空间。

11.2.2 选择哪种迁移方法

如果您的系统磁盘由单个分区(不包括隐藏的系统保留分区)组成,您可以尝试使用克隆工具迁移至 SSD。如需更多信息,请参阅[克隆硬盘](#)。

但在大多数情况下,我们建议您使用备份与恢复方法。此方法更灵活,可加强对迁移的控制。请参阅[使用备份与恢复方法迁移至 SSD](#)。

11.2.3 Acronis Cyber Protect Home Office 无法识别 SSD 时的操作

Acronis Cyber Protect Home Office 有时可能无法识别 SSD。

在这种情况下,请检查 BIOS 中是否能够识别 SSD。

如果您计算机的 BIOS 未显示 SSD,请检查电源和数据线的连接是否正确。您还可以尝试更新 BIOS 和 SATA 驱动程序。如果这些建议无法帮到您,请联系 SSD 制造商的支持部门。

如果您的计算机的 BIOS 确实显示了 SSD

1. 根据您使用的操作系统,在“搜索”字段或“运行”字段中键入 `cmd` 然后按 **Enter** 键。
2. 在命令行提示符处输入:

```
diskpart  
list disk
```

屏幕上将显示连接至您计算机的磁盘。查看您 SSD 的磁盘编号。使用其大小作为参考。

3. 要选择此磁盘,请运行以下命令:

```
select disk N
```

此处的 N 是您的 SSD 的磁盘编号。

4. 要从 SSD 中删除所有信息并使用默认内容覆盖 MBR,请运行以下命令:

```
clean  
exit  
exit
```

启动 Acronis Cyber Protect Home Office,并检查它是否能检测到 SSD。如果它能检测到 SSD,请使用“添加新磁盘工具”在占用整个磁盘空间的磁盘上创建单个分区。创建分区后,请查看分区前的可用空间是否为 1 MB。如需更多信息,请参阅[添加新硬盘](#)。

检查您的 Acronis 可启动媒体是否可识别 SSD

1. 从 Acronis 可启动媒体启动。
2. 在主菜单中选择**工具与实用工具 -> 添加新磁盘**,**磁盘选择**屏幕将显示有关系统中所有硬盘的信息。使用此操作检查在恢复环境中能否检测到 SSD。
3. 如果屏幕显示您的 SSD,单击**取消**即可。

如果可启动媒体未能识别 SSD, 且 SSD 控制器模式为 AHCI, 您可尝试将此模式更改为 IDE(或在某些 BIOS 品牌中更改为 ATA), 并检查问题是否得到解决。

警告!

注意! 更改此模式后请勿启动 Windows, 否则可能导致严重的系统问题。启动 Windows 前, 您必须将此模式返回到 AHCI。

如果更改模式后可启动媒体检测到 SSD, 您可使用以下步骤在可启动媒体下进行恢复或克隆:

1. 关闭计算机。
2. 启动至 BIOS, 将模式从 AHCI 更改为 IDE(或在某些 BIOS 品牌中更改为 ATA)。
3. 从 Acronis 可启动媒体启动。
4. 恢复或克隆磁盘。
5. 启动至 BIOS 并将 IDE 更改回 AHCI。
6. 启动 Windows。

上述建议不起作用时的操作

您可以尝试创建基于 WinPE 的媒体。此媒体可能会提供必要的驱动程序。有关详细信息, 请参阅[创建 Acronis 可启动媒体](#)。

11.2.4 使用备份与恢复方法迁移至 SSD

以下步骤适用于所有支持的操作系统。首先, 让我们来介绍一个简单的案例: 您的系统磁盘由单个分区组成。请注意, Windows 7 及更高版本的系统磁盘可能拥有隐藏的系统保留分区。

我们建议您将系统迁移至不包含分区(磁盘空间未分配)的空的 SSD 中。请注意, 如果您的 SSD 为新硬盘并且以前未使用过, 则它不包含分区。

将系统迁移至 SSD

1. 启动 Acronis Cyber Protect Home Office。
2. 如果您没有 Acronis 可启动媒体, 请创建一个。若需进行此操作, 请在工具部分单击**创建可启动媒体**, 然后按照屏幕上的指示操作。
3. 将整个系统驱动器(在磁盘备份模式下)备份到系统硬盘之外的硬盘和 SSD 上。
4. 关闭计算机并卸下您的系统硬盘。
5. 将 SSD 安装到硬盘所在的插槽中。

注意

对于某些 SSD 品牌, 您可能需要将 SSD 插入 PCI Express 插槽。

6. 从 Acronis 可启动媒体启动。
7. 验证备份, 确保该备份可用于恢复。要执行此操作, 请单击左侧窗格上的**恢复**并选择备份。单击右键并从快捷菜单中选择**验证存档**, 然后单击**继续**。
8. 验证完成后, 右键单击该备份, 然后在快捷菜单中选择**恢复**。
9. 在恢复方法步骤中选择**恢复整个磁盘和分区**, 然后单击**下一步**。

10. 在恢复内容步骤中选择系统磁盘。
11. 单击**新建位置**, 选择 SSD 作为系统磁盘的新位置, 然后单击**接受**。
12. 在下一步中单击**继续**以开始恢复。
13. 恢复完成之后, 退出单机版 Acronis Cyber Protect Home Office。
14. 尝试从 SSD 启动, 然后确保 Windows 和应用程序工作正常。

如果您的系统硬盘还包含隐藏恢复或诊断分区(这种情况在笔记本电脑中较为常见), 则步骤或会有所不同。在恢复到 SSD 的过程中, 您通常需要手动调整分区的大小。有关说明, 请参阅[恢复具有隐藏分区的磁盘](#)。

12 工具

Acronis 工具和实用工具包括保护工具、加载工具、克隆磁盘实用工具、安全与隐私权实用工具以及磁盘管理实用工具。

保护工具

- "Acronis 异机还原"(第 209 页)
- "Acronis 启动恢复管理器"(第 177 页)
- "Acronis 媒体生成器"(第 166 页)
- "Acronis Secure Zone"(第 184 页)
- "Try&Decide"(第 179 页)

磁盘克隆

- "磁盘克隆实用工具"(第 152 页)

安全与隐私权

- "Acronis DriveCleanser"(第 192 页)
- "系统清理"(第 197 页)

磁盘管理

- "添加新硬盘"(第 188 页)

映像加载

- "加载映像"(第 205 页)
- "卸载映像"(第 206 页)

12.1 Acronis 媒体生成器

Acronis 媒体生成器允许您使 USB 闪存驱动器、外部驱动器或空白 CD/DVD 成为可启动媒体。如果 Windows 无法启动,请使用可启动媒体来运行单机版 Acronis Cyber Protect Home Office 并恢复您的计算机。

您可以创建多种类型的可启动媒体:

- **Acronis 可启动媒体**

建议大多数用户采用此类型。

- **带有 Acronis 插件的基于 WinPE 的媒体**

在预安装环境中运行 Acronis Cyber Protect Home Office 可提高与计算机硬件的兼容性,因为预安装环境使用的是 Windows 驱动程序。

当 Acronis 可启动媒体无法帮助您启动计算机时,我们建议您创建此类型的媒体。

要使用此选项,您需要安装以下组件之一:

- Windows 自动安装工具包 (AIK)。

要创建 WinPE 3.0,必须要有此组件。

- Windows 评估和部署工具包 (ADK)。要创建 WinPE 4.0、WinPE 5.0 和 WinPE 10.0, 必须要有此组件。

- **带有 Acronis 插件的基于 WinRE 的媒体**

此类型的可启动媒体与基于 WinPE 的媒体类似, 但它具有重要的优势 — 您无需从 Microsoft 网站下载 WADK 或 WAIK。Windows Recovery Environment 已包含在 Windows Vista 以及更高版本的 Windows 中。Acronis Cyber Protect Home Office 使用系统中的这些文件来创建基于 WinRE 的媒体。与基于 WinPE 的媒体类似, 您可以添加驱动程序来实现与硬件的更好兼容性。但是, 基于 WinRE 的媒体仅可在创建它的计算机上或者使用相同操作系统的计算机上使用。

注意事项

- 建议您在每次更新 Acronis Cyber Protect Home Office 后创建新的可启动媒体。
- 如果使用非光学媒体, 则媒体必须具有 FAT16 或 FAT32 文件系统。
- Acronis 媒体生成器仅支持 x64 WinPE 3.0、WinPE 4.0、WinPE 5.0 和 WinPE 10.0。
- 您的计算机必须满足以下要求:
 - 对于 WinPE 3.0 — 至少 256 MB RAM
 - 对于 WinPE 4.0 — 至少 512 MB RAM
 - 对于 WinPE 5.0 — 至少 1 GB RAM
 - 对于 WinPE 10.0 — 至少 512 MB RAM
- 如果 Acronis 媒体生成器不识别 USB 闪存驱动器, 您可以尝试使用位于 <https://kb.acronis.com/content/1526> 的 Acronis 知识库文章中介绍的步骤。
- 从可启动媒体启动时, 将无法对安装 Ext2/Ext3/Ext4、ReiserFS 和 Linux SWAP 文件系统的磁盘或分区进行备份。
- 从可启动媒体启动并使用单机版 Acronis Cyber Protect Home Office 时, 将无法恢复利用 Windows XP 及更高版本操作系统所提供的加密功能进行加密的文件与文件夹。如需更多信息, 请参阅 [备份的文件级安全设置](#)。但是, 使用 Acronis Cyber Protect Home Office 加密功能加密的备份将无法被恢复。
- 如果您决定在已具有 Survival Kit 的驱动器上创建可启动媒体, Acronis 媒体生成器将尝试仅使用可启动媒体覆盖和更新隐藏分区, 而不格式化整个驱动器。

12.1.1 创建 Acronis 可启动媒体

1. 插入 USB 闪存驱动器或外部驱动器 (HDD/SSD), 或者放入空白 CD 或 DVD。
2. 启动 Acronis Cyber Protect Home Office。
3. 在工具部分, 单击 **应急媒体生成器**。
4. 选择创建方法。
 - **简单** - 这是最轻松的选项。Acronis Cyber Protect Home Office 将为您的计算机选择最佳媒体类型。如果您使用 Windows 7 或更高版本, 将创建基于 WinRE 的媒体。
 - **高级** — 此选项使您可以选择媒体类型。这意味着您不仅可以为您的计算机创建可启动媒体, 还可以为运行其他 Windows 版本的计算机创建可启动媒体。有关详细信息, 请参阅 [Acronis 媒体生成器](#)。

如果您选择基于 Linux 的媒体, 则选择要放置在媒体上的 Acronis 组件。请确保您选择的组件与目标计算机架构兼容。有关详细信息, 请参阅 [可移动媒体设置](#)。

如果您选择基于 WinRE 或基于 WinPE 的媒体, 则:

- 选择媒体的架构类型:32 位或 64 位。请注意, 32 位可启动媒体仅适用于 32 位计算机, 而 64 位媒体可与 32 位和 64 位计算机兼容。
- 选择您要用于创建可启动媒体的工具包。如果您选择 WAIK 或 WADK 并且未将所选的工具包安装在计算机上, 则首先需要从 Microsoft 网站下载它, 然后安装所需的组件: Deployment Tools 和 Windows Preinstallation Environment (Windows PE)。如果 WinPE 文件已在您的计算机上并且它们存储在非默认文件夹中, 只需指定其位置, Acronis 插件将添加到现有的 WinPE 映像。
- 为了实现与硬件更好的兼容性, 可以选择要添加到映像的驱动程序。

5. 为该媒体选择一个目标位置:

- **CD**
- **DVD**
- **外部驱动器**
- **USB 闪存驱动器**

如果您的驱动器内有不支持的文件系统, 则 Acronis Cyber Protect Home Office 将建议您将其格式化为 FAT 文件系统。

警告!

格式化将永久清除磁盘上的所有数据。

- **ISO 映像文件**

您将需要指定 .iso 文件的文件名及目标文件夹。

.iso 文件创建完成后, 您可以将其刻录至 CD 或 DVD。例如, 在 Windows 7 及更高版本中, 您可以使用内置刻录工具执行此操作。在文件资源管理器中, 双击创建的 ISO 映像文件, 然后单击刻录。

- **WIM 映像文件**(仅适用于基于 WinPE 的媒体)

Acronis Cyber Protect Home Office 将 Acronis 插件从 Windows AIK 或 Windows ADK 添加至 .wim 文件。您需要为新 .wim 文件指定文件名及目标文件夹。

要使用 .wim 文件创建可启动媒体, 您需要先将文件转换为 .iso 文件。有关详细信息, 请参阅从 [.wim 文件创建 .iso 文件](#)。

注意

如果 Acronis 媒体生成器在此驱动器中检测到以前创建的 Acronis Survival Kit, 它将尝试仅用可启动媒体覆盖和更新隐藏分区, 而不格式化整个驱动器。

6. 单击**继续**。

12.1.2 Acronis 可启动媒体启动参数

您可在此设置 Acronis 可启动媒体启动参数以便配置媒体启动选项, 从而与不同硬件更好地兼容。多种选项可供选择(nousb、nomouse、noapic 等)。这些参数是向高级用户提供的。在进行 Acronis 可启动媒体的启动测试时, 若遇到任何硬件兼容问题, 最好联系 Acronis 技术支持。

添加启动参数

1. 在**参数**字段输入命令。可以输入多个命令,用空格隔开。
2. 单击**下一步**以继续。

启动 Linux 内核前可应用的其他参数

说明

以下参数可用于在特殊模式下加载 Linux 内核:

- **acpi=off**

禁止 ACPI 且可能对个别硬件配置有帮助。

- **noapic**

禁止 APIC(高级可编程中断控制器)且可能对个别硬件配置有帮助。

- **nousb**

禁止 USB 模块加载。

- **nousb2**

禁用 USB 2.0 支持。USB 1.1 设备仍可使用此选项。选用此选项可允许在 USB 1.1 模式中使用部分 USB 驱动器(若无法在 USB 2.0 模式中使用)。

- **quiet**

此参数在默认情况下处于启用状态,不显示启动消息。将其删除会导致在运行程序前加载 Linux 内核并提供命令 **shell** 时启动消息显示。

- **nodma**

禁止所有 IDE 磁盘驱动器的 DMA。防止内和在某些硬件上冻结。

- **nofw**

禁止 FireWire (IEEE1394) 支持。

- **nopcmcia**

禁止 PCMCIA 硬件检测。

- **nomouse**

禁用鼠标支持。

- **[module name]=off**

禁止模块(如, **sata_sis=off**)。

- **pci=bios**

强制使用 PCI BIOS,不直接访问硬件设备。例如,计算机上有一个非标准 PCI 主机桥时可使用此参数。

- **pci=nobios**

不允许使用 PCI BIOS, 仅允许使用直接硬件访问方式。例如, 可能因 BIOS 的问题, 启动中遇到死机时, 可以使用此参数。

- **pci=biosirq**

使用 PCI BIOS 调用来获得中断路由表。此类调用被认为有时不太稳定, 使用时会发生死机, 但有时却是获得中断路由表的唯一方法。若内核无法分配 IRQ 或发现主板上的次要 PCI 总线, 请尝试使用此选项。

- **vga=ask**

显示适合视频卡使用的可用视频模式列表并可选择适合视频卡和显示器的最佳视频模式。如果自动选择的视频模式不适合您的硬件, 请尝试使用此选项。

12.1.3 向现有 .wim 映像添加驱动程序

有时, 带有 Acronis 插件的基本 WinPE 磁盘没有用于特定硬件(例如存储设备控制器)的驱动程序。添加它们的最便捷方式是在 **应急媒体生成器** 中选择“高级”模式, 然后指定要添加的驱动程序。您可以将驱动程序手动添加到现有的 .wim 文件, 然后创建带有 Acronis 插件的 ISO 文件。

警告!

注意! 您只能添加文件扩展名为 .inf 的驱动程序。

以下过程基于位于 <https://technet.microsoft.com/> 上的一篇 MSDN 文章。

创建自定义 Windows PE 映像

1. 如果您没有带 Acronis 插件的 .wim 文件, 请启动 **应急媒体生成器** 并通过选择 **WIM 文件** 作为基于 WinPE 的媒体的目标位置来创建它。有关详细信息, 请参阅 [创建 Acronis 可启动媒体](#)。
2. 根据您的 Windows AIK 或 Windows ADK 的版本, 执行以下操作之一:
 - 在 **开始** 菜单中, 单击 **Microsoft Windows AIK**, 右键单击 **Windows PE 工具命令提示**, 然后选择 **以管理员身份运行**。
 - 在 **开始** 菜单中, 单击 **Microsoft Windows AIK**, 右键单击 **部署工具命令提示**, 然后选择 **以管理员身份运行**。
 - 在 **开始** 菜单中, 单击 **Windows Kits**, 再单击 **Windows ADK**, 右键单击 **部署和映像工具环境**, 然后选择 **以管理员身份运行**。
3. 运行 `Copype.cmd` 脚本来创建含有 Windows PE 文件的文件夹。例如, 在命令提示符中输入:

```
copype amd64 C:\winpe_x64
```

4. 例如, 将 .wim 文件复制到文件夹 C:\winpe_x64\。默认情况下, 该文件名为 `AcronisBootablePEMedia.wim`。
5. 使用 DISM 工具将基本映像安装到本地目录。要执行此操作, 请键入:

```
Dism /Mount-Wim /WimFile:C:\winpe_x64\AcronisBootablePEMedia.wim /index:1  
/MountDir:C:\winpe_x64\mount
```

6. 使用带有 Add-Driver 选项的 DISM 命令添加硬件驱动程序。例如, 要添加位于文件夹 C:\drivers\ 中的 Mydriver.inf 驱动程序, 请键入:

```
Dism /image:C:\winpe_x64\mount /Add-Driver /driver:C:\drivers\mydriver.inf
```

7. 对您需要添加的每个驱动程序重复上一步骤。
8. 使用 DISM 命令提交更改:

```
Dism /Unmount-Wim /MountDir:C:\winpe_x64\mount /Commit
```

9. 从生成的 .wim 文件创建 PE 映像(.iso 文件)。有关详细信息, 请参阅从 .wim 文件创建 .iso 文件。

12.1.4 从 .wim 文件创建 .iso 文件

要使用 .wim 文件创建可启动媒体, 您需要先将文件转换为 .iso 文件。

从生成的 .wim 文件创建 PE 映像(.iso 文件)

1. 根据您的 Windows AIK 或 Windows ADK 的版本, 执行以下操作之一:
 - 在开始菜单中, 单击 **Microsoft Windows AIK**, 右键单击 **Windows PE 工具命令提示**, 然后选择以**管理员身份运行**。
 - 在开始菜单中, 单击 **Microsoft Windows AIK**, 右键单击 **部署工具命令提示**, 然后选择以**管理员身份运行**。
 - 在开始菜单中, 单击 **Windows Kits**, 再单击 **Windows ADK**, 右键单击 **部署和映像工具环境**, 然后选择以**管理员身份运行**。
2. 运行 Copype.cmd 脚本来创建含有 Windows PE 文件的文件夹。例如, 在命令提示符中输入:

```
copype amd64 C:\winpe_x64
```

3. 替换包含新创建的 .wim 文件(例如 AcronisBootablePEMedia.wim) 的 Windows PE 文件夹中的默认 boot.wim 文件。如果 AcronisBootablePEMedia.wim 文件位于 c:\ 上, 则:
对于 WinPE 3.0, 键入:

```
copy c:\AcronisBootablePEMedia.wim c:\winpe_x64\ISO\sources\boot.wim
```

对于 WinPE 4.0、WinPE 5.0 或 WinPE 10.0, 键入:

```
copy "c:\AcronisBootablePEMedia.wim" c:\winpe_x64\media\sources\boot.wim
```

4. 使用 **Oscdimg** 工具。要创建 .iso 文件, 键入:

```
oscdimg -n -bc:\winpe_x64\etfsboot.com c:\winpe_x64\ISO c:\winpe_x64\winpe_x64.iso
```

或者, 要使媒体在 BIOS 和 UEFI 计算机上均可启动, 请键入:

```
oscdimg -m -o -u2 -udfver102 -bootdata:2#p0,e,bc:\winpe_x64\fwfiles\etfsboot.com#pEF,e,bc:\winpe_x64\fwfiles\efisys.bin c:\winpe_x64\media c:\winpe_x64\winpe_x64.iso
```

5. 使用第三方工具将 .iso 文件刻录到 CD, 您将拥有包含 Acronis Cyber Protect Home Office 的可启动的 Windows PE 光盘。

12.2 确保可启动媒体随时可用

要最大化恢复计算机的机会, 必须测试计算机是否可以从可启动媒体启动。此外, 还必须检查可启动媒体是否识别所有计算机设备, 如硬盘驱动器、鼠标、键盘和网络适配器。

如果您购买了含有可启动 CD 的盒装版产品而未更新 Acronis Cyber Protect Home Office, 您可以测试该 CD。否则, 请创建新的可启动媒体。有关详细信息, 请参阅[创建 Acronis 可启动媒体](#)。

12.2.1 要测试可启动媒体, 请执行以下操作:

注意

如果使用外接驱动器存储备份, 从可启动 CD 启动之前, 必须连接这些驱动器。否则, 程序可能检测不到驱动器。

1. 配置计算机以能够从可启动媒体启动。然后, 将可启动媒体设备(CD-ROM/DVD-ROM 或 USB 驱动器)设置为第一启动设备。有关详细信息, 请参阅[设置 BIOS 启动顺序](#)。
2. 如果拥有可启动 CD, 请在看到“按任意键以从 CD 启动”提示时, 按下任意键以开始从 CD 启动。如果 5 秒内没有按键, 将需要重新启动计算机。
3. 启动菜单出现后, 选择 **Acronis Cyber Protect Home Office**。

注意

如果您的无线鼠标不能正常工作, 请将其替换为有线鼠标。同样的建议也适用于键盘。

注意

如果没有备用鼠标或键盘, 请联系 Acronis 支持。他们将为您创建包含适合您的鼠标和键盘型号的驱动程序的自定义可启动 CD。请注意, 找到相应的驱动程序并制作自定义可启动 CD 可能需要一些时间。此外, 这可能不适用于某些型号。

4. 程序启动时, 建议您尝试从备份恢复一些文件。进行恢复测试可确保可启动 CD 可用于恢复操作。此外, 您还可确保程序检测到系统中存在的所有硬盘驱动器。

注意

如果您有备用硬盘驱动器, 强烈建议您在该硬盘驱动器上进行系统分区的恢复测试。

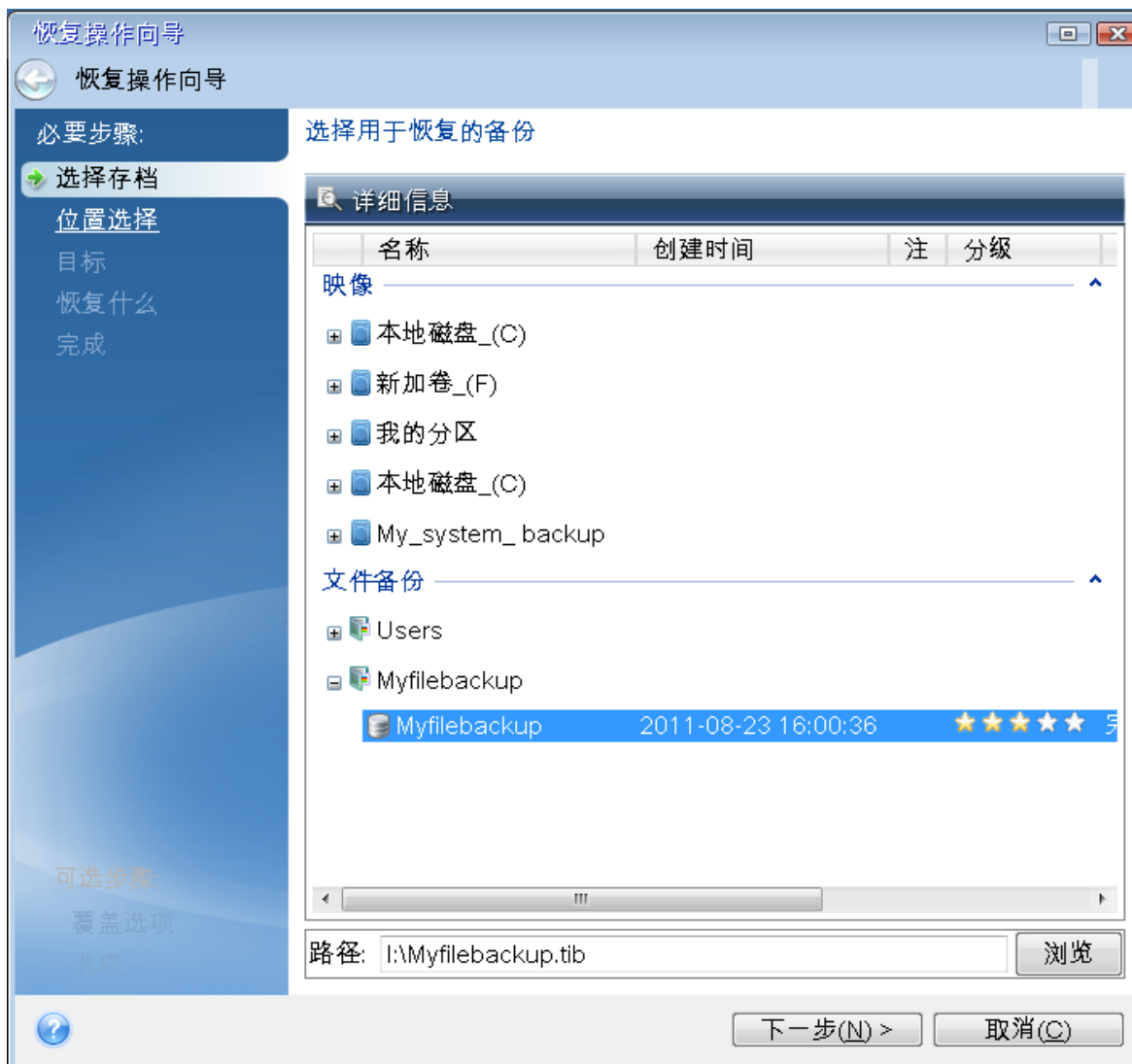
12.2.2 如何进行恢复测试, 以及检查驱动器和网络适配器

1. 如果您拥有文件备份, 则单击工具栏上的**恢复 -> 文件恢复**可启动恢复向导。

注意

如果您只拥有磁盘和分区备份, 则恢复向导也会启动且恢复过程将相似。在这种情况下, 需要在**恢复方式**步骤中选择**恢复所选文件和文件夹**。

2. 在**存档位置**步骤中选择一个备份, 然后单击**下一步**。



3. 使用可启动 CD 恢复文件时, 可以只为要恢复的文件选择一个新位置。因此, 只需在**位置选择**步骤中单击**下一步**。
4. **目标位置**窗口打开后, 确认是否所有驱动器均显示在**我的电脑**下。

注意

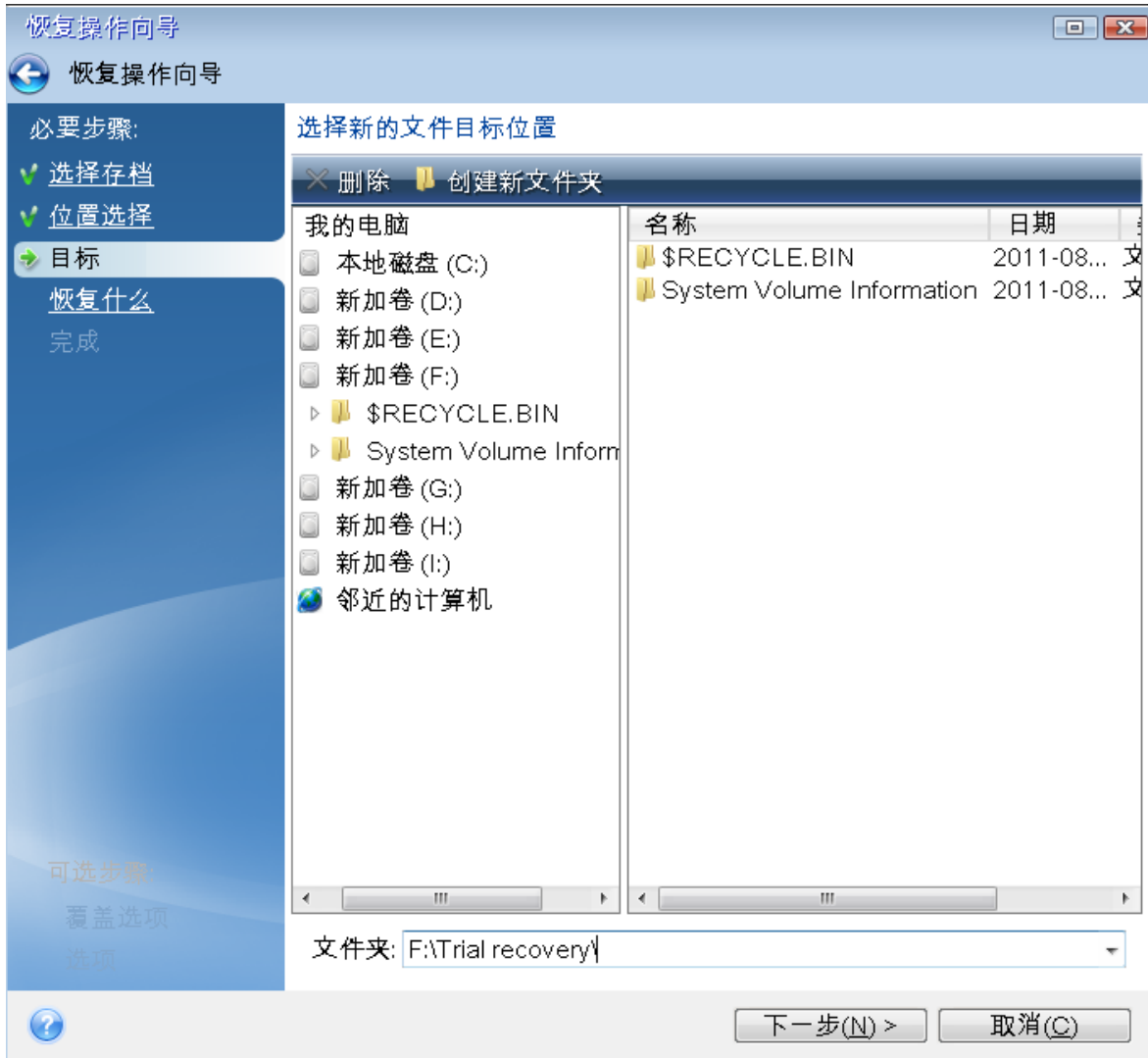
如果将备份存储在网络中, 请确认是否可以访问网络。

注意

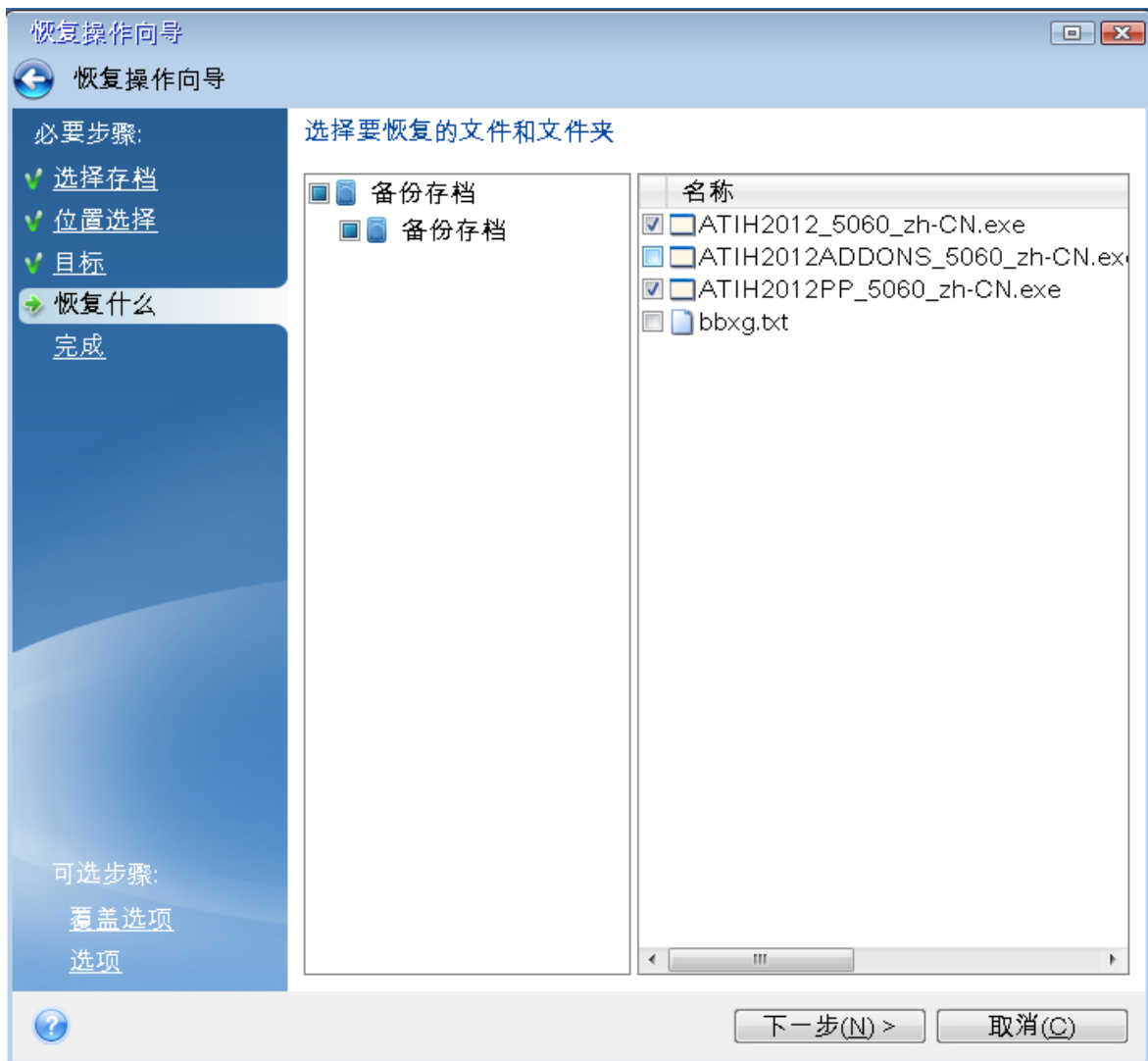
如果网络中未显示计算机，但是在**我的电脑**下找到**邻近的计算机**图标，请手动指定网络设置。要执行此操作，请选择**工具与实用工具 > 选项 > 网络适配器**以打开窗口。

注意

如果**我的电脑**下没有**邻近计算机**图标，则可能是网卡或随 Acronis Cyber Protect Home Office 提供的网卡驱动程序有问题。



5. 选择文件的目标位置，然后单击**下一步**。
6. 通过选择文件复选框，然后单击**下一步**来选择要恢复的多个文件。



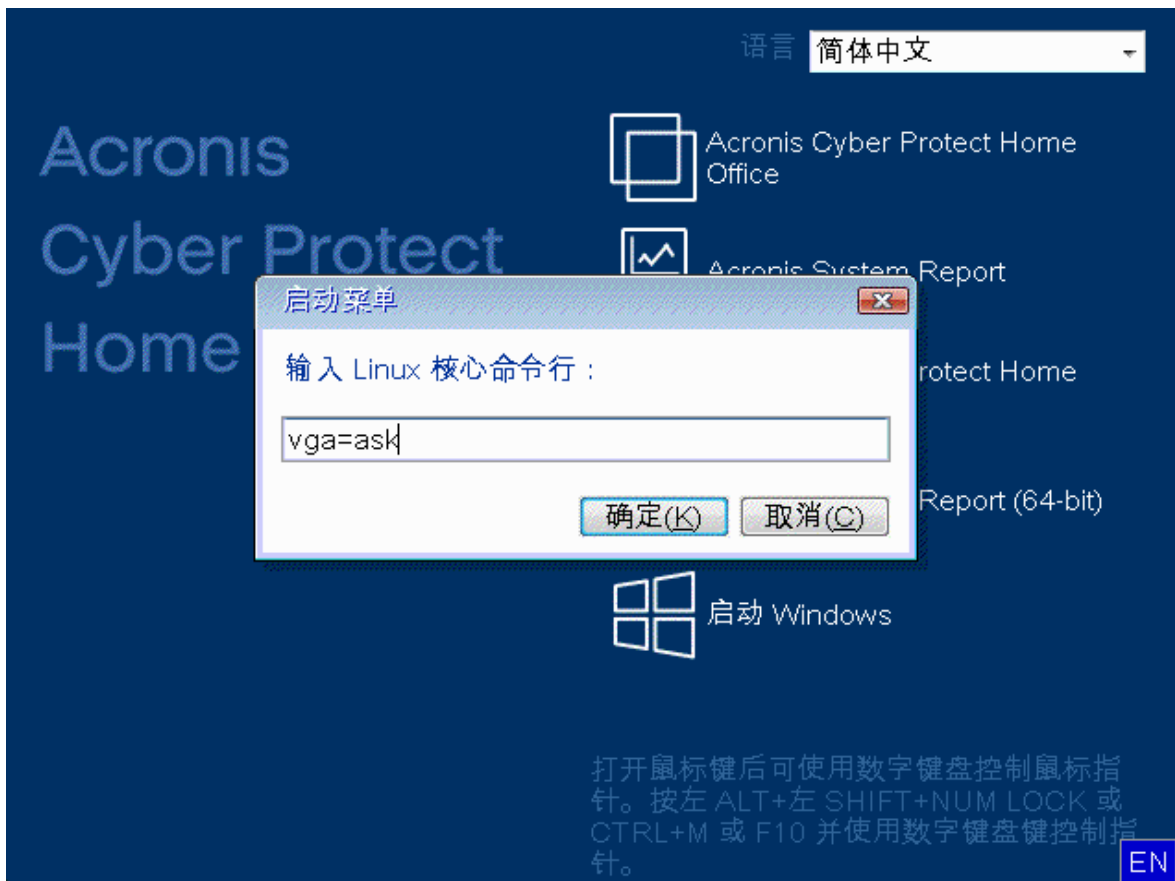
7. 单击“摘要”窗口中的**继续**以开始恢复。
8. 完成恢复操作后，退出单机版 Acronis Cyber Protect Home Office。

现在，您可以确定可启动 CD 将在需要时帮助您。

12.2.3 在从可启动媒体启动时选择视频模式

当从可启动媒体启动时，将根据显卡和显示器的规格自动选择优化的视频模式。然而，有时候程序可能选择了错误的视频模式，这种模式并不适合您的硬件。在这种情况下，可以按下列步骤选择合适的视频模式：

1. 开始从可启动媒体启动。显示启动菜单时，将鼠标移至 **Acronis Cyber Protect Home Office** 项目上并按 F11 键。
2. 当显示命令行时，键入 "vga=ask" (不带引号) 并单击**确定**。



3. 在启动菜单中选择 **Acronis Cyber Protect Home Office** 以继续从可启动媒体启动。要查看可用的视频模式, 请在显示合适的消息时按下 Enter 键。
4. 选择认为最适合您的监视器的视频模式, 并在命令行中键入它的编号。例如, 在键入 338 时会选择视频模式 1600x1200x16(请参见下图)。


```

333 1024x768x16 VESA      334 1152x864x16 VESA      335 1280x960x16 VESA
336 1280x1024x16 VESA     337 1400x1050x16 VESA     338 1600x1200x16 VESA
339 1792x1344x16 VESA     33A 1856x1392x16 VESA     33B 1920x1440x16 VESA
33C 320x200x32 VESA       33D 320x400x32 VESA       33E 640x400x32 VESA
33F 640x480x32 VESA       340 800x600x32 VESA       341 1024x768x32 VESA
342 1152x864x32 VESA     343 1280x960x32 VESA     344 1280x1024x32 VESA
345 1400x1050x32 VESA    346 1600x1200x32 VESA    347 1792x1344x32 VESA
348 1856x1392x32 VESA    349 1920x1440x32 VESA    34A 1366x768x8 VESA
34B 1366x768x16 VESA     34C 1366x768x32 VESA     34D 1680x1050x8 VESA
34E 1680x1050x16 VESA    34F 1680x1050x32 VESA    350 1920x1200x8 VESA
351 1920x1200x16 VESA    352 1920x1200x32 VESA    353 2048x1536x8 VESA
354 2048x1536x16 VESA    355 2048x1536x32 VESA    356 320x240x8 VESA
357 320x240x16 VESA      358 320x240x32 VESA      359 400x300x8 VESA
35A 400x300x16 VESA      35B 400x300x32 VESA      35C 512x384x8 VESA
35D 512x384x16 VESA     35E 512x384x32 VESA     35F 854x480x8 VESA
360 854x480x16 VESA     361 854x480x32 VESA     362 1280x720x8 VESA
363 1280x720x16 VESA    364 1280x720x32 VESA    365 1920x1080x8 VESA
366 1920x1080x16 VESA    367 1920x1080x32 VESA    368 1280x800x8 VESA
369 1280x800x16 VESA    36A 1280x800x32 VESA    36B 1440x900x8 VESA
36C 1440x900x16 VESA    36D 1440x900x32 VESA    36E 720x480x8 VESA
36F 720x480x16 VESA     370 720x480x32 VESA     371 720x576x8 VESA
372 720x576x16 VESA     373 720x576x32 VESA     374 800x480x8 VESA
375 800x480x16 VESA     376 800x480x32 VESA     377 1280x768x8 VESA
378 1280x768x16 VESA    379 1280x768x32 VESA

Enter a video mode or "scan" to scan for additional modes: _

```

5. 请耐心等待，直到 Acronis Cyber Protect Home Office 启动为止，并确保监视器上显示的“欢迎”窗口的视频品质适合您。

要测试其它视频模式，请关闭 Acronis Cyber Protect Home Office 并重复上面的过程。

在找到适用于您的硬件的最佳视频模式后，可以创建新的可启动媒体，它会自动选择这种视频模式。

要执行此操作，请启动 Acronis 媒体生成器，选择需要的媒体组件，在“可启动媒体启动参数”步骤中，在命令行中键入前缀为“0x”的模式编号（本例中为 0x338），然后象往常一样创建媒体。

12.3 Acronis 启动恢复管理器

“Acronis Startup Recovery Manager”无需加载操作系统，即可启动 Acronis Cyber Protect Home Office。凭借此功能，仅使用 Acronis Cyber Protect Home Office 即可恢复受损的分区，即使操作系统无法启动。与从 Acronis 可移动媒体启动不同，您无需独立的媒体或网络连接即可启动 Acronis Cyber Protect Home Office。

注意

Acronis 启动恢复管理器不可在运行 Windows 的平板电脑上使用。

激活 Acronis 启动恢复管理器

1. 启动 Acronis Cyber Protect Home Office。
2. 在工具部分中，单击**所有工具**，然后双击**激活 Acronis 启动恢复管理器**。
3. 在打开的窗口中，单击**激活**。



若发生故障, 请开启计算机, 并在显示“按 F11 运行 Acronis 启动恢复管理器”消息时按 F11。如此, 系统将启动单机版 Acronis Cyber Protect Home Office, 该版本与完整版略微不同。

取消激活 **Acronis 启动恢复管理器**

1. 启动 Acronis Cyber Protect Home Office。
2. 在工具部分中, 单击**所有工具**, 然后双击**激活 Acronis 启动恢复管理器**。
3. 在打开的窗口中, 单击**取消激活**。

12.3.1 其他信息

独立 Acronis Cyber Protect Home Office 的磁盘代号有时与 Windows 识别驱动器的方式不同。例如, 在单机版 Acronis Cyber Protect Home Office 中识别的 D: 磁盘可能与 Windows 中的 E 盘对应。磁盘标签和分区大小信息、文件系统、驱动器容量、制造商以及型号等信息会帮助您正确识别磁盘和分区。

启用 Try&Decide 后, 您将无法使用以前激活的 Acronis 启动恢复管理器。在 Try 模式中重新启动计算机, 将使您能够再次使用 Acronis 启动恢复管理器。

Acronis 启动恢复管理器影响其他加载程序吗?

激活 Acronis 启动恢复管理器后, 它将以自身可启动代码覆盖主可启动记录 (MBR)。若您已安装任何第三方启动管理器, 则需要激活“启动恢复管理器”后重新激活它们。对于 Linux 载入器(如 LiLo 和 GRUB), 您可考虑在激活 Acronis 启动恢复管理器前, 将它们安装到 Linux 根(或可启动)分区可启动记录而非 MBR 中。

UEFI 启动机制与 BIOS 不同。任何 OS 加载程序或其他启动程序都有自己的启动变量, 来定义到相应加载程序的路径。所有加载程序都存储在称为 EFI 系统分区的特殊分区上。当您在 UEFI 启动系统中激活 Acronis 启动恢复管理器时, 它将通过写入自身的启动变量来更改启动顺序。此变量将添加到变量列表并且不会更改它们。由于所有加载程序都是独立的, 并且相互之间无任何影响, 因此在激活 Acronis 启动恢复管理器之前或之后无需更改任何项目。

12.4 Try&Decide

当您打开 Try&Decide 后, 计算机处于 Try 模式下。在此之后, 您可以进行任何可能存在危险的操作, 无需担心可能会损害操作系统、程序或数据。当您关闭 Try&Decide 后, 您需要决定是将更改应用到计算机还是放弃更改。

12.4.1 在哪些情况下 Try&Decide 可以提供帮助

在您尝试进行以下操作之前, 我们建议您打开 Try&Decide:

- 更改任何系统设置, 特别是当您不确定这些更改会如何影响您的计算机时。
- 安装系统更新、驱动程序等。
- 安装不熟悉的应用程序。
- 打开来自未知发件人的电子邮件附件。
- 访问可能包含潜在的问题内容的网站。

注意

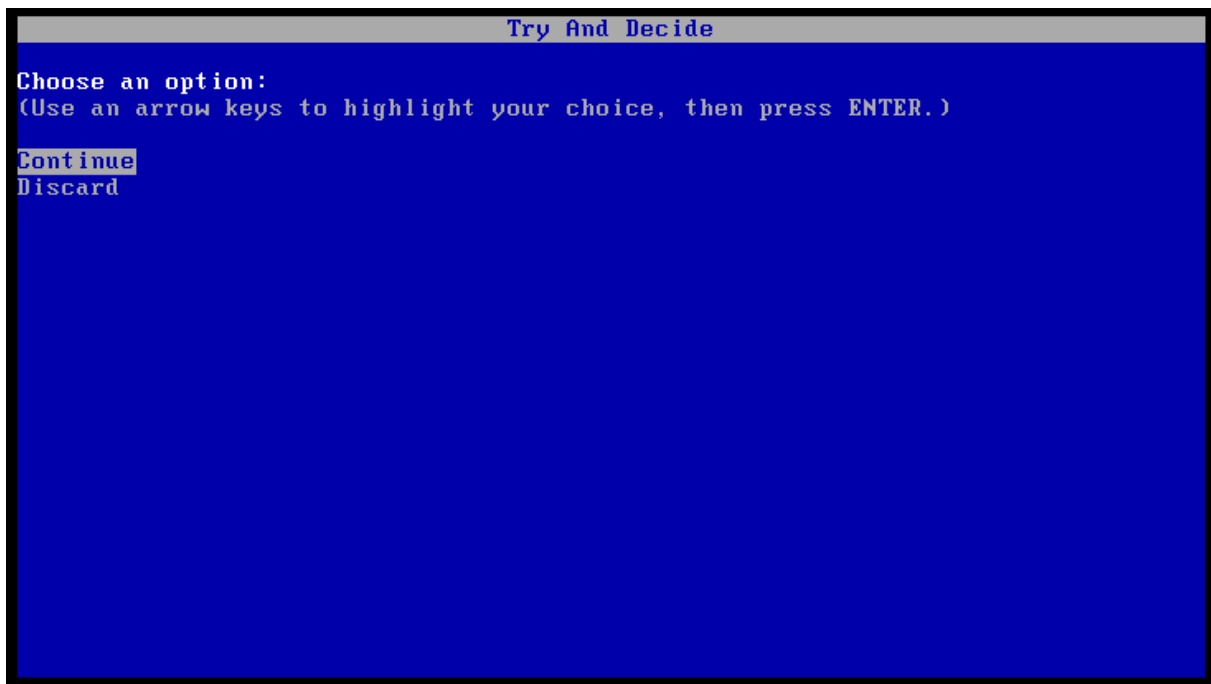
请切记, 如果从 POP 邮件服务器下载电子邮件, 或在 Try 模式下创建新文件或编辑现有文档, 然后决定放弃更改, 那么这些文件、文档更改和邮件将不再存在。在此情况下, 请将新文件和编辑的文档保存到驱动器(例如 USB 闪存驱动器), 然后将其拔下, 之后再放弃更改。

12.4.2 在计算机重新启动后, Try&Decide 如何工作

Try&Decide 可一直保持开启, 因为此模式在重新启动操作系统后仍能“存活”。

Try 模式下计算机因任何原因重新启动, 在操作系统启动前, 您将看到一个对话框, 为您提供两种选择 - 停止运行该模式并放弃更改, 或继续在此模式下运行。此操作可放弃导致系统故障的更改。另一方面, 例如, 若您在安装应用程序后重新启动, 可在启动 Windows 后继续在 Try 模式下运行。

在 Try 模式下, 计算机的每次“软”重启都会导致高达 500MB 的 Try&Decide 内存管理数据存储到用于存储虚拟更改的存储区。



12.4.3 使用 Try&Decide 的限制

如果使用的是 Windows 7、Windows 8 或 Windows 10, 请注意, 程序在 Try 模式下时可能会占用较多的可用磁盘空间, 即使计算机处于闲置状态。这是因为内务管理活动, 如索引, 正在背景中运行。

请注意, 在 Try 模式中工作时将遭遇系统性能下降的问题。此外, 应用更改的过程也需要较长的时间, 尤其是连续几天都开启 Try 模式时。

请注意, Try&Decide 不能对磁盘分区内的更改进行跟踪, 因此无法在 Try 模式下对分区执行虚拟操作, 如调整分区大小或更改分区配置。此外, 不可在使用 Try&Decide 时同时使用磁盘碎片整理或磁盘错误检查程序等实用工具, 因为这样可能会对文件系统造成不可挽回的损坏, 并导致系统磁盘无法启动。

启动 Try 模式后, 您将无法使用以前激活的 Acronis 启动恢复管理器。在 Try 模式中重新启动计算机, 将使您能够再次使用 Acronis 启动恢复管理器。

Try&Decide 和不间断备份不能同时工作。启动 Try 模式将挂起不间断备份。在停止 Try 模式后, 不间断备份将恢复。

在启动 Try 模式后, 您将无法使用“休眠”省电模式。

无法使用 Try&Decide 保护动态磁盘。

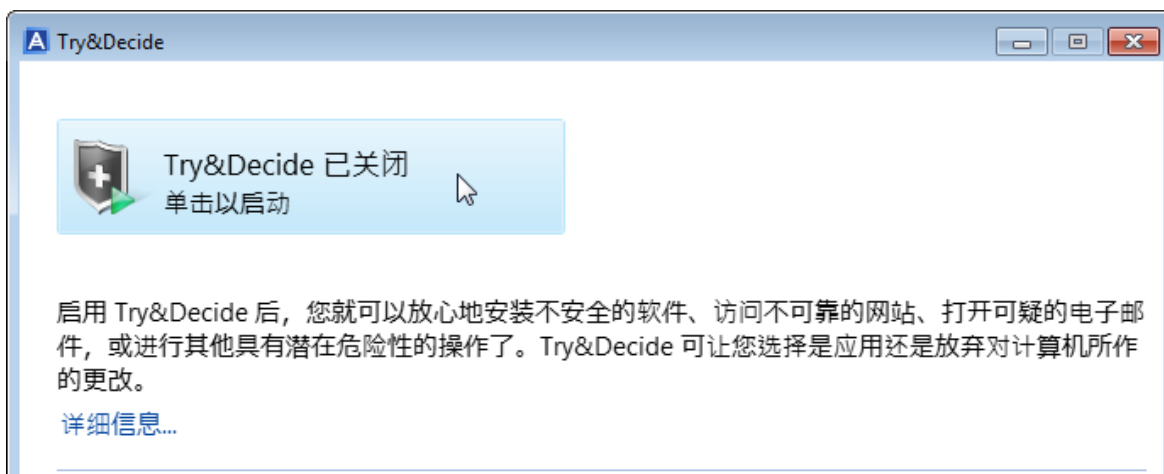
如果您系统中的分区通过 BitLocker 加密, 则 Try&Decide 不起作用。

Try&Decide 不能保护 Acronis Secure Zone 或者将其用作保存虚拟更改的存储。

12.4.4 使用 Try&Decide

1. 启动 Acronis Cyber Protect Home Office。
2. 在工具部分中, 单击 **Try&Decide**。

3. 如有必要,可设置 Try&Decide 选项。有关详细信息,请参阅 [Try&Decide 选项和通知](#)。
4. 若要启动 Try 模式,请单击 **Try&Decide** 图标。程序可启动追踪针对操作系统和文件所作的全部更改,并暂时将全部更改存储在所选磁盘上。



5. 执行您希望尝试的所有更改。

注意

当为存储虚拟更改所选的位置中的磁盘空间仅达到应用更改所需的最低值时,程序会询问您是应用还是放弃更改。如果您忽略警告消息,程序将在磁盘已满时自动重新启动并放弃更改。

6. 若要停止 Try 模式,请单击 **Try&Decide** 窗口中的 **Try&Decide** 图标。



7. 在以下选项中选择一项:
 - 若您想保留对系统所做的更改,请选择 **应用更改**。
 - 若要加快应用的进程,请选择 **重启应用更改**。单击此按钮, Try&Decide 会重启您的计算机,并在重启时应用更改。

- 若您想要系统返回至开启 Try 模式前的状态, 请选择**放弃更改**。当您选择此选项时, 将会显示一个弹出窗口, 其中包含以下选项:**重启以放弃更改**和**不重启**。如果您选择**不重启**选项, Try&Decide 功能会保持启用状态, 并且将不会放弃更改。

注意

如果已选择**放弃更改**并且已重新启动安装有多个操作系统的计算机时, 您将无法启动在 Try 模式下运行之外的操作系统。第二次重新启动可恢复原始 MBR 并使其他操作系统可启动。

12.4.5 Try&Decide 选项和通知

您可以在 Try&Decide 窗口中更改 Try&Decide 选项。若要恢复设置的默认值, 请单击“重置设置为默认”。

受保护的分区

若要更改此设置, 请执行以下操作:

1. 单击设置名称旁边的分区盘符。此时将打开“分区选择”窗口。
2. 选择要保护的分区, 然后单击**确定**。

默认情况下, Try&Decide 保护系统分区(磁盘 C), 但是您也可选择对系统中的其他任何分区实施保护。

虚拟更改的存储

若要更改此设置, 请执行以下操作:

1. 单击设置名称旁边的分区盘符。此时将打开“虚拟更改存储”窗口。
2. 选择您要用作虚拟更改存储的分区, 然后单击**确定**。

默认情况下, Try&Decide 将信息保存到磁盘 C 上的可用空间。

注意

选择保护多个分区时, 您不能选择要保护的分区来存储虚拟更改。此外, 您不能选择外接硬盘驱动器。

通知

若要更改默认通知设置, 请单击**更改警告设置**。此时将打开“设置”窗口。

- 剩余磁盘空间 - 如果虚拟更改存储中的可用空间值开始少于指定的值, 程序将显示一条通知消息。
- 启动 Try&Decide 后的已用时间 - 程序会通知您 Try&Decide 的运作时间是否已超过您指定的时间段。

12.4.6 Try&Decide: 典型使用案例

Try&Decide 功能可在各种环境下为您提供帮助, 例如:

软件评估

有时在安装新软件之前打开 Try 模式可能会有帮助。例如,当您需要执行以下操作时,我们建议您打开 Try 模式:

- 选择防病毒软件。

众所周知,安装防病毒软件会严重削弱一些应用程序的功能,甚至令这些应用程序在防病毒软件安装后拒绝可启动。您可以测试防病毒软件的试用版。若遇到任何问题,请放弃系统的更改并尝试其他供应商的防病毒软件。

- 安装程序的试用版。

众所周知,Windows 控制面板的“添加或删除程序”组件无法保证能完全卸载应用程序。如果您不喜欢安装的程序,可放弃系统中的更改。在这种情况下,Try&Decide 已完全删除程序,您无需担心。

- 安装可疑软件。

如果您不信任您要安装的软件的供应商或者软件的来源未知,请在安装此软件之前打开 Try 模式。如果出现任何差错,请放弃在 Try 模式下所做的更改。

文件恢复

您不小心删除了一些文件,并且清空了回收站。随后您记得删除的文件包含重要的数据,现在您想尝试使用适当的软件恢复被删除的文件。然而,有时候您可能会犯错误,并尝试恢复被删除的文件,使事情变得比尝试恢复文件之前更糟。因此,您可继续以下操作:

- 打开 Try 模式。
- 启动恢复删除文件实用程序
- 实用程序扫描磁盘并搜索删除的文件和文件夹条目后,它会显示其找到的删除条目(若有),并提供保存其可恢复的任何东西的机会。您总有可能会选择错误的文件,而在您恢复文件时,实用程序可能会覆盖您试图恢复的文件。若并非 Try&Decide 导致的,则此错误将是致命的,文件将永久丢失。
- 但您现在仅需放弃在 Try 模式下所作的更改,并尝试在再次打开 Try 模式后恢复文件即可。这样的尝试可能会重复,直至您相信您已尽全力恢复文件。

网络隐私

假设您不想任何人知道您曾访问过哪些网站,或打开过哪些网页 - 我们都有私隐权。但问题是,为使您的网上冲浪更舒适、快速,系统会在特殊的隐藏文件内存储此类信息及更多数据:您收到的 Cookie,您所作的搜索引擎查询,您输入的 URL 等。清理互联网临时文件、删除 Cookie、清理最近使用浏览器工具打开的网页历史记录时,不会完全删除此类信息。因此窥探者可使用特殊的软件查看该信息。

打开 Try 模式,随心所欲地浏览网络。之后,如果您想要删除所有活动痕迹,请放弃在 Try 模式下所做的更改。

12.5 Acronis Secure Zone

Acronis Secure Zone 是一个特殊的安全分区，您可以在计算机上创建该分区来存储备份。Acronis Secure Zone 具有一个 FAT32 文件系统。

当您创建 Acronis Secure Zone 时，它会显示在文件资源管理器的**其他**部分。您可以像浏览普通分区那样浏览 Acronis Secure Zone。

若 Acronis Secure Zone 受密码保护，则除查看版本详细信息外的其他任何操作均须输入密码。

12.5.1 Acronis Secure Zone 清理

如果 Acronis Secure Zone 中没有足够的空间用于新备份，您可以：

- 取消备份操作，增加 Acronis Secure Zone 的大小，然后再次运行备份。
- 取消备份操作，在 Acronis Secure Zone 中手动删除一些备份，然后再次运行备份。
- 确定您想自动删除同一类型(文件级或磁盘级)中最早的备份以及所有后续增量版本和差异版本。在此之后，如果可用空间仍然不足，则 Acronis Cyber Protect Home Office 会请求确认并将删除下一个完整备份。此过程将会重复出现，直到获得足够存储新备份的可用空间。如果在删除所有以前的备份之后仍然没有足够的空间，系统会取消备份。

若要防止安全区溢出，请执行以下操作：

1. 选择预定备份。
2. 单击**选项**。
3. 在**高级**选项卡上，展开**错误处理**部分。
4. 选中**ASZ 中空间不足时，删除最早的备份**复选框。
5. 单击**确定**。

有关详细信息，请参阅[错误处理](#)。

您不能将 Acronis Secure Zone 用于在 Try 模式下存储虚拟系统更改。在停止 Try&Decide 会话后，Try&Decide 数据将自动被清除。

Acronis Cyber Protect Home Office 不会在 Acronis Secure Zone 中自动删除不间断备份版本。此类版本只能手动删除。如需更多信息，请参阅[Acronis 不间断备份数据存储](#)。

12.5.2 创建和管理 Acronis Secure Zone

1. 单击**开始**按钮 —> **Acronis**(产品文件夹) —> **Acronis Secure Zone**。
“管理 Acronis Secure Zone”向导将打开。
2. 请执行以下任一操作：
如果您想创建 Acronis Secure Zone，请指定其**位置**和**大小**。
如果您想修改 Acronis Secure Zone，请选择一种操作：
 - [增大或减小大小](#)
 - [删除](#)

- 更改密码

按向导步骤执行。

3. 在**完成**步骤上, 单击**继续**。

注意

这一操作可能需要重新启动计算机。

12.5.3 Acronis Secure Zone 位置

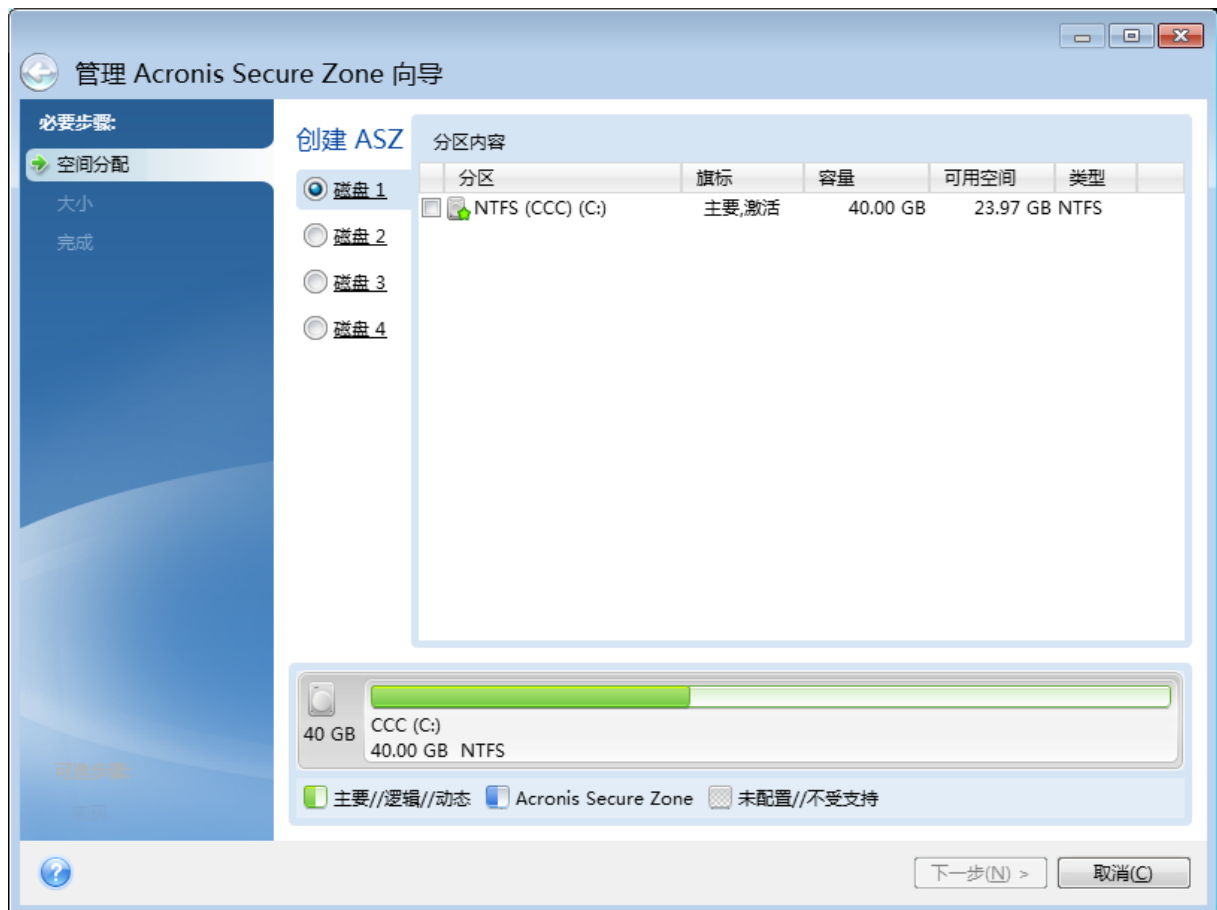
指定 *Acronis Secure Zone* 的位置

1. 选择要在上面创建 Acronis Secure Zone 的硬盘。
2. 选择要从中获取未分配和/或可用空间的一个或多个分区。必要时调整所选分区的大小, 以便为 Acronis Secure Zone 提供空间。

注意

Acronis Secure Zone 不能在动态磁盘和动态卷上创建。

3. 单击**下一步**。

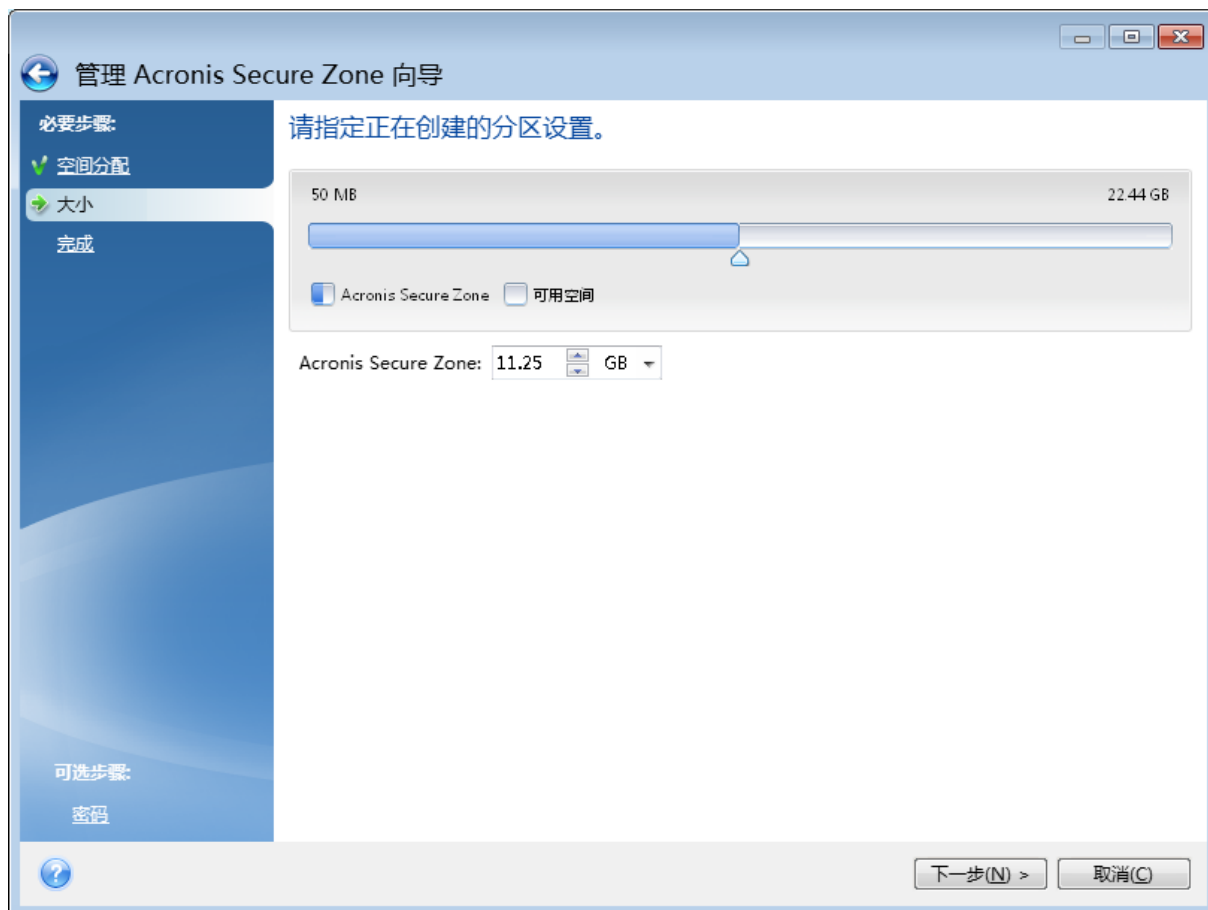


增加或减小 *Acronis Secure Zone* 的大小

1. 请选择分区，其空间将用于增加 Acronis Secure Zone 的大小或接收减小 Acronis Secure Zone 的大小后获得的可用空间。您也可选择有未分配空间的分区。
2. 单击下一步。

12.5.4 Acronis Secure Zone 的大小

要指定 Acronis Secure Zone 的大小，请将滑块拖至适当的位置或键入精确值。



最小大小约为 50 MB，视硬盘几何参数而定。最大大小等于磁盘的未分配空间，加上在上一步选择的所有分区上的总可用空间。

创建/增大 Acronis Secure Zone 时，程序将首先使用未分配的空间。若未分配的空间低于所需大小，则会减小选定分区的大小。调整分区的大小可能需要重新可启动计算机。

减小 Acronis Secure Zone 的大小时，若硬盘上有任何未分配的空间，则会将其与 Acronis Secure Zone 所释放的空间一起分配给选定的分区。因此，磁盘上不会留有未分配的空间。

警告！

将系统分区减至最小，可能会阻止操作系统启动。

12.5.5 Acronis Secure Zone 保护

您可为 Acronis Secure Zone 设置密码保护，防止未经授权的访问。

程序会在执行任何操作时要求提供相应密码, 这些操作包括数据备份和恢复、加载映像或验证 Acronis Secure Zone 中的备份、对 Acronis Secure Zone 执行调整大小和删除操作等 Acronis Secure Zone 相关操作。

设置 Acronis Secure Zone 的密码

1. 选择**设置密码**。
2. 在**密码**字段中输入密码。
3. 在**确认**字段中重新键入先前输入的密码。
4. [可选步骤] 您还可以选择一个在您忘记密码时系统会提问的密码提示问题。从列表选择一个密码提示问题, 然后输入答案。
5. 单击**下一步**以继续。

管理 Acronis Secure Zone 向导

设置或更改 Acronis Secure Zone 的密码

必要步骤:

- 动作选择
- 密码
- 完成

不保护(D)

设置密码(W)

输入新密码(E):

确认(E):

秘密提示问题(Q): 您父亲的中间名是什么?

答案(A):

下一步(N) > 取消(C)

注意

修复或更新不会影响 Acronis Cyber Protect Home Office 密码。但是, 如果在将 Acronis Secure Zone 保留在磁盘上时删除然后再安装程序, 则将会重置 Acronis Secure Zone 的密码。

12.5.6 正在删除 Acronis Secure Zone

警告!

Acronis Secure Zone 删除操作会自动销毁区域内存储的所有备份。

选择用以接收 Acronis Secure Zone 所释放空间的分区。若选择几个分区，则会按各个分区的大小比例分配空间。

而且，您可以选择在卸载程序时删除 Acronis Secure Zone。

12.6 添加新硬盘

若无足够空间保存数据，则可用更高容量的新磁盘替代旧磁盘，或添加新磁盘并将其仅用于存储数据，而仍将系统保留在旧磁盘上。

添加新硬盘

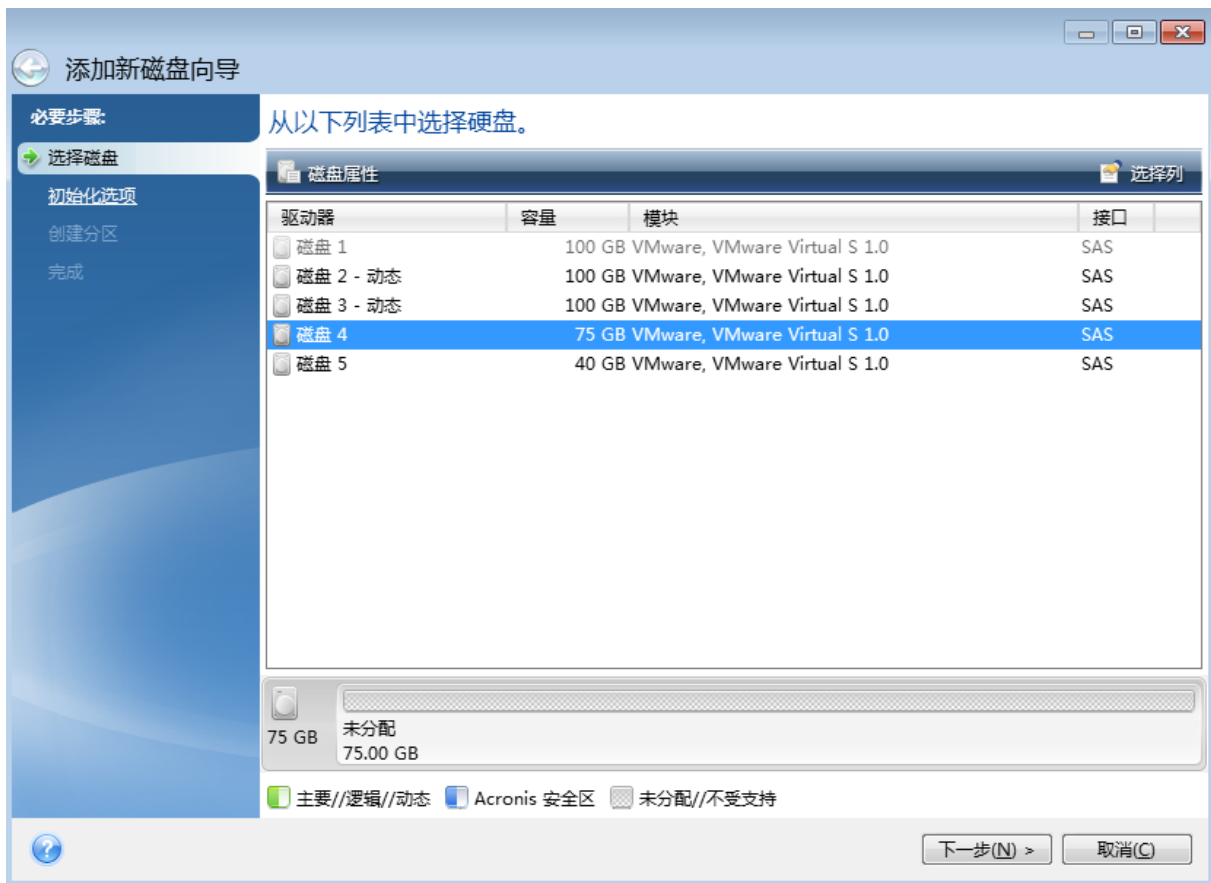
1. 关闭您的计算机，然后安装新磁盘。
2. 打开计算机。
3. 单击**开始**按钮 > **Acronis**(产品文件夹) > **添加新磁盘**。
4. 按向导步骤执行。
5. 在**完成**步骤中，确保配置的磁盘配置符合您的需求，然后单击**继续**。

12.6.1 选择硬盘

选择您已经添加到计算机的磁盘。若已添加多个磁盘，请选择其一，然后单击**下一步**继续。之后，通过重启“添加新磁盘向导”便可添加其它磁盘。

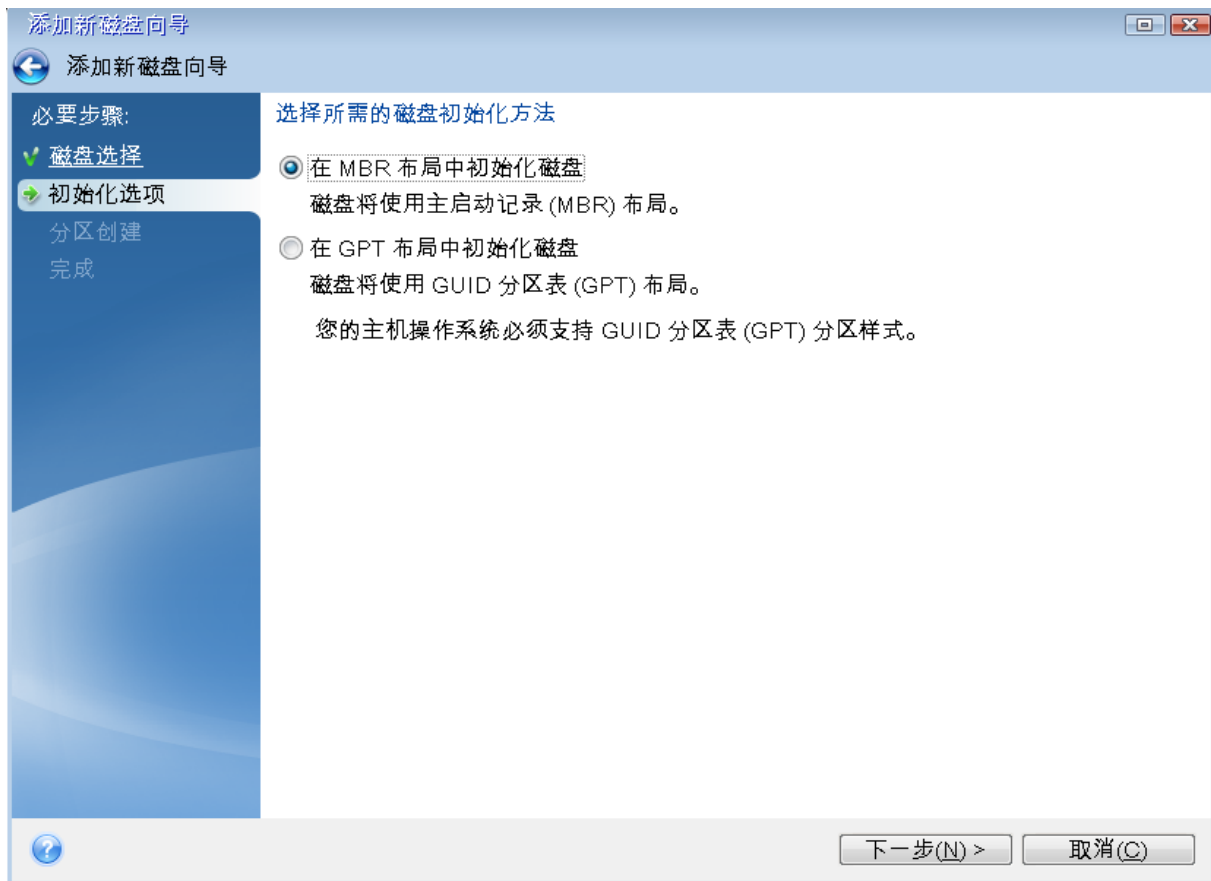
注意

若新磁盘上已有任何分区，Acronis Cyber Protect Home Office 会提醒您这些分区会被删除。



12.6.2 选择初始化方法

Acronis Cyber Protect Home Office 支持 MBR 和 GPT 分区。GUID 分区表 (GPT) 是一种优于旧 MBR 分区方法的新硬盘分区方法。如果操作系统支持 GPT 磁盘, 则可选择要初始化的新磁盘作为 GPT 磁盘。



- 若要添加 GPT 磁盘, 请单击在 **GPT 布局中初始化磁盘**。
- 若要添加 MBR 磁盘, 请单击在 **MBR 布局中初始化磁盘**。

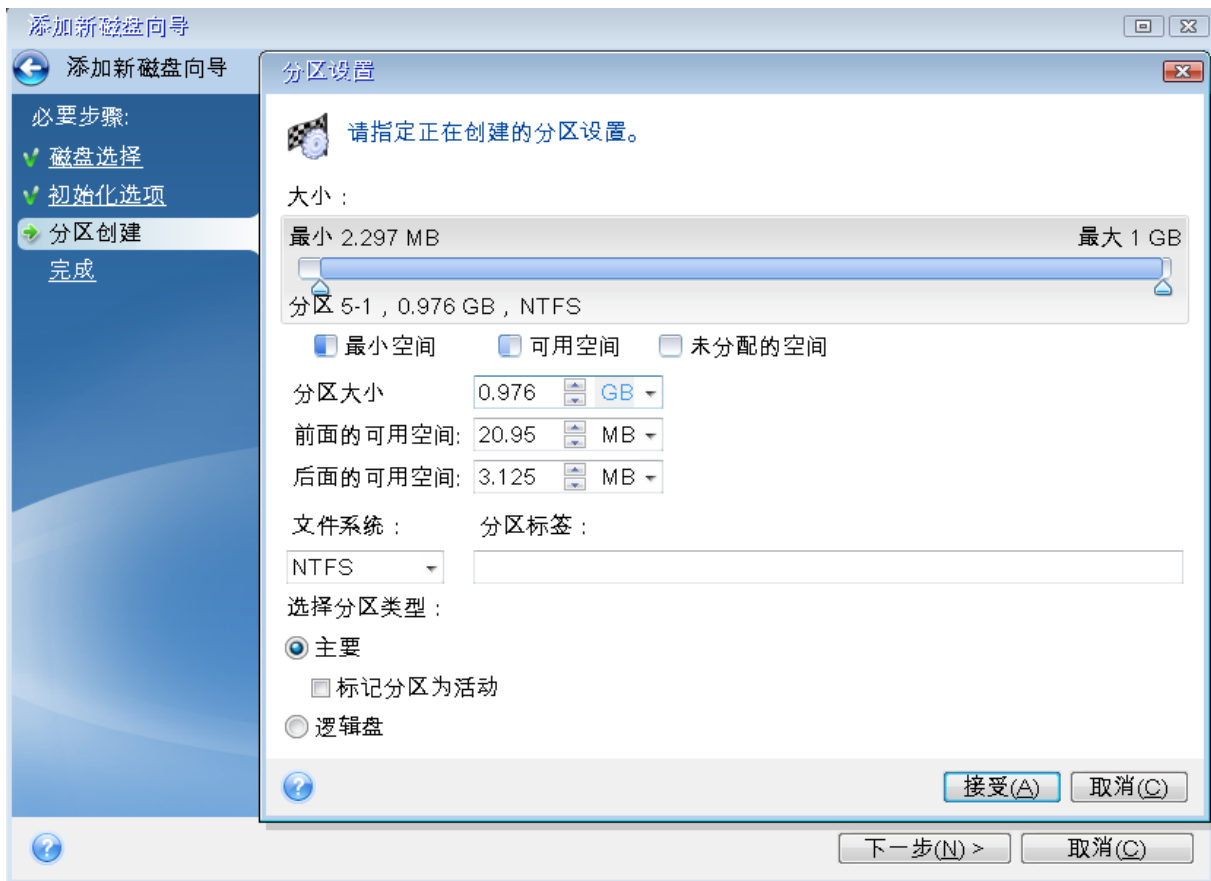
选择所需的初始化方法后, 单击**下一步**。

12.6.3 创建新分区

若要使用硬盘上的空间, 首先应对硬盘进行分区。分区是将硬盘空间划分成多个逻辑区域(称为分区)的过程。各逻辑分区可作为带有指定驱动器代号、自身文件系统等属性的独立磁盘使用。

创建新分区

1. 在向导的**分区创建**步骤中, 选择未分配的空间, 然后单击**创建新分区**。
2. 为正在创建的分​​区指定以下设置:
 - 大小及位置
 - 文件系统
 - 分区类型(仅适用于 MBR 磁盘)
 - 分区代号与标签有关详细信息, 请参阅[分区设置](#)。
3. 单击**接受**。



分区设置

大小

若要重新调整分区大小, 请执行以下任一操作:

- 指向分区边框。当光标变成双箭头时, 拖动光标来扩大或缩小分区大小。
- 在分区大小字段中输入所需的分区大小。

若要调整分区位置, 请执行以下任一操作:

- 将相应分区拖动到新位置。
- 在调整前的可用空间或调整后的可用空间字段中输入所需的大小。

注意

在您创建分区时, 程序可能会为满足系统需求在创建分区前保留一些未分配空间。

文件系统

您可保留分区不格式化, 也可在以下文件系统类型中选择:

- **NTFS** 是 Windows NT、Windows 2000、Windows XP 及更高版本操作系统的原生文件系统。如果您使用的是上述操作系统, 请选择该文件系统类型。请注意, Windows 95/98/Me 和 DOS 无法访问 NTFS 分区。

- **FAT 32** 是 FAT 文件系统改进后的 32 位版本, 支持容量高达 2 TB。
- **FAT 16** 是 DOS 的原生文件系统。大部分操作系统均可识别。但是, 若磁盘驱动器容量大于 4 GB, 则无法在 FAT16 中进行格式化。
- **Ext2** 是 Linux 的原生文件系统。其速度足够快, 但不属于日志文件系统。
- **Ext3** - 在 Red hat Linux 7.2 版本中正式引入, Ext3 是 Linux 的日志文件系统。它与 Linux Ext2 前后兼容。它在 32 位和 64 位体系结构中有多个日志模式, 而且具备广泛的跨平台兼容性。
- **Ext4** 为新的 Linux 文件系统, 与 ext3 相比有改进。它可以完全向后兼容 ext2 和 ext3, 而 ext3 只能部分向前兼容 ext4。
- **ReiserFS** 是 Linux 的一种日志文件系统。一般来说, 它比 Ext2 更可靠更快捷。请选择此类型作为 Linux 的数据分区。
- **Linux Swap** 是 Linux 的一种交换分区。若要通过 Linux 来添加更多交换空间, 请选择此类型。

分区代号

选择为分区指定的代号。若选择**自动**, 程序会按字母排列顺序分配第一个未使用的驱动器代号。

分区标签

分区标签是指为分区指定的名称, 方便您识别分区。例如, 装有操作系统的分区可称为“系统”、数据分区可称为“数据”等等。分区标签为可选属性。

分区类型(这些设置仅适用于 MBR 磁盘)

您可将新分区定义为主分区或逻辑分区。

- **主分区** - 若计划通过此分区启动, 请选择此参数。否则, 最好创建一个新分区作为逻辑驱动器。每个驱动器只能创建四个主分区, 或三个主分区和一个扩展分区。

注意

若您拥有几个主分区, 则同一时间只能有一个分区是活动分区, 其他主分区都将被隐藏, 操作系统无法“看到”。

- **标记为活动分区** - 若打算在此分区安装操作系统, 请勾选此复选框。
- **逻辑** - 若不打算通过该分区安装和启动操作系统, 请选择此参数。逻辑驱动器是经过分区并被分配为独立单元的物理磁盘驱动器的一部分, 但作为独立的驱动器运行。

12.7 安全与隐私权工具

12.7.1 Acronis DriveCleanser

Acronis DriveCleanser 允许您永久销毁所选硬盘和分区上的所有数据。在这一销毁过程中, 您可以使用某种预设算法, 也可以创建自己的算法。有关详细信息, 请参阅[算法选择](#)。

为何需要？

在废弃旧磁盘之前对其进行格式化时，信息没有被永久销毁且仍可被恢复。这是您的个人信息最终会落入他人之手的一种途径。要防止这一点，我们建议您在以下情况下使用 Acronis DriveCleanser：

- 使用新硬盘驱动器替换旧硬盘驱动器且打算不再使用旧硬盘驱动器。
- 将您的旧硬盘驱动器送给您的亲友。
- 将您的旧硬盘驱动器出售。

如何使用 Acronis DriveCleanser

永久销毁磁盘上的数据



1. 单击**开始**按钮 —> **Acronis**(产品文件夹) —> **Acronis DriveCleanser**。
Acronis DriveCleanser 向导将会打开。
2. 在**来源选择**步骤上，选择要抹除的硬盘和分区。有关详细信息，请参阅[来源选择](#)。
3. 在**算法选择**步骤上，选择您想用于销毁数据的算法。有关详细信息，请参阅[算法选择](#)。
4. [可选步骤] 您可以创建自己的算法。有关详细信息，请参阅[创建自定义算法](#)。
5. [可选步骤] 在**抹除后操作**步骤中，选择数据销毁之后要对分区和磁盘执行的操作。有关详细信息，请参阅[抹除后的操作](#)。
6. 在**完成**步骤中，确保配置设置正确。要开始此过程，请勾选**永久擦除所选分区**复选框，然后单击**继续**。

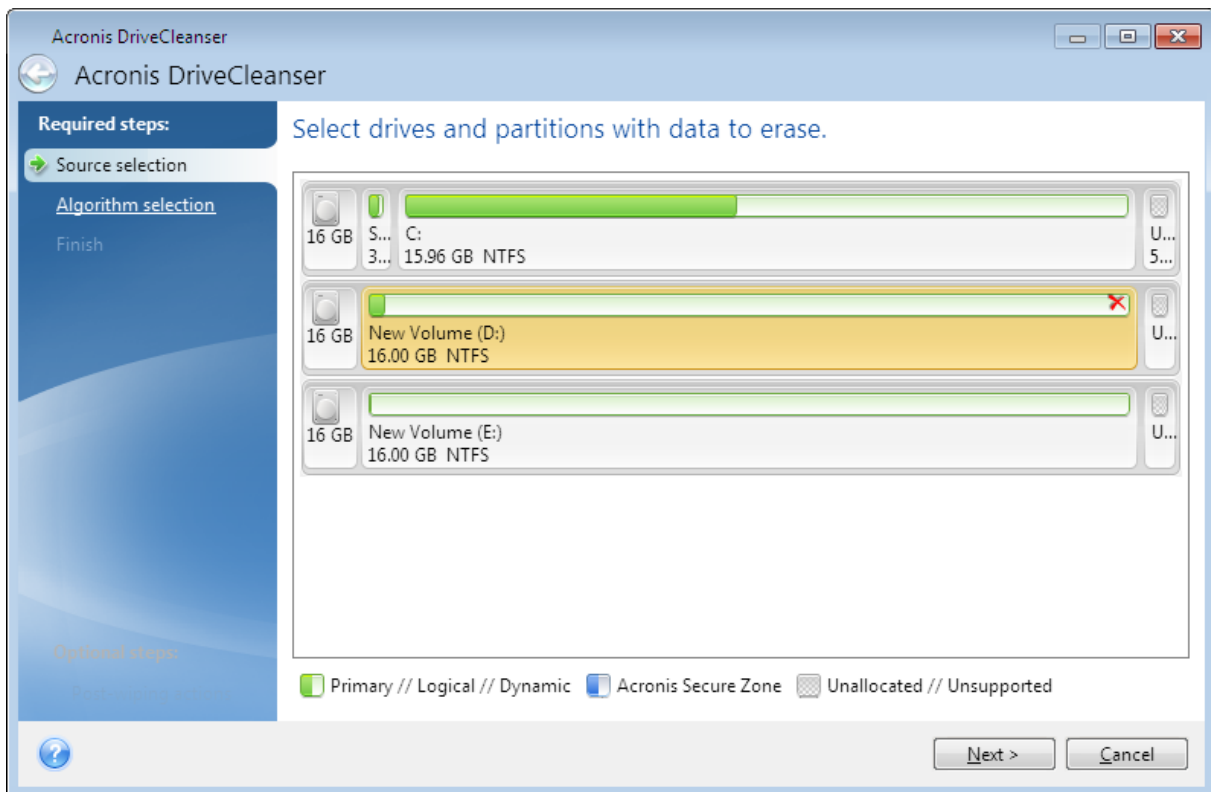
警告！

请注意，根据所选分区的总大小和所选的数据销毁算法，数据销毁可能需要几个小时。

来源选择

在**来源选择**步骤中，选择要销毁数据的分区和磁盘：

- 要选择分区，请单击相应的矩形。红色标记 () 表明该分区已选中。
- 要选择整个硬盘，请单击硬盘图标 ()。



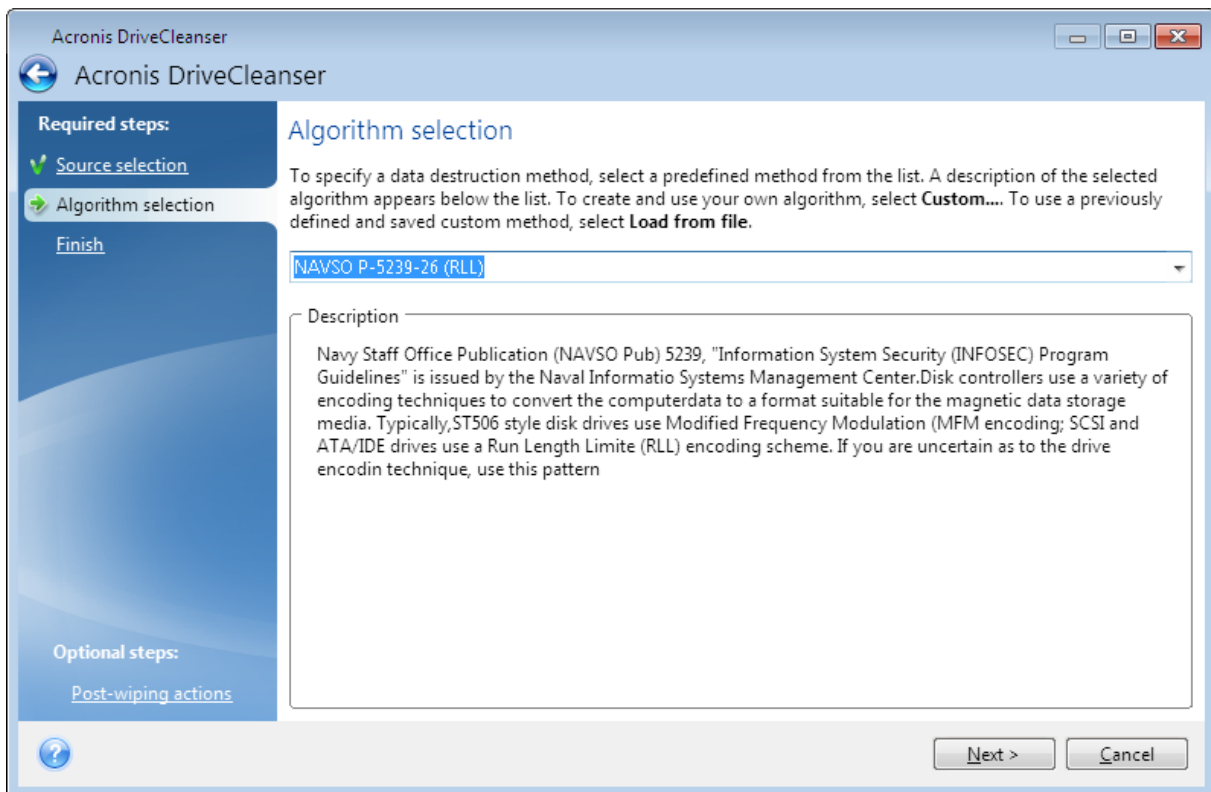
注意

Acronis DriveCleanser 无法擦除动态磁盘和 GPT 磁盘上的分区，所以这些磁盘将不会显示。

算法选择

在**算法选择**步骤中，执行以下任一操作：

- 要使用某种预设算法，请选择所需的算法。有关详细信息，请参阅[硬盘抹除方式](#)。
- [仅针对高级用户] 要创建自定义算法，请选择**自定义**。然后，在**算法定义**步骤中继续创建算法。之后，您将能够将创建的算法保存到以 *.alg 为扩展名的文件中。
- 要使用以前保存的自定义算法，请选择**从文件加载**，并选择包含您的算法的文件。



创建自定义算法

算法定义

算法定义步骤会向您显示未来算法的模板。

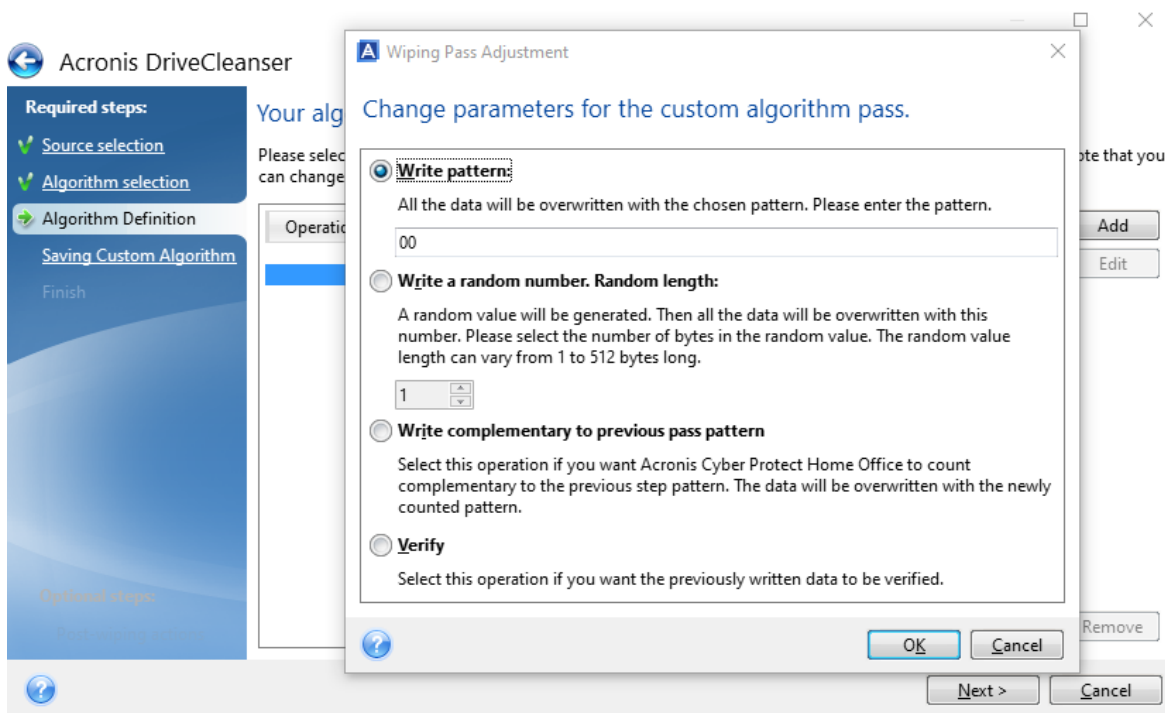
表格具有以下图例：

- 第一栏包含操作的类型(将符号写入磁盘;验证写入的内容)。
- 第二栏包含要写入磁盘的数据的模式。

每一行均定义一种将在一次传递中执行的操作。要创建算法, 请向表格中添加您认为安全的数据销毁所需要的行数。

添加新写入

1. 单击**添加**。打开“**抹除次数调整**”窗口。



2. 选择一个选项：

- **写入模式**

输入十六进制值，例如，以下类型的值：0x00、0xAA 或 0xCD 等等。这些值的长度为 1 字节，但是它们最长可达 512 字节。除这些值之外，您可输入任何长度的随机十六进制值(最大 512 字节)。

注意

若二进制值用 10001010 (0x8A) 顺序表示，则互补二进制值将会用 01110101 (0x75) 序列表示。

- **写入随机数字**

以字节为单位指定随机数字的长度。

- **根据上次写入模式写入互补值**

Acronis Cyber Protect Home Office 会为上次写入期间写入磁盘的值添加一个互补值。

- **验证**

Acronis Cyber Protect Home Office 会验证上次写入期间写入磁盘的值。

3. 单击**确定**。

编辑现有写入

1. 选择相应的行，然后单击**编辑**。

打开“**抹除次数调整**”窗口。

注意

当您选择多行时，新的设置将会被应用到所有选定的写入值。

2. 更改设置，然后单击**确定**。

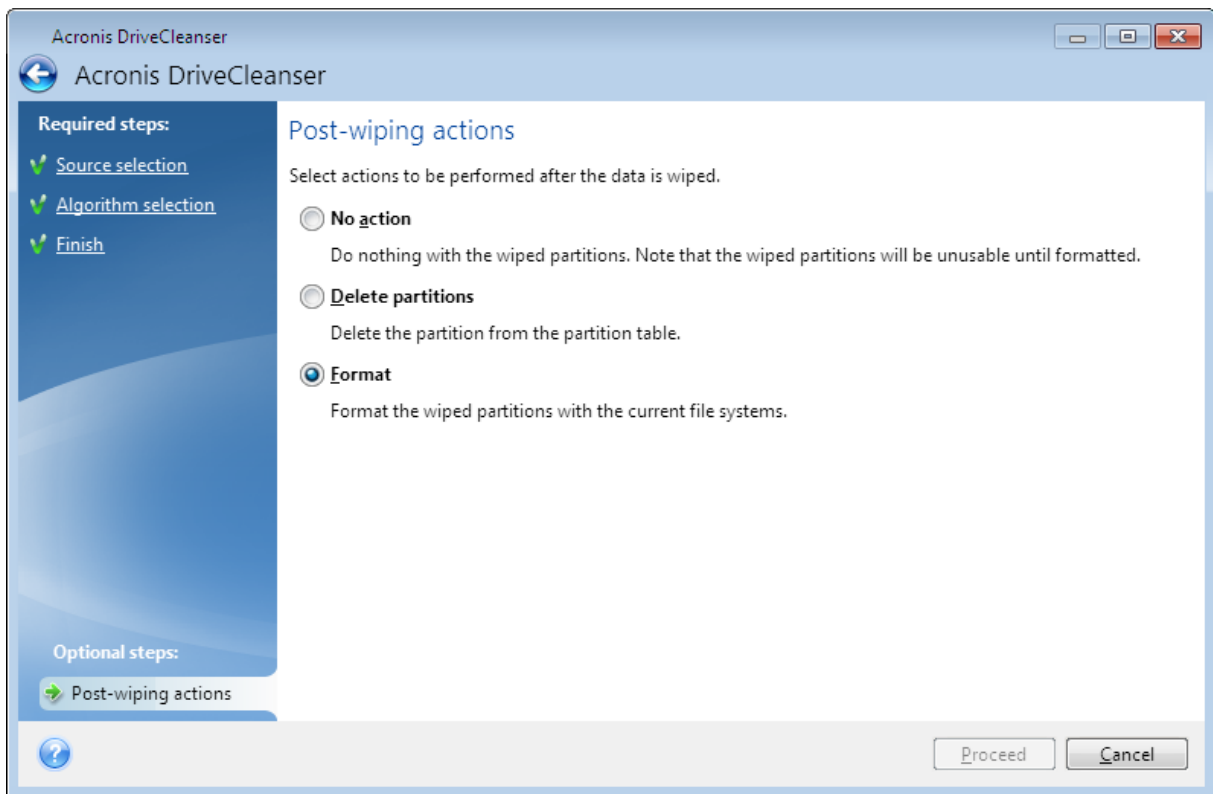
将算法保存到文件

1. 在**保存自定义算法**步骤中，选择**保存到文件**，然后单击**下一步**。
2. 在打开的窗口中，指定文件名和位置，然后单击**确定**。

抹除后的操作

在“抹除后操作”窗口上，您可选择要在选定分区上执行的数据销毁操作。Acronis DriveCleanser 提供三种选项：

- **无操作** - 仅用以下选定的算法销毁数据
- **删除分区** - 销毁数据并删除分区
- **格式化** - 销毁数据并格式化分区(默认)。



12.7.2 系统清理

系统清理向导可让您安全删除计算机操作的所有痕迹，包括用户名、密码和其他个人信息。

它可以进行以下操作：

- 安全销毁 **Windows 回收站** 中的数据。
- 从适当的 Windows 文件夹内删除 **临时文件**。
- 清理 **硬盘可用空间** 内先前存储信息的所有痕迹。
- 删除在本地局域网中连接的磁盘和计算机上 **文件和计算机搜索** 的痕迹。
- 清理 **最近使用的文档** 列表。
- 清理 **Windows 运行** 列表。
- 清理 **打开/保存的文件** 历史记录。
- 使用 **网络凭据** 清理用户有连接的网上邻居列单。
- 清理 **Windows 预取目录**，Windows 将您已执行以及最近运行程序的相关信息保存在此目录中。

注意

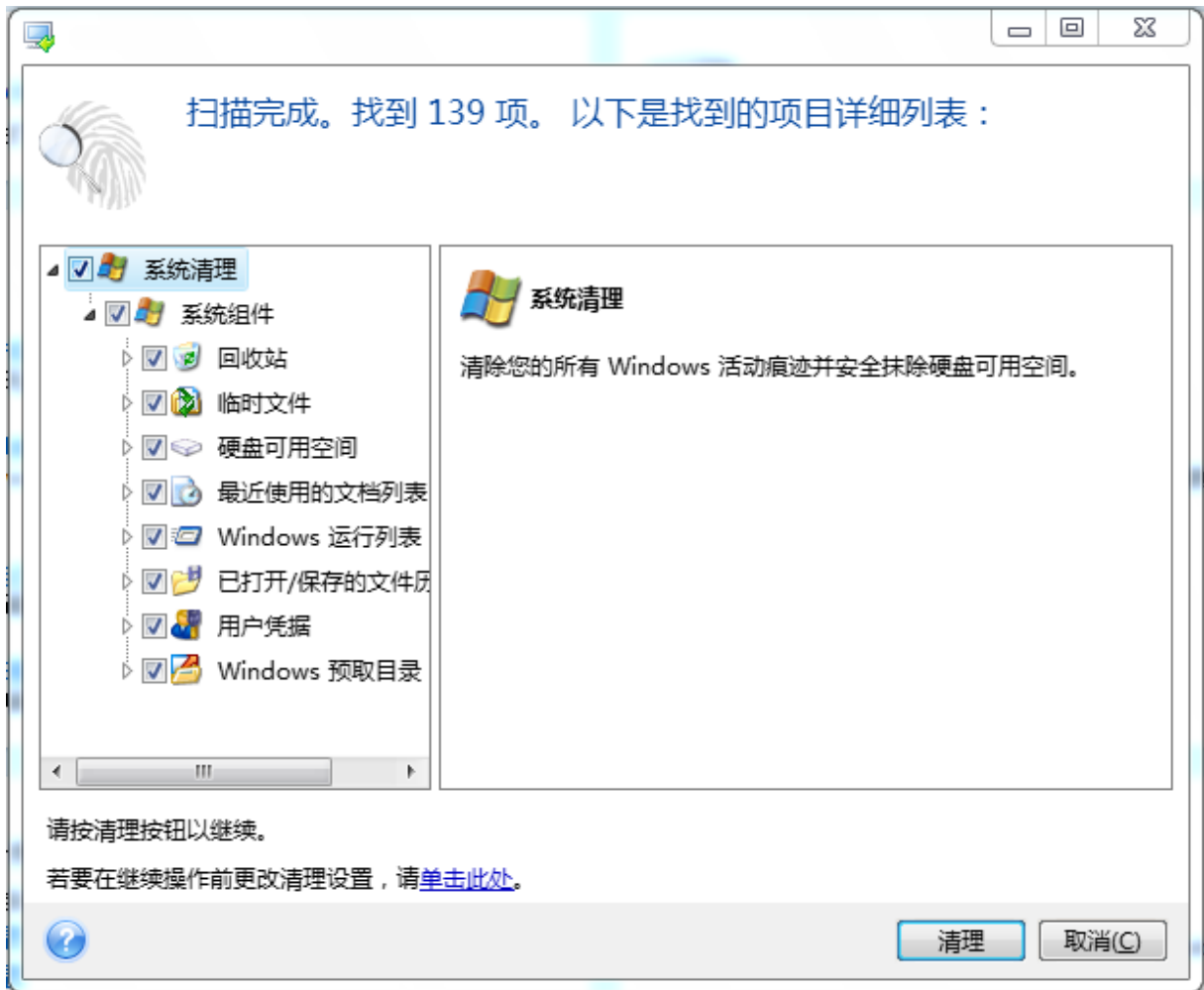
Windows 7 及更高版本的操作系统不会存储有关文件和计算机搜索的信息。此外，已打开/保存文件的相关信息会以不同方式被存储在注册表中，因此向导会以不同的方式显示这些信息。

注意

请注意，Windows 会保留密码直至会话终止，因此只有在注销或重启计算机以终止当前的 Windows 会话后，系统才会清除网络用户凭据列表。

要启动系统清理向导，请依次单击 **开始** 按钮 —> **Acronis**(产品文件夹) —> **系统清理**。

启动向导后，系统将搜索 Windows 存储的所有用户操作痕迹。搜索完成后，其结果会显示在向导窗口的上方。



您可查看搜索结果并手动选择想要删除的项目。

单击[单击此处](#)超链接文本以更改清理设置，然后继续。

单击**清理**以便开始删除已找到的项目。

清理设置

在清理设置窗口中，您可以更改每个系统组件的清理设置。其中部分设置适用于所有组件。

要更改组件的清理设置

- 请展开树形图中的**系统组件**项并选择要更改的组件清理设置。您可以通过清理向导启用或禁用组件扫描。如需进行此操作，请勾选或取消勾选**启用**复选框。
如有需要，您还可扩大组件，自定义所需的数据销毁方法和要清理的文件，清理您曾用来查找本地网络内计算机的注册表搜索字符串等。如需进行此操作，请单击组件旁的三角，并从列表中选择选项进行设置。
- 设置所需组件的属性后单击**确定**保存设置。这些设置会成为您下次可启动清理向导时的默认设置。

若先前已更改清理设置，可随时单击**还原默认设置**按钮返回至程序默认设置。

系统组件：

- 回收站
- 临时文件
- 硬盘可用空间
- 查找计算机列表
- 查找文件列表
- 最近使用的文档列表
- Windows 运行列表
- 打开/保存的文件历史记录
- 用户凭据
- Windows 预取目录

清理选项默认值

通过单击[数据销毁方法](#)选项页面上的[单击更改此设置...](#)链接,可以访问默认清理选项。

更改默认清理选项

1. 在树形图上选择要更改的组件清理设置。
2. 在更改选项后,单击**确定**保存设置。

若先前已更改清理设置,可随时单击**还原默认设置**按钮返回至程序默认设置。

一般

默认情况下,每次清理结束(**显示概要**复选框已勾选)后,即会显示概要对话框。若不显示概要对话框,请取消复选框。

清理选项

系统清理采用多项最流行的数据销毁方法。在此,您可以选择默认为所有其他组件使用的常见数据销毁方法。

数据销毁方法在本指南的[硬盘抹除方式](#)中作了详细介绍。

指定清理选项

可自定义以下清理选项:

- 数据销毁方法
- 默认选项
- 文件
- 驱动器可用空间
- 计算机
- 命令
- 网上邻居过滤器

数据销毁方法

系统清理采用多项最流行的数据销毁方法。您需要在这里选择希望使用的数据销毁方法。

- **使用常用方法** - 若将此参数处于选定状态, 程序便会使用默认方法(初始设置为“快速销毁”方法)。

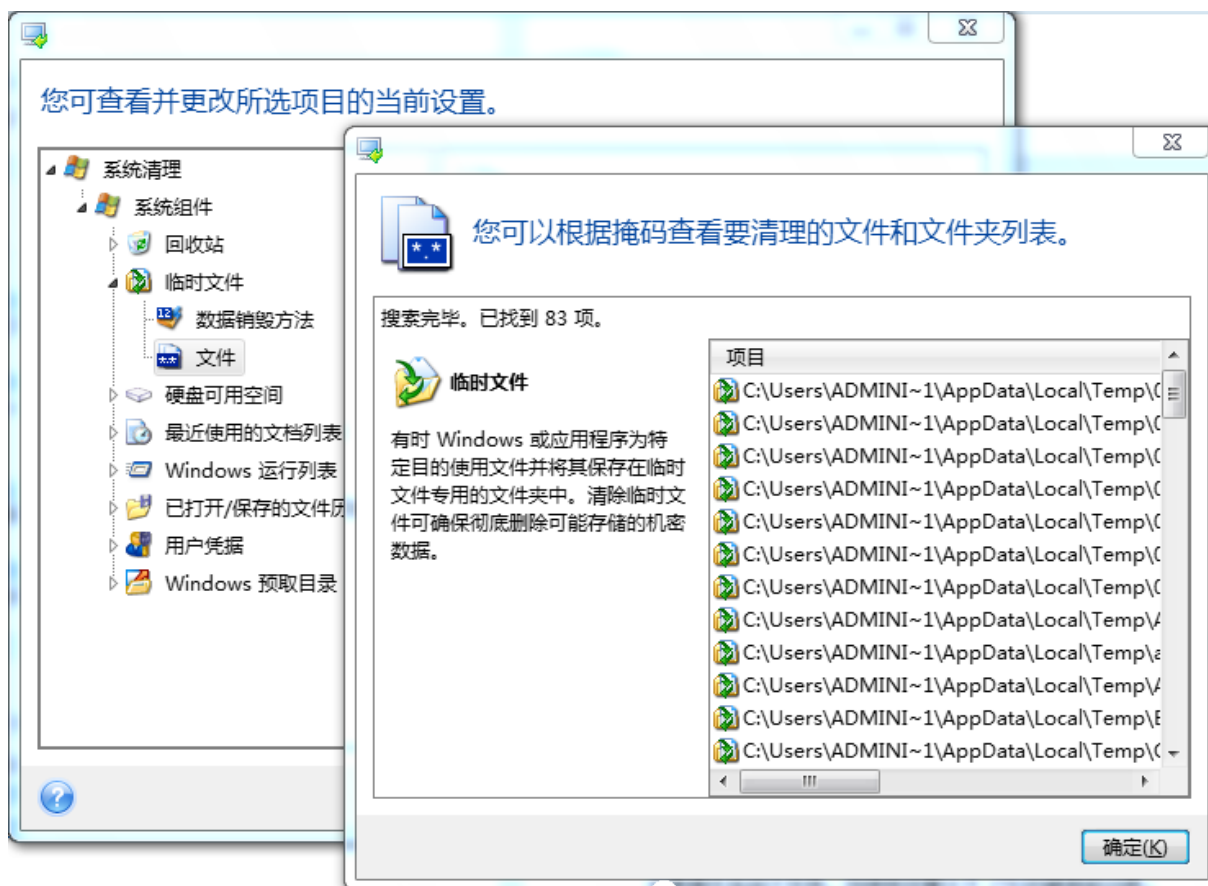
若需要将另一种销毁方法设置为默认方法, 请单击相应的链接。

- **使用为此组件自定义的方法** - 选择此参数, 可让您从下拉列表中选择其中一种预设的数据销毁方法。

数据销毁方法在本指南的[硬盘抹除方式](#)中作了详细介绍。

文件

“文件”设置可定义使用系统清理向导清理的文件名, 并可与搜索字符串一起使用。



在 Windows 操作系统下, 搜索字符串可代表完整或部分文件名。搜索字符串可包含任何字母数字符号, 包括逗号和 Windows 通配符, 并可有类似于以下的值:

- *.* - 清理具有任何文件名和扩展名的所有文件。
- *.doc - 清理含指定扩展名的所有文件 - 此处指 Microsoft 文档文件。
- read*.* - 清理扩展名和文件名中以“read”开头的文件。

- read?.* - 清理任何扩展名和文件名以“read”开头、名称由五个字母组成且第五个字母随机的所有文件。

例如, 上一个搜索字符串将移除 read1.txt 和 ready.doc 文件, 但文件名更长的 readiness.txt 文件将被保留(扩展名除外)

您可输入多个不同的搜索字符串, 并以分号隔开, 例如:

.bak;.tmp;*.~~~ (搜索字符串之间无空格)

将清理文件名与至少其中一项搜索字符串相符合的所有文件。

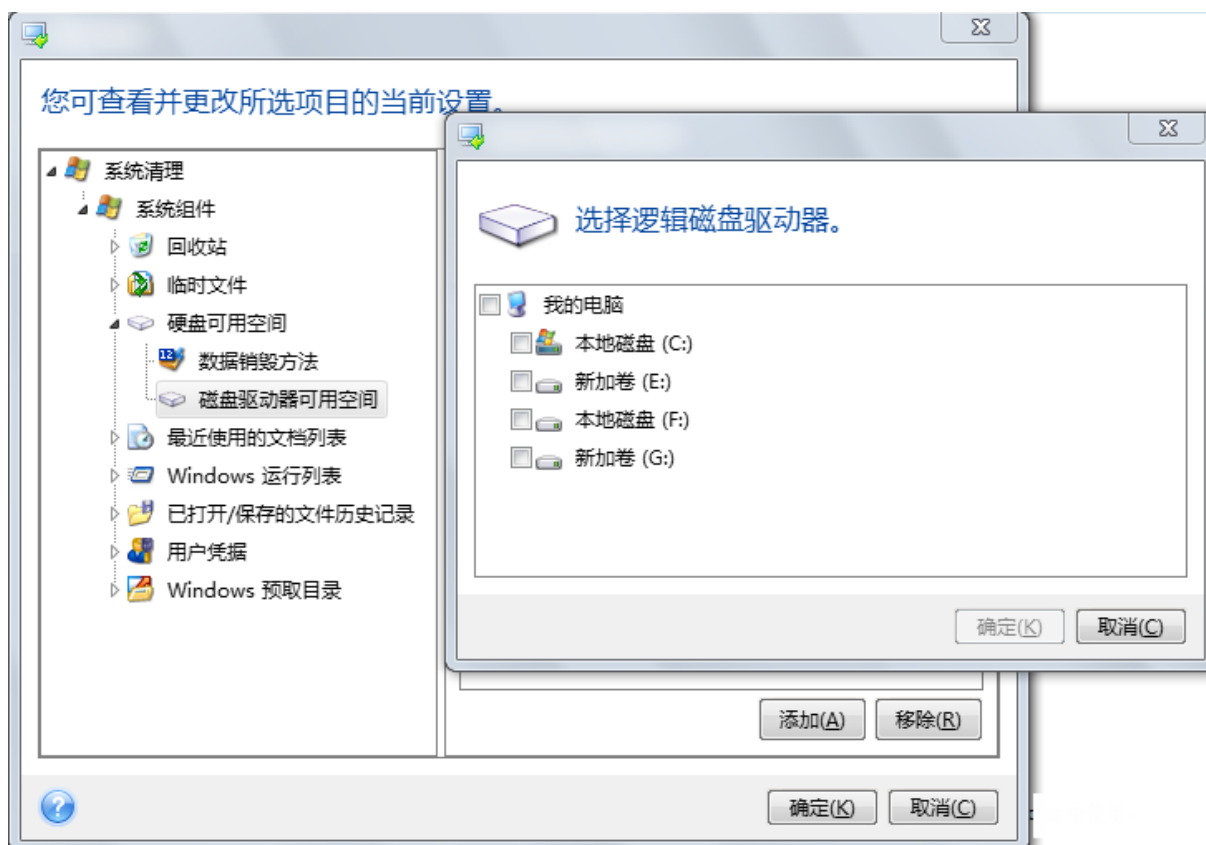
输入“文件”设置值后, 即可浏览与搜索字符串相符的文件。要进行此操作, 请单击**显示文件**。您将看到一个窗口, 其中显示所找到文件的名称。这些文件将被清理。

驱动器可用空间

您可在手动指定要清理可用空间的物理和/或逻辑驱动器。默认情况下, 系统清理将清理所有可用驱动器上的可用空间。

若要更改此参数设置, 可使用**移除**按钮从列表中将无需清理可用空间的驱动器删除。

若要将这些驱动器重新添加至列表, 请使用**添加**按钮。



计算机

可使用**计算机**设置清理您在本地网查找计算机时用过的注册表搜索字符串。这些字符串将保留网络中您感兴趣信息的有关情况。这些项目也应被删除以维护机密性。

计算机设置与**文件**设置相似。它是可包含任意数量完整或部分计算机名称(以分号隔开)的字符串。根据 Windows 规则,计算机搜索字符串须与**计算机**设置值相比后才能删除。

若仅需删除所有本地网计算机搜索字符串(适用于大部分情形),可使用此设置的默认值。要还原默认设置:

- 请选择**查找计算机列表**组件
- 请确保已勾选了**启用**复选框。
- 请选择**计算机**设置,确保未勾选其文本框。

如此,所有计算机搜索字符串将从注册表中删除。

输入**计算机**设置值后,您可浏览系统清理向导在注册表中找到的搜索字符串。若要进行此操作,请单击**显示计算机**。您会看到一个窗口,其中显示网络中搜索的完整和部分的计算机名称。这些项目将被删除。

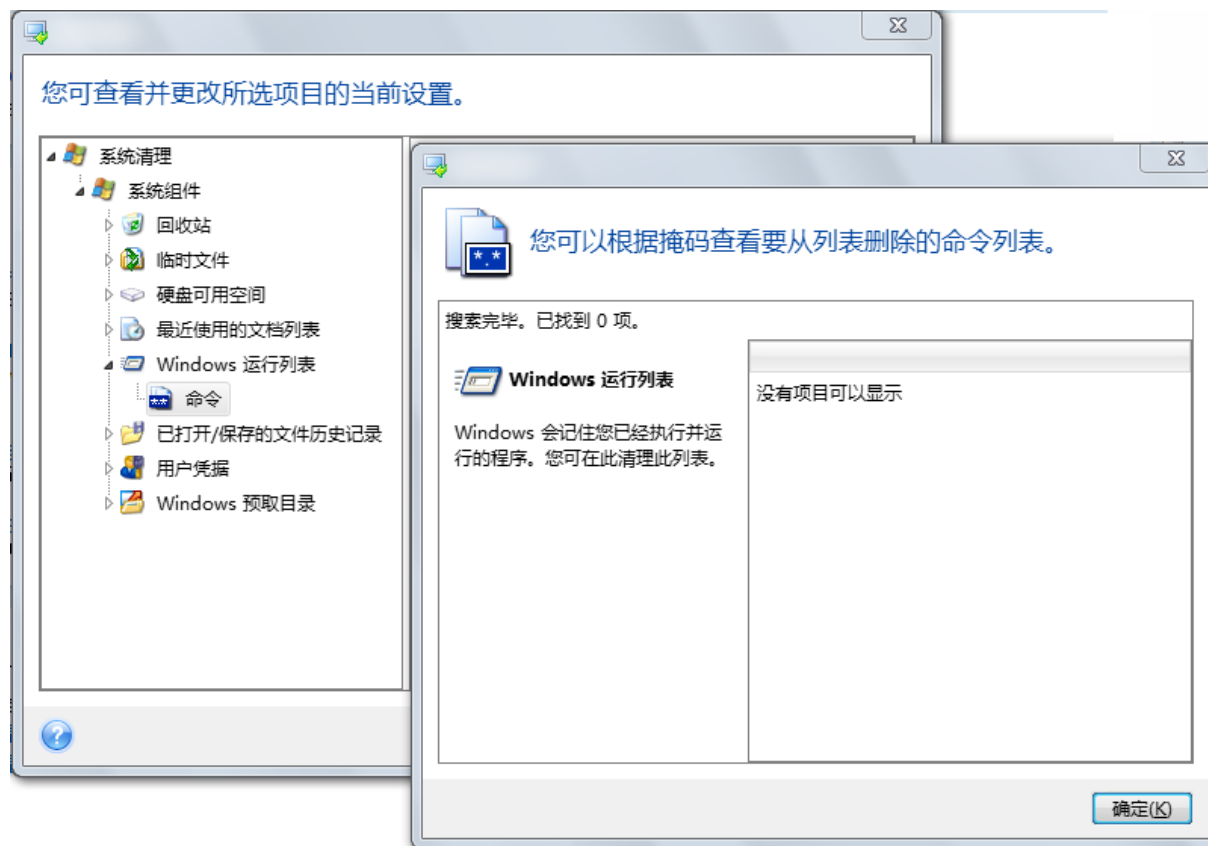
“命令”设置

在此,您可在 **Windows 运行列表**清理过程中选择要移除的命令。

此模板可能包含任何以分号隔开的命令名称或部分命令名称,如:

help; cmd; reg

这样将移除所有名称符合或包含您输入的任何名称或名称部分的命令。



网上邻居过滤器

您可在输入任何使用网络凭据(用户名和密码)连接的网上邻居、服务器、FTP 服务器、网络共享等的主机名或 IP 地址(以分号隔开)。输入主机名和 IP 地址时可使用 * 和 ? 等通配符。

单击**显示网上邻居**查看您用要删除的凭据访问过的网上邻居列表。

预览

扫描完成后,扫描的结果会显示在向导窗口的上部分供使用。默认情况下,清理时会扫描所有系统组件。若要自定义需要和不需要扫描的系统组件,请更改默认清理设置。

您可查看搜索结果并手动选择/取消选择要清理/保留的项目。为帮助您作出正确选择,所有组件均附有简要说明。只需单击组件的名称窗口的左侧就会显示其相关说明。

若需选择/取消选择组件

- 展开系统清理树形图中的**系统组件**并确保勾选要清理的组件。若不想清理组件,只需取消勾选其复选框即可。
- 若需要,您可以扩大组件细化处理,选中/取消选中组件内容。

指定清理组件后,请单击**清理**按钮继续。

注意

Windows 7 及更高版本的操作系统不会存储有关文件和计算机搜索的信息。此外,已打开/已保存文件的信息会以不同方式存储在注册表中,因此向导程序会以不同的方式显示这些信息。

清理进度

操作状态窗口报告当前操作的状态。

进度条指示所选操作的完成进度。

有些情况下,可能需要很长时间才能完成操作。若出现这种情况,请勾选**完成后关闭计算机**复选框。这样,当操作完成后,Acronis Cyber Protect Home Office 将关闭计算机。

12.7.3 硬盘抹除方式

存在什么问题?

通过不安全的方法删除硬盘上的信息(例如,通过简单的 Windows 删除)后,信息很容易被恢复。使用专用设备甚至可以恢复被重复覆盖的信息。

泄露原理

数据是按二进制序列 1 和 0 存储在硬盘上的,由硬盘上各个不同的磁化部分表示。

一般而言, 写在硬盘上的 1 会被其控制器读作 1, 0 则会被读作 0。若使用 1 覆盖 0, 这一条件下的结果为 0.95, 反之亦然 - 若使用 1 覆盖 1, 则结果为 1.05。这些差异与控制器无关。但若使用专用设备, 很容易就可读出“潜伏”的 1 和 0 的顺序。

Acronis 使用的信息抹除方法

有关彻底信息抹除的详细原理, 请参阅 Peter Gutmann 的文章。请参阅 https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html 上的“安全删除磁存储器和固态存储器中的数据”。

序号	算法(写入方法)	次数	刻录
1.	美国国防部 5220.22-M	4	1(第 1 次) - 每个扇区内每个字节的随机选择符号; 2 - 第 1 次写入内容的补充; 3 - 随机符号再次出现; 4 - 写入验证。
2.	美国: NAVSO P-5239-26 (RLL)	4	1(第 1 次) - 所有扇区均为 0x01; 2 - 0x27FFFFFF; 3 - 随机符号序列; 4 - 验证。
3.	美国: NAVSO P-5239-26 (MFM)	4	1(第 1 次) - 所有扇区均为 0x01; 2 - 0x7FFFFFFF; 3 - 随机符号序列; 4 - 验证。
4.	德国: VSITR	7	1 第 1 次至第 6 次 - 备选顺序: 0x00 和 0xFF; 第 7 次 - 0xAA; 即 0x00、0xFF、0x00、0xFF、0x00、0xFF、0xAA。
5.	俄罗斯: GOST P50739-95	1	第 6 至第 4 安全级别系统的每个扇区内每个字节均归为逻辑零(数字 0x00)。 第 3 至第 1 安全级别系统的每个扇区内每个字节的随机选择符号(数字)。
6.	Peter Gutmann 法	35	Peter Gutmann 法非常精密。该方法建立在他的硬盘信息抹除理论上(请参阅磁存储器和固体存储器数据的安全销毁)。
7.	Bruce Schneier 法	7	Bruce Schneier 在其所著的《实用加密方法》一书内提出了 7 次覆盖方法。1 第 1 次 - 0xFF; 第 2 次 - 0x00; 然后以加密安全伪随机序列重复五次。
8.	快速	1	所有要抹除的扇区均归为逻辑零(数字 0x00)。

12.8 加载映像

将映像加载为虚拟驱动器, 即可像访问物理驱动器一样来访问映像。您可以加载包含分区或整个磁盘驱动器的本地备份, 然后选择要加载的分区。加载之后:

- 一个新磁盘将显示在每个已加载分区所在的系统中。
- 您可以在文件资源管理器和其他文件管理器中在只读模式下查看映像内容。

注意

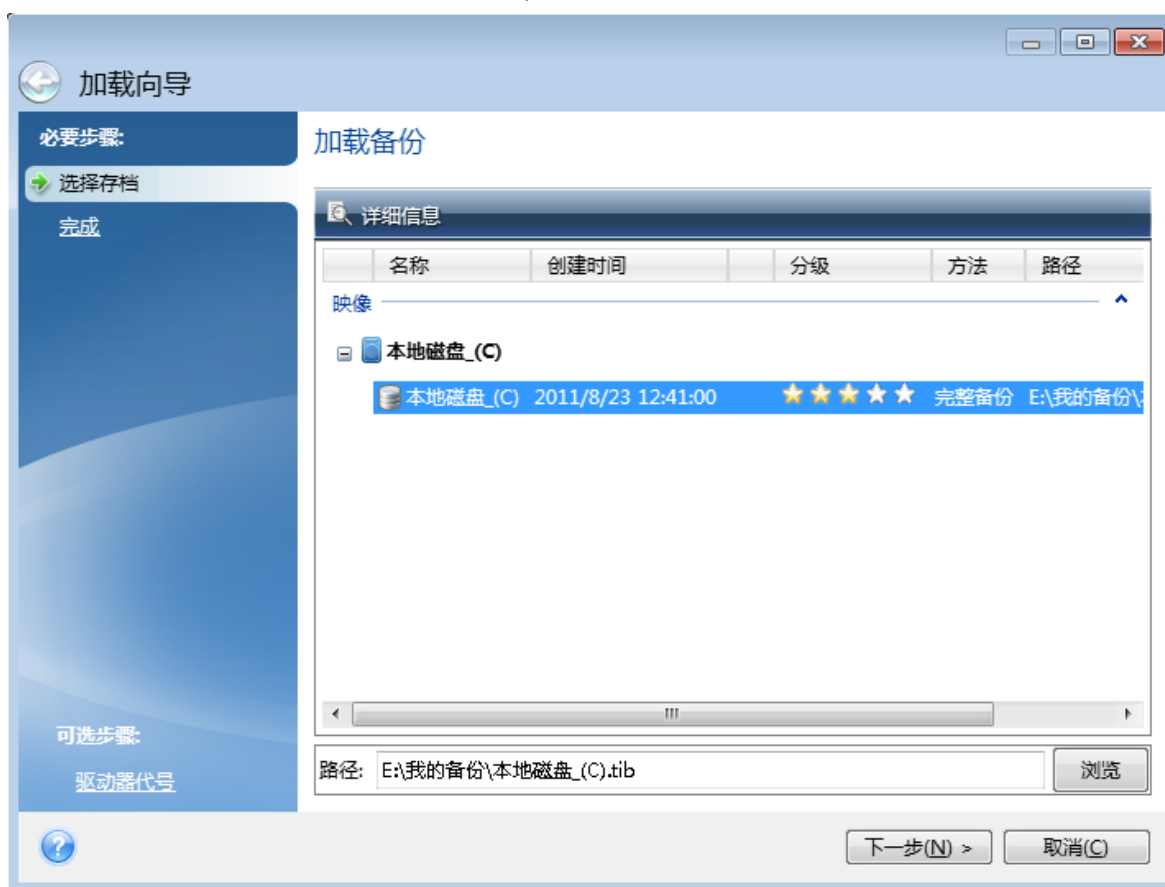
本节所述内容仅支持 FAT 和 NTFS 文件系统。

注意

如果磁盘备份存储在 FTP 服务器上, 则不能加载它。

12.8.1 如何加载映像

1. 在文件资源管理器中, 右键单击要加载的映像文件, 然后单击**加载映像**。
加载向导将打开。
2. 按创建日期/时间选择要加载的备份。这样, 您便可浏览某一时刻的数据状态。



3. [可选步骤] 在**驱动器代号**步骤上, 从**加载代号**下拉列表中选择要指定给虚拟磁盘的代号。如果不希望加载分区, 请从列单中选择**不加载**或清除该分区的复选框。
4. 单击**继续**。
5. 连接映像后, 程序会运行文件资源管理器, 并显示其内容。

12.9 卸载映像

建议您在所有必要操作完成后卸载虚拟磁盘, 因为保留虚拟磁盘会占用大量系统资源。

若要卸载映像, 请执行以下任一操作:

- 在文件资源管理器中，右键单击磁盘图标，然后单击**卸载**。
- 重启或关闭计算机。

12.10 使用 .vhd(x) 文件

可以将磁盘或分区的 Acronis 备份(.tib 文件)转换为虚拟硬盘(.vhd(x) 文件)。

12.10.1 .vhd(x) 文件的使用方法

- 您可以从已转换的 .vhd(x) 文件启动计算机，以测试备份是否有效以及是否可以恢复到可启动操作系统。
- 您可以保留已转换的 .vhd(x) 文件，以便在出现紧急情况时使用。例如，如果您的计算机无法启动，而您又需要立即运行它，则可以从 .vhd(x) 文件启动。
- 在 Windows 7 中，可以将 .vhd(x) 文件加载为额外的驱动器。.vhd(x) 文件可包含任何分区 - 系统或非系统。
- 您可以将已转换的 .vhd(x) 文件作为虚拟机运行。

12.10.2 限制和其他信息

- 不能将文件备份转换为 .vhd(x) 文件。
- 若要从已转换的 .vhd(x) 文件启动，它必须包含：
 - 相同计算机的系统分区。不能使用相同的 .vhd(x) 文件启动其他计算机。
 - Windows 7 或更高版本的操作系统。
- 对已启动或加载的 .vhd(x) 文件进行的任何更改都会保存到其中。如果您从 .vhd(x) 文件启动并对未备份的数据进行更改，这些更改将影响活动的系统。
- 单机版 Acronis Cyber Protect Home Office 在从可启动媒体启动时不支持转换操作。
- Acronis Cyber Protect Home Office 不能转换包含原来位于多个磁盘驱动器上的动态卷(例如跨区动态卷或带区动态卷)的 .tib 文件。

12.10.3 转换 Acronis 备份

Windows 7 及更高 Windows 版本的企业版和旗舰版用户若要使用已转换 .vhd(x) 文件启动操作系统，可以将系统分区的 .tib 格式映像转换为 .vhd(x) 格式。或者，他们可能希望能够加载映像且无需使用 Acronis Cyber Protect Home Office。

将 Acronis 磁盘映像(.tib 文件)转换为 Windows 备份(.vhd(x) 文件)

1. 启动 Acronis Cyber Protect Home Office。
2. 转至**备份**部分。
3. 在备份列表中，单击要转换的备份旁边的下箭头，然后单击**转换为 VHD**。
若备份受密码保护，则 Acronis Cyber Protect Home Office 会要求输入密码。请注意，生成的 .vhd(x) 文件将丢失密码保护。
4. 选择要转换的备份版本。

转换增量备份需要所有先前的增量备份以及初始完整备份。转换差异备份需要初始完整备份。转换结果始终为完整备份。

5. 为要创建的文件指定路径。

文件可保存至 Acronis Cyber Protect Home Office 支持的任何本地存储(Acronis Secure Zone 和 CD/DVD 除外)。此外, 还可将文件保存至 SMB 共享。

6. [可选步骤] 在转换备份时, 可以选中 **完成后启动虚拟机** 复选框。如果选中该复选框, Acronis Cyber Protect Home Office 将重新启动计算机, 并使用创建的 .vhd(x) 文件运行 Hyper-V 虚拟机。

例如, 若所选要转换的 .tib 映像包括两个不同物理硬盘中的分区, 则程序会为这两个物理硬盘分别创建一个 .vhd(x) 文件。

12.11 备份设置的导入及导出

Acronis Cyber Protect Home Office 可以让您导入及导出备份设置。如果您在新计算机上安装了 Acronis Cyber Protect Home Office 后需要将设置迁移到该计算机, 可能就会需要此功能。如果您将来打算升级到下一个 Acronis Cyber Protect Home Office 版本, 保存此设置也非常有用。

这种迁移可使您在新计算机上配置备份变得更加容易。您只需导出设置, 然后将其导入其它计算机。设置以脚本文件的形式导出。

设置的内容可能随备份类型的不同而不同。如为“传统的”磁盘和文件类型备份, 则设置包含以下项目:

- 备份项目列表
- 备份选项
- 备份位置
- 预定
- 备份方案
- 自动清理规则
- 备份版本命名规则

不间断备份的设置如下:

- 不间断保护项目列表
- 不间断备份数据的存储位置(如果存在多个位置, 则为位置列表)

注意

您不能将线上备份的设置从一台计算机导入到另一台计算机。

导出备份设置

1. 启动 Acronis Cyber Protect Home Office。
2. 在侧边栏上, 单击 **设置 > 备份设置传输**, 再单击 **将设置保存至文件**, 然后浏览到目标位置以保存包含这些设置的脚本文件。

导入备份设置

1. 在另一台计算机上启动 Acronis Cyber Protect Home Office。
2. 在侧边栏上, 单击 **设置 > 备份设置传输**, 再单击 **从文件导入设置**, 然后显示包含这些设置的脚本文件的路径。

导入设置后, 您可能需要对其进行一些更改以适应新环境。例如, 可能需要改变备份项目列表、备份目标位置等。

如要将某些备份复制到另一台计算机上, 建议将这些备份的设置一并导出。这样您就不会丢失所复制备份的某些功能。

12.12 Acronis 异机还原

Acronis 异机还原可让您在不同硬件上创建可启动系统克隆。当要将系统磁盘恢复到一台计算机, 但其配备的处理器、主板或大容量存储设备不同于初始备份的系统时, 请使用该实用工具。这可能会很有用, 例如, 更换有故障的主板后或在决定要将系统从一台计算机迁移到另一台上时。

12.12.1 它可以解决什么问题?

可在创建系统磁盘映像的硬件或相同硬件上轻松还原该映像。但是, 如果您尝试在不同的硬件上还原, 则恢复的系统将无法启动。这是因为新硬件与映像中包含的关键驱动程序不兼容。该实用工具会查找并安装对于操作系统启动至关重要的设备(例如存储控制器、主板或芯片集)的驱动程序。

12.12.2 我如何使用?

在开始恢复到不同硬件之前, 请确保您具有:

- [系统磁盘备份](#) 或 [整个 PC 备份](#)
- [Acronis 可启动媒体](#)
- [Acronis 异机启动媒体](#)

注意

如果您在计算机上安装了 Acronis Cyber Protect Home Office 和 Acronis 异机启动媒体生成器, 则可以将 Acronis Cyber Protect Home Office 和 Acronis 异机启动放置在相同的媒体上。有关详细信息, 请参阅 [创建 Acronis 异机启动媒体](#)。

要将系统恢复到不同硬件, 请执行以下操作:

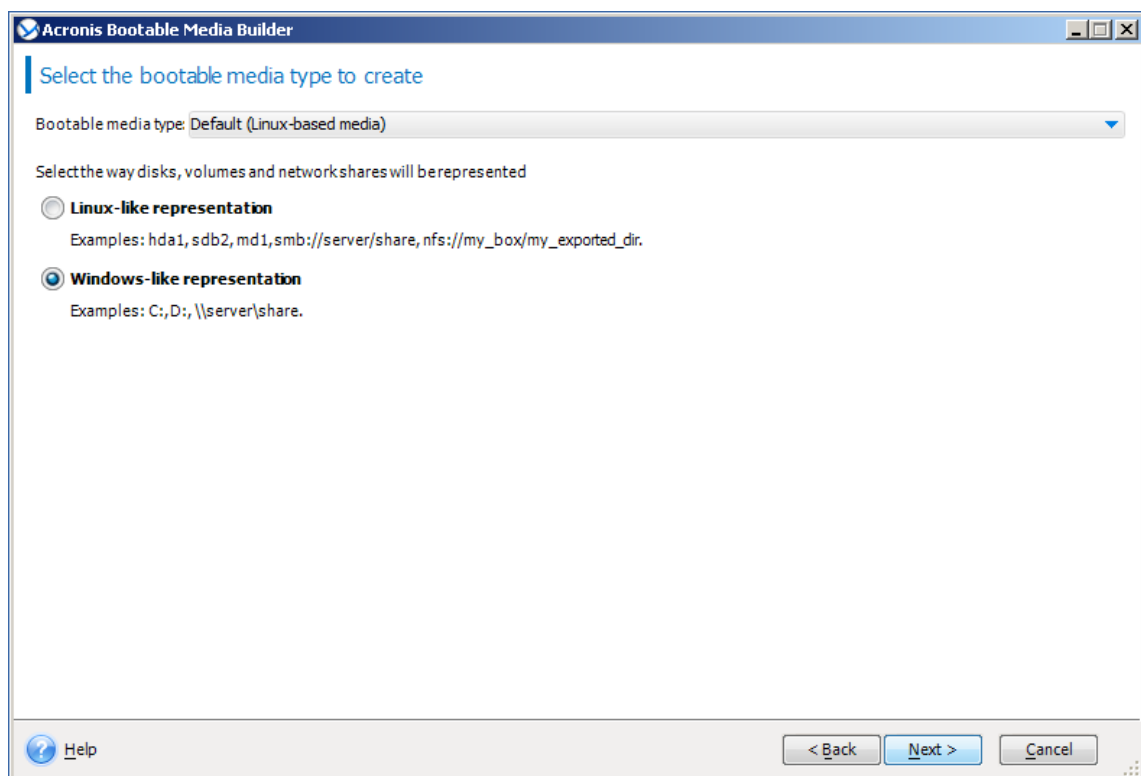
1. 使用 Acronis 可启动媒体启动目标计算机, 然后从系统备份或整个 PC 备份恢复系统。有关详细信息, 请参阅 [在可启动媒体下将系统恢复到新磁盘](#)。
2. 使用 Acronis 异机启动媒体启动目标计算机, 然后按照屏幕上的说明使系统可启动。有关详细信息, 请参阅 [使用 Acronis 异机还原](#)。

12.12.3 创建 Acronis 异机启动媒体

Acronis 异机启动媒体用于使您的计算机在恢复到不同硬件之后可启动。有关详细信息, 请参阅 [Acronis 异机还原](#)。

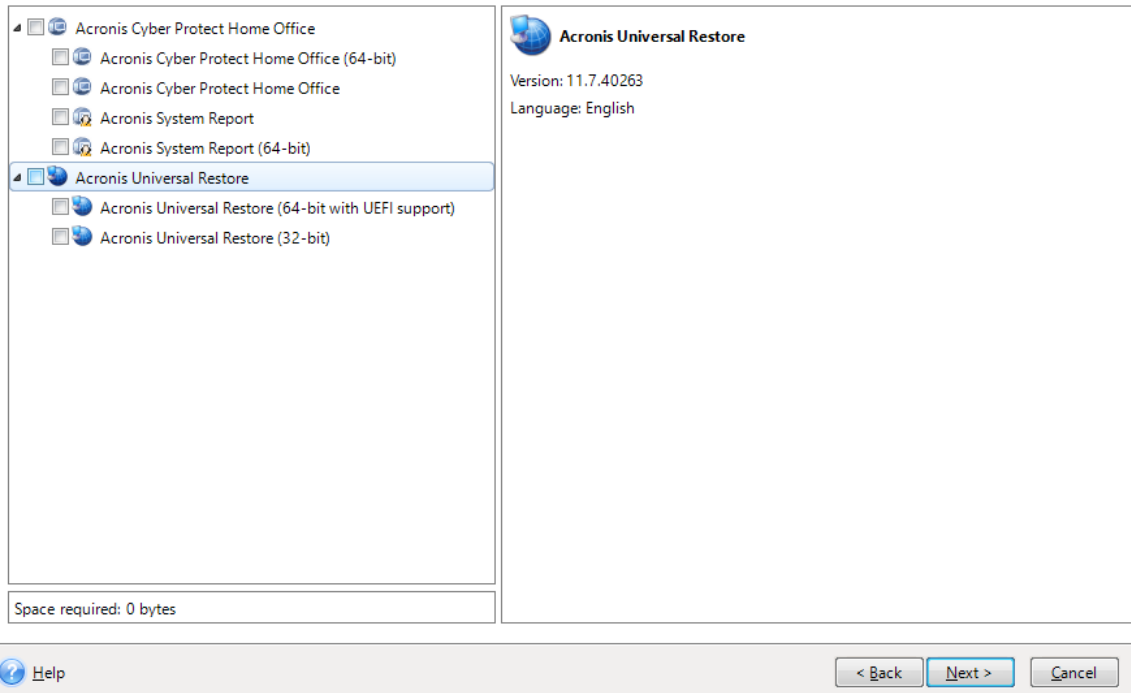
创建 Acronis 异机启动媒体

1. 启动 Acronis Cyber Protect Home Office。
2. 在工具部分中，单击 **Acronis 异机还原**。
3. 单击**下载**以获取 Acronis 异机启动媒体生成器。
4. 运行下载的文件并安装媒体生成器。
5. 插入要使其可启动的 USB 闪存驱动器或空白 DVD。
6. 要启动 Acronis 异机启动媒体生成器，请执行以下操作之一：
 - 在工具部分中，单击 **Acronis 异机还原**。
 - 单击**启动**按钮，打开已安装程序的列表，然后单击**运行异机启动媒体生成器**。
7. 请确保：
 - 基于 Linux 的媒体选作可启动媒体类型。
 - 类似 Windows 的表示形式选作磁盘和卷的表示方式。



8. [可选] 指定 Linux 内核参数。有关详细信息，请参阅[可启动媒体启动参数](#)。
9. 选择要放置在媒体上的 Acronis 组件。

Select the Acronis components to place on the bootable media



您可以选择 32 位和/或 64 位组件。32 位组件也可以在 64 位硬件上运行。但是，您需要通过 64 位组件来启动使用统一可扩展固件接口 (UEFI) 的 64 位计算机。

若要在不同类型的硬件上使用媒体，请选择两种相应类型的组件。在从生成的媒体启动计算机时，您将可以在启动菜单中选择 32 位或 64 位组件。

如果您的计算机上安装了 Acronis Cyber Protect Home Office，也可以将其放置在媒体上。在这种情况下，您将拥有一个同时包含恢复到不同硬件所需的两个组件的可启动媒体。

10. 为该媒体选择一个目标位置：

- **CD**
- **DVD**
- **USB 闪存驱动器**
- **ISO 映像文件**

您将需要指定 .iso 文件的文件名及目标文件夹。

.iso 文件创建完成后，您可以将其刻录至 CD 或 DVD。例如，在 Windows 7 及更高版本中，您可以使用内置刻录工具执行此操作。在文件资源管理器中，双击创建的 ISO 映像文件，然后单击**刻录**。

11. 指定要由 Acronis 异机启动使用的大容量存储驱动程序。

您不必立即添加这些驱动程序。您可以在稍后将 Acronis 异机启动应用于计算机时执行该操作。

12. 单击**继续**。

创建媒体后，将其从计算机上拔出。这就是您的 Acronis 异机启动媒体。

12.12.4 使用 Acronis 异机还原

准备

准备驱动程序

在将异机还原应用到 Windows 操作系统之前,请确保您具有新 HDD 控制器和芯片集的驱动程序。这些驱动程序对于启动操作系统非常重要。使用硬件供应商提供的 CD 或 DVD, 或者从供应商的网站下载驱动程序。驱动程序文件应具有 *.inf、*.sys 或 *.oem 扩展名。如果您下载的是 *.exe、*.cab 或 *.zip 格式的驱动程序,请使用第三方应用程序对其进行解压缩。

检查在可启动环境中对驱动程序的访问权限

确保在可启动媒体环境下工作时对具有驱动程序的设备具有访问权限。如果设备在 Windows 中可用,而基于 Linux 的媒体无法检测到它,请使用基于 WinPE 的媒体。

异机还原设置

自动驱动程序搜索

指定程序搜索硬件抽象层 (HAL)、HDD 控制器驱动程序和网络适配器驱动程序的位置:

- 如果驱动程序位于供应商的光盘或其他可移动媒体上,请打开**搜索可移动媒体**。
- 如果驱动程序位于网络文件夹或可启动媒体上,请通过单击**添加文件夹**指定文件夹的路径。

此外,异机还原还将搜索 Windows 默认驱动程序存储文件夹(通常是 WINDOWS/inf)。

无论如何也要安装的大容量存储驱动程序

如果存在以下情况,您需要该设置:

- 硬件具有特定的大容量存储控制器,如 RAID(特别是 NVIDIA RAID)或光纤通道适配器。
- 如果自动驱动程序搜索不能帮助启动系统,

请通过单击**添加驱动程序**指定适当的驱动程序。即使程序找到更适合的驱动程序,仍会安装在此处指定的驱动程序,但会发出相应的警告。

异机还原流程

在指定所需的设置后,单击**确定**。

该过程完成后,您将能够配置网络连接并为视频适配器、USB 和其他设备指定驱动程序。

13 疑难解答

13.1 解决最常见的问题

下面列出了用户在 Acronis Cyber Protect Home Office 中遇到的最常见问题。您可以在 [Acronis 知识库](#) 中查看对应的解决方案。

在程序启动时签名失败

错误消息“您已经超过了此许可号的最大激活数”

错误消息“该许可号已注册到另一帐户”

在 File Explorer 中浏览备份时，文件和文件夹未显示

错误消息“插入外部驱动器”

备份到 Acronis Cloud 失败，并显示错误消息“写入错误”或“写入文件时出错”或“FES 请求失败”

恢复到新硬件之后系统进入蓝屏死机 (BSOD) 状态，并且由于缺少驱动程序显示错误消息“Stop 0x0000007B”

请查看完整的常用解决方案列表，网址为：<https://kb.acronis.com/true-image-known-solutions>。

另请参阅有关恢复失败的故障排除信息，网址为：<https://kb.acronis.com/content/46340>。

13.2 Acronis 系统报告

当您联系 Acronis 支持团队时，他们通常需要相关的系统信息才能解决您的问题，有时获取此类信息并不便捷，可能会占用很长时间。

生成系统报告 工具可以创建包含所有必需技术信息的系统报告，并允许您将这些信息保存为文件。如有必要，您可以在问题说明中附加已创建的文件，并将它发送到支持团队。这会简化和加快对解决方案的搜索。

若要生成系统报告，请执行以下操作之一：

- 在侧边栏上，单击**帮助**，然后单击**生成系统报告**。
- 按 **CTRL+F7**。注意，即使 Acronis Cyber Protect Home Office 正在执行任何其他操作，您仍可以使用此组合键。
- 如果您使用的是 Windows 11，请单击**所有应用 > Acronis > Acronis 系统报告**。
- 如果您使用的是 Windows 10，请在**开始**菜单中，单击**Acronis > Acronis 系统报告**。
- 如果您使用的是 Windows 7 或 8，请单击**开始 > 所有程序 > Acronis > Acronis 系统报告**。

报告生成后

- 若要保存生成的系统报告，请单击**保存**，并在打开的窗口中为创建的文件指定位置。
- 若要不保存报告退出主程序窗口，请单击**取消**。

您可以将这一工具作为一个独立组成部分置于可启动媒体上，以便在计算机无法启动时生成系统报告。从媒体启动后，您可以在不运行 Acronis Cyber Protect Home Office 的情况下生成报告。只需

插入 USB 闪存驱动器，然后单击 **Acronis 系统报告** 图标。所生成的报告将保存在 USB 闪存驱动器内。

将 **Acronis 系统报告** 工具放置在可启动媒体上

1. 勾选 **Acronis 媒体生成器** 向导中 **应急媒体内容选择** 页面上的 **Acronis 系统报告** 复选框。
2. 单击 **下一步** 以继续。

从命令行提示符处创建系统报告

1. 以管理员身份运行 Windows 命令处理程序 (cmd.exe)。
2. 将当前目录更改为 Acronis Cyber Protect Home Office 安装文件夹。若要执行此操作，请输入：

```
cd C:\Program Files (x86)\Acronis\CyberProtectHomeOffice
```

3. 若要创建系统报告文件，请输入：

```
SystemReport
```

将在当前文件夹中创建文件 **SystemReport.zip**。

如果您想要为报告文件指定自定义名称，请键入新名称而不是 <文件名>：


```
SystemReport.exe /filename:<file name>
```

在可启动媒体下生成系统报告

1. 如果您没有 Acronis 可启动媒体，请创建一个。有关详细信息，请参阅 [Acronis 媒体生成器](#)。
2. 在 BIOS 中设置启动顺序，以便您的可启动媒体设备 (CD、DVD 或 USB 驱动器) 成为第一个启动设备。有关详细信息，请参阅 [设置 BIOS 启动顺序](#)。
3. 从 Acronis 可启动媒体启动，并选择 **Acronis Cyber Protect Home Office**。

注意

您可以插入 USB 闪存驱动器并单击 **Acronis 系统报告**，而不是单击 **Acronis Cyber Protect Home Office**。在这种情况下，程序将生成报告并自动将其保存到闪存驱动器。

4. 单击“帮助”图标 ( 旁边的箭头，然后选择 **生成系统报告**。
5. 在生成报告后，单击 **保存**，并在打开的窗口中为创建的文件指定位置。
程序会将报告存档为 zip 文件。

13.3 Acronis 智能错误报告

如果问题由程序中的错误操作造成，Acronis Cyber Protect Home Office 将显示相应的错误消息。错误消息包含事件代码以及该错误的简短说明。

13.3.1 如果您连接了互联网

若要查看提供建议解决方案的 Acronis 知识库文章以便更正错误，请单击 **知识库** 按钮。

此时将打开确认窗口，它会列出要通过互联网发送到 Acronis 知识库的信息。单击**确定**以允许发送信息。

如果您希望以后在发送此类消息时无需确认，请选中**始终发送且无需确认**复选框。

13.3.2 如果您没有连接互联网

1. 在错误窗口中，请单击**更多详细信息**并记下事件代码。代码可能如下所示：

0x000101F6 - 普通事件代码示例。

0x00970007+0x00970016+0x00970002 - 复合事件代码示例。有时，错误可能发生在低级程序模块中，然后传播到更高级别的模块，从而导致这些模块也出现错误。这种情况下就可能会显示这种代码。

2. 如果已建立互联网连接或者可以使用其它连接了互联网的计算机，请访问：<https://kb.acronis.com/errorcode/>。

如果知识库无法识别事件代码，则说明知识库中还没有解决该问题的文章。在这种情况下，请打开 [Acronis 客服中心](#) 的故障表单。

13.4 向 Acronis 发送反馈

我们经常对我们的产品和服务进行改进，以使它们更实用、更可靠、更快速。您可以通过反馈表单指出我们应该解决的不便之处和缺陷，以便让 Acronis Cyber Protect Home Office 变得更好。请花几分钟时间告诉我们您对我们的产品的看法、建议新功能或报告问题。我们一定会认真阅读并分析所有反馈。

注意

我们不会回复所有反馈信息。如果您在使用 Acronis Cyber Protect Home Office 时需要帮助，请联系技术支持。

将反馈发送至 Acronis


1. 在侧边栏上单击**帮助**，然后单击**发送反馈**。反馈表单将会打开。

A Send Feedback to the Acronis team ✕

Share your thoughts about Acronis Cyber Protect Home Office or report a problem.

Reason ▼

Enter your feedback here

 Attach file...

Attach system report [What is this?](#)

We cannot reply to all messages sent via this form, but we do read and analyze your feedback.

Send

2. 从列表中选择反馈原因。
3. 键入您的意见和建议。
4. 提供您的姓名和电子邮件。
5. [可选步骤]您也可以附加文件和 Acronis 系统报告。有关详细信息，请参阅 [Acronis 系统报告](#)。当您遇到严重问题时，例如，当 Acronis Cyber Protect Home Office 停止响应时，我们建议您附加系统报告。
6. 单击**发送**。

13.5 如何收集崩溃转储

由于 Acronis Cyber Protect Home Office 或 Windows 崩溃可以由不同原因引起, 因此必须分别调查各个崩溃案例。如果您能提供以下信息, Acronis 客服中心将能够帮到您:

如果 Acronis Cyber Protect Home Office 崩溃, 请提供以下信息:

1. 说明遇到此问题前执行的确切步骤及顺序。
2. 崩溃转储。有关如何收集此类转储的信息, 请参阅 Acronis 支持知识库 (KB) 文章, 地址为 <https://kb.acronis.com/content/27931>。

如果 Acronis Cyber Protect Home Office 导致 Windows 崩溃

1. 说明遇到此问题前执行的确切步骤及顺序。
2. Windows 转储文件。有关如何收集此类转储的信息, 请参阅 Acronis 支持知识库文章, 地址为 <https://kb.acronis.com/content/17639>。

如果 Acronis Cyber Protect Home Office 挂起

1. 说明遇到此问题前执行的确切步骤及顺序。
2. 进程的用户转储。请参阅 Acronis 支持知识库文章, 地址为 <https://kb.acronis.com/content/6265>。
3. Procmon 日志。请参阅 Acronis 支持知识库文章, 地址为 <https://kb.acronis.com/content/2295>。

如果您无法访问该信息, 请联系 Acronis 客服中心, 获取上传文件的 FTP 链接。

此信息有助于加快找到解决方案。

13.6 Acronis 客户体验计划

Acronis 客户体验计划 (CEP) 可让 Acronis 客户对 Acronis 产品的功能、设计和开发提供意见。客户可通过该计划向我们提供各种信息, 包括主机和/或虚拟机的硬件配置信息、使用最多(和最少)的功能以及所遇到的具体问题。我们将在这些信息的基础上对 Acronis 产品和使用最多的功能加以改进。

加入或退出 Acronis 客户体验计划的方法

1. 在侧栏上, 点击 **设置**。
2. 要退出该计划, 请清除 **参与 Acronis 客户体验计划** 复选框。

若选择参加, 我们将每隔 90 天自动收集一次技术数据。我们将不会收集任何个人数据, 如, 您的姓名、地址、电话号码或键盘输入。加入 CEP 是自愿行为, 其最终结果旨在对软件加以改进并增强其功能, 使其能够更好地满足客户的需求。

词汇表

A

Acronis Active Protection

一种保护数据免遭勒索软件侵害的技术。勒索软件是一种恶意软件，它会阻止访问某些文件或整个系统，然后实施勒索以取消阻止。此技术基于启发式方法，可使用实时模式监控计算机中运行的进程并通知用户对计算机中的数据进行了加密。如果对文件进行了加密，可以从临时副本或备份恢复文件。

Acronis Notary

该技术允许用户查看经过公证的文件自备份以来是否有过修改。Notary 基于选择进行公证的文件的哈希代码计算哈希代码，然后将哈希代码发送至基于区块链的数据库。区块链技术可保证哈希代码不会更改。因此，可以通过对比数据库中的哈希和您想要检查的文件的哈希轻松地验证文件的可信性。

Acronis Secure Zone

在硬盘上存储备份的安全分区。优点：可将磁盘恢复至磁盘备份所在的磁盘 提供一种经济方便的方法，保护数据免受软件故障、病毒攻击以及操作错误的影响 无需使用独立的媒体或网络连接来备份或恢复数据 限制：1) Acronis Secure Zone 不能在动态磁盘上创建。2) 当您从可启动媒体、通过 启动恢复管理器或 BartPE 启动时，Acronis Secure Zone 在恢复环境中不可用作备份的位置。

Acronis 启动恢复管理器

当按下 F11 时，在启动时允许启动独立版的保护工具。启动恢复管理器无需使用可启动媒体。启动恢复管理器对移动用户尤为方便。如果发生故障，用户可重新启动计算机，根据提示“按 F11 运行启动恢复管理器...”来按 F11，并采用与使用普通可启动媒体相同的方法执行数

据恢复。限制：无法在动态磁盘上组织；需要手动配置启动加载程序，如 LILO 和 GRUB；需要重新激活第三方加载程序。

Acronis 驱动器

一种包含本地和云存档的虚拟驱动器。在收藏夹下的 File Explorer 中可以访问该驱动器，并且可以在只读模式下访问已存档文件。

备

备份

与备份操作相同。使用备份设置创建和管理一组备份版本。一个备份可包含使用完整和增量备份方式创建的多个备份版本。属于同一备份的备份版本通常存储在相同位置。

备份版本

单次备份操作的结果。从物理角度看，它是一份文件或文件集，包含在特定日期与时间所备份数据的副本。由 Acronis Cyber Protect Home Office 创建的备份版本文件的文件扩展名为 .tibx。备份版本合并所生成的 TIBX 文件也称为备份版本。

备份版本链

最少两个备份版本序列，包含第一个完整备份版本和后续的一个或多个增量或差异备份版本。备份版本链将持续到下一个完整备份版本（若有）。

备份操作

创建计算机硬盘数据副本的操作，用以将数据恢复或还原至特定日期和时间。

备份设置

用户在创建新备份时配置的一组规则。该规则控制备份进程。稍后，您可编辑备份设置来转换或者优化备份进程。

不

不间断保护

不间断保护 - 启动不间断备份功能时的执行过程。

不间断备份

不间断备份实为用 Acronis 不间断备份功能创建的磁盘/分区或文件备份。这是由一个完整备份和一系列在短时间间隔内创建的增量备份版本组成的一组备份。它可提供几乎连续的数据保护，也就是说，它允许您根据需要可在任何恢复点恢复以前的数据状态。

差

差异备份

一种用于保存对备份中的上一个完整备份版本所作的更改的备份方法。一种用于创建差异备份版本的备份流程。

差异备份版本

差异备份版本存储对上次完整备份版本数据的更改。您需要访问相应的完整备份版本来从差异备份版本中恢复数据。

磁

磁盘备份(映像)

以打包形式包含磁盘或分区上每一扇区副本的备份。一般情况下，仅复制包含数据的扇区。允许制作原始映像，即复制所有磁盘扇区，此功能可制作不受支持的文件系统的映像。

存

存档

因存档操作而创建的文件。该文件包括用户选择进行存档的一组压缩文件。存档可以存储在 Cloud 或本地存储中(如外置硬盘驱动器或 NAS)，并且可以在虚拟 Acronis Drive 上在只读模式下访问它们。

存档操作

该操作可以将您选择的文件进行压缩并将它们移到 Cloud 或本地存储，如外置硬盘驱动器或 NAS。该操作的主要目的是通过将旧文件或大型文件移到其他存储，从而腾出硬盘驱动器上的空间。完成后，文件已从原始位置删除并且可以在 Acronis Drive 上在只读模式下访问。

公

公证

“记住”文件状态并将此状态定义为可信的过程。在公证期间，Acronis Notary 基于选择进行公证的文件的哈希代码计算哈希代码，然后将哈希代码发送至基于区块链的数据库。

公证备份

包含已通过 Acronis Notary 进行公证的文件的备份。

恢

恢复

恢复操作是一个通过备份将受损数据还原至先前正常状态的过程。

经

经过公证的文件

已通过 Acronis Notary 进行公证的文件。在将某个文件添加到公证备份并将其哈希代码发送

至基于区块链的数据库之后, 该文件变为经过公证。

可

可启动媒体

包含独立版 Acronis Cyber Protect Home Office 的物理媒体 (CD、DVD、USB 驱动器或计算机 BIOS 支持作为启动设备的其它媒体)。可启动媒体最常用于恢复无法启动的操作系统, 访问和备份在损坏的系统中存留的数据, 在裸机上部署操作系统, 在裸机上创建基本卷或动态卷, 或者逐个扇区备份文件系统不受支持的磁盘。

可疑进程

Acronis Active Protection 使用行为启发式方法并分析程序(进程)执行的一系列行为, 然后与恶意软件行为模式数据库中的一系列事件进行比较。如果程序的行为与勒索软件类似并试图修改用户文件, 则它将被视作可疑程序。

数

数据同步

数据同步是在两个或更多同步的文件夹中保持数据一致的过程。这些文件夹可能位于同一台计算机或通过本地网络或通过互联网连接的不同计算机上。在同步文件夹中创建、复制、修改或删除文件或子文件夹时, 在其它同步文件夹中也将自动完成同样的操作。反之亦然 - 其它同步文件夹发生更改时, 您的文件夹中也会发生同样的更改。

同

同步

与数据同步相同。在同步所有者计算机上配置的同步设置。使用相应的同步框可管理创建的同步。创建同步并不表示会启动同步过程。其它用户也可以参加创建的同步。

同步的文件版本

位于同步文件夹中的文件每次修改后的状态。文件版本可能存储在 Acronis Cloud 上。

完

完整备份

一种用于保存所有要备份的选定数据的备份方法。一种用于创建完整备份版本的备份流程。

完整备份版本

包含所有要备份数据的自足式备份版本。您无需访问任何其它备份版本即可从完整备份版本中恢复数据。

线

线上备份

联机备份 - 使用 Acronis 联机备份创建的备份。线上备份存储在名为 Cloud 的特殊存储中, 可通过 Internet 进行访问。联机备份的一个主要优点是可将所有备份保存在远程位置上。它可以保证所有已备份数据均可安全独立于用户本地存储之外。

验

验证

用于检查是否能够从特定的备份版本恢复数据的操作。对于完整备份版本, 程序仅验证完整备份版本。对于差异备份版本, 程序将验证初始完整备份版本和所选差异备份版本。对于增量备份版本, 程序将验证初始完整备份版本、所选的增量备份版本及其从备份版本到所选的增量备份版本的整个链(若有)。若链中包含一个或多个差异备份版本, 程序只会验证(除初始完整备份版本和所选增量备份版本以外)链中最新的差异备份版本, 以及差异备份版本与所选增量备份版本之间的所有后续增量备份版本(若有)。

移

移动备份

包含来自移动设备(如智能手机或平板电脑)文件的备份。

增

增量备份

一种用于保存对备份中的上一个备份版本(所有类型)所作的更改的备份方法。一种用于创建增量备份版本的备份流程。

增量备份版本

存储对上次备份版本数据所作更改的备份版本。您需要访问同一备份中的其它备份版本才能从增量备份版本中还原数据。

索引

.vhd(x) 文件的使用方法 207

“

“保护”仪表盘 138

“备份”选项卡 78

“活动”选项卡 77

“命令”设置 203

1

1. 整个 PC 备份“两个完整版本” 61

2

2. 文件备份“每日增量版本 + 每周完整版本” 62

3

3. 磁盘备份“每两个月创建一次完整版本 + 每
一个月创建两个差异版本” 62

32 位或 64 位组件 70

A

Acronis ASign 85

Acronis Cloud 17

Acronis Cloud 快速入门 31

Acronis Cyber Protect Home Office 使用区块链
技术的方式 83

Acronis Cyber Protect Home Office 无法识别
SSD 时的操作 163

Acronis DriveCleanser 192

Acronis Mobile 53

Acronis Secure Zone 184

Acronis Secure Zone 保护 186

Acronis Secure Zone 的大小 186

Acronis Secure Zone 清理 184

Acronis Secure Zone 位置 185

Acronis True Image 2020 版本之前创建的备份
文件的命名约定 44

Acronis 不间断备份数据存储 42

Acronis 可启动媒体启动参数 168

Acronis 客户体验计划 217

Acronis 媒体生成器 166

Acronis 启动恢复管理器 177

Acronis 使用的信息抹除方法 205

Acronis 不间断备份 41

Acronis 系统报告 213

Acronis 帐户 30

Acronis 智能错误报告 214

Acronis 专利技术 9

Acronis 异机还原 101, 209

Active Protection 138

B

BIOS 启动的系统、MBR、支持 UEFI 108, 157

BIOS 启动系统、GPT、非 Windows 110, 159

BIOS 启动系统、GPT、支持 UEFI 110, 159

BIOS 启动系统、MBR、不支持 UEFI 108, 157

BIOS 启动系统、MBR、非 Windows 109, 158

C

Cloud 备份和副本的错误处理 71

- F**
- FTP 连接 40
- S**
- SSD 大小 162
- T**
- Try&Decide 179
- Try&Decide 选项和通知 182
- Try&Decide: 典型使用案例 182
- U**
- UEFI 启动的系统、MBR、支持 UEFI 111, 160
- UEFI 启动系统、GPT、支持 UEFI 112, 161
- UEFI 启动系统、GPT、非 Windows 113, 162
- UEFI 启动系统、MBR、不支持 UEFI 111, 160
- UEFI 启动系统、MBR、非 Windows 112, 161
- UEFI 是什么? 103
- W**
- Web 过滤 140
- Web 应用程序 31
- Windows“开始”菜单 45
- 安**
- 安全与隐私权工具 192
- 安装和删除 Acronis Cyber Protect Home Office 14
- 保**
- 保护 138
- 保护家庭数据 134
- 保护系统 20
- 保留 TIB 格式的备份 11
- 保留规则 42
- 备**
- 备份 Office 365 数据 53-54
- 备份 PC 上的所有数据 22
- 备份、恢复和克隆的常见问题 47
- 备份保护 66
- 备份保留副本 69
- 备份操作菜单 76
- 备份操作的通知 63
- 备份操作的性能 73
- 备份磁盘和分区 49
- 备份到不同位置 80
- 备份的文件级安全设置 72
- 备份方案 11, 58
- 备份分割 68
- 备份活动和统计数据 77
- 备份计算机 20
- 备份快照 74
- 备份您的文件 25
- 备份前/后命令 67
- 备份设置的导入及导出 208
- 备份数据 49
- 备份文件命名 10, 44
- 备份文件与文件夹 50
- 版**
- 版本链方案 59
- 版权声明 9

备份选项 54
备份验证选项 69
备份移动设备 51

笔

笔记本电脑电源设置 75

编

编辑用于备份的用户命令 68
编辑用于恢复的用户命令 125

表

表 1. 超过 2 TB 的目标磁盘 105
表 2. 小于 2 TB 的目标磁盘 107

不

不间断备份 - 常见问题 43
不间断备份限制 41

操

操作优先级 73, 127

差

差异方式 37

尝

尝试确定崩溃原因 90

创

创建 Acronis Survival Kit 24
创建 Acronis 可启动媒体 22, 167
创建 Acronis 异机启动媒体 209
创建和管理 Acronis Secure Zone 184
创建同步 149

创建新分区 190
创建自定义算法 195

磁

磁盘/分区备份包含哪些内容? 34
磁盘备份中去除了哪些内容? 34
磁盘恢复模式 125
磁盘克隆和迁移 152
磁盘克隆实用工具 152

从

从 .wim 文件创建 .iso 文件 171
从 Acronis Cloud 恢复您的系统 118
从 Acronis Cloud 中删除数据 87
从备份中排除项目 64
从存档中排除哪些数据? 129
从克隆中排除项目 155
从云恢复磁盘 117

存

存储类型 147
存档数据 129-130
存在什么问题? 204

错

错误处理 71

大

大小 191

单

单一版本方案 59

<p>电</p> <p>电子邮件通知 63, 128, 136</p> <p>订</p> <p>订购许可信息 32</p> <p>动</p> <p>动态磁盘的操作限制 14</p> <p>动态分割备份 80</p> <p>发</p> <p>发生事件时执行操作参数 57</p> <p>防</p> <p>防病毒扫描 142</p> <p>防病毒设置 142</p> <p>防勒索软件保护 139</p> <p>访</p> <p>访问您的存档文件 132</p> <p>分</p> <p>分区标签 192</p> <p>分区布局 105</p> <p>分区代号 192</p> <p>分区类型(这些设置仅适用于 MBR 磁盘) 192</p> <p>分区设置 191</p> <p>分区属性 102</p> <p>复</p> <p>复制激活 79</p>	<p>覆</p> <p>覆盖文件选项 126</p> <p>高</p> <p>高级设置 56</p> <p>工</p> <p>工具 166</p> <p>工作方式 41, 117</p> <p>公</p> <p>公证备份 81</p> <p>共</p> <p>共享数据 133</p> <p>购</p> <p>购买完整版 17</p> <p>关</p> <p>关于恢复动态/GPT 磁盘和卷 113</p> <p>关于同步功能 147</p> <p>管</p> <p>管理检测到的问题 144</p> <p>管理自定义备份方案 61</p> <p>恢</p> <p>恢复 Office 365 数据 123-124</p> <p>恢复操作的通知 127</p> <p>恢复操作的性能 127</p> <p>恢复操作选择 124</p> <p>恢复磁盘和分区 90</p>
---	--

恢复到先前的文件版本 150

恢复动态卷 113

恢复分区和磁盘 101

恢复过程的示例 114

恢复后的分区样式 114

恢复基本卷和磁盘 114

恢复计算机 28

恢复前/后命令 125

恢复数据 90

恢复文件和文件夹 121

恢复至 UEFI 系统的示例 114

恢复中断时的操作 118

基

基本概念 33

激

激活次数太多问题 16

计

计划 55

计算机 202

计算机关机 72

计算机重新启动 126

技

技术支持 19

加

加密 131

加载映像 205

检

检查在可启动环境中对驱动程序的访问权限
212

简

简介 10

将

将备份复制到 Acronis Cloud 79

将算法保存到文件 197

将系统从 HDD 迁移至 SSD 162

将系统恢复到同一硬盘 91

将现有备份添加至列表 81

解

解决最常见的问题 213

决

决定存储备份的位置 38

可

可移动媒体设置 70

可以和不可以同步的内容 147

可以恢复哪些项目? 124

可以使用以下方案手动清理本地备份: 11

可用磁盘空间阈值 63, 127

可在何处获取这些应用程序? 53

克

克隆磁盘 27

克隆磁盘向导 152

克隆硬盘驱动器 26

	其他要求 12	
块		启
块修改跟踪器 (CBT) 38		启动之前, 27
快		迁
快捷菜单命令 46		迁移方法 108, 156
来		签
来源选择 193		签署文件 85
漏		清
漏洞评估 143		清理 Acronis Cloud 上的空间 87
每		清理 TIBX 格式备份 11
每日备份参数 57		清理备份、备份版本和副本 85
每月备份参数 57		清理进度 204
每周备份参数 57		清理设置 199
抹		清理选项 200
抹除后的操作 197		清理选项默认值 200
内		驱
内置商店 18		驱动器可用空间 202
排		确
排除内容与方式 65		确保可启动媒体随时可用 172
配		任
配置 Active Protection 140		任务栏上的 Acronis Cyber Protect Home Office 按钮 45
配置保护排除项 145		任务栏通知中心 45
配置防病毒扫描 142		如
其		如果您连接了互联网 214
其他信息 178		如果您没有连接互联网 215

如何访问受密码保护的备份 67
如何恢复删除的文件 150
如何加载映像 206
如何将初始系统迁移至更大的硬盘驱动器？ 104
如何进行恢复测试, 以及检查驱动器和网络适配器 173
如何确保数据的安全性 32
如何使用 Acronis DriveCleanser 193
如何使用默认排除设置 64
如何收集崩溃转储 217
如何在 BIOS 中启用 UEFI? 104

入

入门 20

软

软件评估 183

删

删除复制到云的备份版本 88
删除复制到云的备份副本的版本 88
删除同步 150
删除整个备份 87
删除整个备份副本 85
删除整个备份及其副本 85

上

上述建议不起作用时的操作 164

什

什么是 Acronis ASign? 85
什么是 Acronis Cyber Protect Home Office? 10

什么是家庭数据保护? 134
什么是区块链? 83
什么是数据存档? 129

升

升级 Acronis Cyber Protect Home Office 18

实

实时保护 139

使

使用 .vhd(x) 文件 207
使用 Acronis 异机还原 212
使用 Try&Decide 180
使用 Try&Decide 的限制 180
使用 Wi-Fi 网络备份到 Acronis Cloud 75
使用备份与恢复方法迁移至 SSD 164
使用备份执行的操作 76
使用区块链技术 83
使用在线控制面板恢复数据 136

试

试用版信息 17

手

手动分区 154
手动管理您的订购许可 17
手动清理备份和副本版本 86
手动验证文件的可信性 84

受

受保护的分区 182

数
数据存档选项 131
数据类型 147
数据销毁方法 201
数据中心 131

搜
搜索备份内容 123

算
算法定义 195
算法选择 194

它
它可以解决什么问题? 209

添
添加新硬盘 188

通
通知 182
通知区域 148

同
同步 17
同步数据 147
同步图标 148
同步文件的版本 149

统
统一扩展固件接口 (UEFI) 103

完
完成恢复之后 101
完整、增量和差异备份 35
完整方式 35

网
网络连接传输速率 73
网络隐私 183
网上邻居过滤器 204

维
维护和支持计划 19

为
为备份准备一个新磁盘 39
为何备份 Office 365 数据? 53
为何需要? 26, 193
为什么使用 UEFI? 104
为什么要复制? 79

文
文件 201
文件备份与磁盘/分区映像之间的差别 34
文件恢复 183
文件恢复选项 126
文件系统 191
文件资源管理器 148
文件资源管理器中的文件级恢复 46

我
我如何使用? 209

无
无论如何也要安装的大容量存储驱动程序 212

系
系统清理 197
系统要求与支持的媒体 12

下
下载保护更新 146

限
限制和其他信息 207

线
线上备份保护 67

向
向 Acronis 发送反馈 215
向导 46
向现有 .wim 映像添加驱动程序 170
向在线控制面板添加新设备 134

泄
泄露原理 204

卸
卸载映像 206

虚
虚拟更改的存储 182

选
选择初始化方法 189

选择哪种迁移方法 163
选择硬盘 188
选择用于备份的数据中心 74

压
压缩级别 73

验
验证备份 80
验证设置 41
验证文件的可信性 83
验证选项 125

要
要测试可启动媒体, 请执行以下操作: 172

一
一般 200
一般限制 17
一次性清理 89

移
移动备份的本地目标位置 53

疑
疑难解答 41, 213

已
已复制数据的保护 80

异
异机还原流程 212
异机还原设置 212

	在计算机重新启动后, Try&Decide 如何工作 179
映像创建模式 66	在可启动媒体下将系统恢复到新磁盘 95
	在列表中对备份排序 79
	在哪些情况下 Try&Decide 可以提供帮助 179
	增
	增量方式 36
	针
	针对 Zoom、Cisco Webex 和 Microsoft Teams 的保护 145
	正
	正在激活 Acronis Cyber Protect Home Office 15
	正在删除 Acronis Secure Zone 187
	支
	支持的 Internet 连接类型 13
	支持的操作系统 12
	支持的存储媒体 14
	支持的文件系统 13
	指
	指定清理选项 200
	转
	转换 Acronis 备份 207
	准
	准备 212
	准备恢复 90
	准备驱动程序 212
映	
映像创建模式 66	
硬	
硬盘抹除方式 204	
用	
用户界面语言 20	
与	
与 Windows 集成 45	
预	
预览 204	
远	
远程备份数据 135	
远程存储器 31	
云	
云存档与在线备份 130	
在	
在 Acronis True Image(2020 或 2021) 和 Acronis Cyber Protect Home Office 中创 建的备份 10	
在 Acronis True Image(2020 或 2021) 和 Acronis Cyber Protect Home Office 中创 建的备份文件的命名约定 44	
在 BIOS 或 UEFI BIOS 中设置启动顺序 116	
在崩溃后恢复系统 90	
在从可启动媒体启动时选择视频模式 175	
在隔离区中管理文件 144	

自

自定义方案 60

自定义方案示例 61

自动清理备份版本 86

自动清理副本版本 86

自动驱动程序搜索 212

最

最低系统要求 12