Acronis

acronis.com

安克诺斯数据保护软件 15

Update 6

用户指南

修改：2023/6/15

目录

版权声明

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。

Acronis 安克诺斯数据保护软件 15 版本

Acronis 安克诺斯数据保护软件 15 在以下版本中可用：

- 安克诺斯数据保护软件 Essentials
- 安克诺斯数据保护软件 Standard
- 安克诺斯数据保护软件 Advanced
- Cyber Backup Standard
- Cyber Backup Advanced

有关每个版本中所包含功能的详细信息，请参阅 Acronis 安克诺斯数据保护软件 15 版本比较(包括云部署)。

Acronis 安克诺斯数据保护软件 15 的所有版本都按受保护工作负载的数量及其类型(工作站、服务器和虚拟主机)进行许可。安克诺斯数据保护软件 版本仅可与订阅许可一起使用。网络备份版本同时提供订购许可证和永久许可证。有关可用选项的详细信息，请参阅 "许可证授权"(第 21 页)。

版本 15 的永久许可号不能与 Acronis Cyber Backup 12.5 中的备份代理程序一起使用。但是，即使管理服务器升级到版本 15，这些代理程序也仍将继续使用其旧的许可证密钥。

备份订阅许可可以与 12.5 版代理程序一起使用，即使代理程序升级到版本 15 也是如此。安克诺斯数据保护软件 订阅许可只能由 15 版代理程序使用。

在 15 版管理服务器上注册的 12.5 版备份代理程序无法执行脱离主机的数据处理操作，例如备份复制、备份验证、清理或转换为虚拟机。

注意

不同版本的功能有所不同。您的许可证可能无法使用本文档中描述的某些功能。有关每个版本中所包含功能的详细信息，请参阅 Acronis 安克诺斯数据保护软件 15 版本比较(包括云部署)。

操作系统支持的 安克诺斯数据保护软件 功能

安克诺斯数据保护软件 功能在以下操作系统上受支持：

- Windows：Windows 7 及更高版本，Windows Server 2008 R2 及更高版本。
  Windows Defender Antivirus 管理在 Windows 8.1 及更高版本上受支持。
- Linux：CentOS 7.x、CentOS 8.0、Virtuozzo 7.x、Acronis Cyber Infrastructure 3.x。
  其他 Linux 发行版和版本也可能支持 安克诺斯数据保护软件 功能，但尚未经过测试。
- macOS：10.13.x 及更高版本(仅支持防病毒和反恶意软件保护)。

重要事项

安克诺斯数据保护软件 功能仅支持用于已安装保护代理程序的计算机。对于无代理程序模式下受保护的虚拟机，例如受适用于 Hyper-V 的代理程序、适用于 VMware 的代理程序或适用于 Scale Computing 的代理程序保护的虚拟机，仅支持备份。

安克诺斯数据保护软件 功能	Windows	Linux	macOS

取证备份	是	否	否
连续数据保护 (CDP)			
文件和文件夹的 CDP	是	否	否
通过应用程序跟踪更改的文件的 CDP	是	否	否
自动发现和远程安装			
基于网络的发现	是	否	否
基于 Active Directory 的发现	是	否	否
基于模板的发现(从文件导入计算机)	是	否	否
手动添加设备	是	否	否
Acronis 反恶意软件保护			
基于进程行为的勒索软件检测(基于人工智能)	是	否	否
加密挖矿进程检测	是	否	否
实时防恶意软件保护	是	否	是
自动从本地缓存恢复受影响的文件	是	否	否
Acronis 备份文件的自我保护	是	否	否
Acronis 软件的自我保护	是	否	否
便携式可执行文件的静态分析	是	否	是*
外部驱动器保护(HDD、闪存驱动器、SD 卡)	是	否	否
网络文件夹保护	是	否	否
服务器端保护	是	否	否
保护 Zoom、WebEx、Microsoft Teams 和其他远程工作保护	是	否	否
手动反恶意软件扫描	是	否	是
扫描存档文件	是	否	是
文件/文件夹排除	是	否	是**
进程排除	是	否	否

公司范围的白名单	是	否	是
行为检测	是	否	否
隔离	是	否	是
URL 过滤 (http/https)	是	否	否
Windows Defender Antivirus 管理	是	否	否
Microsoft Security Essentials 管理	是	否	否
漏洞评估			
操作系统及其原生应用程序的漏洞评估	是	是***	否
第三方应用程序的漏洞评估	是	否	否
修补程序管理			
修补程序自动批准	是	否	否
手动修补程序安装	是	否	否
自动安装修补程序	是	否	否
故障安全修补:作为保护计划的一部分,在安装修补程序之前备份计算机	是	否	否
如果备份正在运行,则取消计算机重新启动	是	否	否
数据保护计划			
扫描计算机以查找不受保护文件	是	否	否
不受保护位置概述	是	否	否
数据保护地图中的保护动作	是	否	否
磁盘运行状况			
基于人工智能 (AI) 的 HDD 和 SSD 运行状况控制	是	否	否
基于 Acronis Cyber Protection Operations Center (CPOC) 警报的智能保护计划			
威胁源	是	否	否
修复向导	是	否	否
备份扫描			

扫描加密备份	是	否	否
扫描本地存储、网络共享和 Acronis 云存储中的磁盘备份	是	否	否
安全恢复			
在恢复过程中使用“Acronis 防病毒和反恶意软件保护”进行反恶意软件扫描	是	否	否
远程桌面			
通过基于 HTML5 的客户端连接	是	否	否
通过原生 Windows RDP 客户端连接	是	否	否
远程擦除	是****	否	否
网络安全保护监视器	是	否	是

* 只支持对 macOS 上的计划扫描进行便携式可执行文件的静态分析。

** 文件/文件夹排除仅在指定 macOS 上将不会由实时保护或预定扫描进行扫描的文件和文件夹的情况下适用。

*** 漏洞评估取决于特定发行版的官方安全警告的可用性，例如 https://lists.centos.org/pipermail/centos-announce、https://lists.centos.org/pipermail/centos-cr-announce 以及其他。

**** 远程擦除仅适用于运行 Windows 10 或更高版本的计算机。

许可证授权

要使用 Acronis 安克诺斯数据保护软件 保护工作负载，您需要一个许可证。安装 Acronis 安克诺斯数据保护软件 不需要许可证。

许可证类型

Acronis 安克诺斯数据保护软件 随订阅许可提供。在自购买之日起的有效期内，提供无限更新和免费技术支持。有效期结束后，现有保护计划会停止工作，并且无法创建新的保护计划。

可以续订旧版永久许可。某些功能(例如，云部署或云到云备份)不随永久许可提供。

还提供试用版许可。它让您可以在许可证激活后的 30 天内访问所有产品功能。

有关不同许可选项的更多详细信息，请参阅我们知识库中的“Acronis 安克诺斯数据保护软件 15：许可和升级/降级常见问题解答”。可以通过访问 https://www.acronis.com/company/licensing.html，来查看 Acronis 许可策略。

重要事项
Acronis 安克诺斯数据保护软件 15 更新 3 引入了新的许可模式。它需要通过许可证来注册和激活本地管理服务器。

在 Acronis 安克诺斯数据保护软件 15 更新 3 及更高版本中许可

在 Acronis 安克诺斯数据保护软件 15 更新 3 及更高版本中，不会在管理服务器(`https://<管理服务器的 IP 地址>:<端口>`)的本地中控台中添加任何许可号。

相反，可以在 Acronis 客户门户 (`https://account.acronis.com`) 中将许可证添加到您的帐户中，然后在 Acronis 安克诺斯数据保护软件 云中控台 (`https://cloud.acronis.com`) 中管理许可证。

离线管理服务器的许可证管理需要在本地中控台和云中控台中进行操作。

要了解有关本地中控台和云中控台的详细信息，请参阅 "Acronis 帐户、本地和云中控台"(第 23 页)。

开始使用具有 Acronis 安克诺斯数据保护软件 15 更新 3 及更高版本的管理服务器

1. 在 Acronis 客户门户 (`https://account.acronis.com`) 中，向您的帐户添加一个或多个许可证。
   在线购买的许可证会自动添加到此帐户中。
2. [对于本地部署模式] 激活管理服务器。
3. 为管理服务器分配许可证。

管理服务器的类型

根据部署模式，可以使用以下类型的管理服务器：

- 云管理服务器
- 本地管理服务器
  - 在线管理服务器
  - 离线管理服务器

您的 Acronis 帐户中可以有多个管理服务器。还可以将混合部署模式与云管理服务器和本地管理服务器一起使用。

如果使用多个管理服务器，可以在它们之间拆分许可证配额。有关如何执行此操作的详细信息，请参阅 "将许可证配额转移到另一个管理服务器"(第 32 页)。

云管理服务器

使用云部署时，无需在网络中安装并维护管理服务器。使用已部署在 Acronis 数据中心的管理服务器，只需为您的工作负载安装保护代理程序。

云管理服务器无需激活。它始终在线，并且许可信息会在服务器和您的 Acronis 帐户之间自动同步。

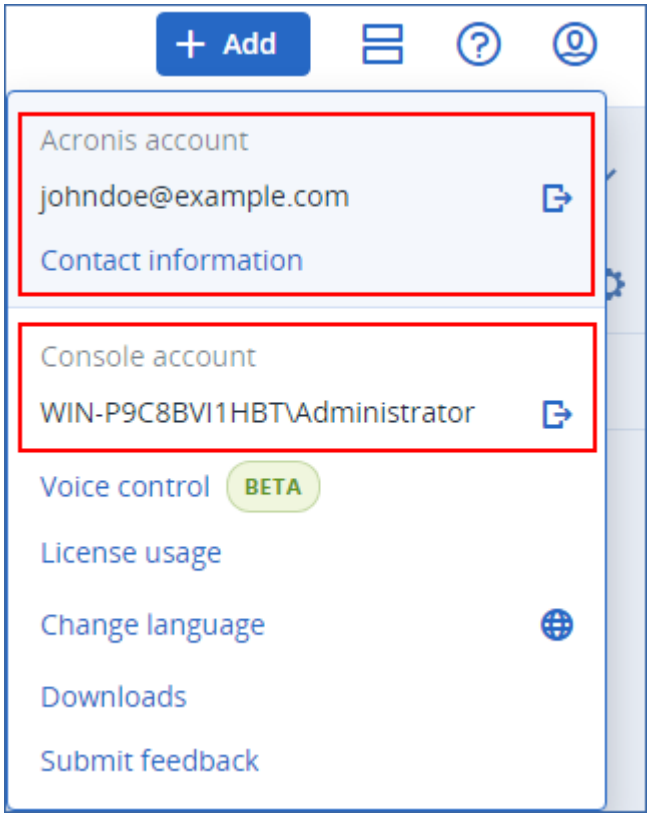
本地管理服务器

使用本地部署时，将在网络中安装管理服务器和保护代理程序。您可以有未连接到 Internet 的离线管理服务器，也可以有能够访问 Internet 的在线管理服务器。

本地管理服务器需要激活。有关激活的详细信息，请参阅 "激活管理服务器"(第 26 页)。

注意

已激活本地管理服务器的本地中控台中会显示两个不同的帐户：Acronis 帐户，用于同步许可信息；和中控台帐户，用于访问本地中控台本身。



在线本地管理服务器

当首次访问本地中控台时，通过登录到您的 Acronis 帐户，即可通过 Internet 激活在线管理服务器。

离线本地管理服务器

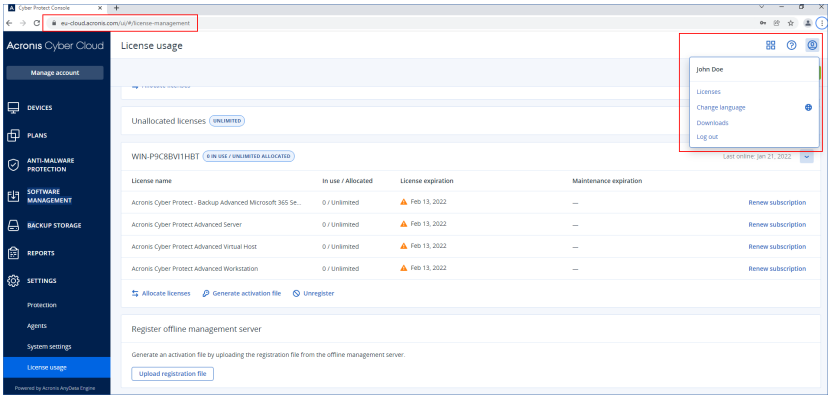
通过文件，手动激活离线管理服务器，并将其许可信息同步到您的 Acronis 帐户。

Acronis 帐户、本地和云中控台

要使用 Acronis 安克诺斯数据保护软件 并管理您的许可证及其使用情况，您需要一个 Acronis 帐户。您的所有许可证和管理服务器都已注册到该帐户。

使用此帐户，可以访问以下中控台：

- 云中控台 (https://cloud.acronis.com)

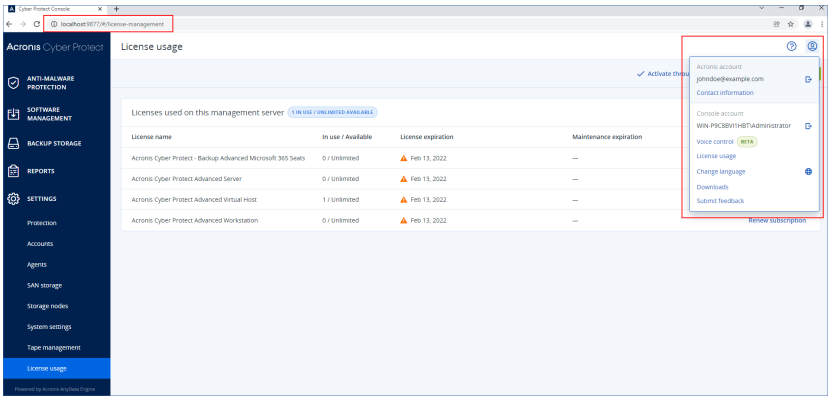


注意

在登录到云中控台后，其 URL 会更改并显示您帐户所属的确切数据中心。例如，https://eu-cloud.acronis.com 或 https://jp-cloud.acronis.com。

云中控台是您管理许可证的主要位置。在此处的**设置 > 许可证使用情况**选项卡上，可以将可用许可证和许可证配额分配给特定的管理服务器、将许可证配额重新分配给另一个管理服务器，或完成注册离线管理服务器。

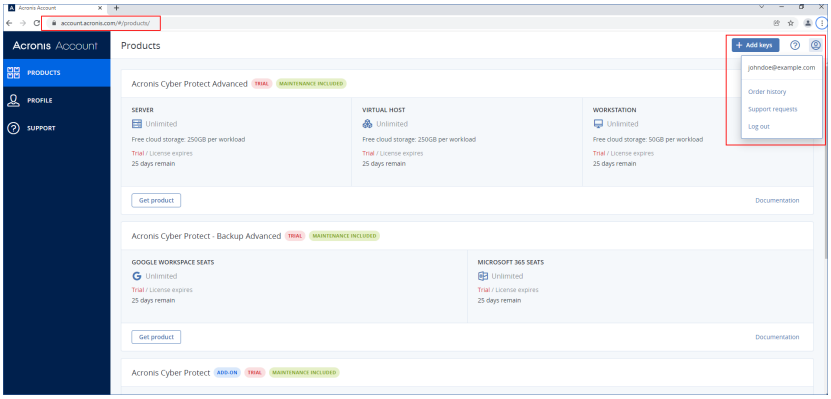
- 本地管理服务器的本地中控台(https://<管理服务器的 IP 地址>:<端口>)



在此处，可以查看分配的许可证、它们的配额和使用情况以及它们的到期日期。

激活离线管理服务器或为其分配许可证时，可以使用本地中控台和云中控台。

- Acronis 客户门户 (https://account.acronis.com)



在 Acronis 客户门户中，可以管理您购买的产品：例如，通过检查订购许可的到期日期、添加新的许可号、注册许可证续订或请求升级。还可以联系支持团队、下载产品安装文件以及访问产品文档。

管理许可证

下表汇总了可用操作，并显示了执行它们的位置。

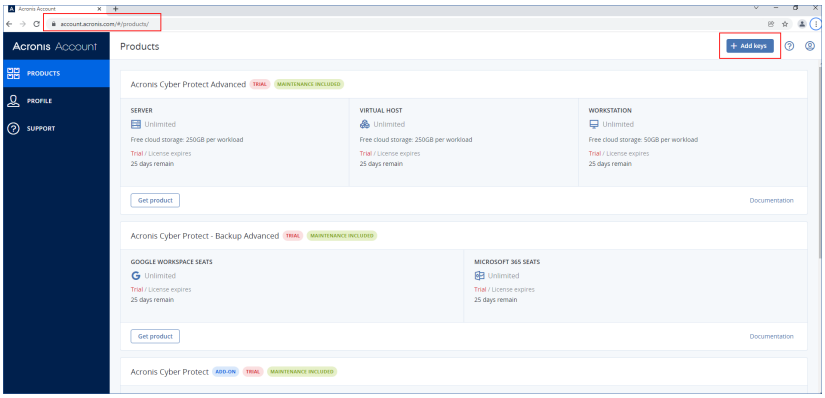
操作	位置
将许可证添加到帐户	在 Acronis 客户门户 (https://account.acronis.com) 中添加许可证。在线购买的许可证会自动添加到此处。
激活管理服务器	通过在您的帐户中注册管理服务器来激活它。 通过登录到您的帐户，在本地中控台（https://<管理服务器的 IP 地址>:<端口>）中激活在线管理服务器。 离线管理服务器的激活需要在本地中控台和云中控台中进行操作。
将许可证分配给管理服务器 修改现有的许可证分配	在在线管理服务器上，使用云中控台 (https://cloud.acronis.com) 分配许可证。分配的许可证会自动同步到管理服务器。 在离线管理服务器上，通过激活文件分配许可证。此步骤要求您使用管理服务器的本地中控台（https://<管理服务器的 IP 地址>:<端口>）和云中控台 (https://cloud.acronis.com)。
将许可证指派给工作负载	此操作是自动的。
从帐户中注销管理服务器	通过使用云中控台 (https://cloud.acronis.com)，注销在线管理服务器。 通过停用文件注销离线管理服务器。此步骤要求您使用离线管理服务器的本地中控台（https://<管理服务器的 IP 地址>:<端口>）和云中控台 (https://cloud.acronis.com)。 要注销您无权访问的离线管理服务器，只能使用云中控台。

将许可证添加到 Acronis 帐户

要使用许可证，必须将其添加到 Acronis 帐户中。在线购买的许可证会自动添加到您的帐户中。必须手动添加离线购买的许可证。

在 Acronis 帐户中添加许可证

1. 使用您的帐户凭据，登录到 Acronis 客户门户 (https://account.acronis.com)。
2. 在导航菜单中，单击**产品**。
3. 单击**添加密钥**。



4. 输入一个或多个许可号(每行一个),然后单击**添加**。

> **注意**
> 一次最多可以输入 100 个许可号。

许可证现已添加到您的帐户,可以在云中控台 (https://cloud.acronis.com) 中管理其使用情况。

重要事项

在升级到 Acronis 安克诺斯数据保护软件 15 更新 3 之前,将本地存储的永久许可导出到一个文件,然后将它们添加到您的 Acronis 帐户。

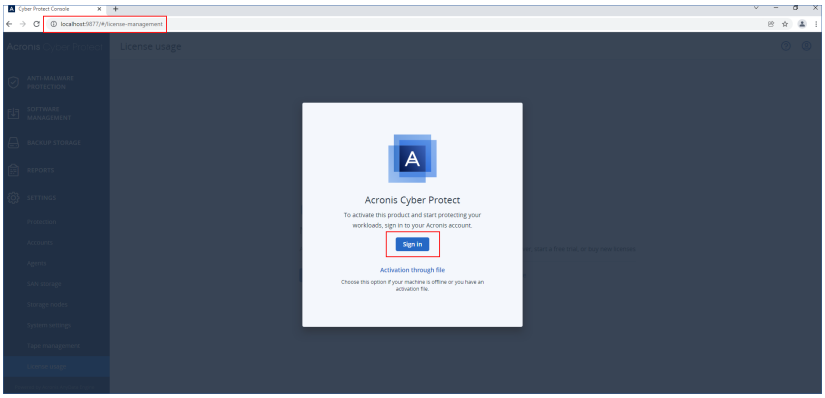
要查看在管理服务器上本地输入的许可号,请转到 `https://<管理服务器的 IP 地址>:<端口>/api/account_server/v2/licensing/legacy/license_keys`。

激活管理服务器

通过在您的 Acronis 帐户中注册管理服务器来激活它。

激活在线管理服务器

1. 在安装 Acronis 安克诺斯数据保护软件 管理服务器后,打开其本地中控台(`https://<管理服务器的 IP 地址>:<端口>`)。
2. 在打开的对话框中,单击**登录**。



3. 登录到您的 Acronis 帐户。

结果,将自动注册并激活管理服务器。

要开始保护您的工作负载，请为该服务器分配至少一个许可证。有关如何分配许可证的详细信息，请参阅 "将许可证分配给管理服务器"(第 29 页)。

注意

在线管理服务器需要访问 Internet，才能将许可信息同步到您的 Acronis 帐户。如果此类服务器离线超过 30 天，则其保护计划将停止工作，并且您的工作负载将不受保护。

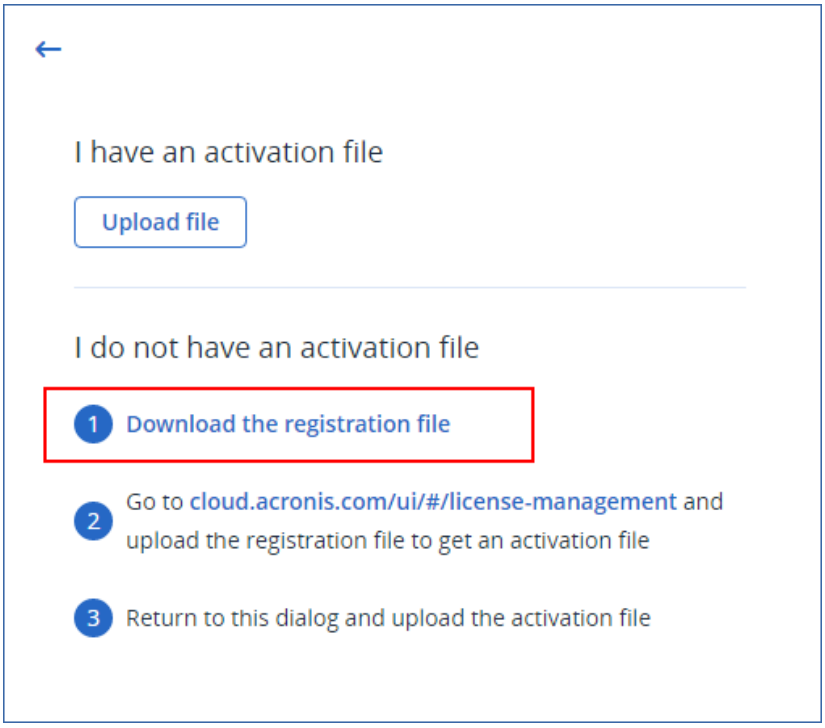
如果在本地中控台中从您的 Acronis 帐户注销，则无法同步许可信息。如果您在 30 天内未再次登录，则保护计划将停止工作，您的工作负载将变得不受保护。

激活离线管理服务器

离线管理服务器的激活需要在本地中控台和云中控台中进行操作。

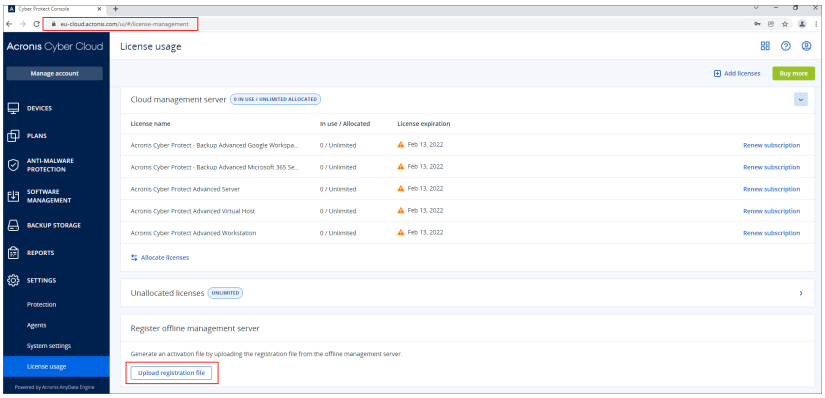
要访问云中控台，您需要第二台连接到 Internet 的计算机。

1. 在安装 Acronis 安克诺斯数据保护软件 管理服务器后，打开其本地中控台(`https://<管理服务器的 IP 地址>:<端口>`)。
2. 在打开的对话框中，单击**通过文件激活**。
3. 在**我没有激活文件**下，单击**下载注册文件**。



注册文件将下载到您的计算机上。

4. 在可以访问 Internet 的计算机上，登录到云中控台 (`https://cloud.acronis.com`)，然后转到**设置** > **许可证使用情况**。
5. 在**注册离线管理服务器**部分中，单击**上传注册文件**。



6. 在打开的对话框中，单击**浏览**，然后选择从离线管理服务器下载的注册文件。
7. 在打开的对话框中，单击**下载文件**。
   激活文件将下载到您的计算机上。

重要事项

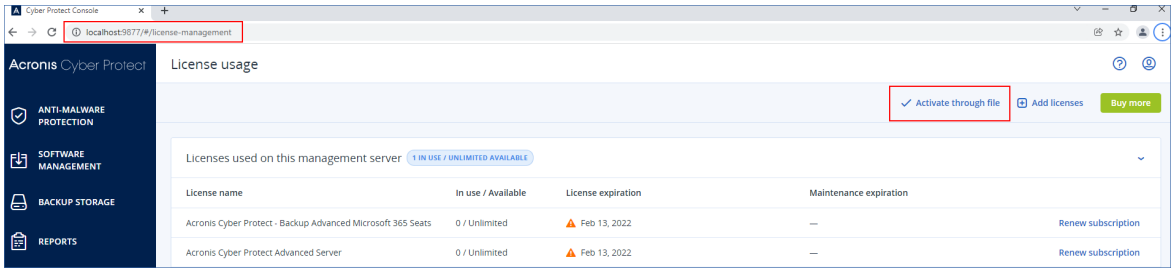
如果此离线管理服务器是您环境中唯一的管理服务器，则您 Acronis 帐户中的许可证将自动分配给它。激活文件将包含此信息，因此无需额外分配。

如果这不是您环境中唯一的管理服务器，则在激活后，必须按照 "将许可证分配给管理服务器"（第 29 页）中的步骤操作来分配许可证。

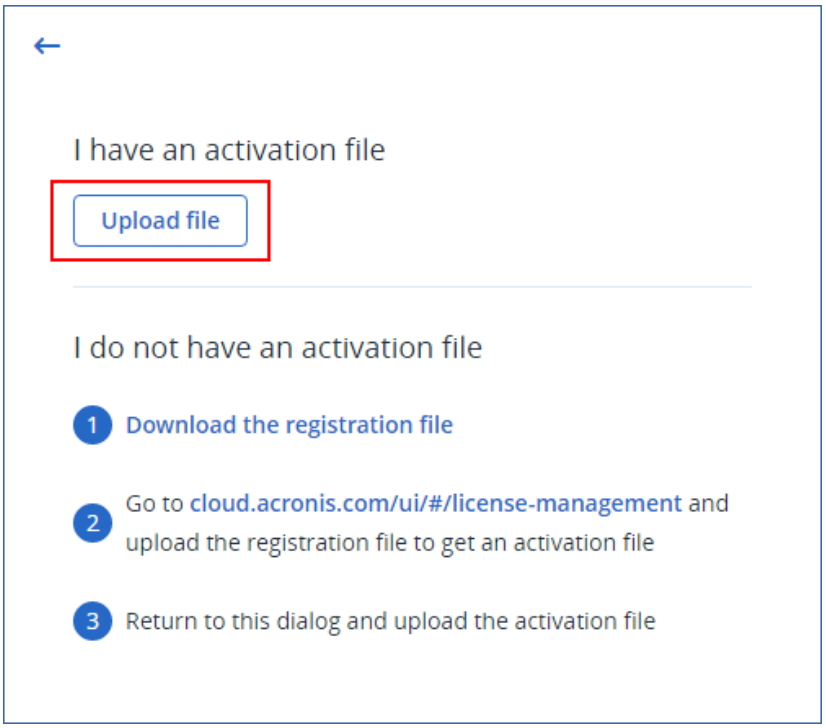
8. 在离线管理服务器（`https://`<管理服务器的 IP 地址>:<端口>）的本地中控台中，转到**通过文件激活**对话框。

注意

如果**通过文件激活**对话框未打开，请导航到**设置 > 许可证使用情况**，然后单击**通过文件激活**。



9. 在**我有激活文件**下，单击**上传文件**，然后选择从云中控台下载的激活文件。



结果，离线管理服务器会在您的 Acronis 帐户中注册并激活。

注意
可能无法激活在 UUID 不唯一的虚拟机上运行的管理服务器。例如，当克隆虚拟机或使用 VMware vCenter Converter 转换虚拟机时，该虚拟机的 UUID 可能会重复。如果您遇到类似问题，请联系我们的支持团队。

有关如何防止 VMware 虚拟机上出现 UUID 重复的详细信息，请参阅编辑具有重复的 UUID.bios 的虚拟机 (1002403)。

将许可证分配给管理服务器

要使用许可证，必须将其配额或其配额的共享分配给管理服务器。可以为管理服务器分配多个许可证。此外，可以拆分许可证配额并将配额的不同共享分配给不同的管理服务器。

注意
如果您的 Acronis 帐户中只有一个管理服务器，则您所有的许可证都会自动分配给该服务器。要了解如何将许可证重新分配给另一个管理服务器，请参阅 "将许可证配额转移到另一个管理服务器"（第 32 页）。

如果您的 Acronis 帐户中有多个管理服务器，则新许可证将显示在云中控台 (`https://cloud.acronis.com`) 中的**未分配的许可证**下。您需要手动分配这些许可证。

许可证的所有操作都会自动同步到在线管理服务器。要将分配更改同步到离线管理服务器，请创建一个新的激活文件，然后重复分配步骤。要了解有关不同管理服务器的更多信息，请参阅 "管理服务器的类型"（第 21 页）。

将许可证分配给在线管理服务器

1. 在云中控台 (https://cloud.acronis.com) 中，依次单击**设置 > 许可证使用情况**。
2. 导航到要为其分配许可证的管理服务器。
3. 单击**分配许可证**。
4. 在打开的对话框中，指定要分配给此服务器的许可证和许可证配额。
5. 单击**保存**。

结果，许可信息会自动同步到管理服务器，然后可以使用分配的许可证来保护您的工作负载。

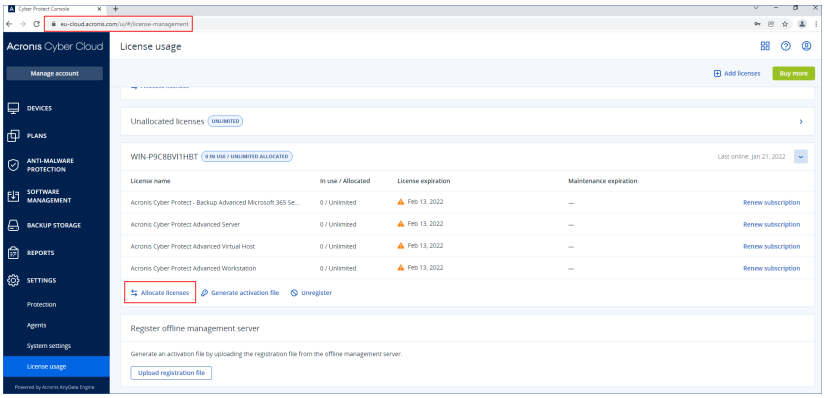
要修改分配，请重复上述步骤。

重要事项
如果修改后的许可证配额小于保护代理程序的数量，则负载最少的代理程序将停止工作。此选择是自动的。如果该操作不符合您的需要，请手动重新指派可用许可证。

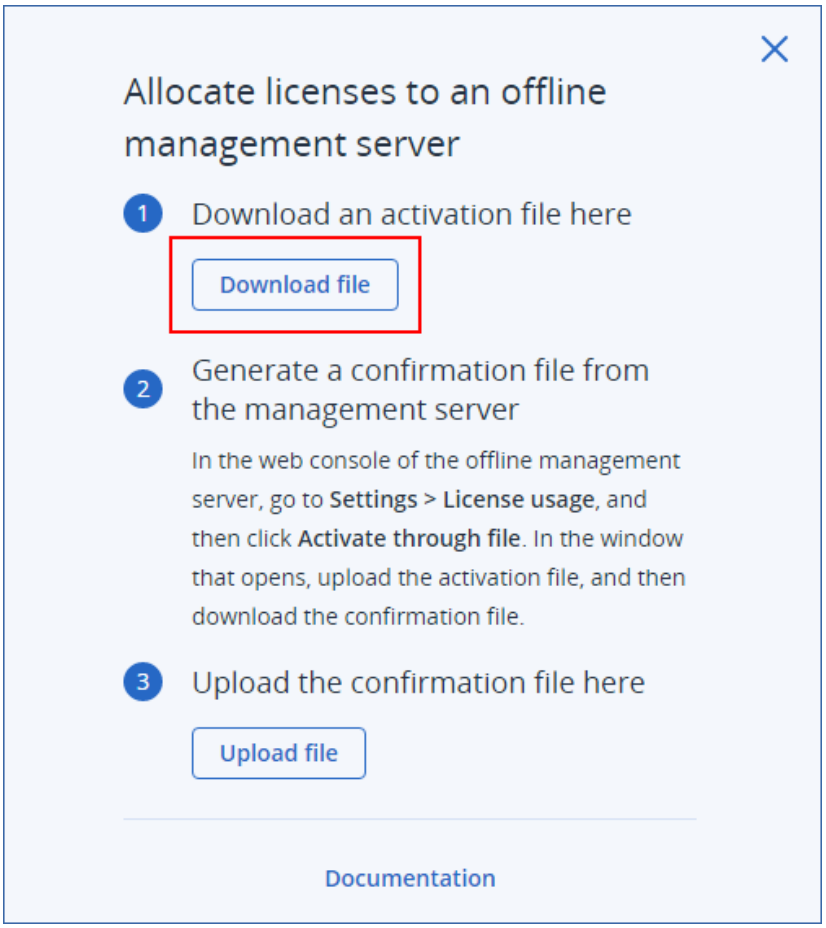
将许可证分配给离线管理服务器

要将许可证分配给离线管理服务器，您需要同时使用云中控台和本地中控台。要访问云中控台，您需要第二台连接到 Internet 的计算机。

1. 在可以访问 Internet 的计算机上，登录到云中控台 (https://cloud.acronis.com)，然后依次单击**设置 > 许可证使用情况**。
2. 导航到要为其分配许可证的管理服务器。
3. 单击**分配许可证**。

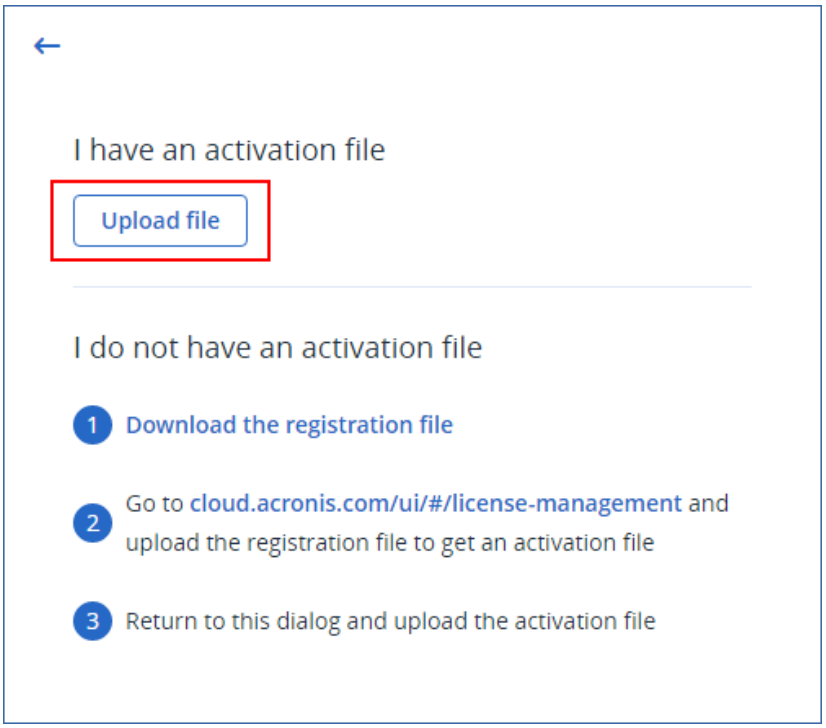


4. 在打开的对话框中，指定要分配给此服务器的许可证和许可证配额。
5. 单击**保存**。
6. 在**将许可证分配给离线管理服务器**对话框中，单击**下载文件**。



激活文件将下载到您的计算机上。

7. 在离线管理服务器(`https://`<管理服务器的 `IP` 地址>:<端口>)的本地中控台中，导航到**设置** > **许可证使用情况**，然后单击**通过文件激活**。
8. 在打开的对话框中的**我有激活文件**下，单击**上传文件**，然后选择从云中控台下载的激活文件。



结果，许可信息将在您的 Acronis 帐户和离线管理服务器之间同步。

要增加已分配的许可证配额，请重复上述步骤。

要减少已分配的许可证配额，请参阅 "减少分配给离线管理服务器的许可证配额"(第 32 页)。

将许可证配额转移到另一个管理服务器

可以将许可证配额从一个管理服务器转移到另一个管理服务器。当分配给某个管理服务器的许可证未由任何工作负载在使用并且需要将更多许可证用于另一个管理服务器时，此选项可能很有用。

注意

如果您的 Acronis 帐户中只有一个管理服务器，则您所有的许可证都会自动分配给该服务器。

如果您的 Acronis 帐户中有多个管理服务器，则新许可证将显示在云中控台 (https://cloud.acronis.com) 中的**未分配的许可证**下。您需要手动分配这些许可证。

将许可证配额转移到另一个管理服务器

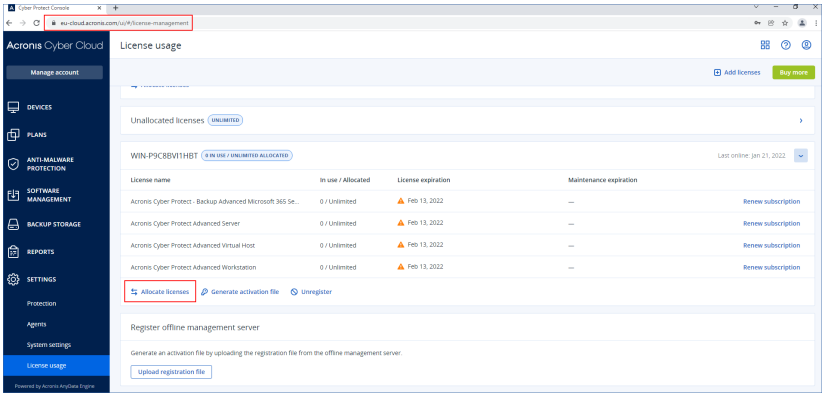
1. 按照 "将许可证分配给管理服务器"(第 29 页) 中的步骤操作，减少分配给原始管理服务器的许可证配额。

   已释放的许可证配额会显示在云中控台的**未分配许可证**部分中。
2. 按照 "将许可证分配给管理服务器"(第 29 页) 中的步骤操作，将许可证配额分配给第二个管理服务器。

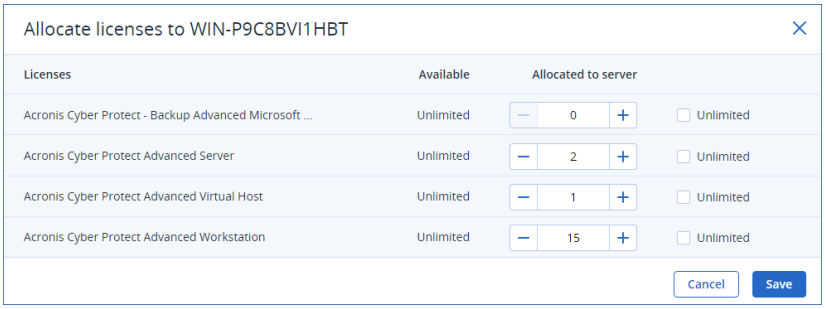
减少分配给离线管理服务器的许可证配额

要减少分配给离线管理服务器的许可证配额，您需要同时使用云中控台和本地中控台。要访问云中控台，您需要第二台连接到 Internet 的计算机。

1. 在可以访问 Internet 的计算机上，登录到云中控台 (https://cloud.acronis.com)，然后依次单击**设置 > 许可证使用情况**。
2. 导航到要为其分配许可证的管理服务器，然后单击**分配许可证**。

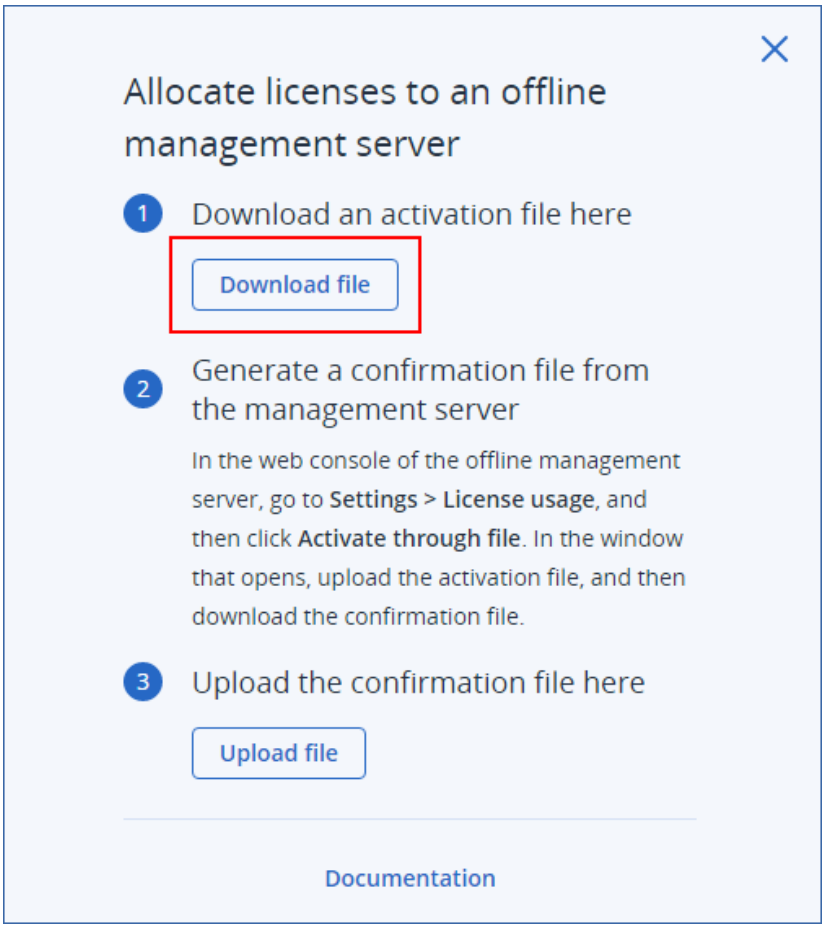


3. 在打开的对话框中，修改已分配给该服务器的许可证和许可证配额，然后单击**保存**。



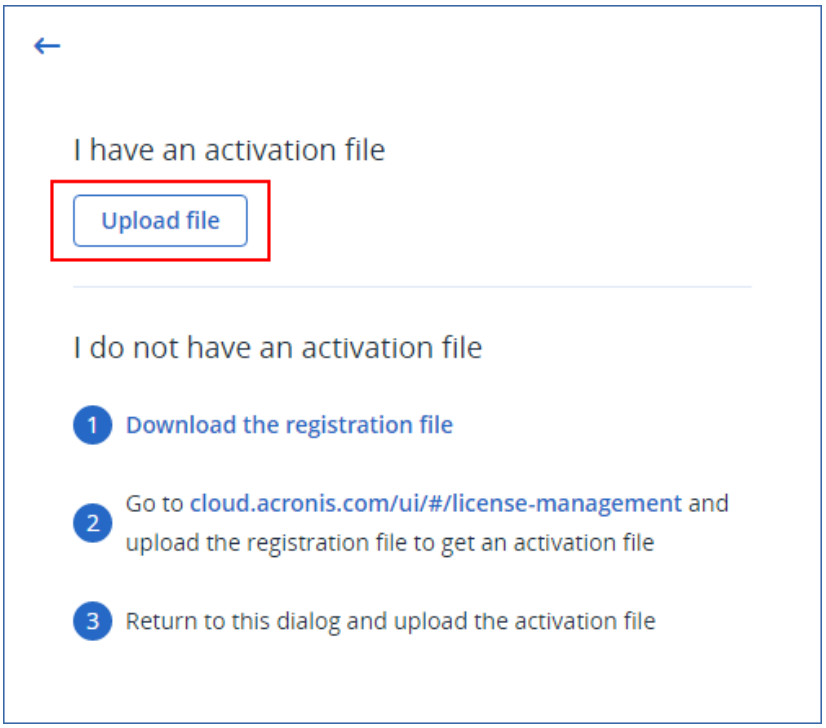
新的分配现在正等待处理。要取消它，请单击**删除此分配**。

4. 在**将许可证分配给离线管理服务器**对话框中，单击**下载文件**。

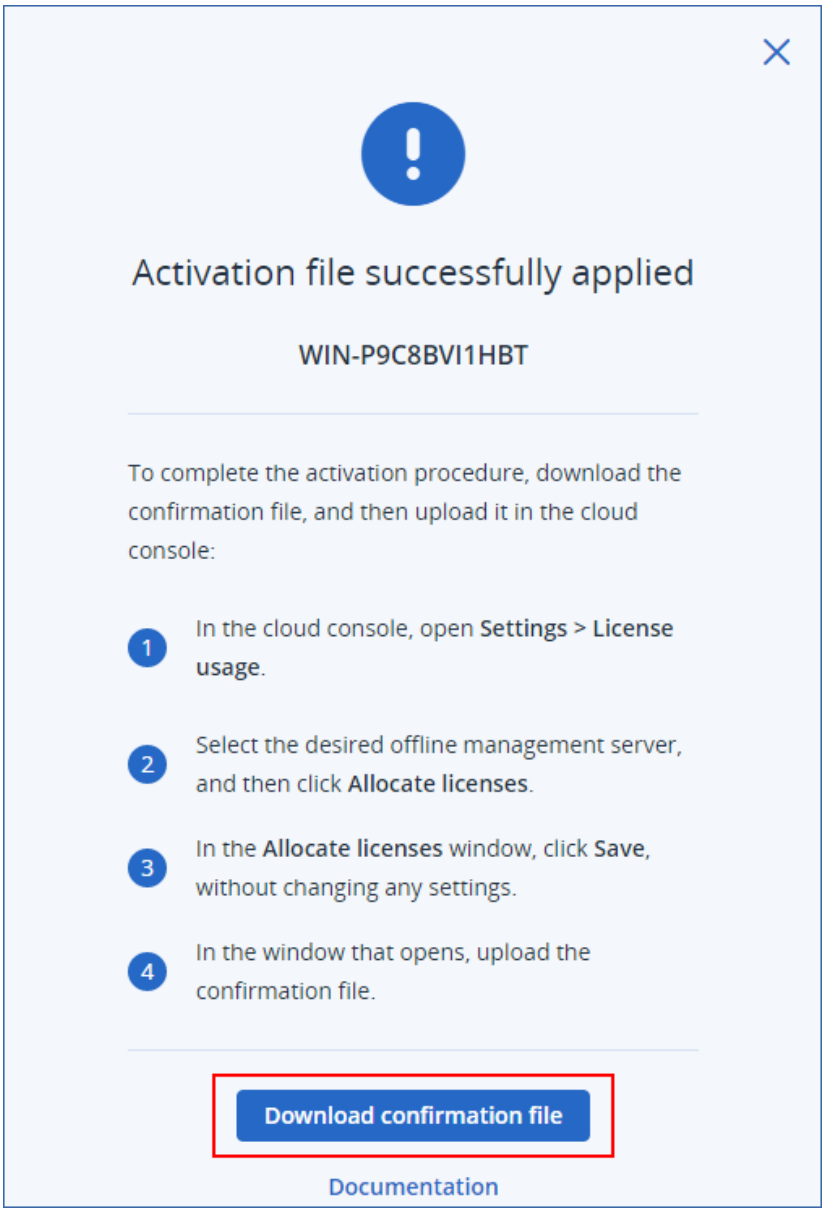


激活文件将下载到您的计算机上。

5. 在离线管理服务器(`https://<管理服务器的 IP 地址>:<端口>`)的本地中控台中，导航到**设置** > **许可证使用情况**，然后单击**通过文件激活**。
6. 在打开的对话框中的**我有激活文件**下，单击**上传文件**，然后选择从云中控台下载的激活文件。

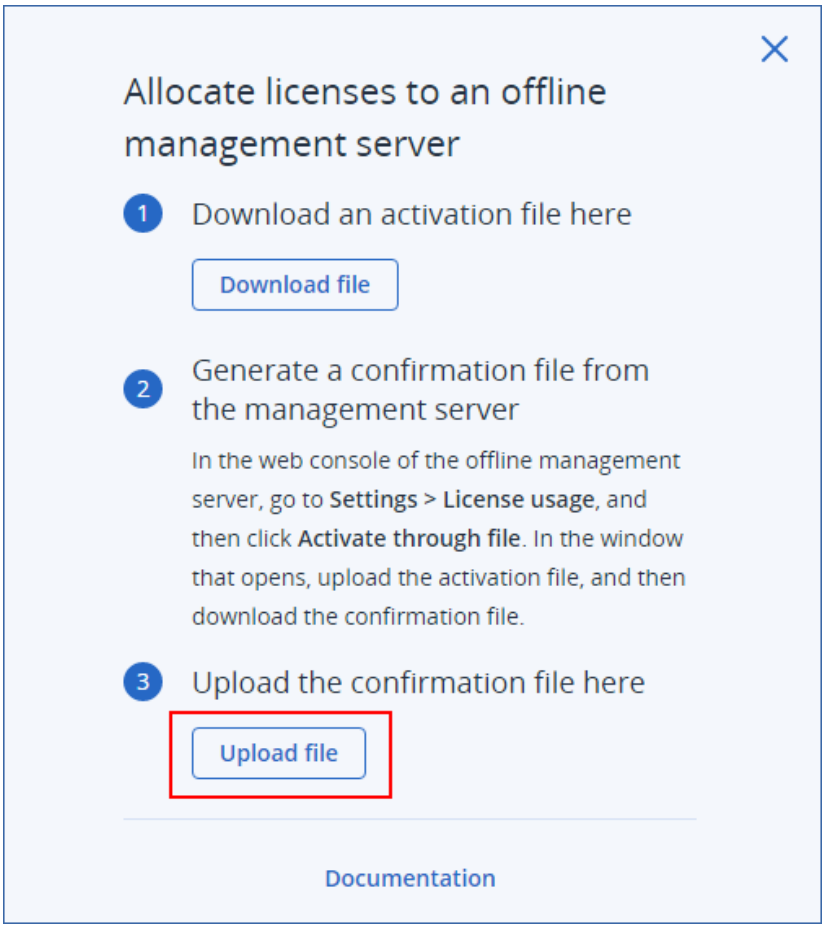


7. 在打开的对话框中，单击**下载确认文件**。



确认文件将下载到您的计算机上。

8. 在云中控台 (https://cloud.acronis.com) 中，依次单击**设置** > **许可证使用情况**。
9. 导航到要为其分配许可证的管理服务器，然后单击**分配许可证**。
10. 在打开的对话框中，单击**保存**，而不更改任何设置。
11. 在**将许可证分配给离线管理服务器**对话框中，单击**上传文件**，然后选择从离线管理服务器下载的确认文件。



结果，许可信息将在您的 Acronis 帐户和离线管理服务器之间同步。

重要事项
如果修改后的许可证配额小于保护代理程序的数量，则负载最少的代理程序将停止工作。此选择是自动的。如果该操作不符合您的需要，请手动重新指派可用许可证。

为工作负载指派许可证

管理服务器会在此服务器上注册的工作负载之间分发已分配的许可证。

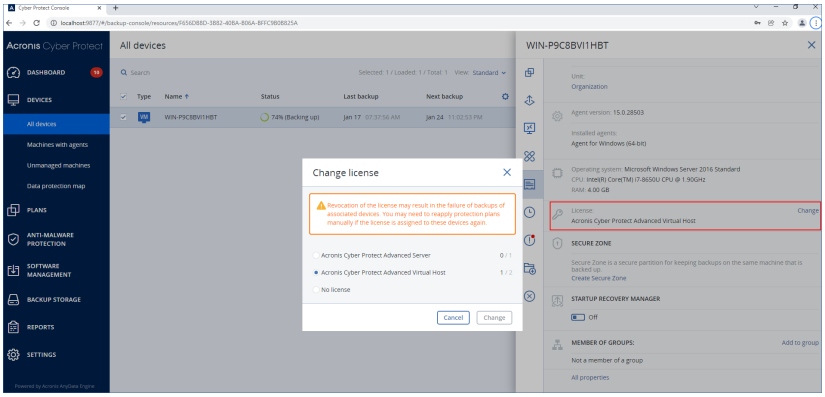
首次将保护计划应用于该工作负载时，管理服务器会向工作负载指派许可证。如果为管理服务器分配了多个许可证，则它会根据工作负载的类型、操作系统和所需的保护级别为工作负载指派最合适的许可证。

要检查已指派的许可证，请在管理服务器的 Web 中控台中，选择所需的工作负载，然后单击**详细信息**。

将许可证手动重新指派给工作负载

1. 在管理服务器的 Web 中控台中，单击**设备**，然后选择所需的工作负载。
2. 单击**详细信息**。
3. [对于本地管理服务器] 导航到**许可证**部分，然后单击**更改**。
4. [对于云管理服务器] 导航到**服务配额**部分，然后单击**更改**。

5. 选择所需许可证(服务配额),然后单击**更改**。



限制

对于离线管理服务器,许可证配额的当前使用情况仅会显示在本地中控台中。离线管理服务器不会将此数据同步到您的 Acronis 帐户,并且它在云中控台中不可用。

已知问题

在云中控台中,可能不会正确地显示**虚拟主机**许可证的许可证使用情况或指派。有关详细信息,请参阅此知识库文章。

注销管理服务器

注销在线管理服务器

1. 在云中控台 (https://cloud.acronis.com) 中,依次单击**设置** > **许可证使用情况**。
2. 导航到所需管理服务器,然后单击**注销**。
3. **注销管理服务器**窗口即会显示。
4. 输入与帐户关联的电子邮件地址以确认注销。
5. 单击**注销**。

因此,分配给已注销服务器的所有许可证都将被释放,并可以分配给帐户中的另一个管理服务器。在已注销管理服务器的本地中控台中,许可证重置为零。

注销离线管理服务器

有两个不同的入口点可用于注销脱机管理服务器:

在本地中控台中:

1. 在本地中控台中,单击显示帐户的行上的**注销**。**注销管理服务器**窗口即会显示。
2. 在**登录名**字段中,键入与本地管理员相关联的电子邮件地址。
3. 单击**注销**。
4. **注销成功**弹出屏幕即会显示。
5. 单击**下载注销文件**。
6. 在云中控台中,单击**注销**。**注销管理服务器**窗口即会显示。
7. 单击**注销脱机管理服务器**。**注销脱机管理服务器**窗口即会显示。

8. 单击**浏览**，然后选择从本地中控台下载的注销文件。
9. 单击**注销**。

在云中控台中：

1. 在可以访问 Internet 的计算机上，登录到云中控台 (https://cloud.acronis.com)，然后依次单击**设置** > **许可证使用情况**。
2. 导航到所需管理服务器，然后单击**注销**。**注销管理服务器**窗口即会显示。
3. 单击**注销脱机管理服务器**。**注销脱机管理服务器**窗口即会显示。
4. 在要注销的管理服务器(https://<管理服务器的 IP 地址>:<端口>)的本地中控台中，转到**设置** > **许可证使用情况**，然后单击**注销**。注销文件即会下载到您的计算机上。
5. 在云中控台中，返回到**注销脱机管理服务器**窗口。
6. 单击**浏览**，然后选择从本地中控台下载的注销文件。
7. 单击**注销**。
8. 或者，如果您无权访问装有管理服务器的计算机，请单击**我无权访问装有管理服务器的计算机**。

警告！
此计算机将被永久阻止并从您的帐户中删除。您将无法在其上再次注册管理服务器。

因此，分配给已注销服务器的所有许可证都将被释放，并可以分配给帐户中的另一个管理服务器。在已注销管理服务器的本地中控台中，许可证重置为零。

在 Acronis 安克诺斯数据保护软件 15 更新 2 及更早版本中许可

要开始使用 Acronis 安克诺斯数据保护软件 15 更新 2 及更早版本，需要向管理服务器添加至少一个许可号。应用保护计划时，将自动向计算机指派许可证。

还可以手动指派和吊销许可。只有组织管理员才可以对许可执行手动操作。有关管理员的详细信息，请参阅 "单位和管理帐户"(第 547 页)。

将许可号添加到管理服务器

在 Acronis 安克诺斯数据保护软件 15 更新 2 及更早版本中，将许可号添加到管理服务器。

将许可号添加到管理服务器

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **许可证**。
2. 单击**添加密钥**。
3. 输入一个或多个许可号，每行一个密钥。
4. 单击**添加**。
5. [添加订阅许可密钥时] 要激活订阅许可，请登录到您的 Acronis 帐户。
   a. 在登录表单中，输入您用于 Acronis 客户门户 (https://account.acronis.com) 的凭据，然后单击**登录**。

b. 确认您的帐户，然后单击**同步**。

c. 操作完成后，单击**完成**。

6. 在**添加许可号**面板中，单击**完成**。

注意

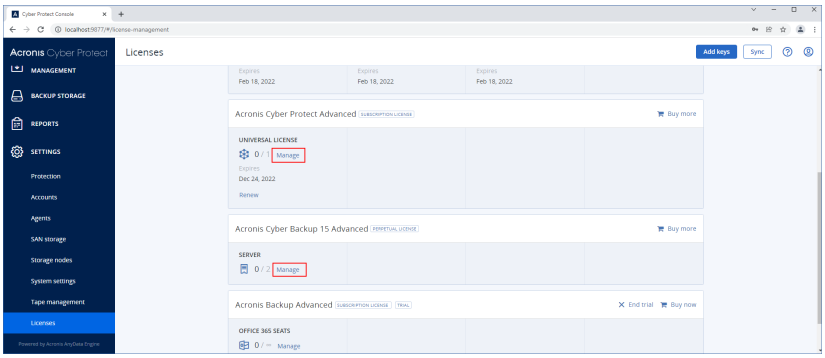
可以自动导入在 Acronis 帐户中注册的订阅许可密钥，而不是再次将它们添加到管理服务器。要导入许可号，请在**添加许可号**面板中，单击**与 Acronis 帐户同步**，然后登录到您的 Acronis 帐户。

管理订购许可证

在将许可证指派给工作负载之前，必须先将许可号添加到管理服务器。有关如何执行此操作的详细信息，请参阅 "将许可号添加到管理服务器"(第 39 页)。

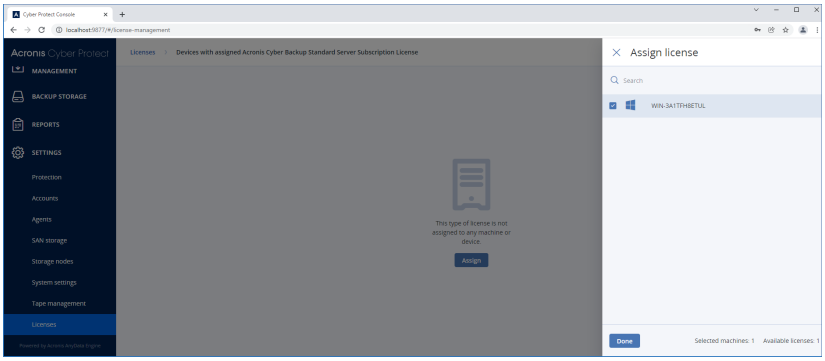
将订阅许可指派给工作负载

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **许可证**。
2. 导航到所需的许可证，然后单击**管理**。



3. 单击**指派**。

将显示可以为其指派此许可证的工作负载。



4. 选择一个工作负载，然后单击**完成**。

吊销工作负载中的订阅许可

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **许可证**。
2. 导航到所需的许可证，然后单击**管理**。

将显示为其指派了此许可证的所有工作负载。

3. 选择要吊销其中许可证的工作负载。

4. 单击**吊销**。
5. 确认您的决定。

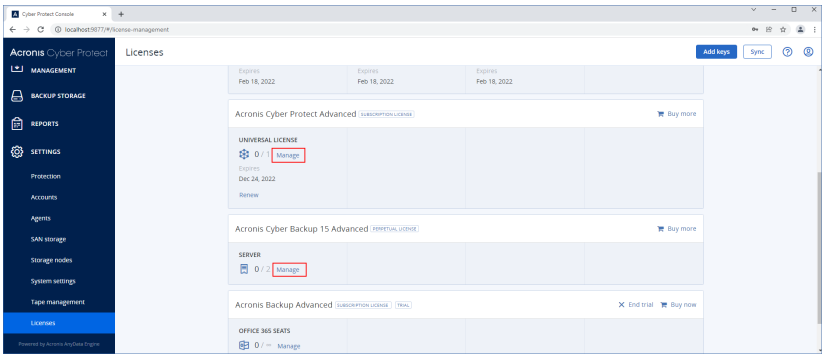
   吊销的许可证会被释放，可以将其指派给另一个工作负载。

管理永久性许可证

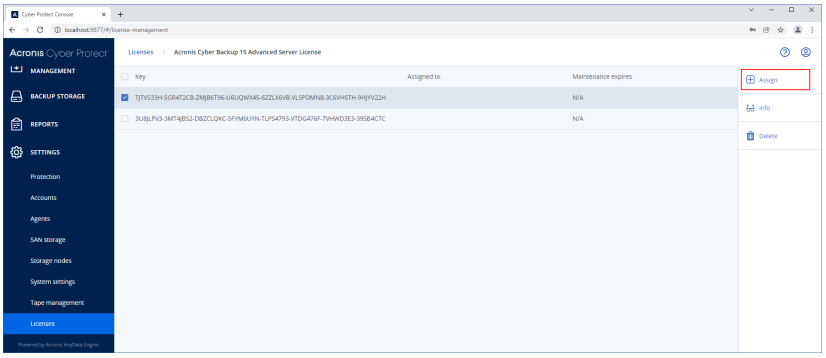
在将许可证指派给工作负载之前，必须先将许可号添加到管理服务器。有关如何执行此操作的详细信息，请参阅 "将许可号添加到管理服务器"(第 39 页)。

将永久许可指派给工作负载

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **许可证**。
2. 导航到所需的许可证，然后单击**管理**。



   将显示对应于选定许可证的许可号。
3. 选择要指派给工作负载的许可号。
4. 单击**指派**。



   将显示可以为其指派此许可号的工作负载。
5. 选择一个工作负载，然后单击**完成**。

吊销工作负载中的永久许可

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **许可证**。
2. 选择所需许可证，然后单击**管理**。

   将显示对应于选定许可证的许可号。在**已指派到**列中，查看为其指派了此许可号的工作负载。
3. 选择要吊销的许可号。
4. 单击**吊销**。

5. 确认您的决定。

   吊销的许可号会保留在许可证列表中，可以将其指派给另一个工作负载。

安装

安装概述

Acronis 安克诺斯数据保护软件 支持两种部署方法:本地部署和云部署。两者之间的主要区别在于 Acronis 安克诺斯数据保护软件 管理服务器的位置。

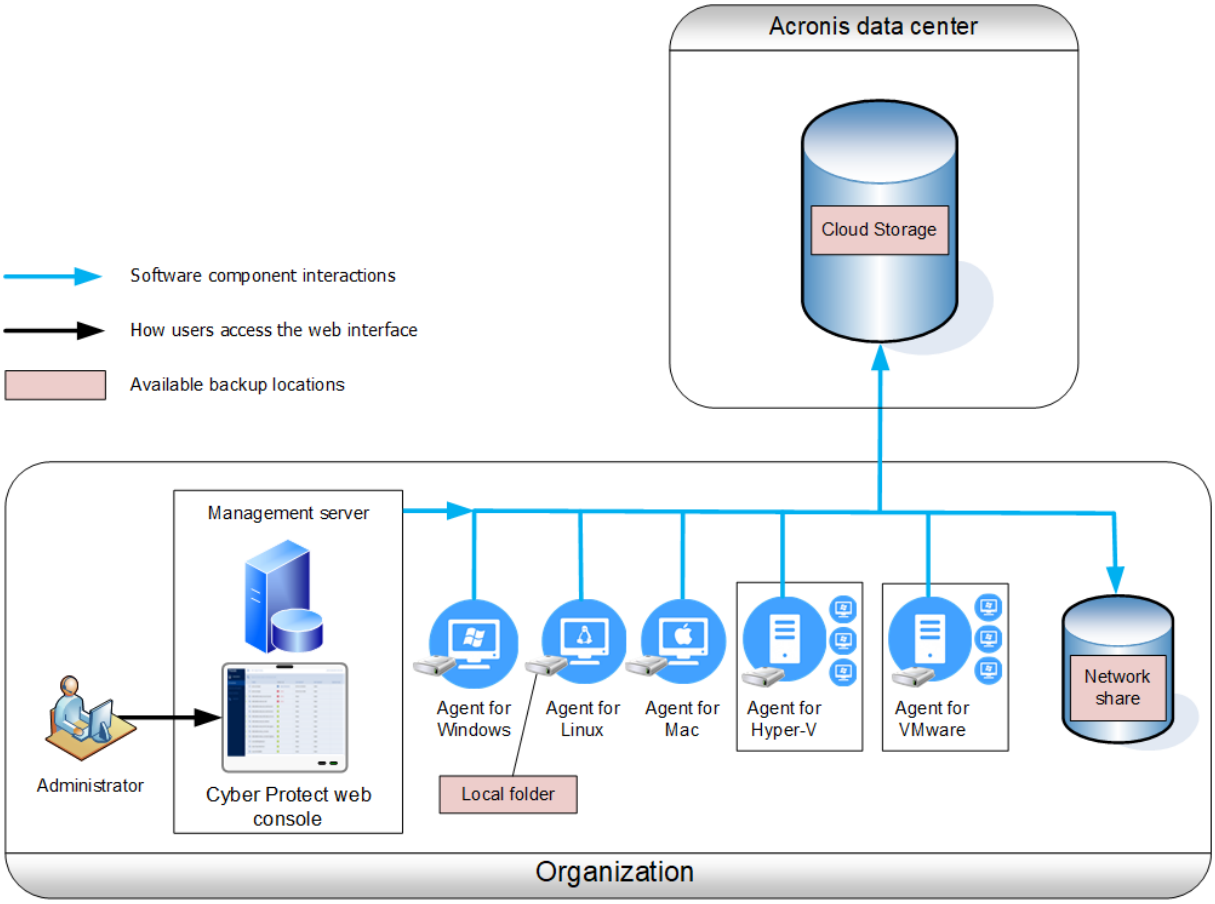
管理服务器是管理您所有备份的中心点。使用本地部署时,它会安装在本地网络中;使用云部署时,它会位于一个 Acronis 数据中心中。该服务器的 Web 界面名为 安克诺斯数据保护软件 Web 中控台。

管理服务器负责与保护代理程序进行通信,并执行总体计划管理功能。在每次保护活动之前,代理程序都会参考管理服务器来验证先决条件。有时,与管理服务器的连接可能会丢失,这将妨碍部署新的保护计划。但是,如果已将保护计划部署到计算机,则在与管理服务器的通信丢失后,代理程序将继续为操作提供 30 天的保护。

这两种类型的部署都需要将保护代理程序安装在要备份的每台计算机上。支持的存储类型也都相同。云存储空间与 Acronis 安克诺斯数据保护软件 许可证分开出售。

本地部署

本地部署意味着所有产品组件都安装在本地网络上。只有此部署方法适用于永久性许可证。此外,当您的计算机未连接到 Internet 时,也只能使用此方法。



管理服务器位置

您可以在运行 Windows 或 Linux 的计算机上安装管理服务器。

建议在 Windows 中执行安装，因为可以通过管理服务器将代理程序部署到其他计算机。使用高级许可证时，可以创建组织结构单元并向其中添加管理员。这样，您就可以将保护管理委派给访问权限严格限制在对应单元内的其他人员。

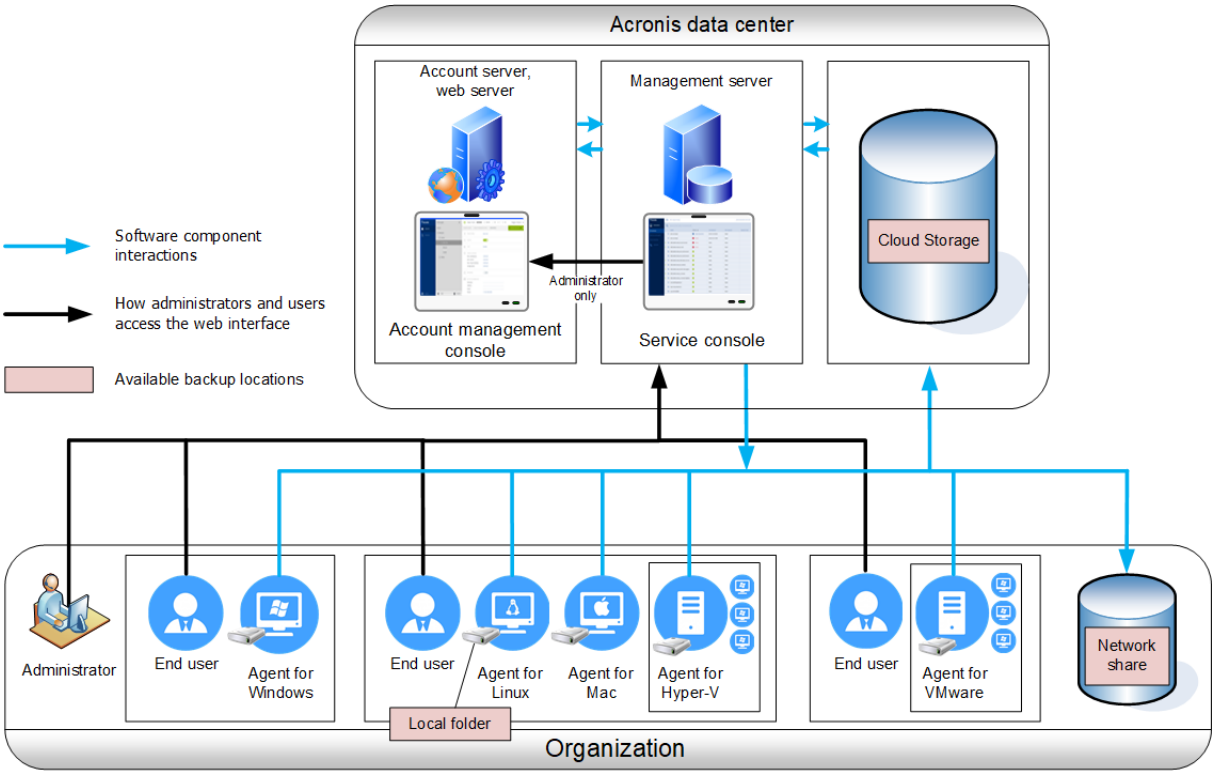
如果在仅具有 Linux 的环境中，则建议在 Linux 中执行安装。需要在要备份的计算机上以本地方式安装代理程序。

云部署

云部署意味着管理服务器位于其中一个 Acronis 数据中心中。此方法的好处是无需维护本地网络中的管理服务器。可以将 Acronis 安克诺斯数据保护软件 视为 Acronis 向您提供的网络安全保护服务。

对帐户服务器的访问权限使您可以创建用户帐户、为帐户设置服务使用量配额以及创建用户组(单元)来反映组织的结构。每一位用户都可以访问 安克诺斯数据保护软件 Web 中控台、下载所需代理程序，然后只需花几分钟的时间就可以将它安装在计算机上。

可以在单元级别或组织级别创建管理员帐户。每一个帐户都具有范围受限在其控制区域的视图。用户仅有权访问自己的备份。



下表汇总了本地部署和云部署之间的区别。每列会列出仅在相应部署类型中可用的功能。

本地部署	云部署
• 可以使用永久性许可证 • 可用于气隙环境* 的本地管理服务器 • SFTP 服务器即备份位置 • Acronis Cyber Infrastructure 即备份位置 • 磁带设备和 Acronis 存储节点即备份位置** • 从以前版本的 Acronis 安克诺斯数据保护软件 (包括适用于 VMware 的 Acronis) 升级	• Microsoft 365 数据的云到云备份，包括对组、公用文件夹、OneDrive*** 和 SharePoint Online 数据的保护 • Google Workspace 数据的云到云备份 • 适用于 Mac 的代理程序支持 x64 和基于 ARM 的处理器(如 Apple Silicon M1 和 M2) • 适用于 Virtuozzo 的代理程序(在虚拟机监控程序级别上备份 Virtuozzo 虚拟机) • 适用于 oVirt 的代理程序(在虚拟机监控程序级别上备份 oVirt KVM 虚拟机) • 适用于 Virtuozzo Hybrid Infrastructure 的代理程序(在虚拟机监控程序级别上备份 Virtuozzo Hybrid Infrastructure 虚拟机) • 灾难恢复即云服务****

* 有关激活气隙环境中的管理服务器的详细信息，请参阅 "激活离线管理服务器"(第 27 页)。

** 该功能在标准版中不提供。

***默认情况下，OneDrive 根文件夹不包含在备份操作中。如果选择备份特定的 OneDrive 文件和文件夹，将备份它们。在该设备上不可用的文件将在存档中有无效的内容。

**** 该功能仅与灾难恢复附加组件一起提供。

组件

代理程序

代理程序是在由 Acronis 安克诺斯数据保护软件 管理的计算机上执行数据备份、恢复及其他操作的应用程序。

适用于 Windows 的代理程序会随用于 Exchange 的代理程序、适用于 SQL 的代理程序、适用于 Active Directory 的代理程序以及适用于 Oracle 的代理程序一起安装。例如，如果您安装适用于 SQL 的代理程序，您将能够备份安装了代理程序的整台计算机。

某些代理程序只能安装在具有特定角色或应用程序的计算机上，例如，适用于 Hyper-V 的代理程序安装在运行 Hyper-V 角色的计算机上，适用于 SQL 的代理程序 - 在运行 SQL 数据库的计算机上，用于 Exchange 的代理程序 - 在运行 Microsoft Exchange Server 的邮箱角色的计算机上以及适用于 Active Directory 的代理程序 - 在域控制器上。

根据要备份的内容选择代理程序。下表总结了帮助您进行决策的信息。

您要备份哪些内容?	要安装哪些代理程序?	在哪里安装它?	代理程序可用性	
			本地	Cloud

物理机				
运行 Windows 的物理机上的磁盘、卷和文件	适用于 Windows 的代理程序	在将备份的计算机上。	+	+
运行 Linux 的物理机上的磁盘、卷和文件	适用于 Linux 的代理程序		+	+
运行 macOS 的物理机上的磁盘、卷和文件	适用于 Mac 的代理程序		+	+
应用程序				
SQL 数据库	适用于 SQL 的代理程序	在运行 Microsoft SQL Server 的计算机上。	+	+
Exchange 数据库和邮箱	适用于 Exchange 的代理程序	在运行 Microsoft Exchange Server 的邮箱角色的计算机上。* 如果需要邮箱备份，则可以在对运行 Microsoft Exchange Server 客户端访问角色的计算机具有网络访问权限的任意 Windows 计算机上安装代理程序。	+	+ 无邮箱备份
Microsoft 365 邮箱	适用于 Office 365 的代理程序	在连接到 Internet 的 Windows 计算机上。	+	+
运行 Active Directory 域服务的计算机	适用于 Active Directory 的代理程序	在域控制器上。	+	+
运行 Oracle 数据库的计算机	适用于 Oracle 的代理程序	在运行 Oracle 数据库的计算机上。	+	-
虚拟机				
VMware ESXi 虚拟机	适用于 VMware 的代理程序 (Windows)	在对 vCenter 服务器和虚拟机存储具有网络访问权限的 Windows 计算机上。**	+	+
	适用于 VMware 的代理程序(虚拟	在 ESXi 主机上。	+	+

	设备)			
Hyper-V 虚拟机	适用于 Hyper-V 的代理程序	在 Hyper-V 主机上。	+	+
Scale Computing HC3 虚拟机	适用于 Scale Computing HC3 的代理程序	在 Scale Computing HC3 主机上。	+	+
在 Windows Azure 上托管的虚拟机	与物理机的情况相同***	在将备份的计算机上。	+	+
在 Amazon EC2 上托管的虚拟机			+	+
Citrix XenServer 虚拟机			+****	+
Red Hat Virtualization (RHV/RHEV) 虚拟机				
基于内核的虚拟机 (KVM)				
Oracle 虚拟机				
Nutanix AHV 虚拟机				
移动设备				
运行 Android 的移动设备	适用于 Android 的移动应用	在将备份的移动设备上。	-	+
运行 iOS 的移动设备	适用于 iOS 的移动应用		-	+

*在安装过程中，用于 Exchange 的代理程序会对该代理程序将要在其上运行的计算机检查是否具有足够的可用空间。在粒度恢复期间，临时需要的可用空间为最大 Exchange 数据库的 15%。

**如果 ESXi 使用 SAN 连接存储，则在连接至相同 SAN 的计算机上安装代理程序。代理程序将直接从存储备份虚拟机，而不是通过 ESXi 主机和 LAN。有关详细说明，请参阅“无需 LAN 的备份”。

***如果虚拟机由外部代理程序进行备份，则将该虚拟机视为虚拟。如果代理程序安装在来宾操作系统中，则备份和恢复操作与物理机的操作相同。但是，当在云部署中设置计算机数量的配额时，将计算机视为虚拟。

****使用 Acronis 安克诺斯数据保护软件 高级虚拟主机许可证时，这些虚拟机会被视为虚拟设备(按主机使用许可)。使用 Acronis 安克诺斯数据保护软件 虚拟主机许可证时，这些虚拟机会被视为物理设备(按计算机使用许可)。

其他组件

组件	功能	在哪里安装它?	可用性	
			本地	Cloud
管理服务器	管理服务器集中管理您的所有备份。使用本地部署时，它会在本地网络中。 它管理代理程序并向用户提供 Web 界面。	在运行 Windows 或 Linux 的计算机上。	+	-
Components for Remote Installation	将代理程序安装包保存到本地文件夹。	在运行管理服务器的 Windows 计算机上。	+	-
扫描服务	对云存储、本地文件夹或网络文件夹中的备份启用防恶意软件扫描的可选组件。 扫描服务需要 Microsoft SQL Server 或 PostgreSQL 数据库。它与管理服务器使用的默认 SQLite 数据库不兼容。	在运行管理服务器的 Windows 或 Linux 计算机上。	+	-
可启动媒体生成器	创建可启动媒体。	在运行 Windows 或 Linux 的计算机上。	+	-
命令行工具	通过 **acrocmd** 实用程序支持命令行界面。**acrocmd** 不包含实际执行命令的任何工具。它仅向 安克诺斯 数据保护软件 组件 (代理程序和管理服务器) 提供命令行界面。	在运行 Windows、Linux 或 macOS 的计算机上。	+	+
安克诺斯数据保护软件 15监视器	为适用于 Windows 的代理程序和适用于 Mac 的代理程序提供图形用户界面。它会显示有关已安装代理	在运行 Windows 或 macOS 的计算机上。	+	+

	程序的计算机的保护状态信息，并允许其用户配置备份加密和代理服务器设置。 在 Windows 中，安克诺斯数据保护软件 15 监视器要求将适用于 Windows 的代理程序安装在同一台计算机上。			
存储节点	存储备份。它是编录和重复数据删除所必需的。 存储节点要求将适用于 Windows 的代理程序安装在同一台计算机上。	在运行 Windows 的计算机上。	+	-
目录服务	在存储节点上执行备份编录。	在运行 Windows 的计算机上。	+	-
PXE 服务器	使启动计算机可以通过网络进入可启动媒体。	在运行 Windows 的计算机上。	+	-

将 Acronis 安克诺斯数据保护软件 与您环境中的其他安全解决方案一起使用

可以单独使用 Acronis 安克诺斯数据保护软件，也可以将其与您环境中的其他安全解决方案(例如，独立防病毒软件)一起使用。

在没有其他安全解决方案的情况下，可以将 Acronis 安克诺斯数据保护软件 用于全面网络安全保护，也可以用于传统备份和恢复，具体取决于您的许可证和需求。有关使用每个许可证时可用功能的详细信息，请参阅“Acronis 安克诺斯数据保护软件 15 版本比较，包括云部署”。可以通过仅启用所需模块，来调整保护计划的范围。

可以选择将 Acronis安克诺斯数据保护软件 用于全面网络安全保护(包括防范病毒和其他恶意软件)，即使您的环境中已有其他安全解决方案。在这种情况下，需要禁用或删除其他安全解决方案，以避免冲突。

或者，您可能希望在不禁用或删除当前安全解决方案的情况下增强网络安全保护。这也可以 - 只需确保在保护计划中不使用防病毒和反恶意软件模块。所有其他模块均可自由使用。

限制

- 备份的反恶意软件扫描要求您在安装 安克诺斯数据保护软件 管理服务器时安装扫描服务。
- 仅当 管理服务器安装在运行 Linux 的计算机上时，才可以通过 HTML5 客户端远程访问。

软件要求

支持的 Web 浏览器

Web 界面支持以下 Web 浏览器：

- Google Chrome 29 或更高版本
- Mozilla Firefox 23 或更高版本
- Opera 16 或更高版本
- Windows Internet Explorer 10 或更高版本

注意
在云部署中，不支持 Internet Explorer。

- Microsoft Edge 25 或更高版本
- 在 macOS 和 iOS 操作系统中运行的 Safari 8 或更高版本

在其他 Web 浏览器（包括在其他操作系统中运行的 Safari 浏览器），用户界面可能显示错误，或者某些功能可能不可用。

支持的操作系统和环境

代理程序

适用于 Windows 的代理程序

- Windows XP Professional SP1 (x64)、SP2 (x64)、SP3 (x86)
- Windows XP Professional SP2 (x86) – 通过适用于 Windows 的代理程序特殊版受支持对于此支持的详细信息和限制，请参阅"适用于 Windows XP SP2 的代理程序"。
- Windows XP Embedded SP3
- Windows Server 2003 SP1/2003 R2 及更高版本 – Standard 和 Enterprise 版（x86、x64）

注意
Acronis 安克诺斯数据保护软件 需要安装 Microsoft 的 KB940349 更新，该更新无法单独下载。为了确保源自 KB940349 的功能在计算机上可用，请为 Windows Server 2003 安装当前可用的全部更新。
有关 KB940349 的详细信息，请参阅此知识库文章。

- Windows Small Business Server 2003/2003 R2

- Windows Server 2008 - 标准版、企业版、Datacenter 版、Foundation 版和 Web 版(x86, x64)
- Windows Small Business Server 2008
- Windows 7 - 所有版本(x86、x64)

注意

要在 Windows 7 中使用 Acronis 安克诺斯数据保护软件，必须安装 Microsoft 提供的以下更新：

- Windows 7 扩展安全更新 (ESU)
- KB4474419
- KB4490628

有关所需更新的详细信息，请参阅此知识库文章。

- Windows Server 2008 R2 – 标准版、企业版、Datacenter 版、基础版和 Web 版
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – 所有版本
- Windows 8/8.1 – 除 Windows RT 版以外的所有版本(x86、x64)
- Windows Server 2012/2012 R2 – 所有版本
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 - 家庭版、专业版、教育版、企业版、IoT 企业版和 LTSC(以前称为 LTSB)版
- Windows Server 2016 - 所有安装选项，Nano Server 除外
- Windows Server 2019 - 所有安装选项，Nano Server 除外
- Windows 11 - 所有版本
- Windows Server 2022 - 所有安装选项，Nano Server 除外

适用于 SQL 的代理程序、适用于 Exchange 的代理程序(针对数据库备份和应用程序感知备份)和适用于 Active Directory 的代理程序

这些代理程序中的每一个都可以安装在运行以上所列任一操作系统以及相应的受支持应用程序版本的计算机上，但以下情况除外：

- 适用于 SQL 的代理程序不支持本地部署在 Windows 7 简易版和家庭版(x86, x64)上

适用于 Exchange 的代理程序(针对邮箱备份)

该代理程序可安装在带或不带 Microsoft Exchange Server 的计算机上。

- Windows Server 2008 - 标准版、企业版、Datacenter 版、Foundation 版和 Web 版(x86, x64)
- Windows Small Business Server 2008
- Windows 7 - 所有版本
- Windows Server 2008 R2 – 标准版、企业版、Datacenter 版、基础版和 Web 版
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – 所有版本
- Windows 8/8.1 – 除 Windows RT 版以外的所有版本(x86、x64)
- Windows Server 2012/2012 R2 – 所有版本

- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10 – 家庭版、专业版、教育版和企业版
- Windows Server 2016 - 所有安装选项，Nano Server 除外
- Windows Server 2019 - 所有安装选项，Nano Server 除外
- Windows 11 - 所有版本
- Windows Server 2022 - 所有安装选项，Nano Server 除外

适用于 Office 365 的代理程序

- Windows Server 2008 - 标准版、企业版、Datacenter 版、Foundation 版和 Web 版（仅 x64）
- Windows Small Business Server 2008
- Windows Server 2008 R2 – 标准版、企业版、Datacenter 版、基础版和 Web 版
- Windows Home Server 2011
- Windows Small Business Server 2011 – 所有版本
- Windows 8/8.1 – 除 Windows RT 版之外的所有版本（仅 x64）
- Windows Server 2012/2012 R2 – 所有版本
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016（仅 x64）
- Windows 10 – 家庭版、专业版、教育版和企业版（仅 x64）
- Windows Server 2016 – 除 Nano Server 之外的所有安装选项（仅 x64）
- Windows Server 2019 – 除面向 Nano Server 之外的所有安装选项（仅 x64）
- Windows 11 - 所有版本
- Windows Server 2022 - 所有安装选项，Nano Server 除外

适用于 Oracle 的代理程序

- Windows Server 2008R2 - 标准版、企业版、Datacenter 版和 Web 版（x86、x64）
- Windows Server 2012R2 - 标准版、企业版、Datacenter 版和 Web 版（x86、x64）
- Linux - 受适用于 Linux 的代理程序支持的任何内核和发行版（以下所列）

适用于 Linux 的代理程序

注意
以下 Linux 发行版和内核版本已经过专门测试。但是，即使您的 Linux 发行版或内核版本未在下面列出，由于 Linux 操作系统的特殊性，它仍然可以在所有必需的场景中正常工作。

如果您在结合 Linux 发行版和内核版本使用 Acronis 安克诺斯数据保护软件 时遇到问题，请联系支持团队以进一步调查。

包含从 2.6.9 到 5.19 以及 glibc 2.3.4 或更高版本内核的 Linux，包括以下 x86 和 x86_64 发行版：

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31

- SUSE Linux Enterprise Server 10, 11, 12, 15

  重要事项
  SUSE Linux Enterprise Server 12 和 SUSE Linux Enterprise Server 15 不支持配置 Btrfs。

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– Unbreakable Enterprise Kernel 和 Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*、8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

在不使用 RPM 包管理器的系统(如 Ubuntu 系统)中安装产品之前,需要手动安装此管理器;例如,以根用户身份运行以下命令:`apt-get install rpm`

如果您的 Linux 发行版不支持 D-Bus 机制(例如,Red Hat Enterprise Linux 6.x 或 CentOS 6.x),则由于操作系统不提供 D-Bus 兼容位置,因此 Acronis 安克诺斯数据保护软件 将使用默认位置来存储安全密钥。

* 仅支持从 4.18 到 5.19 的内核

适用于 Mac 的代理程序

注意
不支持基于 ARM 的处理器,如 Apple Silicon M1 和 M2。

- OS X Mavericks 10.9
- OS X Yosemite 10.10
- OS X El Capitan 10.11
- macOS Sierra 10.12
- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13

适用于 VMware 的代理程序(虚拟设备)

此代理程序作为在 ESXi 主机上运行的虚拟设备交付。

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

适用于 VMware 的代理程序 (Windows)

该代理程序作为 Windows 应用程序提供，用于在适用于 Windows 的代理程序的上述任意操作系统中运行，但以下情形除外：

- 32 位操作系统不受支持。
- Windows XP、Windows Server 2003/2003 R2 和 Windows Small Business Server 2003/2003 R2 不受支持。

适用于 Hyper-V 的代理程序

- Windows Server 2008(包含 Hyper-V 角色，仅限 x64) ，包括 Server Core 安装模式
- Windows Server 2008 R2(包含 Hyper-V 角色) ，包括 Server Core 安装模式
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2(包含 Hyper-V 角色) ，包括 Server Core 安装模式
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8、8.1(包含 Hyper-V，仅限 x64)
- Windows 10(包含 Hyper-V) - 专业版、教育版和企业版
- Windows Server 2016(包含 Hyper-V 角色) - 所有安装选项，Nano Server 除外
- Microsoft Hyper-V Server 2016
- Windows Server 2019(包含 Hyper-V 角色) – 所有安装选项，Nano Server 除外
- Microsoft Hyper-V Server 2019
- Windows Server 2022(包含 Hyper-V) – 所有安装选项，Nano Server 除外

适用于 Scale Computing HC3 的代理程序(虚拟设备)

该代理程序作为虚拟设备交付，通过 安克诺斯数据保护软件 Web 中控台部署在 Scale Computing HC3 群集中。该代理程序没有独立的安装程序。

Scale Computing Hypercore 8.8、8.9、9.0

管理服务器(仅适用于本地部署)

在 Windows 中

- Windows 7 - 所有版本(x86、x64)

注意

要在 Windows 7 中使用 Acronis 安克诺斯数据保护软件，必须安装 Microsoft 提供的以下更新：

- Windows 7 扩展安全更新 (ESU)
- KB4474419
- KB4490628

有关所需更新的详细信息，请参阅此知识库文章。

- Windows Server 2008 R2 - 标准版、企业版、Datacenter 版和基础版
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – 所有版本
- Windows 8/8.1 – 除 Windows RT 版以外的所有版本(x86、x64)
- Windows Server 2012/2012 R2 – 所有版本
- Windows Storage Server 2008 R2/2012/2012 R2/2016
- Windows 10 - 家庭版、专业版、教育版、企业版、IoT 企业版和 LTSC(以前称为 LTSB) 版
- Windows Server 2016 - 所有安装选项 , Nano Server 除外
- Windows Server 2019 - 所有安装选项 , Nano Server 除外
- Windows 11 - 所有版本
- Windows Server 2022 - 所有安装选项 , Nano Server 除外

在 Linux 中

注意
以下 Linux 发行版和内核版本已经过专门测试。但是 , 即使您的 Linux 发行版或内核版本未在下面列出 , 由于 Linux 操作系统的特殊性 , 它仍然可以在所有必需的场景中正常工作。

如果您在结合 Linux 发行版和内核版本使用 Acronis 安克诺斯数据保护软件 时遇到问题 , 请联系支持团队以进一步调查。

包含从 2.6.9 到 5.19 以及 glibc 2.3.4 或更高版本内核的 Linux, 包括以下 x86_64 发行版。

不支持 x86 发行版。

- Red Hat Enterprise Linux 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

  重要事项
  SUSE Linux Enterprise Server 12 和 SUSE Linux Enterprise Server 15 不支持配置 Btrfs。

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– Unbreakable Enterprise Kernel 和 Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*、8.5*

- Rocky Linux 8.4*
- ALT Linux 7.0

在不使用 RPM 包管理器的系统(如 Ubuntu 系统)中安装产品之前,需要手动安装此管理器;例如,以根用户身份运行以下命令:`apt-get install rpm`

如果您的 Linux 发行版不支持 D-Bus 机制(例如,Red Hat Enterprise Linux 6.x 或 CentOS 6.x),则由于操作系统不提供 D-Bus 兼容位置,因此 Acronis 安克诺斯数据保护软件 将使用默认位置来存储安全密钥。

* 仅支持从 4.18 到 5.19 的内核

存储节点(仅适用于本地部署)

- Windows Server 2008 - 标准版、企业版、Datacenter 版和 Foundation 版(仅 x64)
- Windows Small Business Server 2008
- Windows 7 - 所有版本(仅 x64)
- Windows Server 2008 R2 - 标准版、企业版、Datacenter 版和 Foundation 版
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – 所有版本
- Windows 8/8.1 – 除 Windows RT 版之外的所有版本(仅 x64)
- Windows Server 2012/2012 R2 – 所有版本
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016
- Windows 10 – 家庭版、专业版、教育版、企业版和 IoT 企业版
- Windows Server 2016 - 所有安装选项,Nano Server 除外
- Windows Server 2019 - 所有安装选项,Nano Server 除外
- Windows Server 2022 - 所有安装选项,Nano Server 除外

适用于 Windows XP SP2 的代理程序

适用于 Windows XP SP2 的代理程序仅支持 32 位版本的 Windows XP SP2。

要保护运行 Windows XP SP1 (x64)、Windows XP SP2 (x64) 或 Windows XP SP3 (x86) 的计算机,请使用常规适用于 Windows 的代理程序。

适用于 Windows XP SP2 的代理程序需要 Acronis Cyber Backup 12.5 许可证。不支持Acronis 安克诺斯数据保护软件15版本的许可。

安装

适用于 Windows XP SP2 的代理程序需要至少 550 MB 磁盘空间和 150 MB RAM。在备份时,代理程序通常消耗约 350 MB 的内存。峰值消耗可能达到 2 GB,具体取决于所处理数据的量。

适用于 Windows XP SP2 的代理程序仅可本地安装在要备份的计算机上。要下载代理程序安装程序,请单击右上角的帐户图标,然后单击**下载** > **适用于 Windows XP SP2 的代理程序**。

无法安装 安克诺斯数据保护软件 监视器和可启动媒体生成器。要下载可启动媒体 ISO 文件，请依次单击右上角的帐户图标 > **下载** > **可启动媒体**。

更新

适用于 Windows XP SP2 的代理程序不支持远程更新功能。要更新代理程序，请下载安装程序的新版本，然后重复安装。

如果已将 Windows XP 从 SP2 更新到 SP3，则卸载适用于 Windows XP SP2 的代理程序，然后安装常规适用于 Windows 的代理程序。

限制

- 仅可进行磁盘级别备份。个别文件可以从磁盘或卷备份中恢复。
- 按事件预定不受支持。
- 设置保护计划的执行条件不受支持。
- 仅以下备份目标受支持：
  - 云存储
  - 本地文件夹
  - 网络文件夹
  - 安全区
- **版本 12** 备份格式和需要**版本 12** 备份格式的功能不受支持。尤其是，物理数据装运不可用。如果启用了**性能和备份窗口**选项，则它仅适用于绿色级别的设置。
- 在 Web 界面中，不支持在恢复期间选择个别磁盘/卷用于恢复和手动磁盘映射。仅可在可启动媒体下使用此功能。
- 脱离主机数据处理不受支持。
- 适用于 Windows XP SP2 的代理程序无法执行以下备份操作：
  - 将备份转换为虚拟机
  - 从备份加载卷
  - 从备份提取文件
  - 导出和手动验证备份。

  您可以使用另一代理程序执行这些操作。
- 适用于 Windows XP SP2 的代理程序创建的备份无法作为虚拟机运行。

支持的 Microsoft SQL Server 版本

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

上述 SQL Server 版本的 SQL Server Express 版本也受支持。

受支持的 Microsoft Exchange Server 版本

- Microsoft Exchange Server 2019 - 所有版本。
- Microsoft Exchange Server 2016 - 所有版本。
- Microsoft Exchange Server 2013 - 所有版本，累积更新 1 (CU1) 及更高版本。
- Microsoft Exchange Server 2010 - 所有版本，所有服务包。从 Service Pack 1 (SP1) 开始，支持邮箱备份和从数据库备份中进行粒度恢复。
- Microsoft Exchange Server 2007 - 所有版本，所有服务包。不支持邮箱备份和从数据库备份中进行粒度恢复。

受支持的 Microsoft SharePoint 版本

安克诺斯数据保护软件 15 支持以下版本的 Microsoft SharePoint：

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

*为了将 SharePoint Explorer 与这些版本一起使用，您需要一个要将数据库附加到其中的 SharePoint 恢复场。

用来建立备份或数据库(您从其中提取数据)的 SharePoint 版本，必须与安装 SharePoint Explorer 的 SharePoint 版本相同。

受支持的 Oracle 数据库版本。

- Oracle 数据库版本 11g，所有版本
- Oracle 数据库版本 12c，所有版本。

仅支持单个实例配置。

受支持的 SAP HANA 版本

在物理机或 VMware ESXi 虚拟机上运行的 RHEL 7.6 中安装的 HANA 2.0 SPS 03。

由于 SAP HANA 不支持使用存储快照恢复多租户数据库容器，因此该解决方案仅支持具有一个租户数据库的 SAP HANA 容器。

所支持的虚拟化平台

下表概述了支持何种虚拟化平台。

注意

以下通过**从来宾操作系统内部进行备份**方法支持的虚拟机监控程序供应商和版本已经过专门测试。但是，即使您使用下面未列出的版本从供应商或虚拟机监控程序运行虚拟机监控程序，**从来宾操作系统内部进行备份**方法仍然可以在所有必需的场景中正常工作。

如果在将 Acronis安克诺斯数据保护软件 与虚拟机监控程序供应商和版本结合使用时遇到问题，请联系支持团队以进一步调查。

平台	Hypervisor 级别备份(无代理备份)	从来宾操作系统内部进行备份
VMware		
VMware vSphere 版本：4.1、5.0、5.1、5.5、6.0、6.5、6.7、7.0、8.0 **VMware vSphere 版本：** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (Free ESXi)**		+
VMware Server(VMware 虚拟服务器) VMware Workstation VMware ACE VMware Player		+
Microsoft* **		
Windows Server 2008 (x64)(包含 Hyper-V) Windows Server 2008 R2 (包含 Hyper-V) Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2(包含 Hyper-V) Microsoft Hyper-V Server 2012/2012 R2 Windows 8、8.1 (x64)(包含 Hyper-V) Windows 10(包含 Hyper-V)	+	+

Windows Server 2016(包含 Hyper-V) - 所有安装选项，Nano Server 除外 Microsoft Hyper-V Server 2016 Windows Server 2019(包含 Hyper-V) – 所有安装选项，Nano Server 除外 Microsoft Hyper-V Server 2019 Windows Server 2022(包含 Hyper-V) – 所有安装选项，Nano Server 除外		
Microsoft Virtual PC 2004 和 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Scale Computing		
Scale Computing Hypercore 8.8、8.9、9.0	+	+
Citrix		
Citrix XenServer 4.1.5、5.5、5.6、6.0、6.1、6.2、6.5、7.0、7.1、7.2、7.3、7.4、7.5、7.6		仅完全虚拟化的 (aka HVM) 来宾。半虚拟化的 (aka PV) 来宾不受支持。
Red Hat 和 Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2、3.0、3.1、3.2、3.3、3.4、3.5、3.6 Red Hat Virtualization (RHV) 4.0、4.1		+
Red Hat Virtualization(由 oVirt 管理) 4.2、4.3、4.4 (仅可用于云部署)	+	+
基于内核的虚拟机 (KVM)		+
由运行在 Red Hat Enterprise Linux 7.6、7.7 或 CentOS 7.6、7.7 上的 oVirt 4.3 管理的基于内核的虚拟机 (KVM) (仅可用于云部署和高级许可证)	+	+
由运行在 Red Hat Enterprise Linux 8.x 或 CentOS Stream 8.x 上的 oVirt 4.4 管理的基于内核的虚拟机 (KVM) (仅可用于云部署和高级许可证)	+	+
由运行在 Red Hat Enterprise Linux 8.x 或 CentOS Stream 8.x 上的 oVirt 4.5 管理的基于内核的虚拟机 (KVM)	+	+

(仅可用于云部署和高级许可证)		
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0、3.3、3.4		仅完全虚拟化的 (aka HVM) 来宾。半虚拟化的 (aka PV) 来宾不受支持。
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x 到 20180425.x		+
Virtuozzo(仅可用于云部署)		
Virtuozzo 6.0.10、6.0.11、6.0.12	+	仅虚拟机。容器不受支持。
Virtuozzo 7.0.13、7.0.14	仅 Ploop 容器。虚拟机不受支持。	仅虚拟机。容器不受支持。
Virtuozzo Hybrid Server 7.5	+	仅虚拟机。容器不受支持。
Virtuozzo Hybrid Infrastructure(仅可用于云部署)		
Virtuozzo Hybrid Infrastructure 3.5、4.0、4.5	+	+
Amazon		
Amazon EC2 实例		+
Microsoft Azure		
Azure 虚拟机		+

***** 在这些版本中，vSphere 5.0 和更高版本上支持虚拟磁盘的 HotAdd 传输。在版本 4.1 上，备份运行速度可能缓慢。

** vSphere Hypervisor 不支持 Hypervisor 级别备份，因为该产品将远程命令行界面 (RCLI) 的访问限制为只读模式。该代理程序在 vSphere Hypervisor 评估阶段工作，无需输入序列号。输入序列号后，代理程序将停止运行。

***支持在装有 Storage Spaces Direct (S2D) 的超融合集群上运行 Hyper-V 虚拟机。Storage Spaces Direct 也支持作为备份存储。

限制

- **容错计算机**

  适用于 VMware 的代理程序仅在 VMware vSphere 6.0 和更高版本中启用了容错时才备份容错计算机。如果已从较早的 vSphere 版本升级，足以针对每台计算机禁用和启用容错。如果使用的是较早的 vSphere 版本，在来宾操作系统中安装代理程序。
- **独立磁盘和 RDM**

  适用于 VMware 的代理程序不能备份处于物理兼容模式下的原始设备映射 (RDM) 磁盘或独立磁盘。代理程序会跳过这些磁盘并向日志添加警告。通过将物理兼容模式下的独立磁盘和 RDM 排除在保护计划之外，即可避免出现这些警告。如果要备份这些磁盘或这些磁盘上的数据，请在来宾操作系统中安装代理程序。
- **传递磁盘**

  适用于 Hyper-V 的代理程序不会备份传递磁盘。在备份期间，代理程序会跳过这些磁盘并向日志添加警告。通过将传递磁盘排除在保护计划之外，即可避免出现这些警告。如果要备份这些磁盘或这些磁盘上的数据，请在来宾操作系统中安装代理程序。
- **Hyper-V 来宾群集**

  适用于 Hyper-V 的代理程序不支持备份是 Windows Server 故障转移群集节点的 Hyper-V 虚拟机。主机级别的 VSS 快照甚至可以临时断开外部仲裁磁盘与群集的连接。如果要备份这些计算机，请在来宾操作系统上安装代理程序。
- **来宾 iSCSI 连接**

  适用于 VMware 的代理程序和适用于 Hyper-V 的代理程序不会备份由在来宾操作系统中工作的 iSCSI 发起程序连接的 LUN 卷。因为 ESXi 和 Hyper-V 虚拟机监控程序未注意到此类卷，这些卷不包含在虚拟机监控程序级快照中，且会在备份中遭忽略，而不发出警告。如果要备份这些卷或这些卷上的数据，请在来宾操作系统中安装代理程序。
- **包含逻辑卷 (LVM) 的 Linux 计算机**

  适用于 VMware 的代理程序和适用于 Hyper-V 的代理程序不支持具有 LVM 的Linux 计算机的以下操作：
  - P2V 和 V2P 的迁移。使用适用于 Linux 的代理程序或可启动媒体来创建要恢复的备份和可启动媒体。
  - 从适用于 Linux 的代理程序或可启动媒体创建的备份运行虚拟机。
  - 将适用于 Linux 的代理程序或可启动媒体创建的备份转换为虚拟机。
- **加密虚拟机**(已在 VMware vSphere 6.5 中引入)
  - 加密虚拟机在未加密状态下备份。如果加密对您至关重要，请在创建保护计划时启用备份加密。
  - 恢复后的虚拟机始终处于未加密状态。完成恢复后，可手动启用加密。

- 如果备份加密的虚拟机，我们建议您还加密运行适用于 VMware 的代理程序的虚拟机。否则，使用加密计算机执行的操作可能比预期要慢。使用 vSphere Web 客户端将 **VM 加密策略**应用到代理程序计算机。
- 加密的虚拟机将通过 LAN 备份，即使您配置代理程序的 SAN 传输模式也是如此。该代理程序将回退在 NBD 传输上，因为 VMware 不支持用于备份加密虚拟磁盘的 SAN 传输。

- **安全启动**（已在 VMware vSphere 6.5 中引入）
  在虚拟机恢复为新虚拟机后，将禁用**安全启动**。完成恢复后，可手动启用此选项。
- VMware vSphere 7.0 不支持 **ESXi 配置备份**。

Linux 程序包

若要将必要的模块添加至 Linux 内核，安装程序需要以下 Linux 程序包：

- 带内核头文件或内核源的程序包。程序包版本必须与内核版本相符。
- GNU Compiler Collection (GCC) 编译器系统。GCC 版本必须是编译内核时所使用的版本。
- Make 工具。
- Perl 解释程序。
- `libelf-dev`、`libelf-devel` 或 `elfutils-libelf-devel` 库用于构建内核（最低版本为 4.15），并使用 CONFIG_UNWINDER_ORC=y 进行配置）。对于某些发行版本（例如 Fedora 28），它们需要与内核标头分开安装。

这些程序包的名称可能随 Linux 的发行版本而异。

在 Red Hat Enterprise Linux、CentOS 和 Fedora 中，通常由安装程序来安装这些程序包。在其它发行版中，如果尚未安装这些程序包或是版本不对，您需要安装所需的程序包。

是否已安装所需的程序包？

如需检查是否已安装这些程序包，请执行以下步骤：

1. 运行以下命令查找内核版本和所需的 GCC 版本：

   ```
   cat /proc/version
   ```

   此命令将返回类似以下内容的行：`Linux version 2.6.35.6` and `gcc version 4.5.1`
2. 运行以下命令，检查是否安装了 Make 工具和 GCC 编译器：

   ```
   make -v
   gcc -v
   ```

   对于 **gcc**，请确保该命令返回的版本与步骤 1 中的 `gcc version` 相同。对于 **make**，只需确保此命令运行即可。
3. 检查是否安装了用于生成内核模块的对应程序包版本：
   - 在 Red Hat Enterprise Linux、CentOS 及 Fedora 中，运行以下命令：

     ```
     yum list installed | grep kernel-devel
     ```

- 在 Ubuntu 环境下，运行以下命令：

```
dpkg --get-selections | grep linux-headers
dpkg --get-selections | grep linux-image
```

无论是哪一种情况，请确保程序包版本与步骤 1 中的 `Linux version` 相同。

4. 运行以下命令以检查是否安装了 Perl 解释程序：

```
perl --version
```

如果您能看到了关于 Perl 版本的信息，则解释程序已安装。

5. 在 Red Hat Enterprise Linux、CentOS 和 Fedora 中，运行以下命令以检查 `elfutils-libelf-devel` 是否已安装：

```
yum list installed | grep elfutils-libelf-devel
```

如果显示关于库版本的信息，则库已安装。

从存储库安装程序包

下表列出了如何在各种 Linux 发行版中安装所需的程序包。

Linux 发行版	程序包名称	如何安装
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	安装程序将使用您的 Red Hat 订购许可自动下载和安装程序包。
	perl	运行以下命令： `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	安装程序将自动下载和安装程序包。
	perl	运行以下命令： `yum install perl`
Ubuntu Debian	**linux-headers** **linux-image** **gcc** **make** **perl**	运行以下命令： `sudo apt-get update` `sudo apt-get install linux-headers-$(uname -r)` `sudo apt-get install linux-image-$(uname -r)` `sudo apt-get install gcc-<package version>`

		`sudo apt-get install make` `sudo apt-get install perl`
SUSE Linux openSUSE	**kernel-source** **gcc** **make** **perl**	sudo zypper install kernel-source sudo zypper install gcc sudo zypper install make sudo zypper install perl

将从该发行版的存储库下载这些程序包并进行安装。

对于其他 Linux 发行版，请参阅关于所需程序包确切名称和安装方法的发行版文档。

手动安装程序包

对于以下情况，您需要**手动**安装程序包：

- 计算机没有处于激活状态的 Red Hat 订购许可或不具备互联网连接。
- 安装程序找不到与内核版本对应的 **kernel-devel** 或 **gcc** 版本。如果可用的 **kernel-devel** 比您的内核时间更新，您需要更新内核或是手动安装匹配的 **kernel-devel** 版本。
- 本地网络上有所需的程序包，您不想花时间自动搜索和下载。

从本地网络或可信的第三方网站获取程序包，然后按照以下说明进行安装：

- 在 Red Hat Enterprise Linux、CentOS 或 Fedora 中，以根用户身份运行以下命令：

  ```
  rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

- 在 Ubuntu 环境下，运行以下命令：

  ```
  sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

示例：在 Fedora 14 环境下手动安装程序包

按照这些步骤在 Fedora 14 环境下将所需程序包安装到 32 位计算机上：

1. 运行以下命令，确定内核版本和所需的 GCC 版本：

   ```
   cat /proc/version
   ```

   此命令的输出内容中包括以下信息：

   ```
   Linux version 2.6.35.6-45.fc14.i686
   gcc version 4.5.1
   ```

2. 获取与此内核版本对应的 **kernel-devel** 和 **gcc** 程序包：

   ```
   kernel-devel-2.6.35.6-45.fc14.i686.rpm
   gcc-4.5.1-4.fc14.i686.rpm
   ```

3. 获取适用于 Fedora 14 的 **make** 程序包：

```
make-3.82-3.fc14.i686
```

4. 以根用户身份运行以下命令，安装程序包：

```
rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
rpm -ivh gcc-4.5.1.fc14.i686.rpm
rpm -ivh make-3.82-3.fc14.i686
```

可以在单个 `rpm` 命令中指定所有这些程序包。安装这些程序包中的任一程序包时都可能需要安装其它程序包来解析从属关系。

与加密软件的兼容性

备份和恢复由*文件级*加密软件加密的数据时不受限制。

*磁盘级*加密软件可以加密动态数据。这就是备份中包含的数据未加密的原因。磁盘级加密软件经常修改系统区域：启动记录、分区表或文件系统表。这些因素影响磁盘级别备份和恢复、恢复系统的启动能力以及对 安全区 的访问。

可备份由以下磁盘级加密软件加密的数据：

- Microsoft BitLocker Drive Encryption
- CheckPoint Harmony Endpoint
- McAfee 端点加密
- PGP Whole Disk Encryption

要确保可靠的磁盘级恢复，请遵循通用规则和特定软件建议。

通用安装规则

强烈建议您在安装保护代理程序之前先安装加密软件。

安全区 的使用方式

无法使用磁盘级加密对 安全区 进行加密。使用 安全区 的唯一方式如下：

1. 安装加密软件。
2. 安装保护代理程序。
3. 创建 安全区。
4. 加密磁盘或其卷时，排除 安全区。

常见备份规则

您可以在操作系统中进行磁盘级别备份。请勿尝试使用可启动媒体进行备份。

特定于软件的恢复过程

Microsoft BitLocker Drive Encryption 和 CheckPoint Harmony Endpoint

可以通过使用带重新启动或可启动媒体的恢复，来恢复系统。

重新启动时恢复

要恢复加密的系统，请按照 "恢复物理机"(第 271 页) 中的步骤操作。

确保满足 "重新启动时恢复"(第 276 页) 中的要求。

注意
对于 Bitlocker 加密的卷，带重新启动的恢复仅可用于运行 Windows 7 及更高版本或 Windows Server 2008 R2 及更高版本的基于 UEFI 的计算机。对于 CheckPoint 加密的卷，带重新启动的恢复仅可用于运行 Windows 10 和 Windows 11 的基于 UEFI 的计算机。

带重新启动的恢复不可用于基于 BIOS 的计算机或者运行 Linux 或 macOS 的计算机。

带可启动媒体的恢复

1. 从可启动媒体启动。
2. 恢复系统。

   重要事项
   备份的数据会恢复为未加密数据。

3. 重新启动恢复的系统。
4. 打开加密软件。

如果只需恢复多分区磁盘的一个分区，请在操作系统下执行恢复。在可启动媒体下进行恢复可能会使 Windows 中恢复的分区无法检测。

McAfee 端点加密和 PGP 整盘加密

只能使用可启动媒体来恢复加密的系统分区。

如果恢复的系统无法启动，请按下面的 Microsoft 知识库文章中所述的方法重新创建主启动记录：https://support.microsoft.com/kb/2622803

与 Dell EMC Data Domain 存储的兼容性

通过 Acronis 安克诺斯数据保护软件，您可以使用 Dell EMC Data Domain 设备作为备份存储。支持保留锁定(监管模式) 。

如果保留锁定已启用，则需要将 `AR_RETENTION_LOCK_SUPPORT` 环境变量添加到装有将此存储用作备份目标的保护代理程序的计算机。

注意
启用了保留锁定的 Dell EMC Data Domain 存储不受适用于 Mac 的代理程序的支持。

在 Windows 中添加变量

1. 以管理员身份登录到具有保护代理程序的计算机。
2. 在**控制面板**中，转到**系统和安全** > **系统** > **高级系统设置**。
3. 在**"高级"选项卡**中，单击**环境变量**。
4. 在**系统变量**面板中，单击**新建**。
5. 在**新系统变量**窗口中，按以下所示添加新的变量：
   - 变量名称：AR_RETENTION_LOCK_SUPPORT
   - 变量值：1
6. 单击**确定**。
7. 在**环境变量**窗口中，单击**确定**。
8. 重新启动计算机。

在 Linux 中添加变量

1. 以管理员身份登录到具有保护代理程序的计算机。
2. 转到 /sbin 目录，然后打开 acronis_mms 文件进行编辑。
3. 在 export LD_LIBRARY_PATH 行的上面，添加以下行：

```
export AR_RETENTION_LOCK_SUPPORT=1
```

4. 保存 acronis_mms 文件。
5. 重新启动计算机。

在虚拟设备中添加变量

1. 以管理员身份登录到虚拟设备计算机。
2. 转到 /bin 目录，然后打开 autostart 文件进行编辑。
3. 在 export LD_LIBRARY_PATH 行的下面，添加以下行：

```
export AR_RETENTION_LOCK_SUPPORT=1
```

4. 保存 autostart 文件。
5. 重新启动虚拟设备计算机。

系统要求

下表总结了适用于典型安装情况的磁盘空间和内存要求。使用默认设置执行安装。

要安装的组件	安装所需磁盘空间	最低内存消耗
适用于 Windows 的代理程序	850 MB	150 MB
适用于 Windows 的代理程序和以下代理程序之一：	950 MB	170 MB

• 适用于 SQL 的代理程序 • 适用于 Exchange 的代理程序		
适用于 Windows 的代理程序和以下代理程序之一： • 适用于 VMware 的代理程序 (Windows) • 适用于 Hyper-V 的代理程序	1170 MB	180 MB
适用于 Office 365 的代理程序	500 MB	170 MB
适用于 Linux 的代理程序	2.0 GB	130 MB
适用于 Mac 的代理程序	500 MB	150 MB
仅适用于本地部署		
Windows 中的管理服务器	1.7 GB	200 MB
Linux 中的管理服务器	1.5 GB	200 MB
管理服务器和适用于 Windows 的代理程序	2.4 GB	360 MB
管理服务器以及运行 Windows、Microsoft SQL Server、Microsoft Exchange Server 和 Active Directory 域服务的计算机上的代理程序	3.35 GB	400 MB
管理服务器和适用于 Linux 的代理程序	4.0 GB	340 MB
存储节点和适用于 Windows 的代理程序 • 仅限 64 位平台 • 要使用重复数据删除，至少需要 8 GB RAM。有关详细信息，请参阅 "重复数据删除最佳实践"(第 532 页) 。	1.1 GB	330 MB

备份期间，一个代理程序通常消耗约 350 MB 内存(在 500-GB 卷备份期间测得) 。峰值消耗可能达到 2 GB，具体取决于所处理数据的量和类型。

备份到大型备份集(600 GB 或更多) 时，每 1 TB 的备份集大约需要 1 GB RAM。

注意
备份到超大备份集(4 TB 或更多) 时，RAM 使用量可能会增加。

在 x64 系统上，在重新启动情况下的可启动媒体和磁盘恢复的操作至少需要 2 GB 内存。

包含一个已注册工作负载的管理服务器消耗 200 MB 内存。工作负载是任何类型的受保护资源 - 例如，物理机、虚拟机、邮箱或数据库实例。每一额外的工作负载会增加大约 2 MB。因此，包含 100 个已注册工作负载的服务器消耗约 400 MB 内存，超过了操作系统和正在运行的应用程序的内存消耗。

已注册工作负载的最大数量为 900-1000。此限制源自管理服务器中内嵌的 SQLite 数据库。

要克服此限制，请在安装管理服务器时指定外部 Microsoft SQL Server 实例。通过使用外部 SQL 数据库，可以将多达 8000 个工作负载注册到管理服务器，而不会显著降低性能。在 8000 个已注册工作负载的情况下，SQL Server 实例将消耗大约 8 GB RAM。

为提高备份性能，请按组管理工作负载，每组最多 500 个工作负载。

支持的文件系统

保护代理程序可以备份可从安装有该代理程序的操作系统访问的任何文件系统。例如，如果 Windows 中安装了相应的驱动程序，适用于 Windows 的代理程序可以备份和恢复 ext4 文件系统。

下表概述了可以备份和恢复的文件系统。限制适用于代理程序和可启动媒体。

文件系统	受支持				限制
	代理程序	WinPE 可启动媒体	基于 Linux 的可启动媒体	Mac 可启动媒体	
FAT16/32	所有代理程序	+	+	+	无限制
NTFS		+	+	+	
ext2/ext3/ext4		+	+	-	
HFS+	适用于 Mac 的代理程序	-	-	+	
APFS		-	-	+	• 支持使用 macOS High Sierra 10.13 启动 • 在恢复到非原始计算机或裸机时，应该手动重新创建磁盘配置。

JFS	适用于 Linux 的代理程序	-	+	-	• 无法从磁盘备份中排除文件 • 无法启用快速增量/差异备份
ReiserFS3		-	+	-	
ReiserFS4		-	+	-	• 无法从磁盘备份中排除文件 • 无法启用快速增量/差异备份 • 无法在恢复期间调整卷大小
ReFS	所有代理程序	+	+	+	
XFS		+	+	+	• 无法从磁盘备份中排除文件 • 无法启用快速增量/差异备份 • 无法在恢复期间调整卷大小 • 不支持从存储在磁带上的备份恢复文件
Linux Swap	适用于	-	+	-	无限制

	Linux 的代理程序				
exFAT	所有代理程序	+	+ 如果备份*存储在* exFAT 上，则可启动媒体无法用于恢复	+	• 仅支持磁盘/卷备份 • 无法从备份中排除文件 • 无法从备份中恢复个别文件

当备份带有未识别或不受支持的文件系统的驱动器时，软件将自动切换到逐扇区模式。逐扇区备份可用于满足以下条件的任一文件系统：

- 基于块
- 跨越单个磁盘
- 具有标准 MBR/GPT 分区方案

如果文件系统不满足这些要求，备份将失败。

重复数据删除

在 Windows Server 2012 及更高版本中，可以为 NTFS 卷启用“重复数据删除”功能。通过仅存储一次卷文件的重复碎片，重复数据删除可减小卷上的使用空间。

您可以在磁盘级备份和恢复启用重复数据删除的卷，而无任何限制。支持文件级备份，但在使用 Acronis VSS Provider 时除外。要从磁盘备份恢复文件，请从备份运行虚拟机或在运行 Windows Server 2012 或更高版本的计算机上加载备份，然后从已加载卷复制文件。

Windows Server 的“重复数据删除”功能与 Acronis Backup 的“重复数据删除”功能无关。

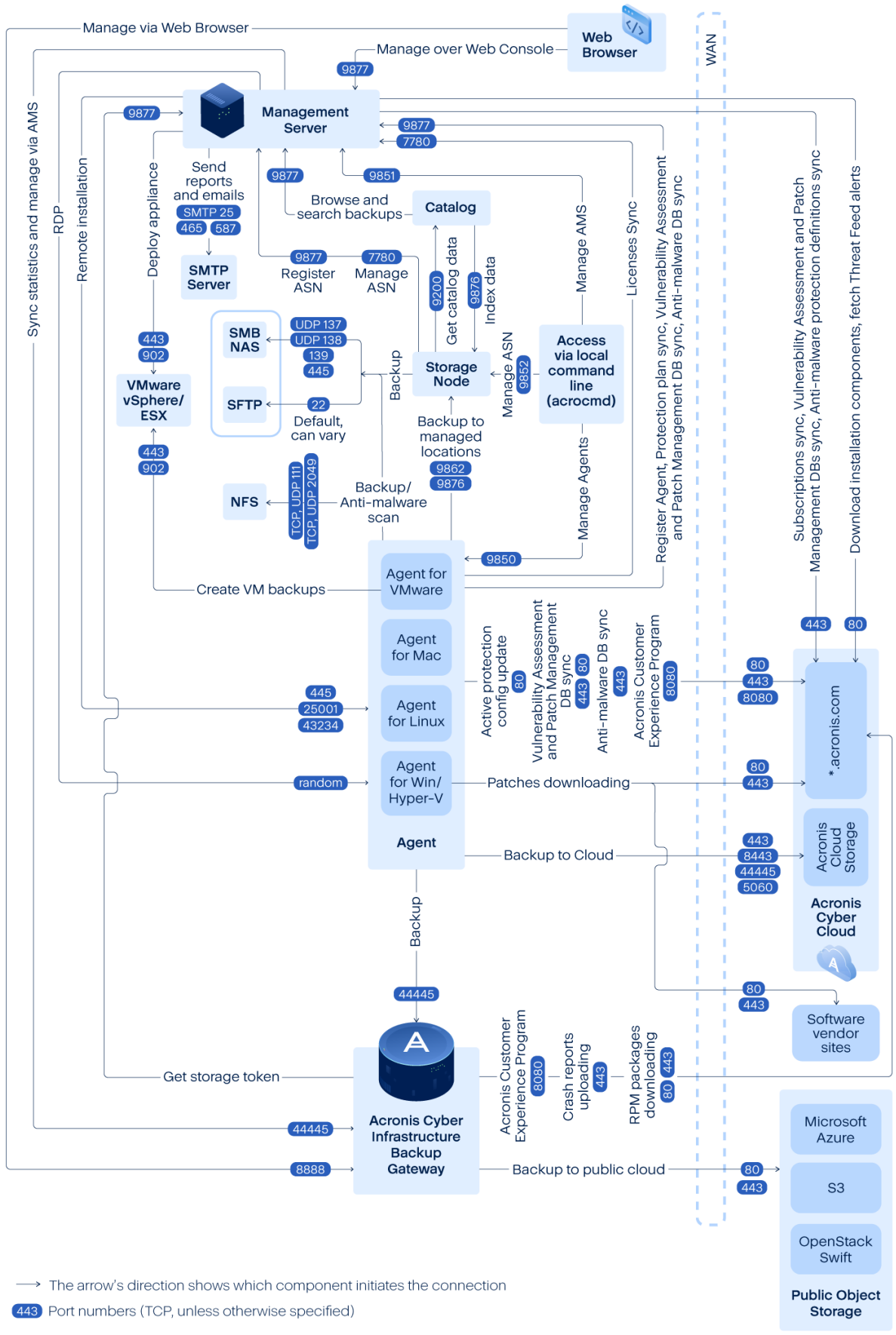
Acronis 安克诺斯数据保护软件 的网络连接图表

本主题包含 Acronis安克诺斯数据保护软件 的连接图表。

访问我们的知识库，以获取 Acronis安克诺斯数据保护软件 使用的端口、服务和进程列表：

- 对于 Windows，请参阅 Windows 服务和进程 (65663)。
- 对于 Linux，请参阅 Linux 组件、服务和进程 (67276)。

网络连接图表 - 安克诺斯数据保护软件 进程



重要事项
网络图中的传出端口是动态的。某些服务还可以将动态端口用于入站连接。在对网络问题进行故障排除时，请确保流量允许通过动态端口。

动态端口由操作系统管理，并是随机指派的。Windows 中的默认动态端口范围是 49152 到 65535。该范围可能因操作系统而异，并可以手动更改。

管理服务器是 Acronis 安克诺斯数据保护软件 的核心组件。它公开了两个 TCP 端口：7780 和 9877。受 TLS 保护的端口 9877 用于提供 REST API 和基于 Web 的用户界面。REST API 端点使用表示为单独的 HTTP 标头或编码为 HTTP Cookie 的 JWT 令牌对请求进行身份验证。端口 7780 使用 ZMTP CURVE 身份验证和加密实现 ZeroMQ 协议。代理程序和存储节点使用端口 7780 与管理服务器异步交换管理消息。管理服务器还会与云服务通信，以通过标准 HTTP 和 HTTPS 端口下载更新。

存储节点是 Acronis 安克诺斯数据保护软件 的存储组件。它公开了 TCP 端口 9876。该端口用于发送和接收备份数据。传输受 TLS 保护，身份验证使用双向 TLS 实现。应用程序级协议是 Acronis 专有的。存储节点通过使用适当的协议和身份验证机制，来与后端存储系统进行通信。

目录是 Acronis 安克诺斯数据保护软件 的一个支持组件。它在存储节点上为数据编制索引以在端口 9876 上访问它，并在端口 9200 上公开索引。

备份网关实现了下一代 Acronis 专有数据访问协议。如果客户选择加入云备份，则会在 Acronis Cyber Cloud 中使用相同的组件。TCP 端口 44445(在 IANA 中注册) 将由网关使用。数据保护是通过 TLS 实现的，身份验证是使用双向 TLS 实现的。备份网关也可以将端口 8888 用于基于 HTTPS 的管理服务。

代理程序会通过端口与管理服务器、存储节点和备份网关通信，如上所述。当基于标准的文件服务 (SMB、NFS) 用作备份目标时，代理程序还可以与它们进行通信。在这种情况下，将使用标准端口和合适的身份验证协议。如果配置此类功能，则适用于 VMware 的代理程序会通过 VMware vSphere 定义的端口使用 VMware vSphere API。

Linux 的漏洞评估通过部署于 Acronis Cyber Cloud 中的 CVSS 服务实现。保护代理程序通过 ping 从列表 https://cloud.acronis.com/services.json 中动态选择最近的数据中心。

本地部署

本地部署包括 "组件"(第 45 页) 部分中所述的许多软件组件。有关这些组件与所需端口之间交互的详细信息，请参阅 "Acronis 安克诺斯数据保护软件 的网络连接图表"(第 72 页)。

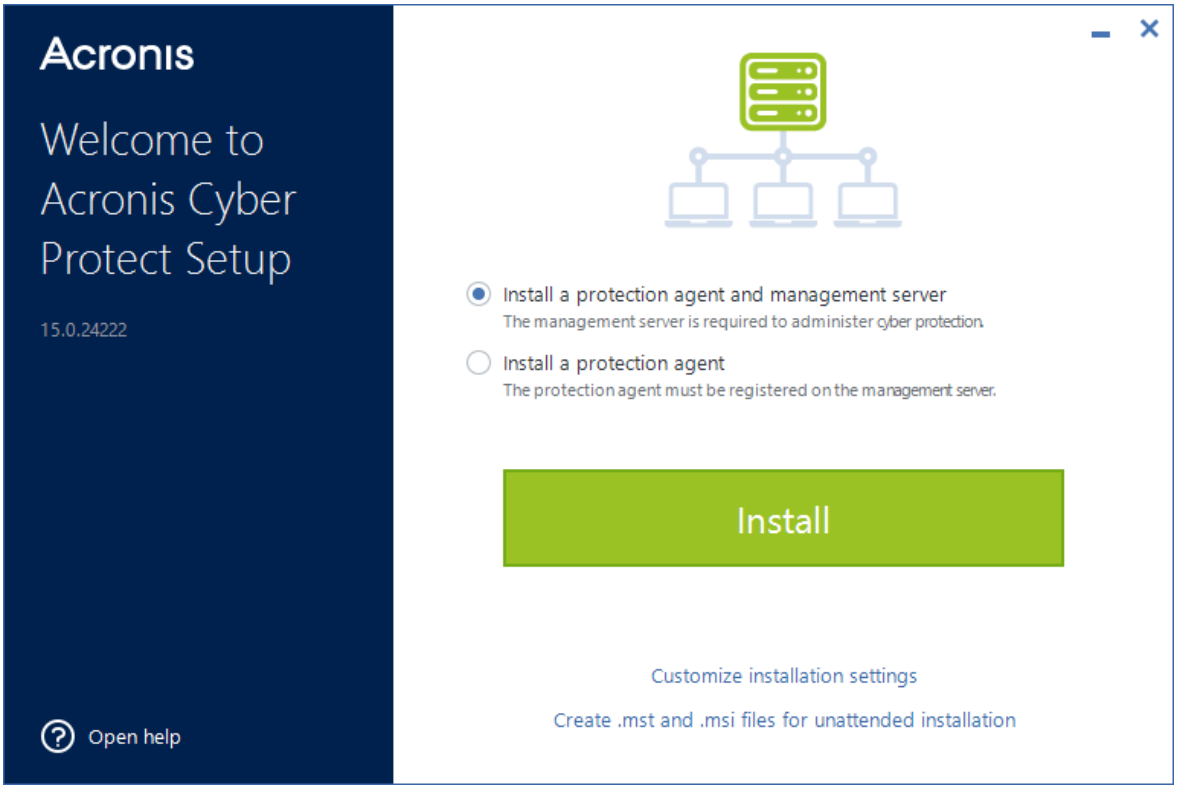
安装管理服务器

在 Windows 中安装

安装管理服务器

1. 以管理员身份登录，然后启动 Acronis 安克诺斯数据保护软件 安装程序。
2. [可选] 要更改安装程序的语言，请单击**设置语言**。
3. 接受许可协议和隐私声明的条款，然后单击**继续**。

4. 保留默认设置**安装安全保护代理程序和管理服务器**。



5. 请执行以下任一操作：
   - 单击**安装**。

     这是安装产品的最简单方法。大部分安装参数将设为默认值。

     系统将安装以下组件：
     - 管理服务器
     - Components for Remote Installation
     - 适用于 Windows 的代理程序
     - 其他代理程序（适用于 Hyper-V 的代理程序、适用于 Exchange 的代理程序、适用于 SQL 的代理程序和适用于 Active Directory 的代理程序），前提是在计算机上检测到各自的虚拟机监控程序或应用程序
     - 可启动媒体生成器
     - 命令行工具
     - 网络安全保护监视器
   - 单击**自定义安装设置**以配置设置。

     您可以选择要安装的组件和指定其他参数。有关详细信息，请参阅 "自定义安装设置"（第 77 页）。
   - 单击**创建 .mst 和 .msi 文件用于无人参与安装**以解压缩安装包。查看或修改将添加到 .mst 文件的安装设置，然后单击**生成**。无需再执行此过程的其他步骤。

     如果要通过组策略部署代理程序，请参阅 "通过“组策略”部署代理程序"（第 156 页）。
6. 继续安装。
7. 安装完成后，单击**关闭**。

要开始使用管理服务器，请登录到 Acronis 帐户或通过激活文件激活它。

自定义安装设置

此部分介绍安装期间可以更改的设置。

要安装的组件

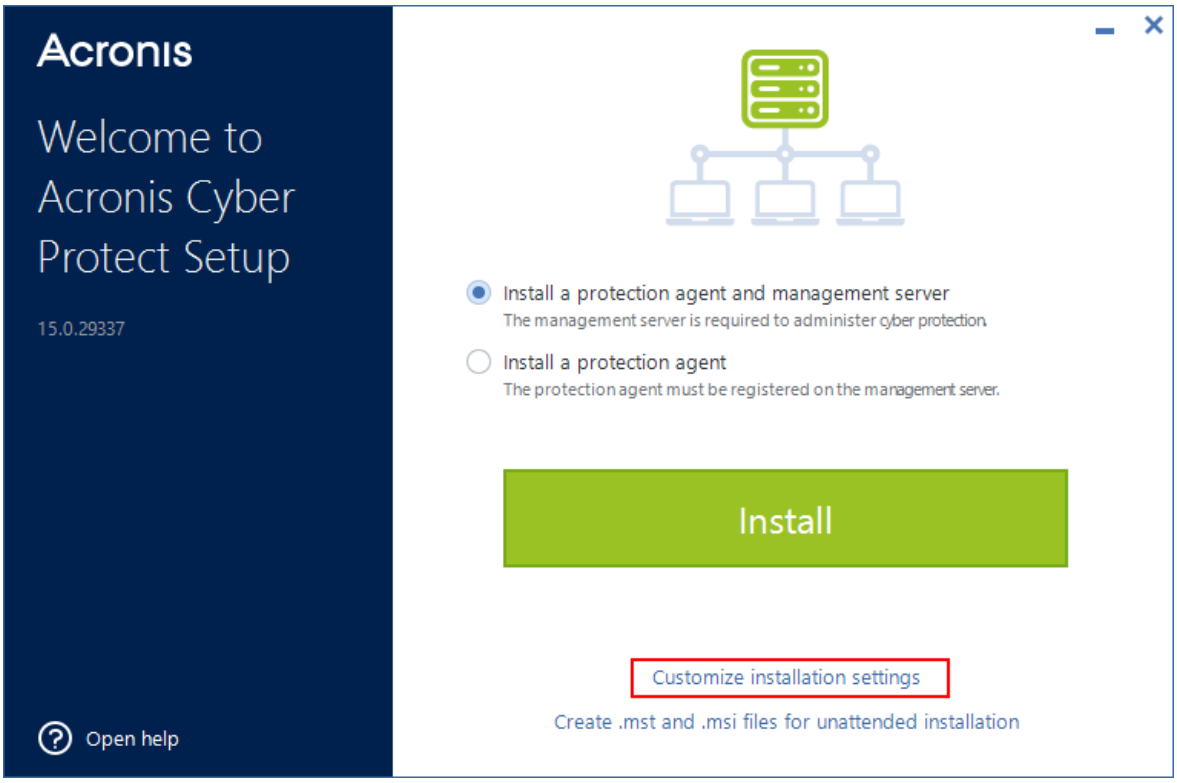
根据是安装管理服务器和保护代理程序，还是仅安装保护代理程序，以下组件默认处于选中状态：

管理服务器和保护代理程序	仅保护代理程序
管理服务器	适用于 Windows 的代理程序
Components for Remote Installation	可启动媒体生成器
适用于 Windows 的代理程序	命令行工具
可启动媒体生成器	安克诺斯数据保护软件监视器
命令行工具	
安克诺斯数据保护软件监视器	

有关可用组件的完整列表，请参阅 "组件"(第 45 页)。

安装可选组件

1. 在安装向导中，单击**自定义安装设置**。



2. 在**安装内容**中，单击**更改**。

3. 选择所需组件，然后单击**完成**。
4. 如果出现提示，请配置选定组件的设置。
5. 单击**安装**。

服务登录帐户

可以分别使用**代理程序服务的登录帐户**和**管理服务器服务的登录帐户**选项，来更改将运行代理程序或管理服务的帐户。

可以选择以下其中一个选项：

- **使用服务用户帐户**（代理程序服务的默认帐户）
  服务用户帐户是用于运行服务的 Windows 系统帐户。此选项的优点是域安全策略不会影响这些帐户的用户权限。默认情况下，该代理程序在**本地系统**帐户下运行。
- **创建新帐户**（管理服务器服务和存储节点服务的默认帐户）
  代理程序、管理服务器和存储节点服务的帐户名称分别为 **Acronis Agent User**、**AMS User** 和 **ASN User**。
- **使用以下帐户**
  如果将产品安装在域控制器上，则安装程序会提示您为每个服务指定现有帐户（或相同帐户）。出于安全原因，安装程序不会自动在域控制器上创建新帐户。
  必须为安装程序在域控制器上运行时指定的用户帐户授予作为服务登录权限。此帐户必须已在域控制器上使用，才能在该计算机上创建其配置文件文件夹。
  有关在只读域控制器上安装代理程序的详细信息，请参阅此知识库文章。
  此外，如果配置装有 SQL 数据库的管理服务器，则选择**使用以下帐户**允许您对 Microsoft SQL Server 使用 Windows 身份验证。

如果选择**创建新帐户**或**使用以下帐户**选项，请确保域安全策略不会影响相关帐户的权限。如果某个帐户被剥夺了安装期间分配的用户权限，则相关组件可能工作不正常，也可能不工作。

服务登录帐户所需的用户权限

保护代理程序在 Windows 计算机上作为 **Managed Machine Service** (MMS) 运行。运行代理程序的帐户必须具有以下权限，才能使代理程序正常工作：

1. MMS 用户必须包含在**备份操作员**和**管理员**组中。在域控制器上，用户必须包含在**域管理员**组中。
2. 必须为 MMS 用户授予对文件夹 `%PROGRAMDATA%\Acronis`（在 Windows XP 和 Server 2003 中为 `%ALLUSERSPROFILE%\Application Data\Acronis`）及其子文件夹的**完全控制**权限。
3. 必须为 MMS 用户授予对以下项中的某些注册表项的**完全控制**权限：`HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`。
4. 在 Windows 中，必须为 MMS 用户分配以下用户权限：
   - **作为服务登录**
   - **调整进程的内存配额**
   - **替换进程级别令牌**
   - **修改固件环境值**

ASN 用户必须在安装有 Acronis 存储节点的计算机上拥有本地管理员权限。

在 Windows 中分配用户权限

注意
此过程使用**作为服务登录**用户权限作为示例。其他用户权限的步骤相同。

1. 以管理员身份登录到计算机。
2. 在**控制面板**中，打开**管理工具**。或者，按键盘上的 Win+R、键入 **control admintools**，然后按 Enter。
3. 打开**本地安全策略**。
4. 展开**本地策略**，然后单击**用户权限分配**。
5. 在右侧窗格中，右键单击**作为服务登录**，然后选择**属性**。
6. 单击**添加用户或组...**，以添加新用户。
7. 在**选择用户或组**窗口中，找到要添加的用户，然后单击**确定**。
8. 在**作为服务登录属性**窗口中，单击**确定**以保存更改。

注意
要为其添加**作为服务登录**用户权限的用户不得列于**本地安全策略**中的**拒绝作为服务登录**策略中。

重要事项
不建议您在安装完成后手动更改登录帐户。

用于管理服务器的数据库

可以使用以下数据库配置管理服务器：

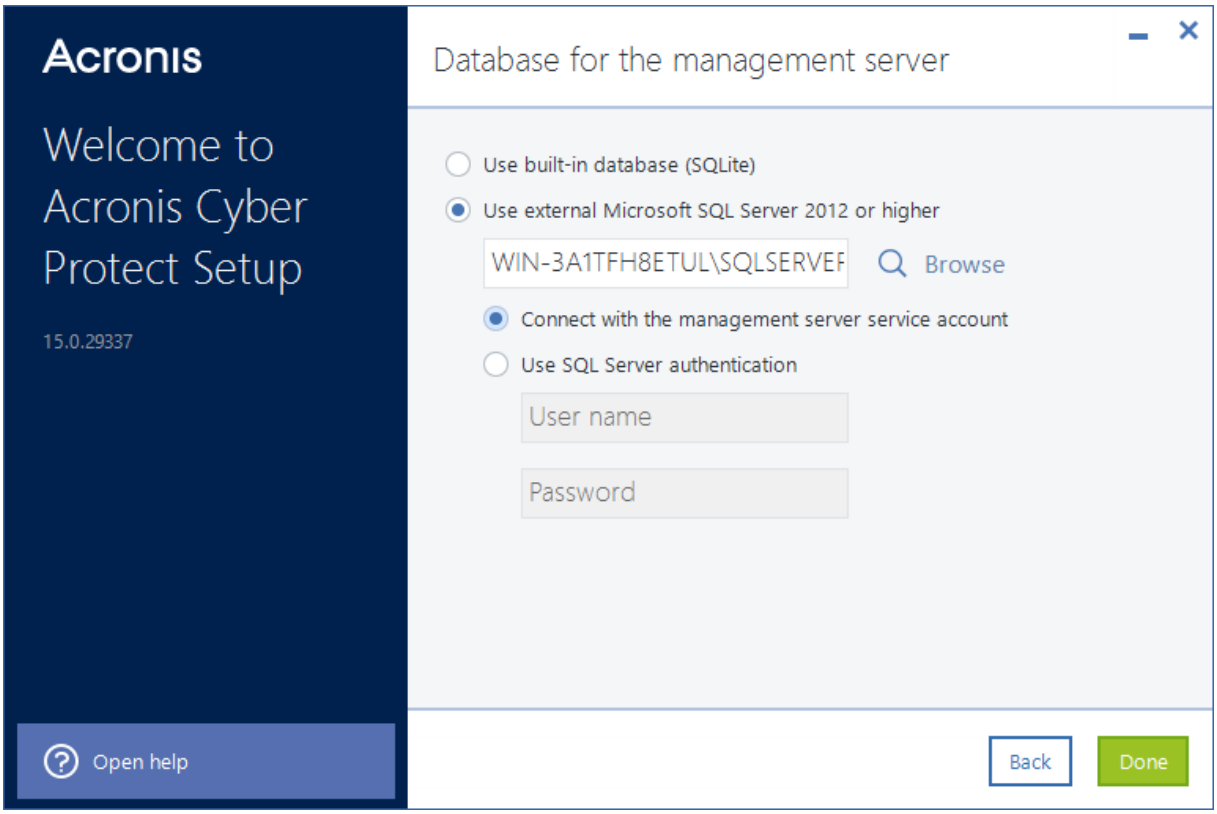
- SQLite

  默认情况下，管理服务器使用内置的 SQLite 数据库。它允许在管理服务器上注册大约 900-1000 个工作负载。SQLite 与扫描服务不兼容。
- Microsoft SQL

  Microsoft SQL 允许在管理服务器上注册多达 8000 个工作负载，而不会显著降低性能。管理服务器、扫描服务和其他程序可以使用相同的 Microsoft SQL 实例。

  支持以下 MS SQL Server 版本：
  - Microsoft SQL Server 2019(在 Windows 中运行)
  - Microsoft SQL Server 2017(在 Windows 中运行)
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2014
  - Microsoft SQL Server 2012

如果 Microsoft SQL 实例是默认实例 **MSSQLSERVER**，则只能指定运行它的计算机的名称。如果实例有自定义名称，则必须使用以下格式指定它：计算机名称\实例名称。



注意

确保在运行 Microsoft SQL 实例的计算机上启用了 SQL Server Browser Service 和 TCP/IP 客户端协议。有关如何启动 SQL Server Browser Service 的详细信息，请参阅 http://msdn.microsoft.com/en-us/library/ms189093.aspx。您可以通过类似过程启用 TCP/IP 协议。

要连接到指定的 Microsoft SQL 实例，可以使用以下身份验证方法：

- Windows 身份验证（**通过管理服务器服务帐户连接**）

  如果通过使用**使用以下帐户**选项为管理服务器服务配置了登录帐户（例如，通过指定 <计算机名称>\Administrator），则可以使用此方法。指定的帐户必须在 Microsoft SQL Server 中具有 **dbcreator** 或 **sysadmin** 角色。

  有关登录帐户的详细信息，请参阅 "服务登录帐户所需的用户权限"（第 78 页）。
- SQL Server 身份验证

  始终可以使用此方法。指定的帐户必须在 Microsoft SQL Server 中具有 **dbcreator** 或 **sysadmin** 角色。

扫描服务

扫描服务是一个可选组件，可对云存储、本地文件夹或网络文件夹中的备份启用防恶意软件扫描。扫描服务要求管理服务器安装在同一台计算机上。

通过安装扫描服务，可以访问以下功能：

- 备份扫描计划
- 备份扫描详细信息小组件

- 公司白名单
- 安全恢复
- 备份列表中的 **状态**栏

可以在安装管理服务器期间安装扫描服务，也可以稍后通过修改现有安装来添加扫描服务。有关如何将可选组件安装为扫描服务的详细信息，请参阅 "安装可选组件"(第 77 页)。

重要事项
扫描服务与管理服务器使用的默认 SQLite 数据库不兼容。

可以使用 Microsoft SQL 或 PostgerSQL 数据库配置扫描服务。有关如何选择数据库的详细信息，请参阅 "备份服务数据库"(第 82 页)。

备份服务数据库

扫描服务与管理服务器的默认数据库 SQLite 不兼容。

如果管理服务器使用 SQLite，则只能使用 PostgreSQL 数据库配置扫描服务。支持 PostgreSQL 9.6 及更高版本。

如果管理服务器使用 Microsoft SQL Server，则可以使用相同的数据库配置扫描服务，而无需其他设置。还可以使用 PostgreSQL 数据库配置扫描服务。

使用 PostgreSQL 数据库配置扫描服务

1. 在安装向导中的**扫描服务的数据库**下，单击**更改**。
2. 选择 **PostgreSQL Server 数据库**。
3. 指定 PostgreSQL 实例主机名，或 IP 地址和端口。
4. 指定具有 **CREATEDB** 权限或是超级用户的用户的凭据。

   注意
   不支持 PostgreSQL 10 及更高版本中的 SCRAM-SHA-256 身份验证方法。

5. 单击**完成**。

端口

可以自定义 Web 浏览器将用于访问管理服务器的端口（默认为 9877）和将用于产品组件之间通信的端口（默认为 7780）。要在安装完成后更改后一个端口，需要重新注册所有组件。

安装过程中会自动配置 Windows 防火墙。如果使用不同的防火墙，确保打开该端口并且接收和发送请求均可通过该防火墙。

代理服务器

可以选择保护代理程序在备份到云存储和从云存储恢复时是否使用 HTTP 代理服务器。

此外，将同一个代理服务器用于不同 Acronis 安克诺斯数据保护软件 组件之间的通信。

要使用代理服务器，请指定其主机名或 IP 地址以及端口号。如果代理服务器需要身份验证，请指定访问凭据。

注意
使用代理服务器时，无法更新保护定义（即防病毒和防恶意软件定义、高级检测定义、漏洞评估和修补程序管理定义）。

在 Linux 中安装

准备

1. 如果您想要同时安装适用于 Linux 的代理程序以及管理服务器，请确保该计算机上已安装必要的 Linux 程序包。

2. 选择要由管理服务器使用的数据库。

局限性

在 Linux 计算机上运行的管理服务器不支持远程安装保护代理程序(例如，在自动发现步骤中使用的保护代理程序)。有关可能的解决方法的详细信息，请参阅我们的知识库：https://kb.acronis.com/content/69553。

安装

若要安装管理服务器，至少需要 4GB 的可用磁盘空间。

安装管理服务器

1. 以根用户身份，导航到安装文件所在的目录、使文件可执行，然后运行它。

   ```
   chmod +x <installation file name>
   ```

   ```
   ./<installation file name>
   ```

2. 接受许可证协议的条款。
3. [可选] 选择您要安装的组件。

   默认情况下，将安装以下组件：
   - 管理服务器
   - 适用于 Linux 的代理程序
   - 可启动媒体生成器
4. 指定 Web 浏览器要用于访问管理服务器的端口。默认值为 9877。
5. 指定将用于产品组件之间的通信的端口。默认值为 7780。
6. 单击**下一步**以继续执行安装。
7. 安装完成后，选择**打开 Web 中控台**，然后单击**退出**。安克诺斯数据保护软件 Web 中控台将在默认 Web 浏览器中打开。

要开始使用管理服务器，请登录到 Acronis 帐户或通过激活文件激活它。

Acronis 安克诺斯数据保护软件 设备

使用 Acronis 安克诺斯数据保护软件 设备，可轻松获取装有以下软件的虚拟机：

- CentOS
- Acronis 安克诺斯数据保护软件 组件：
  - 管理服务器
  - 适用于 Linux 的代理程序
  - 适用于 VMware 的代理程序 (Linux)

设备以 .zip 存档的形式提供。该存档包含 .ovf 和 .iso 文件。可将 .ovf 文件部署到 ESXi 主机，或者使用 .iso 文件来启动现有虚拟机。该存档还包含应置于与 .ovf 相同的目录中的 .vmdk 文件。

注意
VMware 主机客户端(即用于管理独立 ESXi 6.0+ 的 Web 客户端)不允许部署内含 ISO 映像的 OVF 模板。如果您遇到上述情况,请创建满足以下要求的虚拟机,然后使用 .iso 文件来安装软件。

虚拟设备的要求如下所示:

- 最低系统要求:
  - 2 个 CPU
  - 6 GB RAM
  - 一个 10 GB 虚拟磁盘(建议 40 GB)
- 在 VMware 虚拟机设置中,依次单击**选项**选项卡 > **一般** > **配置参数**,然后确保 `disk.EnableUUID` 参数值为 `true`。

局限性

在 Linux 计算机上运行的管理服务器(包括 Acronis 安克诺斯数据保护软件 设备)不支持远程安装保护代理程序(例如,在自动发现步骤中使用的保护代理程序)。有关可能的解决方法的详细信息,请参阅我们的知识库:https://kb.acronis.com/content/69553。

安装软件

1. 请执行以下任一操作:
   - 通过 .ovf 部署设备。完成部署后,打开生成的计算机。
   - 从 .iso 启动现有虚拟机。
2. 选择**安装或更新 Acronis 安克诺斯数据保护软件**,然后按 **Enter**。等待初始安装窗口显示。
3. [可选]若要更改安装设置,请选择**更改设置**,然后按 **Enter**。您可以指定以下设置:
   - 设备的主机名(默认为 `AcronisAppliance-<随机部分>`)。
   - 将用于登录到 安克诺斯数据保护软件 Web 中控台的"根"帐户的密码(默认为**未指定**)。
     如果保留默认值,则在安装 Acronis 安克诺斯数据保护软件 后,系统将提示您指定密码。如果没有该密码,您将无法登录到 安克诺斯数据保护软件 Web 中控台和 Cockpit Web 中控台。
   - 网络界面卡的网络设置:
     - **使用 DHCP**(默认)
     - **设置静态 IP 地址**

     如果计算机有多个网络界面卡,软件将随机选择一个并向其应用这些设置。
4. 选择**使用当前设置安装**。

结果,将在计算机上安装 CentOS 和 Acronis 安克诺斯数据保护软件。

进一步操作

完成安装后,该软件会显示指向 安克诺斯数据保护软件 Web 中控台和 Cockpit Web 中控台的链接。连接到 安克诺斯数据保护软件 Web 中控台以开始使用 Acronis 安克诺斯数据保护软件:添加更多设备、创建备份计划等。

若要添加 ESXi 虚拟机，请依次单击**添加** > **VMware ESXi**，然后为 vCenter 服务器或独立 ESXi 主机指定地址和凭据。

在 Cockpit Web 中控台中，没有已配置的 Acronis 安克诺斯数据保护软件 设置。提供中控台，以便于操作和进行疑难解答。

更新软件

1. 下载并解压缩新设备版本的 .zip 存档。
2. 从上一步中解压缩的 .iso 启动计算机。
   a. 将 .iso 保存到您的 vSphere 数据存储。
   b. 将 .iso 连接到计算机的 CD/DVD 驱动器。
   c. 重新启动计算机。
   d. [仅在第一次更新期间] 按 **F2**，然后更改启动顺序，以便 CD/DVD 驱动器处于第一位。
3. 选择**安装或更新 Acronis 安克诺斯数据保护软件**，然后按 **Enter**。
4. 选择**更新**，然后按 **Enter**。
5. 在更新完成后，请断开 .iso 与计算机的 CD/DVD 驱动器的连接。

结果，将更新 Acronis 安克诺斯数据保护软件。此外，如果 .iso 文件中的 CentOS 版本高于磁盘上的版本，则在更新 Acronis 安克诺斯数据保护软件 之前会先更新操作系统。

从 安克诺斯数据保护软件 Web 中控台添加计算机

可以通过以下方法之一添加计算机：

- 通过下载安装程序并在目标计算机上本地运行它。
- 通过在目标计算机上远程安装保护代理程序。

限制

- 远程安装仅适用于在 Windows 计算机上运行的管理服务器。目标计算机也必须运行 Windows。
- 运行 Windows XP 的计算机不支持远程安装。
- 域控制器不支持远程安装。要了解如何在域控制器上安装保护代理程序，请参阅 "在 Windows 中安装"(第 92 页)。确保通过选择**代理程序服务的登录帐户**下的**使用以下帐户**来自定义安装设置。要了解有关此选项的更多信息，请参阅 "服务登录帐户所需的用户权限"(第 78 页)。

添加运行 Windows 的计算机

可以通过在 安克诺斯数据保护软件 Web 中控台中远程安装保护代理程序，或通过下载安装程序并在本地运行，来添加 Windows 计算机。

远程安装代理程序

重要事项

在开始安装之前，请确保满足远程安装的先决条件，并且您的环境中至少有一个代理程序可用作部署代理程序。有关详细信息，请参阅 "远程安装的先决条件"(第 86 页) 和 "部署代理程序"(第 88 页) 。

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设备** > **所有设备**。
2. 单击**添加**。
3. [要安装适用于 Windows 的代理程序] 单击 **Windows**。
4. [要安装另一个支持的代理程序] 单击对应于要保护的应用程序的按钮。

   以下代理程序可用：
   - 适用于 Hyper-V 的代理程序
   - 适用于 SQL 的代理程序 + 适用于 Windows 的代理程序
   - 适用于 Exchange 的代理程序 + 适用于 Windows 的代理程序

     如果依次单击了 **Microsoft Exchange Server** > **Exchange 邮箱**，并且已注册至少一个适用于 Exchange 的代理程序，则转到步骤 9。
   - 适用于 Active Directory 的代理程序 + 适用于 Windows 的代理程序
   - 适用于 Office 365 的代理程序
5. 在打开的窗格中，选择部署代理程序。
6. 指定目标计算机的主机名或 IP 地址以及具有该计算机的管理权限的帐户的凭据。

   建议您使用内置的管理员帐户。要使用另一个帐户，请将该帐户添加到管理员组并修改目标计算机的注册表，如下文中所述：https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows。
7. 选择代理程序将用于访问管理服务器的该服务器的名称或 IP 地址。

   默认情况下，服务器名称处于选中状态。如果您的管理服务器有多个网络接口，或者您遇到导致代理程序注册失败的 DNS 问题，则可能需要改为选择 IP 地址。
8. 单击**安装**。
9. [如果在步骤 4 中已选择 **Microsoft Exchange Server** > **Exchange 邮箱**] 指定 Microsoft Exchange Server 的**客户端访问**服务器角色 (CAS) 已启用的计算机。有关详细信息，请参阅 "邮箱备份"(第 389 页) 。

下载代理程序并在本地安装

1. 在 安克诺斯数据保护软件 Web 中控台中，单击右上角的帐户图标，然后单击**下载**。
2. 单击所需的 Windows 安装程序的名称。

   安装程序即会下载到您的计算机上。
3. 在要保护的计算机上运行安装程序。有关详细信息，请参阅 "在 Windows 中安装"(第 92 页) 。

远程安装的先决条件

- 为了能够在运行 Windows 7 或更高版本的远程计算机上成功安装，此计算机上的**控制面板** > **文件夹选项** > **查看** > **使用共享向导**选项必须处于*禁用*状态。

- 为了能够在*非* Active Directory 域成员的远程计算机上成功安装，必须在该计算机上*禁用*用户帐户控制 (UAC)。有关如何禁用它的详细信息，请参阅 "禁用 UAC"(第 87 页) 。
- 默认情况下，在任何 Windows 计算机上进行远程安装都需要内置 Administrator 帐户的凭据。要使用另一个管理员帐户的凭据执行远程安装，用户帐户控制 (UAC) 远程限制必须处于*禁用*状态。有关如何禁用它们的详细信息，请参阅 "禁用 UAC 远程限制"(第 88 页) 。
- 远程计算机上的“文件和打印机共享”必须处于*启用*状态。若要访问该选项：
  - [在运行 Windows 2003 Server 的计算机上] 转到**控制面板** > **Windows 防火墙** > **例外** > **文件和打印机共享**。
  - [在运行 Windows Server 2008、Windows 7 或更高版本的计算机上] 转到**控制面板** > **Windows 防火墙** > **网络和共享中心** > **更改高级共享设置**。
- Acronis 安克诺斯数据保护软件 使用 TCP 端口 **445**、**25001** 和 **43234** 进行远程安装。

  当您启用“文件和打印机共享”时，端口 **445** 将自动打开。端口 43234 和 25001 将自动通过 Windows 防火墙打开。如果使用不同的防火墙，请确保这三个端口已打开(添加到例外) 以用于接收和发送请求。

  远程安装完成后，端口 **25001** 将通过 Windows 防火墙自动关闭。如果要在将来远程更新代理程序，则端口 **445** 和 **43234** 需要保持打开。在每次更新期间，端口 **25001** 都通过 Windows 防火墙自动打开和关闭。如果使用其他防火墙，请将这三个端口都保持打开。

注意
运行 Windows XP 的计算机不支持远程安装。

注意
域控制器不支持远程安装。要了解如何在域控制器上安装保护代理程序，请参阅 "在 Windows 中安装"(第 92 页) 。确保通过选择**代理程序服务的登录帐户**下的**使用以下帐户**来自定义安装设置。要了解有关此选项的更多信息，请参阅 "服务登录帐户所需的用户权限"(第 78 页) 。

用户帐户控制 (UAC) 的要求

在运行 Windows 7 或更高版本且不是 Active Directory 域成员的计算机上，集中式管理操作(包括远程安装) 要求禁用 UAC 和 UAC 远程限制。

禁用 UAC

根据操作系统，执行以下操作之一：

- **在 Windows 8 之前的 Windows 操作系统中：**

  转到**控制面板 > 查看方式：小图标 > 用户帐户 > 更改用户帐户控制设置**，然后将滑块移到**从不通知**。然后，重新启动计算机。
- **在任一 Windows 操作系统中**：
  1. 打开注册表编辑器。
  2. 找到以下注册表项：**HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. 对于 **EnableLUA** 值，将设置更改为 **0**。
  4. 重新启动计算机。

禁用 UAC 远程限制

1. 打开注册表编辑器。
2. 找到以下注册表项：**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. 对于 **LocalAccountTokenFilterPolicy** 值，将设置更改为 **1**。

   如果 **LocalAccountTokenFilterPolicy** 值不存在，请将其创建为 DWORD（32 位）。有关该值的更多信息，请参阅 Microsoft 文档：https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows。

注意
出于安全原因，建议在完成管理操作（例如远程安装）后，将两项设置还原为其原始状态：**EnableLUA=1** 和 **LocalAccountTokenFilterPolicy=0**。

部署代理程序

要从 安克诺斯数据保护软件 Web 中控台在远程计算机上安装保护代理程序，您的环境中必须至少已安装一个代理程序。此代理程序将用作远程安装的部署代理程序，并将连接到管理服务器和目标远程计算机。

通常，环境中的第一个保护代理程序是与管理服务器一起安装的代理程序。但是，可以选择环境中的每个适用于 Windows 的代理程序作为部署代理程序。

注意
当使用“自动发现”功能在多台计算机上安装保护代理程序时，部署代理程序称为发现代理程序。

部署代理程序的工作方式

1. 部署代理程序连接到管理服务器，并下载 `web_installer.exe` 文件。
2. 部署代理程序使用远程计算机的主机名或 IP 地址以及您指定的管理员凭据连接到该计算机，然后将 `web_installer.exe` 文件上传到该计算机。
3. 在远程计算机上，`web_installer.exe` 文件在无人参与模式下运行。
4. 根据所需安装的范围，Web 安装程序从管理服务器上的 `installation_files` 文件夹中检索其他安装包，然后使用 `msiexec` 命令将这些安装包安装在目标计算机上。

   `installation_files` 文件夹位于以下位置：

   - Windows：`\Program Files\Acronis\RemoteInstallationFiles\`
   - Linux：`/usr/lib/Acronis/RemoteInstallationFiles/`
5. 安装完成后，将在管理服务器上注册代理程序。

用于远程安装的组件

默认情况下，当安装管理服务器时，将安装用于远程安装的组件。

根据运行管理服务器的计算机的操作系统，可以在以下位置找到这些组件：

- Windows：`%Program Files%\Acronis\RemoteInstallationFiles\installation_files`
- Linux：`/usr/lib/Acronis/RemoteInstallationFiles/installation_files`

如果从旧版本的 Acronis 安克诺斯数据保护软件 升级，或者在安装管理服务器时明确排除了**用于远程安装的组件**，则这些位置可能不可用。在这种情况下，您需要通过更新和修改 Acronis 安克诺斯数据保护软件 的现有安装，来手动添加用于远程安装的组件。

将用于远程安装的组件添加到现有安装中

1. 从 Acronis 网站下载 Acronis 安克诺斯数据保护软件 的最新安装文件。
   选择与操作系统的位数相对应的安装文件。在大多数情况下，您将需要 **Windows 64 位**安装文件。如果您需要在 32 位计算机上远程安装保护代理程序，则下载 **Windows 32/64 位**安装文件。
2. 在运行管理服务器的计算机上，启动安装文件，然后选择**更新**。
3. 在更新完成后，再次启动安装文件，然后选择**修改当前安装**。
4. 选择**用于远程安装的组件**，然后单击**完成**。

在安装完成后，您将能够从 安克诺斯数据保护软件 Web 中控台在远程计算机上安装保护代理程序。

添加运行 Linux 的计算机

只能通过在本地安装保护代理程序来添加 Linux 计算机。不支持远程安装。

添加运行 Linux 的计算机

1. 在 安克诺斯数据保护软件 Web 中控台中，依次单击**所有设备** > **添加**。
2. 单击 **Linux**。
   安装程序即会下载到您的计算机上。
3. 在要保护的计算机上运行安装程序。有关详细信息，请参阅 "在 Linux 中安装"(第 94 页)。

添加运行 macOS 的计算机

只能通过在本地安装保护代理程序来添加 macOS 计算机。不支持远程安装。

添加运行 macOS 的计算机

1. 在 安克诺斯数据保护软件 Web 中控台中，依次单击**所有设备** > **添加**。
2. 单击 **Mac**。
   安装程序即会下载到您的计算机上。
3. 在要保护的计算机上运行安装程序。有关详细信息，请参阅 "在 macOS 中安装"(第 95 页)。

添加 vCenter 或 ESXi 主机

将 vCenter 或独立 ESXi 主机添加到管理服务器有四种方法：

- 部署适用于 VMware 的代理程序(虚拟设备)
  在大多数情况下都建议使用这种方法。虚拟设备将自动部署到由指定的 vCenter 所管理的每一台主机。您可以选择主机并自定义虚拟设备设置。
- 安装适用于 VMware 的代理程序 (Windows)
  出于卸载备份或无需 LAN 的备份的目的，您可能想要在运行 Windows 的物理机上安装适用于 VMware 的代理程序。

- **卸载备份**

  当您的生产 ESXi 主机负载过重，以致于虚拟设备的运行不符合需要时使用。
- **无需 LAN 的备份**

  如果 ESXi 使用 SAN 连接存储，则在连接至相同 SAN 的计算机上安装代理程序。代理程序将直接从存储备份虚拟机，而不是通过 ESXi 主机和 LAN。有关详细说明，请参阅"无需 LAN 的备份"。

如果管理服务器在 Windows 中运行，则代理程序将自动部署到指定的计算机。否则，需要手动安装代理程序。

- 注册已安装的适用于 VMware 的代理程序

  这是在重新安装管理服务器之后的必要步骤。此外，可以注册并配置根据 OVF 模板部署的适用于 VMware(虚拟设备) 的代理程序。
- 配置已注册的适用于 VMware 的代理程序

  这是在手动安装适用于 VMware 的代理程序 (Windows) 或部署 Acronis 安克诺斯数据保护软件设备之后的必要步骤。此外，可以将已配置的适用于 VMware 的代理程序与其他 vCenter 服务器或独立 ESXi 主机相关联。

通过 Web 界面部署适用于 VMware 的代理程序(虚拟设备)

1. 依次单击**所有设备** > **添加**。
2. 单击 **VMware ESXi**。
3. 选择**作为虚拟设备部署到 vCenter 的每台主机**。
4. 指定 vCenter 服务器或独立 ESXi 主机的地址和访问凭据。建议您使用指派了**管理员**角色的帐户。否则，提供在 vCenter 服务器或 ESXi 上具有必要权限的帐户。
5. 选择代理程序将用于访问管理服务器的该服务器的名称或 IP 地址。

   默认情况下，服务器名称处于选中状态。如果您的管理服务器有多个网络接口，或者您遇到导致代理程序注册失败的 DNS 问题，则可能需要改为选择 IP 地址。
6. [可选] 单击**设置**以自定义部署设置：
   - 要部署代理程序的 ESXi 主机(前提是在上一步中指定了 vCenter 服务器) 。
   - 虚拟设备名称。
   - 将包含该设备的数据存储。
   - 将包含该设备的资源集区或 vApp。
   - 虚拟设备的网络适配器将连接到的网络。
   - 虚拟设备的网络设置。您可以选择 DHCP 自动配置，也可以手动指定值(包括静态 IP 地址) 。
7. 单击**部署**。

安装适用于 VMware 的代理程序 (Windows)

准备

遵循"添加运行 Windows 的计算机"部分中所述的准备步骤进行操作。

安装

1. 依次单击**所有设备** > **添加**。
2. 单击 **VMware ESXi**。
3. 选择**在运行 Windows 的计算机上远程安装**。
4. 选择部署代理程序
5. 指定目标计算机的主机名或 IP 地址以及在该计算机上具有管理权限的帐户的凭据。
6. 选择代理程序将用于访问管理服务器的该服务器的名称或 IP 地址。
   默认情况下，服务器名称处于选中状态。如果您的管理服务器有多个网络接口，或者您遇到导致代理程序注册失败的 DNS 问题，则可能需要改为选择 IP 地址。
7. 单击**连接**。
8. 指定 vCenter 服务器或独立 ESXi 主机的地址和凭据，然后单击**连接**。建议您使用指派了**管理员**角色的帐户。否则，提供在 vCenter 服务器或 ESXi 上具有必要权限的帐户。
9. 单击**安装**以安装代理程序。

注册已安装的适用于 VMware 的代理程序

本部分介绍通过 Web 界面注册适用于 VMware 的代理程序。

其他注册方法：

- 您可以通过在虚拟设备 UI 中指定管理服务器，注册适用于 VMware 的代理程序（虚拟设备）。请参阅“根据 OVF 模板部署适用于 VMware 的代理程序（虚拟设备）”部分的“配置虚拟设备”下的步骤 3。
- 适用于 VMware 的代理程序 (Windows) 会在其本地安装过程中进行注册。

注册适用于 VMware 的代理程序

1. 依次单击**所有设备** > **添加**。
2. 单击 **VMware ESXi**。
3. 选择**注册已安装的代理程序**。
4. 选择部署代理程序
5. 如果注册*适用于 VMware 的代理程序 (Windows)*，请指定安装了该代理程序的计算机的主机名或 IP 地址，以及在该计算机上具有管理权限的帐户凭据。
   如果注册*适用于 VMware 的代理程序(虚拟设备)*，请指定虚拟设备的主机名或 IP 地址，以及运行该设备的 vCenter 服务器或独立 ESXi 主机的凭据。
6. 选择代理程序将用于访问管理服务器的该服务器的名称或 IP 地址。
   默认情况下，服务器名称处于选中状态。如果您的管理服务器有多个网络接口，或者您遇到导致代理程序注册失败的 DNS 问题，则可能需要改为选择 IP 地址。
7. 单击**连接**。
8. 指定 vCenter 服务器或 ESXi 主机的主机名或 IP 地址以及用于访问它的凭据，然后单击**连接**。建议您使用指派了**管理员**角色的帐户。否则，提供在 vCenter 服务器或 ESXi 上具有必要权限的帐

户。

9. 单击**注册**以注册该代理程序。

配置已注册的适用于 VMware 的代理程序

本部分介绍如何在 Web 界面中将适用于 VMware 的代理程序与 vCenter 服务器或 ESXi 相关联。还可以在适用于 VMware(虚拟设备) 的代理程序中控台中执行上述操作。

通过使用此步骤，还可以更改代理程序与 vCenter 服务器或 ESXi 的现有关联。还可以在适用于 VMware(虚拟设备) 的代理程序中控台中或通过依次单击**设置** > **代理程序** > 代理程序 > **详细信息** > **vCenter/ESXi** 来执行上述操作。

配置适用于 VMware 的代理程序

1. 依次单击**所有设备** > **添加**。
2. 单击 **VMware ESXi**。
3. 软件将显示按字母顺序第一个显示的未配置的适用于 VMware 的代理程序。
   如果管理服务器上注册的所有代理程序都已配置，则单击**配置已注册的代理程序**，软件将显示按字母顺序第一个显示的代理程序。
4. 如有必要，单击**装有代理程序的计算机**，然后选择要配置的代理程序。
5. 指定或更改 vCenter 服务器或 ESXi 主机的主机名或 IP 地址以及用于访问它的凭据。建议您使用指派了**管理员**角色的帐户。否则，提供在 vCenter 服务器或 ESXi 上具有必要权限的帐户。
6. 单击**配置**可保存更改。

添加 Scale Computing HC3 群集

将 Scale Computing HC3 群集添加到 安克诺斯数据保护软件 管理服务器

1. 在群集中部署适用于 Scale Computing HC3 的代理程序(虚拟设备)。
2. 配置它与该群集和 安克诺斯数据保护软件 管理服务器的连接。

以本地方式安装代理程序

在 Windows 中安装

若要安装适用于 Windows 的代理程序、适用于 Hyper-V 的代理程序、适用于 Exchange 的代理程序、适用于 SQL 的代理程序或适用于 Active Directory 的代理程序

1. 以管理员身份登录，然后启动 Acronis 安克诺斯数据保护软件 安装程序。
2. [可选] 要更改安装程序的语言，请单击**设置语言**。
3. 接受许可协议和隐私声明的条款，然后单击**继续**。
4. 选择**安装安全保护代理程序**。
5. 请执行以下任一操作：
   - 单击**安装**。
     这是安装产品的最简单方法。大部分安装参数将设为默认值。
     系统将安装以下组件：

- 适用于 Windows 的代理程序
- 其他代理程序(适用于 Hyper-V 的代理程序、适用于 Exchange 的代理程序、适用于 SQL 的代理程序和适用于 Active Directory 的代理程序),前提是在计算机上检测到各自的虚拟机监控程序或应用程序
- 可启动媒体生成器
- 命令行工具
- 安克诺斯数据保护软件监视器

- 单击**自定义安装设置**以配置设置。

  您可以选择要安装的组件和指定其他参数。有关详细信息,请参阅 "自定义安装设置"(第 77 页)。
- 单击**创建 .mst 和 .msi 文件用于无人参与安装**以解压缩安装包。查看或修改将添加到 .mst 文件的安装设置,然后单击**生成**。无需再执行此过程的其他步骤。

  如果要通过组策略部署代理程序,请遵循 "通过"组策略"部署代理程序"(第 156 页) 中所述操作。

6. 指定将注册带有代理程序的计算机的管理服务器:
   a. 指定安装了管理服务器的计算机的主机名或 IP 地址。
   b. 指定管理服务器管理员的凭据或注册标记。

      有关如何生成注册标记的详细信息,请参阅 "步骤 1:生成注册标记"(第 157 页)。
   c. 单击**完成**。
7. 如果出现系统提示,请选择要将带有代理程序的计算机添加到组织还是其中一个单位。

   在您管理多个单位或至少有一个单位的组织时,才会出现该提示。否则,会将计算机静默添加到您管理的单位或组织。有关详细信息,请参阅 "单位和管理帐户"(第 547 页)。
8. 继续安装。
9. 安装完成后,单击**关闭**。
10. 如果已安装适用于 Exchange 的代理程序,您将能够备份 Exchange 数据库。如果要备份 Exchange 邮箱,请打开 安克诺斯数据保护软件 Web 中控台,依次单击**添加** > **Microsoft Exchange Server** > **Exchange 邮箱**,然后指定已启用 Microsoft Exchange Server 的**客户端访问**服务器角色 (CAS) 的计算机。有关详细信息,请参阅 "邮箱备份"(第 389 页)。

在没有 Microsoft Exchange Server 的计算机上安装适用于 VMware 的代理程序 (Windows)、适用于 Office 365 的代理程序、适用于 Oracle 的代理程序或适用于 Exchange 的代理程序

1. 以管理员身份登录,然后启动 Acronis 安克诺斯数据保护软件 安装程序。
2. [可选] 要更改安装程序的语言,请单击**设置语言**。
3. 接受许可协议和隐私声明的条款,然后单击**继续**。
4. 选择**安装保护代理程序**,然后单击**自定义安装设置**。
5. 单击**安装内容**旁边的**更改**。
6. 选中对应于要安装的代理程序的复选框。取消选中不想要安装的组件的复选框。单击**完成**以继续。
7. 指定将注册带有代理程序的计算机的管理服务器:
   a. 在 **Acronis 安克诺斯数据保护软件 管理服务器**旁边,单击**指定**。

b. 指定安装了管理服务器的计算机的主机名或 IP 地址。
c. 指定管理服务器管理员的凭据或注册标记。
有关如何生成注册标记的详细信息，请参阅 "步骤 1：生成注册标记"(第 157 页)。
d. 单击**完成**。

8. 如果出现系统提示，请选择要将带有代理程序的计算机添加到组织还是其中一个单位。
在您管理多个单位或至少有一个单位的组织时，才会出现该提示。否则，会将计算机静默添加到您管理的单位或组织。有关详细信息，请参阅 "单位和管理帐户"(第 547 页)。
9. [可选] 更改其他安装设置，如 "自定义安装设置"(第 77 页) 中所述。
10. 单击**安装**以继续安装过程。
11. 安装完成后，单击**关闭**。
12. [仅在安装适用于 VMware (Windows) 的代理程序时] 执行 "配置已注册的适用于 VMware 的代理程序"(第 92 页) 中所述的步骤。
13. [仅在安装适用于 Exchange 的代理程序时] 打开 安克诺斯数据保护软件 Web 中控台，依次单击**添加** > **Microsoft Exchange Server** > **Exchange 邮箱**，然后指定已启用 Microsoft Exchange Server 的**客户端访问**服务器角色 (CAS) 的计算机。有关详细信息，请参阅 "邮箱备份"(第 389 页)。

在 Linux 中安装

准备

1. 确保计算机上已安装必要的 Linux 程序包。
2. 在 SUSE Linux 中安装代理程序时，请确保使用 su 而不是 sudo。否则，当尝试通过 安克诺斯数据保护软件 Web 中控台注册代理程序时，会发生以下错误：无法启动 Web 浏览器。无可用显示。
一些 Linux 发行版(如 SUSE) 在使用 sudo 时不传递 DISPLAY 变量，并且安装程序无法在图形用户界面 (GUI) 中打开浏览器。

安装

要安装适用于 Linux 的代理程序，需要至少 2 GB 可用磁盘空间。

安装适用于 Linux 的代理程序

1. 以根用户身份，导航到安装文件(.i686 或 .x86_64 文件) 所在的目录、使文件可执行，然后运行它。

```
chmod +x <installation file name>
```

```
./<installation file name>
```

2. 接受许可证协议的条款。
3. 指定要安装的组件：
a. 清除 **Acronis 安克诺斯数据保护软件 管理服务器**复选框。
b. 选中要安装的代理程序的复选框。以下代理程序可用：

- **适用于 Linux 的代理程序**
- **适用于 Oracle 的代理程序**

  适用于 Oracle 的代理程序需要另外安装适用于 Linux 的代理程序。

c. 单击**下一步**。

4. 指定将注册带有代理程序的计算机的管理服务器：
   a. 指定安装了管理服务器的计算机的主机名或 IP 地址。
   b. 指定管理服务器管理员的用户名和密码。
   c. 单击**下一步**。
5. 如果出现系统提示，请选择要将带有代理程序的计算机添加到组织还是其中一个单位，然后按 **Enter**。

   在上一个步骤中指定的帐户管理多个单位或至少有一个单位的组织时，才会出现该提示。
6. 如果在计算机上启用了 UEFI 安全启动，则会在安装后通知您需要重新启动系统。请务必记住应使用哪个密码（根用户或“acronis”之一）。

   注意
   该安装生成用于签署内核模块的新密钥。必须通过重新启动计算机将此新密钥注册为计算机所有者密钥 (MOK)。如果不注册新密钥，代理程序将无法运行。如果在安装代理程序后启用 UEFI 安全启动，需要重新安装该代理程序。

7. 安装完成后，执行以下操作之一：
   - 单击**重新启动**（如果在上一个步骤中提示您重新启动系统）。

     在系统重新启动期间，选择 MOK（计算机所有者密钥）管理，选择**注册 MOK**，然后使用上一个步骤中建议的密码注册密钥。
   - 否则，单击**退出**。

疑难解答信息在以下文件中提供：**/usr/lib/Acronis/BackupAndRecovery/HOWtO.InStALL**

在 macOS 中安装

安装适用于 Mac 的代理程序

1. 双击安装文件 (.dmg)。
2. 等待操作系统加载安装磁盘映像。
3. 双击**安装**，然后单击**继续**。
4. [可选] 单击**更改安装位置**以更改将安装软件的磁盘。默认情况下，将选定系统启动磁盘。
5. 单击**安装**。如果出现系统提示，请输入管理员的用户名和密码。
6. 指定其中将注册带有代理程序的计算机的管理服务器：
   a. 指定安装了管理服务器的计算机的主机名或 IP 地址。
   b. 指定管理服务器管理员的用户名和密码。
   c. 单击**注册**。
7. 如果出现系统提示，请选择要将带有代理程序的计算机添加到组织还是其中一个单位，然后单击**完成**。

在上一个步骤中指定的帐户管理多个单位或至少有一个单位的组织时，才会出现该提示。

8. 安装完成后，单击**关闭**。

无人参与安装或卸载

Windows 中的无人参与安装或卸载

本部分介绍如何在运行 Windows 的计算机上，通过使用 Windows 安装程序（即 `msiexec` 程序）在无人参与模式下安装或卸载 Acronis 安克诺斯数据保护软件。在 Active Directory 域中，执行无人参与安装的另一种方法是通过组策略，请参阅 "通过“组策略”部署代理程序"（第 156 页）。

在安装过程中，可以使用称为**转换**（.mst 文件）的文件。转换是一个带有安装参数的文件。还可以在命令行中直接指定安装参数。

创建 .mst 转换并提取安装包

1. 以管理员身份登录，然后启动安装程序。
2. 单击**创建 .mst 和 .msi 文件用于无人参与安装**。
3. [并非在所有安装程序中都可用] 在**组件位数**中，选择 **32 位**或 **64 位**。
4. 在**要安装的内容**中，选择要安装的组件，然后单击**完成**。
   将从安装程序中提取这些组件的安装软件包。
5. 在 **Acronis 安克诺斯数据保护软件 管理服务器**中，选择**使用凭据**或**使用注册标记**。根据您的选择，指定凭据或注册标记，然后单击**完成**。
   有关如何生成注册标记的详细信息，请参阅 "步骤 1：生成注册标记"（第 157 页）。
6. [仅在域控制器上安装时] 在**代理程序服务的登录帐户**中，选择**使用以下帐户**。指定将运行代理程序服务的用户帐户，然后单击**完成**。出于安全原因，安装程序不会自动在域控制器上创建新帐户。

   注意
   必须为指定的用户帐户授予作为服务登录权限。
   此帐户必须已在域控制器上使用，才能在该计算机上创建其配置文件文件夹。

   有关在只读域控制器上安装代理程序的详细信息，请参阅此知识库文章。
7. 查看或修改将添加到 .mst 文件的其他安装设置，然后单击**继续**。
8. 选择将生成 .mst 转换以及会将 .msi 和 .cab 安装包提取到的目标文件夹，然后单击**生成**。

因此，将生成 .mst 转换，并且 .msi 和 .cab 安装包将提取到您指定的文件夹。

使用 .mst 转换安装产品

在命令行上，运行以下命令：

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

其中：

- <软件包名称> 是 .msi 文件的名称。此名称为 **AB.msi** 或 **AB64.msi**，具体取决于操作系统的位数。
- <转换名称> 是转换的名称。此名称为 **AB.msi.mst** 或 **AB64.msi.mst**，具体取决于操作系统的位数。

例如，`msiexec /i AB64.msi TRANSFORMS=AB64.msi.mst`

通过手动指定参数来安装或卸载产品

在命令行上，运行以下命令：

```
msiexec /i <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

此处，<软件包名称> 是 .msi 文件的名称。此名称为 **AB.msi** 或 **AB64.msi**，具体取决于操作系统的位数。

可用参数及其值如 "命令参数"(第 98 页) 中所述。

示例

- 安装管理服务器和用于远程安装的组件。

  ```
  msiexec.exe /i ab64.msi /l*v my_log.txt /qn
  ADDLOCAL=AcronisCentralizedManagementServer,WebConsole,ComponentRegisterFeature
  TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
  AGREEMENT=1 AMS_USE_SYSTEM_ACCOUNT=1
  ```

- 安装适用于 Windows 的代理程序、命令行工具和 安克诺斯数据保护软件 监视器。在之前安装的管理服务器上注册带有代理程序的计算机。

  ```
  msiexec.exe /i ab64.msi /l*v my_log.txt /qn
  ADDLOCAL=AgentsCoreComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
  TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
  AGREEMENT=1 MMS_CREATE_NEW_ACCOUNT=1 REGISTRATION_ADDRESS=10.10.1.1
  ```

- 更新管理服务器、存储节点、目录服务和保护代理程序。

  ```
  msiexec.exe /i ab64.msi /l*v my_log.txt /qn
  ADDLOCAL=AcronisCentralizedManagementServer,BackupAndRecoveryAgent,AgentsCoreComponen
  ts,StorageServer,CatalogBrowser CATALOG_DATA_MIGRATION_PATH="C:\MyFolder\tmp"
  ```

无人参与安装或卸载参数

本部分介绍在 Windows 中的无人参与安装或卸载过程中所用的参数。

除了这些参数，还可以使用 `msiexec` 的其他参数，如 https://msdn.microsoft.com/zh-cn/library/windows/desktop/aa367988(v=vs.85).aspx 中所述。

命令参数

`ADDLOCAL=<list of components>`

要安装的组件使用逗号而非空格字符分隔。所有指定的组件必须在安装之前从安装程序中提取。

组件的完整列表如下所示。

组件	必须一起安装	位数	组件名称/描述
AcronisCentralizedManagementServer	WebConsole	32 位/64 位	管理服务器
WebConsole	AcronisCentralizedManagementServer	32 位/64 位	Web 中控台
ComponentRegisterFeature	AcronisCentralizedManagementServer	32 位/64 位	Components for Remote Installation
AtpScanService	AcronisCentralizedManagementServer	32 位/64 位	扫描服务
AgentsCoreComponents		32 位/64 位	用于代理程序的核心组件
BackupAndRecoveryAgent	AgentsCoreComponents	32 位/64 位	适用于 Windows 的代理程序
ArxAgentFeature	BackupAndRecoveryAgent	32 位/64 位	适用于 Exchange 的代理程序
ArsAgentFeature	BackupAndRecoveryAgent	32 位/64 位	适用于 SQL 的代理程序
ARADAgentFeature	BackupAndRecoveryAgent	32 位/64	适用于 Active

		位	Directory 的代理程序
OracleAgentFeature	BackupAndRecoveryAgent	32 位/64 位	适用于 Oracle 的代理程序
ArxOnlineAgentFeature	AgentsCoreComponents	32 位/64 位	适用于 Office 365 的代理程序
AcronisESXSupport	AgentsCoreComponents	32 位/64 位	适用于 VMware 的代理程序 (Windows)
HyperVAgent	AgentsCoreComponents	32 位/64 位	适用于 Hyper-V 的代理程序
ESXVirtualAppliance		32 位/64 位	适用于 VMware 的代理程序(虚拟设备)
ScaleVirtualAppliance		32 位/64 位	适用于 Scale Computing HC3 的代理程序(虚拟设备)
CommandLineTool		32 位/64 位	命令行工具
TrayMonitor	BackupAndRecoveryAgent	32 位/64 位	安克诺斯数据保护软件监视器
BackupAndRecoveryBootableComponents		32 位/64 位	可启动媒体生成器
PXEServer		32 位/64 位	PXE 服务器
StorageServer	BackupAndRecoveryAgent	64 位	存储节点

CatalogBrowser	JRE 8 Update 111 或更高版本	64 位	目录服务

TARGETDIR=<path>

将安装产品的文件夹。

REBOOT=ReallySuppress

如果已指定参数，则将禁止计算机重新启动。

CURRENT_LANGUAGE=<language ID>

产品语言。可用值如下所示：en、en_GB、cs、da、de、es_ES、fr、ko、it、hu、nl、ja、pl、pt、pt_BR、ru、tr、zh、zh_TW。

ACEP_AGREEMENT={0,1}

如果值为 1，计算机将参与 Acronis 客户体验计划 (ACEP)。

REGISTRATION_ADDRESS=<host name or IP address>:<port>

已安装管理服务器的计算机的主机名或 IP 地址。在 ADDLOCAL 参数中指定的代理程序、存储节点和目录服务将在该管理服务器上进行注册。如果端口号不同于默认值 (9877)，则必须要输入。

使用此参数时，必须指定 REGISTRATION_TOKEN 参数，或指定 REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD 参数。

REGISTRATION_TOKEN=<token>

在 安克诺斯数据保护软件 Web 中控台中生成的注册标记，如通过组策略部署代理程序中所述。

REGISTRATION_LOGIN=<user name>、REGISTRATION_PASSWORD=<password>

管理服务器管理员的用户名和密码。

REGISTRATION_TENANT=<unit ID>

组织内的单位。在 ADDLOCAL 参数中指定的代理程序、存储节点和目录服务将添加到该单位中。

要了解单位 ID，请在 安克诺斯数据保护软件 Web 中控台中，依次单击**设置** > **帐户**、选择单位，然后单击**详细信息**。

如果没有 REGISTRATION_TOKEN，或者 REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD，则该参数不起作用。在此情况下，组件将添加到组织。

如果没有此参数，组件将添加到组织。

REGISTRATION_REQUIRED={0,1}

注册失败时的安装结果。如果值为 1，安装会失败。如果值为 0，则安装会成功完成，即使组件未注册。

REGISTRATION_CA_SYSTEM={0,1}|REGISTRATION_CA_BUNDLE={0,1}|REGISTRATION_PINNED_PUBLIC_KEY=<public key value>

这些互相排斥的参数定义注册期间管理服务器证书检查的方法。如果想要验证管理服务器的真实性以防止 MITM 攻击，则检查证书。

如果值为 1，则验证会使用系统 CA，或相应地与产品一起交付的 CA 捆绑。如果指定了固定公钥，则验证将使用此密钥。如果值为 0 或者参数未指定，则不进行证书验证，但注册流量仍继续加密。

/l*v <log file>

如果已指定参数，详细模式下的安装日志会保存到指定的文件。该日志文件可用于分析安装问题。

管理服务器安装参数

WEB_SERVER_PORT=<port number>

Web 浏览器要用于访问管理服务器的端口。默认端口为 9877。

AMS_ZMQ_PORT=<port number>

将用于产品组件之间进行通信的端口。默认端口为 7780。

SQL_INSTANCE=<instance>

管理服务器使用的数据库。您可以选择任意版本的 Microsoft SQL Server 2012、Microsoft SQL Server 2014 或 Microsoft SQL Server 2016。您选择的实例也可被其它程序使用。

如果没有此参数，将使用内置的 SQLite 数据库。

SQL_USER_NAME=<user name> 和 SQL_PASSWORD=<password>

Microsoft SQL Server 登录帐户的凭据。管理服务器将使用这些凭据来连接到所选的 SQL Server 实例。如果没有这些参数，管理服务器将使用管理服务器服务帐户 (**AMS User**) 的凭据。

用于运行管理服务器服务的帐户

指定以下任一参数：

- AMS_USE_SYSTEM_ACCOUNT={0,1}
  如果值为 1，将使用系统帐户。
- AMS_CREATE_NEW_ACCOUNT={0,1}
  如果值为 1，将创建新帐户。
- AMS_SERVICE_USERNAME=<user name> 和 AMS_SERVICE_PASSWORD=<password>
  将使用指定的帐户。

代理程序安装参数

HTTP_PROXY_ADDRESS=<IP address> 和 HTTP_PROXY_PORT=<port>

代理程序要使用的 HTTP 代理服务器。如果没有这些参数，将不使用代理服务器。

`HTTP_PROXY_LOGIN=<login>` 和 `HTTP_PROXY_PASSWORD=<password>`

HTTP 代理服务器的凭据。如果服务器需要身份验证，请使用这些参数。

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

如果值为 `0` 或参数未指定，代理程序会将代理服务器仅用于备份和从云中恢复。如果值为 `1`，代理程序也将通过代理服务器连接到管理服务器。

`SET_ESX_SERVER={0,1}`

如果值为 `0`，要安装的适用于 VMware 的代理程序将不会连接到 vCenter 服务器或 ESXi 主机。在完成安装后，按照"配置已注册的适用于 VMware 的代理程序"中所述步骤继续操作。

如果值为 `1`，请指定以下参数：

`ESX_HOST=<host name or IP address>`

vCenter 服务器或 ESXi 主机的主机名或 IP 地址。

`ESX_USER=<user name>` 和 `ESX_PASSWORD=<password>`

访问 vCenter 服务器或 ESXi 主机的凭据。

用于运行代理程序服务的帐户

指定以下任一参数：

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`
  如果值为 `1`，将使用系统帐户。
- `MMS_CREATE_NEW_ACCOUNT={0,1}`
  如果值为 `1`，将创建新帐户。
- `MMS_SERVICE_USERNAME=<user name>` 和 `MMS_SERVICE_PASSWORD=<password>`
  将使用指定的帐户。

存储节点安装参数

用于运行存储节点服务的帐户

指定以下任一参数：

- `ASN_USE_SYSTEM_ACCOUNT={0,1}`
  如果值为 `1`，将使用系统帐户。
- `ASN_CREATE_NEW_ACCOUNT={0,1}`
  如果值为 `1`，将创建新帐户。
- `ASN_SERVICE_USERNAME=<user name>` 和 `ASN_SERVICE_PASSWORD=<password>`
  将使用指定的帐户。

目录服务安装参数

`CATALOG_DATA_MIGRATION_PATH=<path>`

使用此参数，将目录数据迁移到 Acronis 安克诺斯数据保护软件 15 更新 4 中的新版本目录服务。指定将在其中导出目录数据的临时文件夹的路径。

SKIP_CATALOG_DATA_MIGRATION=1

使用此参数，跳过迁移目录数据。

参数 SKIP_CATALOG_DATA_MIGRATION 和 CATALOG_DATA_MIGRATION_PATH 是互斥的。

卸载参数

REMOVE={<list of components>|ALL}

要删除的组件使用逗号而非空格字符分隔。

可用组件已在本部分的前面部分中介绍过。

如果值为 ALL，将卸载所有产品组件。此外，您还可以指定以下参数：

DELETE_ALL_SETTINGS={0, 1}

如果值为 1，将删除产品的日志、任务和配置设置。

Linux 中的无人参与安装或卸载

本部分介绍如何在运行 Linux 的计算机上，通过使用命令行在无人参与模式下安装或卸载 Acronis 安克诺斯数据保护软件。

安装或卸载产品

1. 打开终端。
2. 运行以下命令：

   ```
   <package name> -a <parameter 1> ... <parameter N>
   ```

   此处，<包名称> 是安装包（即 .i686 或 .x86_64 文件）的名称。
3. [仅在安装适用于 Linux 的代理程序时] 如果在计算机上启用了 UEFI 安全启动，则会在安装后通知您需要重新启动系统。请务必记住应使用哪个密码（根用户或“acronis”之一）。在系统重新启动期间，选择 MOK（计算机所有者密钥）管理，选择**注册 MOK**，然后使用建议的密码注册密钥。

如果在安装代理程序后启用 UEFI 安全启动，请重复该安装（包括步骤 3）。否则，备份将失败。

安装参数

命令参数

{-i |--id=}<list of components>

要安装的组件使用逗号而非空格字符分隔。

以下组件可安装：

组件	组件描述
AcronisCentralizedManagementServer	管理服务器
BackupAndRecoveryAgent	适用于 Linux 的代理程序
BackupAndRecoveryBootableComponents	可启动媒体生成器

如果没有此参数，将安装以上所有组件。

`--language=<language ID>`

产品语言。可用值如下所示：en、en_GB、cs、da、de、es_ES、fr、ko、it、hu、nl、ja、pl、pt、pt_BR、ru、tr、zh、zh_TW。

`{-d|--debug}`

如果参数已指定，将在详细模式下写入安装日志。日志位于文件 **/var/log/trueimage-setup.log** 中。

`{-t|--strict}`

如果参数已指定，则安装过程中出现的任何警告将导致安装失败。如果没有此参数，即使出现警告，安装也会成功完成。

`{-n|--nodeps}`

如果参数已指定，将在安装过程中忽略缺少的必要 Linux 包。

管理服务器安装参数

`{-W |--web-server-port=}<port number>`

Web 浏览器要用于访问管理服务器的端口。默认端口为 9877。

`--ams-tcp-port=<port number>`

将用于产品组件之间进行通信的端口。默认端口为 7780。

代理程序安装参数

指定以下任一参数：

- `--skip-registration`
  - 请勿在管理服务器上注册代理程序。
- `{-C |--ams=}<host name or IP address>`
  - 已安装管理服务器的计算机的主机名或 IP 地址。将在此管理服务器上注册代理程序。

如果在一个命令中同时安装代理程序和管理服务器，则不论是否使用 `-C` 参数，该代理程序都将在此管理服务器上注册。

使用此参数时，必须指定 `token` 参数，或指定 `login` 和 `password` 参数。

`--token=<token>`

在 安克诺斯数据保护软件 Web 中控台中生成的注册标记，如通过组策略部署代理程序中所述。

`{-g |--login=}<user name>` 和 `{-w |--password=}<password>`

管理服务器管理员的凭据。

`--unit=<unit ID>`

组织内的单位。代理程序将添加到此单位。

要了解单位 ID，请在 安克诺斯数据保护软件 Web 中控台中，依次单击**设置** > **帐户**、选择单位，然后单击**详细信息**。

如果没有此参数，代理程序将添加到组织。

`--reg-transport={https|https-ca-system|https-ca-bundle|https-pinned-public-key}`

注册期间管理服务器证书检查的方法。如果想要验证管理服务器的真实性以防止 MITM 攻击，则检查证书。

如果值为 `https` 或者参数未指定，则不进行证书检查，但注册流量仍继续加密。如果值不为 `https`，则检查会使用系统 CA，或者相应地使用与产品一起交付的 CA 捆绑或固定公钥。

`--reg-transport-pinned-public-key=<public key value>`

固定公钥值。该参数应一起指定或代替 `--reg-transport=https-pinned-public-key` 参数。

- `--http-proxy-host=<IP address>` 和 `--http-proxy-port=<port>`
  - HTTP 代理服务器，代理程序将用于备份和从云中恢复以及用于连接到管理服务器。如果没有这些参数，将不使用代理服务器。
- `--http-proxy-login=<login>` 和 `--http-proxy-password=<password>`
  - HTTP 代理服务器的凭据。如果服务器需要身份验证，请使用这些参数。
- `--no-proxy-to-ams`
  - 保护代理程序将连接到管理服务器，而不使用由 `--http-proxy-host` 和 `--http-proxy-port` 参数指定的代理服务器。

卸载参数

`{-u|--uninstall}`

卸载产品。

`--purge`

删除产品的日志、任务、和配置设置。

信息参数

`{-?|--help}`

显示参数描述。

`--usage`

显示命令使用的简要描述。

`{-v|--version}`

显示安装程序包的版本。

`--product-info`

显示产品名称和安装程序包的版本。

示例

- 安装管理服务器。

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- 安装管理服务器，指定自定义端口。

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer --
web-server-port 6543 --ams-tcp-port 8123
```

- 安装适用于 Linux 的代理程序，并在指定管理服务器上注册它。

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456
```

- 在指定单位中，安装适用于 Linux 的代理程序，并在指定管理服务器上注册它。

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456 -unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

macOS 中的无人参与安装或卸载

本部分介绍如何在运行 macOS 的计算机上，通过使用命令行在无人参与模式下安装、注册和卸载保护代理程序。有关如何下载安装文件 (.dmg) 的信息，请参阅“添加运行 macOS 的计算机”。

安装适用于 Mac 的代理程序

1. 创建将挂载安装文件 (.dmg) 的临时目录。

   ```
   mkdir <dmg_root>
   ```

   此处，`<dmg_root>` 是您选择的名称。
2. 挂载 .dmg 文件。

   ```
   hdiutil attach <dmg_file> -mountpoint <dmg_root>
   ```

   此处，`<dmg_file>` 是安装文件的名称。例如，**AcronisCyberProtect_15_MAC.dmg**

3. 运行安装程序。

```
sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
```

4. 卸载安装文件 (.dmg)。

```
hdiutil detach <dmg_root>
```

示例

-

```
mkdir mydirectory
```

```
hdiutil attach /Users/JohnDoe/AcronisCyberProtect_15_MAC.dmg -mountpoint mydirectory
```

```
sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
```

```
hdiutil detach mydirectory
```

注册适用于 Mac 的代理程序

请执行以下任一操作：

- 在特定管理员帐户下注册代理程序。

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
<management server address:port> -u <user name> -p <password>
```

<管理服务器地址:端口> 是安装了 Acronis 安克诺斯数据保护软件 管理服务器的计算机的主机名或 IP 地址。如果端口号不同于默认值 (9877)，则必须要输入。

<user name> 和 <password> 是将在其下注册代理程序的管理员帐户的凭据。

- 以特定单位注册代理程序。

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent  -o register -a
<management server address:port> -u <user name> -p <password> --tenant <unit ID>
```

要了解单位 ID，请在 安克诺斯数据保护软件 Web 中控台中，依次单击**设置** > **帐户**、选择所需单位，然后单击**详细信息**。

重要事项

管理员只能通过其组织层次级别指定单位 ID 来注册代理程序。单位管理员以其自己的单位及其子单位注册机计算机。组织管理员可以以所有单位注册组织管理员。有关不同管理员帐户的更多信息，请参阅“管理用户帐户和组织单位”。

- 使用注册标记来注册代理程序。

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
<management server address:port> --token <token>
```

注册标记是由 12 个字符组成的序列，由连字符分为三段。可以按"通过组策略部署代理程序"中所述，在 安克诺斯数据保护软件 Web 中控台中生成注册标记。

重要事项
在 macOS 10.14 或更高版本中，需要向保护代理程序授予全盘访问权限。为此，请转到**应用程序** > **实用程序**，然后运行**网络安全保护代理程序助手**。接着，按照应用程序窗口中的说明进行操作。

示例

使用用户名和密码注册。

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  https://10.250.144.179:9877 -u johndoe -p johnspassword
  ```

使用单位 ID 和管理员凭据注册。

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 4dd941c1-c03f-11ea-
  86d8-005056bdd3a0
  ```

使用标记注册。

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  https://10.250.144.179:9877 --token D91D-DC46-4F0B
  ```

卸载适用于 Mac 的代理程序

运行以下命令：

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
  Uninstall.app/Contents/MacOS/AgentUninstall /confirm
  ```

要卸载适用于 Mac 的代理程序删除所有日志、任务和配置设置，请运行以下命令：

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
  Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
  ```

手动注册计算机

除了在代理程序安装期间在 安克诺斯数据保护软件 管理服务器上注册计算机之外，还可以使用命令行接口来注册计算机。例如，如果已经安装代理程序但自动注册失败，或者您想要使用新帐户注
  ```

册现有计算机，可能需要这样做。

注册计算机

在安装代理程序的计算机的命令提示符下，运行以下命令之一：

- 要以特定的管理员帐户注册计算机，请执行以下操作：

  ```
  <path to the registration tool> -o register -a <management server address:port> -u
  <user name> -p <password>
  ```

  <path to the registration tool> 为：
  - 在 Windows 中：%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe
  - 在 Linux 中：/usr/lib/Acronis/RegisterAgentTool/RegisterAgent
  - 在 macOS 中：/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent

  <管理服务器地址:端口> 是安装了 Acronis 安克诺斯数据保护软件 管理服务器的计算机的主机名或 IP 地址。如果使用默认端口 9877，则不必明确指定。

  <user name> 和 <password> 是将在其下注册代理程序的管理员帐户的凭据。
- 要以特定单位注册计算机，请指定单位 ID：

  ```
  <path to the registration tool> -o register -a <management server address:port> u
  <user name> -p <password> --tenant <unit ID>
  ```

  要了解单位 ID，请在 安克诺斯数据保护软件 Web 中控台中，依次单击**设置** > **帐户**、选择所需单位，然后单击**详细信息**。

  重要事项
  管理员只能在其组织层次结构级别上注册代理程序。单位管理员以其自己的单位及其子单位注册机计算机。单位管理员可以以所有单位注册代理程序。有关不同管理员帐户的更多信息，请参阅“管理用户帐户和组织单位”。
- 使用注册标记来注册计算机。

  ```
  <path to the registration tool> -o register -a <management server address:port> --
  token <token>
  ```

  - 注册标记是由 12 个字符组成的序列，由连字符分为三段。有关如何生成注册标记的详细信息，请参阅“通过组策略部署代理程序”。

注销计算机

在安装代理的计算机的命令提示符下，运行以下命令：

```
<path to the registration tool> -o unregister
```

示例

Windows

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --token 3B4C-E967-4FBD
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o unregister
```

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --token 34F6-8C39-4A5C
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 --token 9DBF-3DA9-4DAB
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o unregister
```

带有特殊字符或空格的密码

如果密码中包含特殊字符或空格，请在命令行上键入时将密码括在引号中。

```
<path to the registration tool> -o register -a <management server address:port> -u <user
name> -p <"password">
```

示例(Windows)：

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p "johns password"
```

如果仍然收到错误：

1. 通过访问 https://www.base64encode.org/，将密码编码为 base64 格式。
2. 在命令行上，使用 -b 或 --base64 参数指定编码的密码。

示例(Windows)：

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

检查软件更新

只有组织管理员可使用此功能。

每次登录到 安克诺斯数据保护软件 Web 中控台时，Acronis 安克诺斯数据保护软件 都会检查 网站上是否有可用的新版本。如果是这样的话，则 安克诺斯数据保护软件 Web 中控台会在每个页面底部的**设备**、**计划**和**备份存储**选项卡下显示新版本的下载链接。还可在**设置** > **代理程序**页上获取该链接。

要启用或禁用自动检查更新，请更改**更新**系统设置。

要手动检查更新，请依次单击右上角的问号图标 > **关于** > **检查更新**，或者依次单击问号图标 > **检查更新**。

迁移管理服务器

可以将在 Windows 计算机上运行的管理服务器迁移到同一环境中的另一台 Windows 计算机上。

迁移过程包括以下几个阶段：

1. "源计算机上的操作"(第 112 页)
   在此阶段中，准备原始管理服务器上要迁移的数据。
2. "目标计算机上的操作"(第 113 页)
   在此阶段中，将安装并配置一个新的管理服务器，然后将数据从原始管理服务器复制到新管理服务器。

先决条件

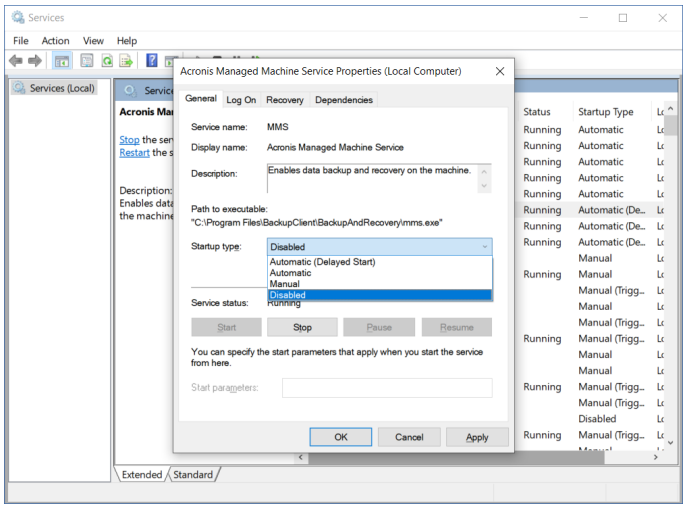
- 管理服务器使用外部 Microsoft SQL Server 数据库。Microsoft SQL Server 实例正在专用计算机上运行。
- 保护代理程序是使用其主机名而不是 IP 地址在管理服务器上注册的。
- 管理服务器的版本为 Acronis 安克诺斯数据保护软件 Update 4(内部版本 29486)或更高版本。
- 源计算机和目标计算机上都安装了相同版本的管理服务器。

源计算机上的操作

在此阶段中，准备要从原始管理服务器迁移的数据。

准备要迁移的数据

1. 在原始管理服务器计算机上，停止所有 Acronis 服务。
   a. 打开**服务**，然后禁止启动 Acronis 服务(**Acronis Active Protection Service** 和 **Acronis Cyber Protection Service** 除外)。



   b. 打开 **Regedit**，然后通过编辑其注册表项来禁用 **Acronis Active Protection Service** 和 **Acronis Cyber Protection Service**：

- 在注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisCyberProtectionService 中，打开 **Start** 值，然后将该值数据设置为 4。
- 在注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisActiveProtectionService 中，打开 **Start** 值，然后将该值数据设置为 4。

2. 重新启动管理服务器计算机，然后验证已禁用的 Acronis 服务是否不在运行。

注意
Acronis Scheduler Service Helper 和 **Acronis TIB Mounter Monitor** 这两项服务可能仍在运行。可以放心地忽略它们。

3. [如果 安克诺斯数据保护软件 监视器组件已安装在管理服务器计算机上] 退出 Acronis 安克诺斯数据保护软件 监视器。
4. 在 Windows 命令提示符下，通过运行以下命令，来更改 %ProgramData%\Acronis 和 %ProgramFiles%\Acronis 文件夹的所有者：

```
takeown /f "%ProgramData%\Acronis" /r /d y
```

```
takeown /f "%ProgramFiles%\Acronis" /r /d y
```

5. 通过运行以下命令，来编辑这些文件夹及其子文件夹的访问权限：

```
icacls "%ProgramData%\Acronis" /grant everyone:F /t
```

```
icacls "%ProgramFiles%\Acronis" /grant everyone:F /t
```

6. 将 %ProgramData%\Acronis 和 %ProgramFiles%\Acronis 文件夹复制到新管理服务器计算机可以访问的网络共享。
7. 关闭原始管理服务器计算机。

接下来，按照 "目标计算机上的操作"(第 113 页) 中的步骤操作。

目标计算机上的操作

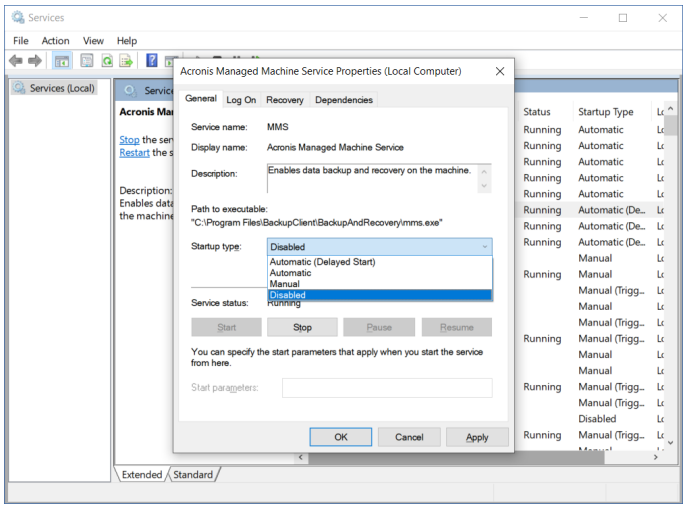
在此阶段中，将安装并配置一个新的管理服务器，然后将数据迁移到该新管理服务器。

在目标计算机上执行操作之前，请确保已完成 "源计算机上的操作"(第 112 页) 中的步骤。

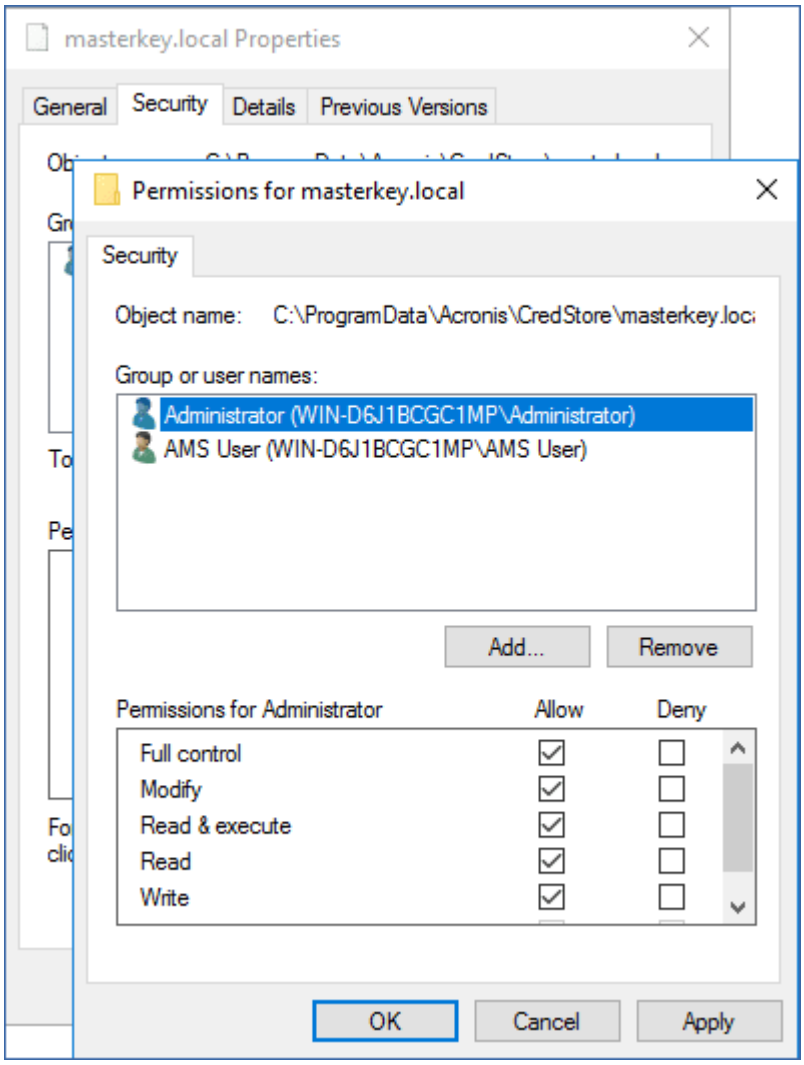
将数据迁移到新的管理服务器

1. 设置将在其上安装新管理服务器的计算机的主机名。此名称必须与装有原始管理服务器的计算机的名称相同。
2. 创建防火墙规则以阻止 TCP 端口 9877 上的所有流量。

3. 运行 Acronis 安克诺斯数据保护软件 安装程序。
   a. 接受许可协议和隐私声明的条款，然后单击**继续**。
   b. 单击**自定义安装设置**。
   c. 在**要安装的内容**中，仅选择以下组件，然后单击**完成**。
      - 管理服务器
      - Components for Remote Installation
      - 可启动媒体生成器
      - 命令行工具
   d. 在**管理服务器的数据库**中，保留默认选项**使用内置 SQLite**。
   e. 在**管理服务器服务的登录帐户**中，使用与原始管理服务器上相同的选项。
4. 停止所有 Acronis 服务。
   a. 打开**服务**，然后禁止启动所有 Acronis 服务。



   b. 重新启动计算机，然后验证已禁用的 Acronis 服务是否不在运行。
5. 导航到 `%ProgramData%\Acronis\CredStore`，然后调整 `masterkey.local` 文件的权限，如下所述：
   a. 将文件所有权授予 **Administrator** 用户帐户。
   b. 授予 **Administrator** 用户帐户**完全控制**权限。



6. 导航到 `%ProgramData%\Acronis\AMS\AccessVault\config`，然后授予 **Administrator** 用户帐户以下文件的**完全控制**权限：
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred`
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json`
7. 将以下文件夹替换为从原始管理服务器计算机复制到网络共享的文件夹：
   - `%ProgramData%\Acronis`
   - `%ProgramFiles%\Acronis`

   重要事项
   覆盖现有文件夹，无需先删除它们。

   注意
   如果您见到 `%ProgramFiles%\Acronis\ShellExtentions` 文件夹无法替换的消息，可以放心地跳过该文件夹。
8. 还原以下文件的权限：

- `%ProgramData%\Acronis\CredStore\masterkey.local` - 从有权限的用户列表中删除 **Administrator** 用户帐户。
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred` - 仅授予 **Administrator** 用户帐户**读取**权限。
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json` - 仅授予 **Administrator** 用户帐户**读取**权限。

9. 为 `NGMP\latest` 文件夹创建目录连接。
   - 在 Windows 命令提示符下，导航到 `%ProgramData%\Acronis\NGMP`，然后删除 `latest` 文件夹。

     ```
     cd %ProgramData%\Acronis\NGMP
     ```

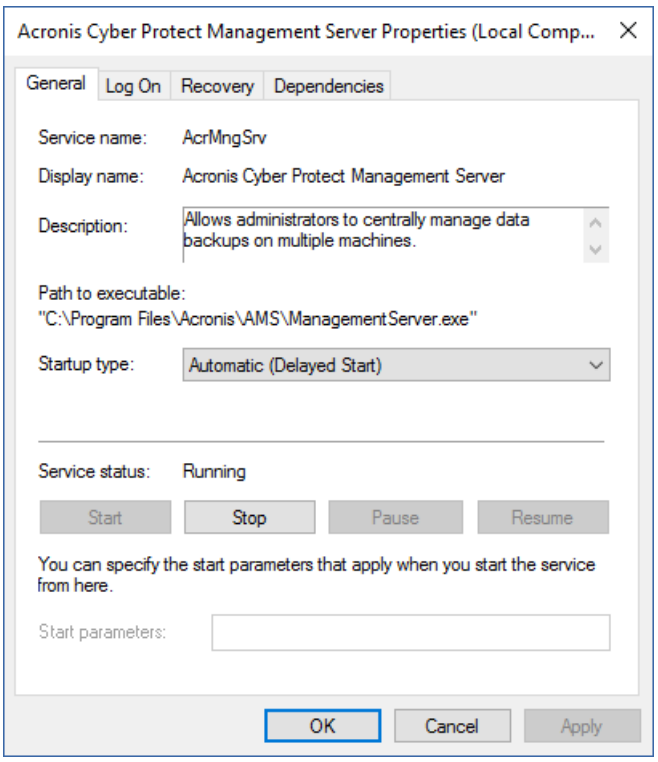
     ```
     rmdir latest
     ```

   - 创建目录连接 `latest`，并将其指向以当前 NGMP 版本命名的文件夹，例如：

     ```
     mklink /j latest C:\ProgramData\Acronis\NGMP\1.0.2653.0
     ```

10. 将新的管理服务器指向原始管理服务器使用的 Microsoft SQL Server 数据库。
    a. 打开 **Regedit**。
    b. 在注册表项 `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\AMS\Settings` 中，修改 `AmsDmlDbProtocol` 值，方法是将其数据更改为 `config://C:\ProgramData\Acronis\AMS\mssql\dml_mssql.config`。
11. 打开**服务**，然后启用所有已禁用的 Acronis 服务。

    将 **Acronis Cyber Protect Management Server** 的启动类型设置为**自动(延迟启动)**，并将所有其他 Acronis 服务的启动类型设置为**自动**。



12. 在防火墙中，允许 TCP 端口 9877 上的所有流量。

13. 重新启动计算机，然后验证所有 Acronis 服务是否正在运行。
14. 运行 Acronis 安克诺斯数据保护软件 安装程序并安装以下项目：
    - 适用于 Windows 的代理程序
    - [可选] 安克诺斯数据保护软件监视器
15. 重新启动计算机。

云部署

激活帐户

当管理员为您创建帐户时，将向您的电子邮件地址发送一封电子邮件。邮件包含以下信息：

- **帐户激活链接。**单击此链接并设置帐户密码。记住在帐户激活页面上显示的登录。
- **指向 安克诺斯数据保护软件 Web 中控台登录页面的链接。**将来使用此链接访问中控台。登录和密码与上一步中相同。

准备

步骤 1

根据您要备份的内容选择代理程序。有关代理程序的信息，请参阅 "组件"(第 45 页)。

步骤 2

下载安装程序。若要查找下载链接，请依次单击**所有设备** > **添加**。

添加设备页面为安装在 Windows 中的每个代理程序提供 Web 安装程序。Web 安装程序是一个小型可执行文件，用于从 Internet 下载主安装程序并将其另存为临时文件。此文件在安装后立即删除。

如果要本地存储安装程序，请通过使用**添加设备**页面底部的链接下载程序包(其中包含 Windows 中所有可供安装的代理程序) 。32 位和 64 位程序包均可用。这些程序包可使您自定义要安装的组件列表。这些程序包还支持无人参与安装，例如，通过“组策略”。此高级方案在 "通过“组策略”部署代理程序"(第 156 页) 中进行介绍。

要下载适用于 Office 365 的代理程序的安装程序，请单击右上角的帐户图标，然后依次单击**下载** > **适用于 Office 365 的代理程序**。

Linux 和 macOS 中的安装从一般安装程序执行。

所有安装程序都需要 Internet 连接，才能在网络安全保护服务中注册计算机。如果没有 Internet 连接，安装将失败。

步骤 3

在安装前，请确保防火墙和网络安全系统的其他组件(如代理服务器) 允许通过以下 TCP 端口的入站和出站连接：

- 端口 **443** 和 **8443**

  这些端口用于访问 安克诺斯数据保护软件 Web 中控台、注册代理程序、下载证书、用户授权和从云存储下载文件。
- 在 **7770 – 7800** 范围内的端口

  代理程序使用这些端口与管理服务器通信。
- 端口 **44445** 和 **55556**

  在备份和恢复期间，代理程序使用这些端口进行数据传输。

如果代理服务器在网络中处于启用状态，请参阅 "代理服务器设置"(第 119 页) 以了解是否需要在运行保护代理程序的每台计算机上配置这些设置。

通过云管理代理程序所需的最低互联网连接速度是 1 Mbit/s(请勿与备份到云时允许的数据传输速率相混淆)。如果您使用的是低带宽连接技术(例如 ADSL)，请考虑此选项。

备份和复制 VMware 虚拟机所需的 TCP 端口

- 端口 **443**

  适用于 VMware 的代理程序(Windows 和虚拟设备)连接到 ESXi 主机/vCenter 服务器上的此端口以执行 VM 管理操作(例如在备份、恢复和 VM 复制操作期间在 vSphere 上创建、更新和删除 VM)。
- 端口 **902**

  适用于 VMware 的代理程序(Windows 和虚拟设备)连接到 ESXi 主机上的此端口以建立 NFC 连接，以便在备份、恢复和 VM 复制操作期间在 VM 磁盘上读取/写入数据。
- 端口 **3333**

  如果适用于 VMware 的代理程序(虚拟设备)在作为 VM 复制目标的 ESXi 主机/簇上运行，则 VM 复制流量不会直接流向 ESXi 主机上的端口 **902**。相反，该流量会从源适用于 VMware 的代理程序流向位于目标 ESXi 主机/簇上的适用于 VMware 的代理程序(虚拟设备)上的 TCP 端口 **3333**。从原始 VM 磁盘读取数据的适用于 VMware 的源代理程序可以位于其他任何地方，并且可以是任何类型：虚拟设备或 Windows。

  负责在适用于 VMware 的目标代理程序(虚拟设备)上接受 VM 复制数据的服务称为“副本磁盘服务器”。此服务负责 WAN 优化技术，例如 VM 复制期间的流量压缩和重复数据删除，包括副本植入(请参阅植入初始副本)。当适用于 VMware 的代理程序(虚拟设备)未在目标 ESXi 主机上运行时，此服务不可用，因此副本植入方案不受支持。

步骤 4

在计划安装保护代理程序的计算机上，请确认其他进程不在使用以下本地端口。

- 127.0.0.1:**9999**
- 127.0.0.1:**43234**
- 127.0.0.1:**9850**

注意
无需在防火墙中打开它们。

Active Protection 服务正在侦听 TCP 端口 **6109**。请验证它是否未被其他进程使用。

更改保护代理程序使用的端口

保护代理程序所需的一些端口可能由您环境中的其他应用程序在使用。为了避免冲突，可以通过修改以下文件，来更改保护代理程序使用的默认端口。

- 在 Linux 中：`/opt/Acronis/etc/aakore.yaml`
- 在 Windows 中：`\ProgramData\Acronis\Agent\etc\aakore.yaml`

代理服务器设置

保护代理程序可以通过 HTTP/HTTPS 代理服务器传输数据。服务器必须通过 HTTP 隧道才能正常工作，不会扫描或干扰 HTTP 通信。不支持中间人代理。

因为安装期间代理程序在云中自行注册，所以必须在安装期间或事先提供代理服务器设置。

在 Windows 中

如果在 Windows(**控制面板** > **Internet 选项** > **连接**)中配置了代理服务器，则安装程序会从注册表读取代理服务器设置，并自动使用它们。此外，还可以在安装期间输入代理服务器设置，或者通过使用以下所述步骤进行事先指定。若要在安装之后更改代理服务器设置，请使用相同步骤。

若要在 Windows 中指定代理服务器设置

1. 创建新的文本文档并在文本编辑器(如记事本)中打开它。
2. 将以下行复制并粘贴到文件中：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
"Login"="proxy_login"
"Password"="proxy_password"
```

3. 将 `proxy.company.com` 替换为您的代理服务器主机名/IP 地址，将 `000001bb` 替换为端口号的十六进制值。例如，`000001bb` 是端口 443。
4. 如果代理服务器需要身份验证，请将 `proxy_login` 和 `proxy_password` 替换为代理服务器凭据。否则，从此文件中删除这些行。
5. 将文档另存为 **proxy.reg**。
6. 以管理员身份运行该文件。
7. 确认要编辑 Windows 注册表。
8. 如果尚未安装保护代理程序，现在可以安装它。否则，执行以下操作来重新启动代理程序：
   a. 在**开始**菜单中，单击**运行**，然后键入：**cmd**
   b. 单击**确定**。
   c. 运行以下命令：

```
net stop mms
net start mms
```

在 Linux 中

使用以下参数运行安装文件：`--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN--http-proxy-password=PASSWORD`。若要在安装之后更改代理服务器设置，请使用以下所述步骤。

若要在 Linux 中更改代理服务器设置

1. 使用文本编辑器打开文件 **/etc/Acronis/Global.config**。
2. 请执行以下任一操作：
   - 如果要在代理程序安装期间指定代理服务器设置，请找到以下部分：

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

   - 否则，将上述各行复制并粘贴到文件中的 `<registry name="Global">...</registry>` 标记之间。
3. 将 地址 替换为新代理服务器主机名称/IP 地址，将 端口 替换为端口号的十进制值。
4. 如果代理服务器需要身份验证，请将 登录 和 密码 替换为代理服务器凭据。否则，从此文件中删除这些行。
5. 保存文件。
6. 通过在任意目录中执行以下命令来重新启动代理程序：

   ```
   sudo service acronis_mms restart
   ```

在 macOS 中

可以在安装期间输入代理服务器设置，也可以通过使用以下所述步骤进行事先指定。若要在安装之后更改代理服务器设置，请使用相同步骤。

若要在 macOS 中指定代理服务器设置

1. 创建文件 **/Library/Application Support/Acronis/Registry/Global.config**，然后在文本编辑器（如 Text Edit）中打开它。
2. 将以下各行复制并粘贴到文件中

   ```
   <?xml version="1.0" ?>
   <registry name="Global">
     <key name="HttpProxy">
       <value name="Enabled" type="Tdword">"1"</value>
       <value name="Host" type="TString">"proxy.company.com"</value>
   ```

```
        <value name="Port" type="Tdword">"443"</value>
        <value name="Login" type="TString">"proxy_login"</value>
        <value name="Password" type="TString">"proxy_password"</value>
      </key>
    </registry>
```

3. 将 `proxy.company.com` 替换为您的代理服务器主机名/IP 地址，将 `443` 替换为端口号的十进制值。
4. 如果代理服务器需要身份验证，请将 `proxy_login` 和 `proxy_password` 替换为代理服务器凭据。否则，从此文件中删除这些行。
5. 保存文件。
6. 如果尚未安装保护代理程序，现在可以安装它。否则，执行以下操作来重新启动代理程序：
   a. 转到**应用程序** > **实用程序** > **终端**
   b. 运行以下命令：

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

在可启动媒体中

在可启动媒体下工作时，可能需要通过代理服务器访问云存储。要指定代理服务器设置，请依次单击**工具** > **代理服务器**，然后指定代理服务器主机名/IP 地址、端口和凭据。

安装代理程序

在 Windows 中

1. 确保计算机连接到 Internet。
2. 以管理员身份登录，然后启动安装程序。
3. [可选] 单击**自定义安装设置**，如果您想要执行以下操作，则可进行相应更改：
   - 更改要安装的组件(尤其是，禁止安装 安克诺斯数据保护软件 监视器和命令行工具)。
   - 更改在网络安全保护服务中注册计算机的方法。可以从**使用 安克诺斯数据保护软件 中控台**(默认设置)切换为**使用凭据**或**使用注册标记**。
   - 更改安装路径。
   - 更改代理程序服务的帐户。
   - 验证或更改代理服务器主机名/IP 地址、端口和凭据。如果在 Windows 中启用代理服务器，将自动检测到并使用它。
4. 单击**安装**。
5. [仅在安装适用于 VMware 的代理程序时] 指定代理程序将备份其虚拟机的 vCenter 服务器或独立 ESXi 主机的地址和访问凭据，然后单击**完成**。建议您使用指派了**管理员**角色的帐户。否则，提供在 vCenter 服务器或 ESXi 上具有必要权限的帐户。
6. [仅在域控制器上安装时] 指定将在其下运行代理程序服务的用户帐户，然后单击**完成**。出于安全原因，安装程序不会自动在域控制器上创建新帐户。

注意

必须为指定的用户帐户授予作为服务登录权限。

此帐户必须已在域控制器上使用，才能在该计算机上创建其配置文件文件夹。

有关在只读域控制器上安装代理程序的详细信息，请参阅此知识库文章。

7. 如果在步骤 3 中继续使用默认的注册方法**使用 安克诺斯数据保护软件 中控台**，请等到显示注册屏幕，然后继续进行下一步。否则，无需执行更多操作。

8. 请执行以下任一操作：
   - 单击**注册计算机**。在打开的浏览器窗口中，登录到 安克诺斯数据保护软件 Web 中控台、查看注册详细信息，然后单击**确认注册**。
   - 单击**显示注册信息**。安装程序将显示注册链接和注册码。可以复制它们，然后在其他计算机上执行注册步骤。在此情况下，您将需要在注册表中输入注册码。注册码在一个小时内有效。或者，可以通过单击**所有设备** > **添加**，向下滚动到**通过代码注册**，然后单击**注册**来访问注册表。

9. **注意**

   请勿退出安装程序，直到确认注册。若要再次启动注册，将需要重新启动安装程序，然后单击**注册计算机**。

结果，计算机将指派给用于登录到 安克诺斯数据保护软件 Web 中控台的帐户。

在 Linux 中

1. 确保计算机连接到 Internet。
2. 以根用户身份运行安装文件。

   如果在网络中启用了代理服务器，则在运行该文件时采用以下格式指定服务器主机名/IP 地址和端口：`--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN--http-proxy-password=PASSWORD`。

   如果要更改在网络安全保护服务中注册计算机的默认方法，请使用以下参数之一运行安装文件：
   - `--register-with-credentials` - 在安装期间要求提供用户名和密码
   - `--token=STRING` - 使用注册标记
   - `--skip-registration` - 跳过注册
3. 选中要安装的代理程序的复选框。以下代理程序可用：
   - **适用于 Linux 的代理程序**
   - **适用于 Virtuozzo 的代理程序**

   如果没有适用于 Linux 的代理程序，则无法安装适用于 Virtuozzo 的代理程序。
4. 如果在步骤 2 中保留使用默认的注册方法，请继续进行下一步。否则，输入网络安全保护服务的用户名和密码，或者等到使用标记注册计算机。

5. 请执行以下任一操作：
   - 单击**注册计算机**。在打开的浏览器窗口中，登录到 安克诺斯数据保护软件 Web 中控台、查看注册详细信息，然后单击**确认注册**。
   - 单击**显示注册信息**。安装程序将显示注册链接和注册码。可以复制它们，然后在其他计算机上执行注册步骤。在此情况下，您将需要在注册表中输入注册码。注册码在一个小时内有效。或者，可以通过单击**所有设备 > 添加**，向下滚动到**通过代码注册**，然后单击**注册**来访问注册表。

6. **注意**
   请勿退出安装程序，直到确认注册。要再次启动注册，将需要重新启动安装程序并重复安装步骤。

   结果，计算机将指派给用于登录到 安克诺斯数据保护软件 Web 中控台的帐户。
7. 如果在计算机上启用了 UEFI 安全启动，则会在安装后通知您需要重新启动系统。请务必记住应使用哪个密码（根用户或“acronis”之一）。

   注意
   安装期间，将生成一个新密钥，用于对 snapapi 模块签名，并注册为计算机所有者密钥 (MOK)。必须重新启动，才能注册此密钥。如果不注册该密钥，代理程序将无法运行。如果在安装代理程序后启用 UEFI 安全启动，请重复该安装（包括步骤 6）。

8. 安装完成后，执行以下操作之一：
   - 单击**重新启动**（如果在上一个步骤中提示您重新启动系统）。
     在系统重新启动期间，选择 MOK（计算机所有者密钥）管理，选择**注册 MOK**，然后使用上一个步骤中建议的密码注册密钥。
   - 否则，单击**退出**。

疑难解答信息在以下文件中提供：**/usr/lib/Acronis/BackupAndRecovery/HOWtO.InStALL**

在 macOS 中

1. 确保计算机连接到 Internet。
2. 双击安装文件 (.dmg)。
3. 等待操作系统加载安装磁盘映像。
4. 双击**安装**。
5. 如果在网络中启用代理服务器，请单击菜单栏中的**保护代理程序**、单击**代理服务器设置**，然后指定代理服务器主机名/IP 地址、端口和凭据。
6. 如果出现提示，请提供管理员凭据。
7. 单击**继续**。
8. 请等待，直到注册屏幕出现。
9. 请执行以下任一操作：
   - 单击**注册计算机**。在打开的浏览器窗口中，登录到 安克诺斯数据保护软件 Web 中控台、查看注册详细信息，然后单击**确认注册**。

- 单击**显示注册信息**。安装程序将显示注册链接和注册码。可以复制它们，然后在其他计算机上执行注册步骤。在此情况下，您将需要在注册表中输入注册码。注册码在一个小时内有效。或者，可以通过单击**所有设备** > **添加**，向下滚动到**通过代码注册**，然后单击**注册**来访问注册表。

10. **提示** 请勿退出安装程序，直到确认注册。要再次启动注册，将需要重新启动安装程序并重复安装步骤。

结果，计算机将指派给用于登录到 安克诺斯数据保护软件 Web 中控台的帐户。

在 Windows 计算机上更改登录帐户

在**选择组件**屏幕上，通过指定**代理程序服务的登录帐户**来定义将运行服务的帐户。可选择以下其中一个选项：

- **使用服务用户帐户**（代理程序服务的默认帐户）
  服务用户帐户是用于运行服务的 Windows 系统帐户。此设置的优点是域安全策略不会影响这些帐户的用户权限。默认情况下，该代理程序在**本地系统**帐户下运行。
- **创建新帐户**
  代理程序的帐户名称将是“Agent User”。
- **使用以下帐户**
  如果将代理程序安装在域控制器上，则系统会提示您为代理程序指定现有帐户（或相同帐户）。出于安全原因，系统不会自动在域控制器上创建新帐户。
  必须为安装程序在域控制器上运行时指定的用户帐户授予作为服务登录权限。此帐户必须已在域控制器上使用，才能在该计算机上创建其配置文件文件夹。
  有关在只读域控制器上安装代理程序的详细信息，请参阅此知识库文章。

如果选择**创建新帐户**或**使用以下帐户**选项，请确保域安全策略不会影响相关的帐户权限。如果帐户被剥夺了安装期间分配的用户权限，则组件可能不会正常工作或不工作。

登录帐户所需的权限

保护代理程序在 Windows 计算机上作为 Managed Machine Service (MMS) 运行。将运行代理程序所使用的帐户必须具有该代理程序的特定权限，才能使它正常工作。因此，应该为 MMS 用户指派以下权限：

1. 包含在**备份操作员**和**管理员**组中。在域控制器上，用户必须包含在**域管理员**组中。
2. 已授予对文件夹 `%PROGRAMDATA%\Acronis`（在 Windows XP 和 Server 2003 中为 `%ALLUSERSPROFILE%\Application Data\Acronis`）及其子文件夹的**完全控制**权限。
3. 已授予对以下项中的某些注册表项的**完全控制**权限：`HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`。
4. 已指派以下用户权限：
   - 作为服务登录
   - 调整进程的内存分配
   - 替换进程级别令牌
   - 修改固件环境值

如何指派用户权限

按照以下说明指派用户权限(本示例使用**作为服务登录**用户权限,与其他用户权限的步骤相同):

1. 使用具有管理权限的帐户登录到计算机。
2. 从**控制面板**打开**管理工具**(或单击 Win+R、键入 **control admintools**,然后按 Enter 键),然后打开**本地安全策略**。
3. 展开**本地策略**,然后单击**用户权限分配**。
4. 在右侧窗格中,右键单击**作为服务登录**,然后选择**属性**。
5. 单击**添加用户或组...**按钮,以添加新用户。
6. 在**选择用户、计算机、服务帐户或组**窗口中,找到要输入的用户,然后单击**确定**。
7. 在**作为服务登录属性**中单击**确定**,以保存更改。

重要事项
确保已向其添加**作为服务登录**用户权限的用户未列于**本地安全策略**的**拒绝作为服务登录**策略中。

请注意,不建议在安装完成后手动更改登录帐户。

无人参与安装或卸载

Windows 中的无人参与安装或卸载

本部分介绍如何在运行 Windows 的计算机上,通过使用 Windows 安装程序(即 `msiexec` 程序)在无人参与模式下安装或卸载保护代理程序。在 Active Directory 域中,执行无人参与安装的另一种方法是通过组策略,请参阅 "通过"组策略"部署代理程序"(第 156 页)。

在安装过程中,可以使用称为**转换**(.mst 文件)的文件。转换是一个带有安装参数的文件。还可以在命令行上直接指定安装参数。

创建 .mst 转换并提取安装包

1. 以管理员身份登录,然后启动安装程序。
2. 单击**创建 .mst 和 .msi 文件用于无人参与安装**。
3. 在**要安装的内容**中,选择要安装的组件,然后单击**完成**。
   将从安装程序中提取这些组件的安装软件包。
4. 在**注册设置**中,选择**使用凭据**或**使用注册标记**。有关如何生成注册标记的详细信息,请参阅 "步骤 1:生成注册标记"(第 157 页)。
5. [仅在域控制器上安装时]在**代理程序服务的登录帐户**中,选择**使用以下帐户**。指定将运行代理程序服务的用户帐户,然后单击**完成**。出于安全原因,安装程序不会自动在域控制器上创建新帐户。

注意
必须为指定的用户帐户授予作为服务登录权限。
此帐户必须已在域控制器上使用，才能在该计算机上创建其配置文件文件夹。

有关在只读域控制器上安装代理程序的详细信息，请参阅此知识库文章。

6. 查看或修改将添加到 .mst 文件的其他安装设置，然后单击**继续**。
7. 选择将生成 .mst 转换以及会将 .msi 和 .cab 安装包提取到的目标文件夹，然后单击**生成**。

使用 .mst 转换安装产品

在命令行上，运行以下命令。

命令模板：

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

其中：

- <软件包名称> 是 .msi 文件的名称。
- <转换名称> 是转换的名称。

命令示例：

```
msiexec /i BackupClient64.msi TRANSFORMS=BackupClient64.msi.mst
```

通过手动指定参数来安装或卸载产品

在命令行上，运行以下命令。

命令模板(正在安装)：

```
msiexec /i <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

此处，<软件包名称> 是 .msi 文件的名称。所有可用参数及其值如 "基本参数"(第 127 页) 中所述。

命令模板(正在卸载)：

```
msiexec /x <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

.msi 程序包必须与要卸载的产品具有相同版本。

无人参与安装或卸载参数

本部分介绍在 Windows 中的无人参与安装或卸载过程中所用的参数。除了这些参数，还可以使用 `msiexec` 的其他参数，如 https://msdn.microsoft.com/zh-cn/library/windows/desktop/aa367988(v=vs.85).aspx 中所述。

基本参数

`ADDLOCAL=<list of components>`

要安装的组件以逗号分隔且没有空格。所有指定的组件必须在安装之前从安装程序中提取。

组件的完整列表如下所示：

组件	必须一起安装	位数	组件名称/描述
MmsMspComponents		32 位/64 位	用于代理程序的核心组件
BackupAndRecoveryAgent	MmsMspComponents	32 位/64 位	适用于 Windows 的代理程序
ArxAgentFeature	BackupAndRecoveryAgent	32 位/64 位	适用于 Exchange 的代理程序
ArsAgentFeature	BackupAndRecoveryAgent	32 位/64 位	适用于 SQL 的代理程序
ARADAgentFeature	BackupAndRecoveryAgent	32 位/64 位	适用于 Active Directory 的代理程序
ArxOnlineAgentFeature	MmsMspComponents	32 位/64 位	适用于 Office 365 的代理程序
OracleAgentFeature	BackupAndRecoveryAgent	32 位/64 位	适用于 Oracle 的代理程序
AcronisESXSupport	MmsMspComponents	64 位	适用于 VMware ESX(i) 的代理程序 (Windows)
HyperVAgent	MmsMspComponents	32 位/64 位	适用于 Hyper-V 的代理程序
CommandLineTool		32 位/64 位	命令行工具

TrayMonitor	BackupAndRecoveryAgent	32 位/64 位	网络安全保护监视器

TARGETDIR= <path>

将安装产品的文件夹。默认情况下，此文件夹为：C:\Program Files\BackupClient。

REBOOT=ReallySuppress

如果已指定参数，则将禁止计算机重新启动。

/l*v <log file>

如果已指定参数，详细模式下的安装日志会保存到指定的文件。该日志文件可用于分析安装问题。

CURRENT_LANGUAGE= <language ID>

产品语言。可用值如下所示：en、bg、cs、da、de、es、fr、hu、id、it、ja、ko、ms、nb、nl、pl、pt、pt_BR、ru、fi、sr、sv、tr、zh、zh_TW。
如果未指定此参数，则产品语言将由系统语言定义，前提是该语言列于上述列表中。否则，产品语言将设置为英语 (en)。

注册参数

REGISTRATION_ADDRESS

这是 安克诺斯数据保护软件 服务的 URL。可以将此参数与 REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD 参数一起使用，也可以与 REGISTRATION_TOKEN 参数一起使用。

- 当将 REGISTRATION_ADDRESS 与 REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD 参数一起使用时，请指定用于**登录**到 安克诺斯数据保护软件 服务的地址。例如，https://cloud.company.com:

- 当将 REGISTRATION_ADDRESS 与 REGISTRATION_TOKEN 参数一起使用时，请指定准确的数据中心地址。这是您在**登录**到 安克诺斯数据保护软件 服务后所见到的 URL。例如，https://eu2-cloud.company.com。

请勿在此处使用 https://cloud.company.com。

REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD

将在 安克诺斯数据保护软件 服务中注册代理程序所使用帐户的凭据。这不能是合作伙伴管理员帐户。

REGISTRATION_PASSWORD_ENCODED

将在 安克诺斯数据保护软件 服务中注册代理程序所使用帐户的密码，以 base64 编码。有关如何编码密码的详细信息，请参阅“手动注册计算机”。

`REGISTRATION_TOKEN`

注册标记是由 12 个字符组成的序列，由连字符分为三段。可以按“通过组策略部署代理程序”中所述，在 Web 中控台中生成注册标记。

`REGISTRATION_REQUIRED={0,1}`

定义注册失败后如何完成安装。如果值为 1，安装也会失败。默认值为 0，因此如果未指定此参数，安装将成功完成，即使代理程序未注册也是如此。

其他参数

要在 Windows 中定义代理程序服务的登录帐户，请使用以下参数之一：

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`
  如果值为 1，代理程序将在**本地系统**帐户下运行。
- `MMS_CREATE_NEW_ACCOUNT={0,1}`
  如果值为 1，代理程序将在名为 **Acronis Agent User** 的新创建帐户下运行。
- `MMS_SERVICE_USERNAME=<user name>` 和 `MMS_SERVICE_PASSWORD=<password>`
  这些参数用于指定将运行代理程序所使用的现有帐户。

有关登录帐户的详细信息，请参阅“在 Windows 计算机上更改登录帐户”。

`SET_ESX_SERVER={0,1}`

- 如果值为 0，要安装的适用于 VMware 的代理程序将不会连接到 vCenter 服务器或 ESXi 主机。如果值为 1，请指定以下参数：
  - `ESX_HOST=<host name>`
    vCenter 服务器或 ESXi 主机的主机名或 IP 地址。
  - `ESX_USER=<user name>` 和 `ESX_PASSWORD=<password>`
    访问 vCenter 服务器或 ESXi 主机的凭据。

`HTTP_PROXY_ADDRESS=<IP address>` 和 `HTTP_PROXY_PORT=<port>`

代理程序要使用的 HTTP 代理服务器。如果没有这些参数，将不使用代理服务器。

`HTTP_PROXY_LOGIN=<login>` 和 `HTTP_PROXY_PASSWORD=<password>`

HTTP 代理服务器的凭据。如果服务器需要身份验证，请使用这些参数。

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

如果值为 0 或参数未指定，代理程序会将代理服务器仅用于备份和从云中恢复。如果值为 1，代理程序也将通过代理服务器连接到管理服务器。

卸载参数

`REMOVE={<list of components>|ALL}`

要删除的组件以逗号分隔且没有空格。如果值为 ALL，将卸载所有产品组件。

此外，您还可以指定以下参数：

DELETE_ALL_SETTINGS={0, 1}

如果值为 1，将删除产品的日志、任务和配置设置。

示例

- 安装适用于 Windows 的代理程序、命令行工具和网络安全保护监视器。使用用户名和密码在 安克诺斯数据保护软件 服务中注册计算机。

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_SYSTEM_
ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com REGISTRATION_LOGIN=johndoe
REGISTRATION_PASSWORD=johnspassword
```

- 安装适用于 Windows 的代理程序、命令行工具和网络安全保护监视器。在 Windows 中为代理程序服务创建一个新的登录帐户。使用标记在 安克诺斯数据保护软件 服务中注册计算机。

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_CREATE_NEW_
ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com REGISTRATION_TOKEN=34F6-
8C39-4A5C
```

- 安装适用于 Windows 的代理程序、命令行工具、适用于 Oracle 的代理程序和网络安全保护监视器。使用用户名和以 base64 编码的密码在 安克诺斯数据保护软件 服务中注册计算机。

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgentFeature,T
rayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_
LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com
REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
```

- 安装适用于 Windows 的代理程序、命令行工具和网络安全保护监视器。使用标记在 安克诺斯数据保护软件 服务中注册计算机。设置 HTTP 代理。

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com
REGISTRATION_TOKEN=34F6-8C39-4A5C HTTP_PROXY_ADDRESS=https://my-proxy.company.com
HTTP_PROXY_PORT=80 HTTP_PROXY_LOGIN=tomsmith HTTP_PROXY_PASSWORD=tomspassword
```

- 卸载所有代理程序并删除其日志、任务和配置设置。

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt REMOVE=ALL DELETE_ALL_
SETTINGS=1 REBOOT=ReallySuppress
```

Linux 中的无人参与安装或卸载

本部分介绍如何在运行 Linux 的计算机上，通过使用命令行在无人参与模式下安装或卸载保护代理程序。

安装或卸载保护代理程序

1.打开终端。

2.请执行以下任一操作：

- 要通过在命令行上指定参数来开始安装，请运行以下命令：

  ```
  <package name> -a <parameter 1> ... <parameter N>
  ```

  此处，<包名称> 是安装包（即 .i686 或 .x86_64 文件）的名称。所有可用参数及其值如“无人参与安装或卸载参数”中所述。
- 要使用在单独的文本文件中指定的参数开始安装，请运行以下命令：

  ```
  <package name> -a --options-file=<path to the file>
  ```

  如果您不希望在命令行上输入敏感信息，则此方法可能非常有用。在这种情况下，可以在单独的文本文件中指定配置设置，并确保只有您可以访问它。将每个参数都放置于一个新行上，后跟所需的值，例如：

  ```
  --rain=https://cloud.company.com
  --login=johndoe
  --password=johnspassword
  --auto
  ```

  或

  ```
  -C
  https://cloud.company.com
  -g
  johndoe
  -w
  johnspassword
  -a
  --language
  en
  ```

  如果在命令行上和文本文件中同时指定了相同的参数，则命令行值优先。

3。如果在计算机上启用了 UEFI 安全启动，则会在安装后通知您需要重新启动系统。请务必记住应使用哪个密码（根用户或“acronis”之一）。在系统重新启动期间，选择 MOK（计算机所有者密钥）管理，选择**注册 MOK**，然后使用建议的密码注册密钥。

如果在安装代理程序后启用 UEFI 安全启动，请重复该安装（包括步骤 3）。否则，备份将失败。

无人参与安装或卸载参数

本部分介绍在 Linux 中进行无人参与安装或卸载过程中所用的参数。

无人参与安装的最小配置包括 -a 和注册参数(例如，--login 和 --password 参数；--rain 和 --token 参数)。可以使用更多参数来自定义安装。

安装参数

基本参数

{-i |--id=} <list of components>

要安装的组件以逗号分隔且没有空格。以下组件在 .x86_64 安装包中提供：

组件	组件描述
BackupAndRecoveryAgent	适用于 Linux 的代理程序
AgentForPCS	适用于 Virtuozzo 的代理程序
OracleAgentFeature	适用于 Oracle 的代理程序

如果没有此参数，将安装以上所有组件。

适用于 Virtuozzo 的代理程序和适用于 Oracle 的代理程序都需要另外安装适用于 Linux 的代理程序。

.i686 安装包仅包含 BackupAndRecoveryAgent。

{-a|--auto}

安装和注册过程将在无需任何进一步用户交互的情况下完成。使用此参数时，必须使用 --token 参数或使用 --login 和 --password 参数指定将在 安克诺斯数据保护软件 服务中注册代理程序所使用的帐户。

{-t|--strict}

如果该参数已指定，则在安装过程中出现的任何警告将导致安装失败。如果没有此参数，即使出现警告，安装也会成功完成。

{-n|--nodeps}

将在安装过程中忽略缺少的必要 Linux 程序包。

{-d|--debug}

将在详细模式下写入安装日志。

--options-file= <location>

安装参数将从文本文件而不是命令行中读取。

--language= <language ID>

产品语言。可用值如下所示：en、bg、cs、da、de、es、fr、hu、id、it、ja、ko、ms、nb、nl、pl、pt、pt_BR、ru、fi、sr、sv、tr、zh、zh_TW。
如果未指定此参数，则产品语言将由系统语言定义，前提是该语言列于上述列表中。否则，产品语言将设置为英语 (en)。

注册参数

指定以下任一参数：

- {-g|--login=} <user name> 和 {-w|--password=}<password>

  将在 安克诺斯数据保护软件 服务中注册代理程序所使用帐户的凭据。这不能是合作伙伴管理员帐户。

- --token= <token>

  注册标记是由 12 个字符组成的序列，由连字符分为三段。可以按"通过组策略部署代理程序"中所述，在 Web 中控台中生成注册标记。

  不能将 --token 参数与 --login、--password 和 --register-with-credentials 参数一起使用。

  - {-C|--rain=} <service address>

    安克诺斯数据保护软件 服务的 URL。

    在使用 --login 和 --password 参数进行注册时，无需显式包含此参数，因为安装程序会默认使用正确地址 - 这将是您用于**登录**到 安克诺斯数据保护软件 服务的地址。例如：

    但是，当将 {-C|--rain=} 与 --token 参数一起使用时，必须指定准确的数据中心地址。这是您在**登录**到 安克诺斯数据保护软件 服务后所见到的 URL。例如：

- --register-with-credentials

  如果已指定此参数，则安装程序的图形界面将启动。要完成注册，请输入将在 安克诺斯数据保护软件 服务中注册代理程序所使用帐户的用户名和密码。这不能是合作伙伴管理员帐户。

- --skip-registration

  如果需要安装代理程序，但计划稍后在 安克诺斯数据保护软件 服务中进行注册，请使用此参数。有关如何执行此操作的详细信息，请参阅"手动注册计算机"。

其他参数

--http-proxy-host= <IP address> 和 --http-proxy-port=<port>

HTTP 代理服务器，代理程序将用于备份和从云中恢复以及用于连接到管理服务器。如果没有这些参数，将不使用代理服务器。

`--http-proxy-login=<login>` 和 `--http-proxy-password=<password>`

HTTP 代理服务器的凭据。如果服务器需要身份验证，请使用这些参数。

`--tmp-dir=<location>`

指定安装过程中存储临时文件的文件夹。默认文件夹为 **/var/tmp**。

`{-s|--disable-native-shared}`

即使系统上可能已经存在可再发行库，在安装过程中也会使用它们。

`--skip-prereq-check`

将不会检查编译 snapapi 模块所需的程序包是否已安装。

`--force-weak-snapapi`

安装程序将不会编译 snapapi 模块。相反，它将使用可能与 Linux 内核不完全匹配的现成模块。不建议使用此选项。

`--skip-svc-start`

安装后，服务将不会自动启动。通常，此参数与 `--skip-registration` 参数一起使用。

信息参数

`{-?|--help}`

显示参数描述。

`--usage`

显示命令使用的简要描述。

`{-v|--version}`

显示安装程序包的版本。

`--product-info`

显示产品名称和安装程序包的版本。

`--snapapi-list`

显示可用的现有 snapapi 模块。

`--components-list`

显示安装程序组件。

旧功能的参数

这些参数与旧组件 agent.exe 有关。

`{-e|--ssl=}<path>`

指定用于 SSL 通信的自定义证书文件的路径。

{-p|--port=} <port>

指定 agent.exe 侦听连接的端口。默认端口为 9876。

卸载参数

{-u|--uninstall}

卸载产品。

--purge

卸载产品并删除其日志、任务和配置设置。使用 --purge 参数时，无需显式指定 --uninstall 参数。

示例

- 在不注册的情况下安装适用于 Linux 的代理程序。

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a --skip-registration
```

- 安装适用于 Linux 的代理程序、适用于 Virtuozzo 的代理程序和适用于 Oracle 的代理程序，然后使用凭据进行注册。

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --login=johndoe --password=johnspassword
```

- 安装适用于 Oracle 的代理程序和适用于 Linux 的代理程序，然后使用注册标记进行注册。

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent,OracleAgentFeature -a --rain=https://eu2-cloud.company.com --token=34F6-8C39-4A5C
```

- 使用单独的文本文件中的配置设置安装适用于 Linux 的代理程序、适用于 Virtuozzo 的代理程序和适用于 Oracle 的代理程序。

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --options-file=/home/mydirectory/configuration_file
```

- 卸载适用于 Linux 的代理程序、适用于 Virtuozzo 的代理程序和适用于 Oracle 的代理程序，然后删除其所有日志、任务和配置设置。

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --purge
```

macOS 中的无人参与安装和卸载

本部分介绍如何在运行 macOS 的计算机上，通过使用命令行在无人参与模式下安装、注册和卸载保护代理程序。有关如何下载安装文件 (.dmg) 的信息，请参阅“添加运行 macOS 的计算机”。

安装适用于 Mac 的代理程序

1. 创建将挂载安装文件 (.dmg) 的临时目录。

   ```
   mkdir <dmg_root>
   ```

   此处，<dmg_root> 是您选择的名称。
2. 挂载 .dmg 文件。

   ```
   hdiutil attach <dmg_file> -mountpoint <dmg_root>
   ```

   此处，<dmg_file> 是安装文件的名称。例如，**AcronisAgentMspMacOSX64.dmg**。
3. 运行安装程序。

   ```
   sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
   ```

4. 卸载安装文件 (.dmg)。

   ```
   hdiutil detach <dmg_root>
   ```

示例

- ```
  mkdir mydirectory
  ```

  ```
  hdiutil attach /Users/JohnDoe/AcronisAgentMspMacOSX64.dmg -mountpoint mydirectory
  ```

  ```
  sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
  ```

  ```
  hdiutil detach mydirectory
  ```

注册适用于 Mac 的代理程序

请执行以下任一操作：

- 在特定帐户下使用用户名和密码来注册代理程序。

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  <service address> -u <user name> -p <password>
  ```

  此处：

  <安克诺斯数据保护软件 服务地址> 是用于**登录**到 安克诺斯数据保护软件 服务的地址。例如：

  <用户名> 和 <密码> 是将在其下注册代理程序的帐户的凭据。这不能是合作伙伴管理员帐户。
- 使用注册标记来注册代理程序。
  ```

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
<service address> --token <token>
```

注册标记是由 12 个字符组成的序列，由连字符分为三段。可以按“通过组策略部署代理程序”中所述，在 安克诺斯数据保护软件 Web 中控台中生成注册标记。

使用注册标记时，必须指定准确的数据中心地址。这是您在**登录**到 安克诺斯数据保护软件 服务后所见到的 URL。例如：

重要事项

如果使用的是 macOS 10.14 或更高版本，请向保护代理程序授予完整磁盘访问权限。为此，请转到**应用程序** > **实用程序**，然后运行**网络安全保护代理程序助手**。接着，按照应用程序窗口中的说明进行操作。

示例

使用用户名和密码注册。

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  https://cloud.company.com -u johndoe -p johnspassword
  ```

使用标记注册。

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  https://eu2-cloud company.com --token D91D-DC46-4F0B
  ```

卸载适用于 Mac 的代理程序

运行以下命令：

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
  Uninstall.app/Contents/MacOS/AgentUninstall /confirm
  ```

要在卸载过程中删除所有日志、任务和配置设置，请运行以下命令：

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
  Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
  ```

手动注册计算机

除了在代理程序安装期间在 安克诺斯数据保护软件 服务中注册计算机之外，还可以使用命令行接口来注册计算机。例如，如果已经安装代理程序但自动注册失败，或者您想要使用新帐户注册现有计算机，可能需要这样做。

注册计算机

在安装代理的计算机的命令提示符下，运行以下命令之一：

- 在当前帐户下注册计算机：

```
<path to the registration tool> -o register -s mms -t cloud --update
```

  - 在此，<注册工具的路径>是：
    - 在 Windows 中：`%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe`
    - 在 Linux 中：`/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
    - 在 macOS 中：`/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`
- 在其他帐户下注册计算机：

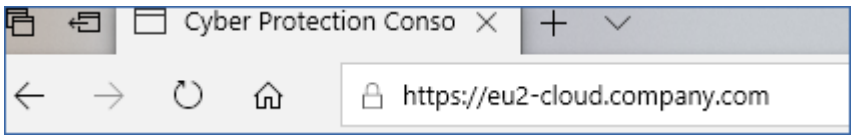
```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name> -p <password>
```

  - 此处，<用户名>和<密码>是注册代理的特定帐户的凭据。这不能是合作伙伴管理员帐户。
    <服务地址> 是用于**登录**到 安克诺斯数据保护软件 服务的 URL。例如，`https://cloud.company.com`。

- 要使用注册标记注册计算机，请执行以下操作：

```
<path to the registration tool> -o register -t cloud -a <service address> --token <token>
```

  - 注册标记是由 12 个字符组成的序列，由连字符分为三段。有关如何生成注册标记的详细信息，请参阅“通过组策略部署代理程序”。
    使用注册标记时，必须指定准确的数据中心地址为<服务地址>。这是您在**登录**到 安克诺斯数据保护软件 服务后所见到的 URL。例如，`https://eu2-cloud.company.com`。



    请勿在此处使用 `https://cloud.company.com`。

注销计算机

在安装代理的计算机的命令提示符下，运行以下命令：

```
<path to the registration tool> -o unregister
```

示例

Windows

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -s mms -t
cloud --update
```

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p johnspassword
```

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://au1-cloud.company.com --token 3B4C-E967-4FBD
```

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -s mms -t cloud --
update
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://cloud.company.com -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -s mms -t cloud --update
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://us5-cloud.company.com --token 9DBF-3DA9-4DAB
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o unregister
```

带有特殊字符或空格的密码

如果密码中包含特殊字符或空格，请在命令行上键入时将密码括在引号中。

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <"password">
```

示例(Windows)：

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p "johns password"
```

如果仍然收到错误：

- 通过访问 https://www.base64encode.org/，将密码编码为 base64 格式。
- 在命令行上，使用 -b 或 --base64 参数指定编码的密码。

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-b -p <encoded password>
```

示例(Windows)：

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -b -p am9obnNwYXNzd29yZA==
```

正在部署适用于 oVirt 的代理程序(虚拟设备)

有关如何部署和配置适用于 oVirt 的代理程序(虚拟设备) 的信息，请参考 Cyber Protection Cloud 文档。

部署适用于 Virtuozzo Hybrid Infrastructure 的代理程序(虚拟设备)

有关如何部署和配置适用于 Virtuozzo Hybrid Infrastructure 的代理程序(虚拟设备) 的信息，请参考 Cyber Protection Cloud 文档。

自动发现计算机

使用“自动发现”，可以执行以下操作：

- 通过检测 Active Directory 域或本地网络中的计算机，自动安装保护代理程序，以及自动将计算机注册到管理服务器。
- 在多台计算机上安装和更新保护代理程序。

- 使用与 Active Directory 同步，以便减少在大型 Active Directory 域中调配资源和管理计算机的工作。

先决条件

要执行自动发现，需要至少一台在本地网络或 Active Directory 域中已安装了保护代理程序的计算机。该代理程序将用作发现代理程序。

重要事项

只有安装在 Windows 计算机上的代理程序才能成为发现代理程序。如果您的环境中没有发现代理程序，将无法使用**添加设备**面板中的**多个设备**选项。

只有运行 Windows 的计算机才支持远程安装代理程序（不支持 Windows XP）。要在运行 Windows Server 2012 R2 的计算机上远程安装，必须在该计算机上安装 Windows update KB2999226。

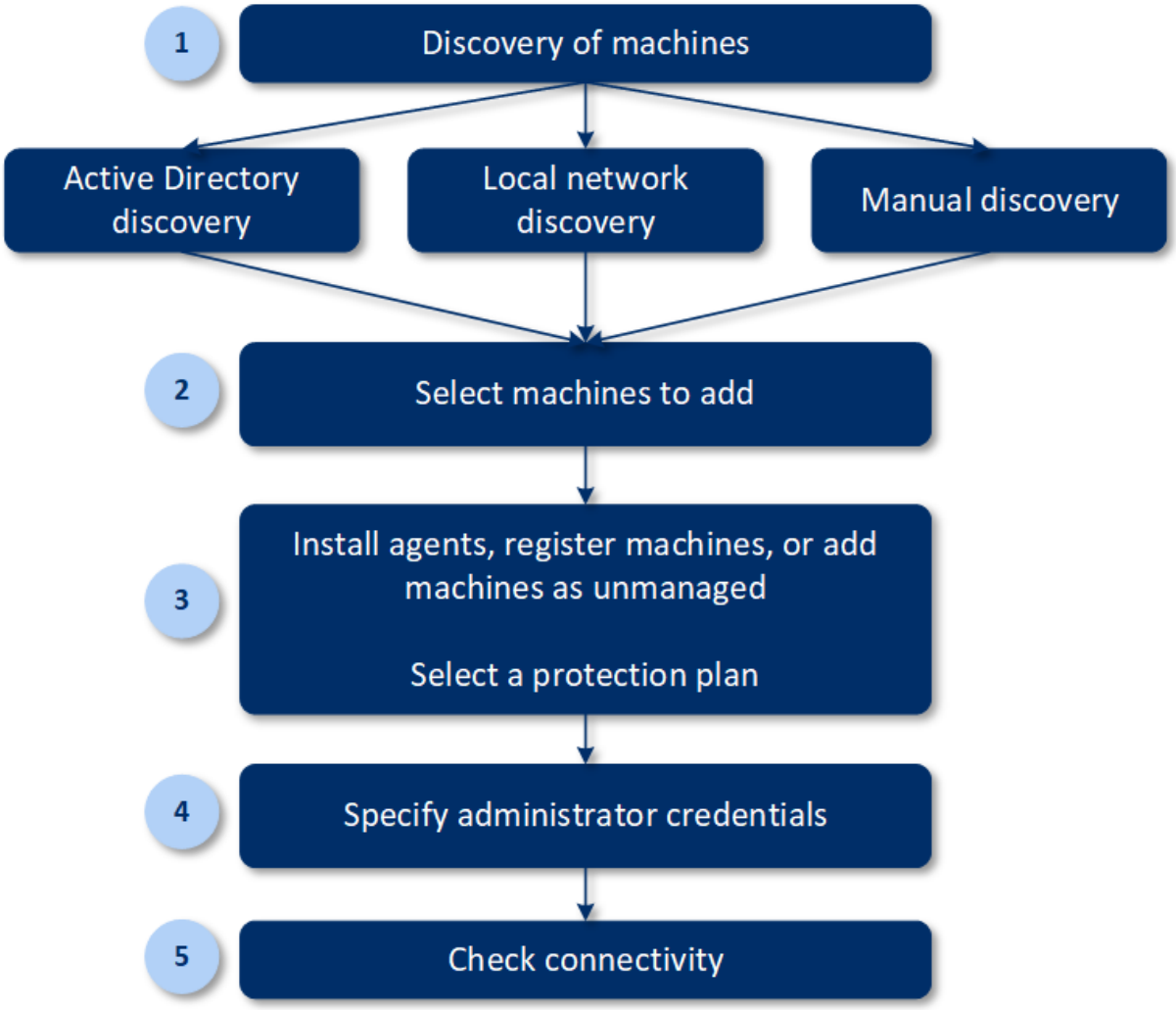
自动发现如何工作

在本地网络发现期间，发现代理程序会使用 NetBIOS 发现、Web 服务发现 (WSD) 和地址解析协议 (ARP) 表收集网络中每台计算机的以下信息：

- 名称（短/NetBIOS 主机名）
- 完全限定域名 (FQDN)
- 域/工作组
- IPv4/IPv6 地址
- MAC 地址
- 操作系统（名称/版本/系列）
- 计算机类别（工作站/服务器/域控制器）

在 Active Directory 发现期间，除了上面所列内容之外，发现代理程序还会收集计算机组织单元 (OU) 的相关信息及其名称和操作系统的相关详细信息。但是，不会收集 IP 和 MAC 地址。

下图总结了自动发现过程。



1. 选择发现方法：
   - Active Directory 发现
   - 本地网络发现
   - 手动发现 - 使用计算机 IP 地址或主机名，或者从文件导入一列计算机

   Active Directory 发现或本地网络发现的结果不会包括安装了保护代理程序的计算机。

   在手动发现期间，将更新并重新注册现有保护代理程序。如果您使用注册代理程序的同一帐户执行自动发现，则代理程序只会更新到最新版本。如果您使用其他帐户执行自动发现，则代理程序将更新到最新版本，并在该帐户所属的租户下重新注册。
2. 选择要添加到租户的计算机。
3. 选择如何添加这些计算机：
   - 在计算机上安装保护代理程序和其他组件，然后在 Web 中控台中注册它们。
   - 在 Web 中控台中注册计算机(如果已安装保护代理程序)。
   - 将计算机作为**非托管计算机**添加到 Web 中控台，无需安装保护代理程序。

   还可以将现有保护计划应用于安装有保护代理程序或在 Web 中控台中注册的计算机。
4. 为选定计算机提供管理员凭据。

5. 选择代理程序将用于访问管理服务器的该服务器的名称或 IP 地址。

   默认情况下，服务器名称处于选中状态。如果您的管理服务器有多个网络接口，或者您遇到导致代理程序注册失败的 DNS 问题，则可能需要改为选择 IP 地址。

6. 验证是否可以使用提供的凭据连接到计算机。

安克诺斯数据保护软件 Web 中控台中显示的计算机分为以下几类：

- **已发现** - 已发现但未安装保护代理程序的计算机。
- **受控** - 已安装保护代理程序的计算机。
- **不受保护** - 未应用保护计划的计算机。不受保护的计算机包括未应用保护计划的已发现计算机和受控计算机。
- **受保护** - 已应用保护计划的计算机。

自动发现和手动发现

在开始发现之前，请确保已满足先决条件。

发现计算机

1. 在 Web 中控台中，转到**设备** > **所有设备**。
2. 单击**添加**。
3. 在**多个设备**中，单击**仅限 Windows**。将打开发现向导。
4. [如果您的组织中有单位] 选择一个单位。然后在**发现代理程序**中，您将能够选择与选定单位及其子单位关联的代理程序。
5. 选择将执行扫描以检测计算机的发现代理程序。
6. 选择发现方法：
   - **搜索 Active Directory**。确保安装有发现代理程序的计算机是 Active Directory 域成员。
   - **扫描本地网络**。如果选定的发现代理程序找不到任何计算机，请选择另一个发现代理程序。
   - **手动指定或从文件导入**。手动定义要添加的计算机或从文本文件导入它们。
7. [如果 Active Directory 发现方法已选中] 选择如何搜索计算机：
   - **在组织单元列表中**。选择要添加的计算机组。
   - **通过 LDAP 术语查询**。使用 LDAP 术语查询来选择计算机。**搜索库**定义搜索位置，而**过滤器**让您可以指定计算机选择的标准。
8. [如果 Active Directory 或本地网络发现方法已选中] 使用列表来选择要添加的计算机。

   [如果手动发现方法已选中] 指定计算机 IP 地址或主机名，或从文本文件导入计算机列表。该文件必须包含 IP 地址/主机名，每行一个。以下是一个示例文件：

   ```
   156.85.34.10
   156.85.53.32
   156.85.53.12
   EN-L00000100
   EN-L00000101
   ```

   在手动添加计算机地址或从文件导入后，代理程序会尝试 Ping 添加的计算机并定义其可用性。
9. 选择执行清查之后要执行的操作：

- **安装代理程序和注册计算机**。通过单击**选择组件**，即可选择要在计算机上安装的组件。有关更多详细信息，请参阅“选择要安装的组件”。最多可以同时安装 100 个代理程序。

  在**选择组件**屏幕上，通过指定**代理程序服务的登录帐户**来定义将运行服务的帐户。可选择以下其中一个选项：

  - **使用服务用户帐户**（代理程序服务的默认帐户）

    服务用户帐户是用于运行服务的 Windows 系统帐户。此设置的优点是域安全策略不会影响这些帐户的用户权限。默认情况下，该代理程序在**本地系统**帐户下运行。
  - **创建新帐户**

    代理程序的帐户名称将是“Agent User”。
  - **使用以下帐户**

    如果将代理程序安装在域控制器上，则系统会提示您为代理程序指定现有帐户（或相同帐户）。出于安全原因，系统不会自动在域控制器上创建新帐户。

  如果选择**创建新帐户**或**使用以下帐户**选项，请确保域安全策略不会影响相关的帐户权限。如果帐户被剥夺了安装期间分配的用户权限，则组件可能不会正常工作或不工作。
- **注册已安装代理程序的计算机**。如果代理程序已安装在计算机上，并且只需要在 安克诺斯数据保护软件 中注册它们，则使用此选项。如果在计算机上找不到任何代理程序，则这些计算机将添加为**不受控**计算机。
- **添加为不受控计算机**。该代理程序将不会安装在计算机上。您将能够在 Web 中控台中查看它们，并稍后安装或注册代理程序。

[如果**安装代理程序和注册计算机**发现后操作已选中] **如有必要，重新启动计算机** - 如果该选项已启用，则计算机将按照完成安装所需的次数重新启动。

在以下情况之一中，可能需要重新启动计算机：

- 先决条件安装已完成，需要重新启动才能继续安装。
- 安装已完成，但需要重新启动，因为一些文件在安装过程中被锁定。
- 安装已完成，但需要重新启动才能使先前安装的其他软件工作。

[如果**如有必要，重新启动计算机**已选中] **如果用户已登录，请勿重新启动计算机** - 如果该选项已启用，则在用户已登录到系统的情况下，计算机将不会自动重新启动。例如，如果用户工作时安装需要重新启动，则系统不会重新启动。

如果先决条件已安装，但重新启动因用户已登录而未能完成，则为了完成代理程序安装，您需要重新启动计算机，然后再开始安装。

如果代理程序已安装，但重新启动未完成，则您需要重新启动计算机。

[如果您的组织中有单位] **注册其计算机的用户** - 选择将注册计算机的单元。

如果已选择前两个发现后操作之一，则还有一个选项可用于将保护计划应用于计算机。如果有多个保护计划，可以选择要使用的保护计划。

10. 指定对所有计算机具有管理员权限的用户的凭据。

重要事项

请注意，仅当指定内置管理员帐户（安装操作系统时创建的第一个帐户）的凭据时，代理程序的远程安装才能进行，而无需任何准备。如果要定义一些自定义管理员凭据，则应按照“添加运行 Windows 的计算机 > 准备”所述进行其他手动准备操作。

11. 选择代理程序将用于访问管理服务器的该服务器的名称或 IP 地址。

    默认情况下，服务器名称处于选中状态。如果您的管理服务器有多个网络接口，或者您遇到导致代理程序注册失败的 DNS 问题，则可能需要改为选择 IP 地址。

12. 系统会检查与所有计算机的连接。如果无法连接到一些计算机，可以更改这些计算机的凭据。

启动发现计算机后，您将在**仪表板** > **活动** > **发现计算机**活动中找到相应任务。

选择要安装的组件

可以在下表中找到必需组件和附加组件的说明：

组件	说明
必需组件	
适用于 Windows 的代理程序	该代理程序备份磁盘、卷、文件，并将安装在 Windows 计算机上。将始终安装它，不可选。
其他组件	
适用于 Hyper-V 的代理程序	该代理程序备份 Hyper-V 虚拟机，并将安装在 Hyper-V 主机上。如果选择并在计算机上检测到 Hyper-V 角色，将安装它。
适用于 SQL 的代理程序	该代理程序备份 SQL Server 数据库，并将安装在运行 Microsoft SQL Server 的计算机上。如果选择并在计算机上检测到应用程序，将安装它。
适用于 Exchange 的代理程序	该代理程序备份 Exchange 数据库和邮箱，并将安装在运行 Microsoft Exchange Server 的“邮箱”角色的计算机上。如果选择并在计算机上检测到应用程序，将安装它。
适用于 Active Directory 的代理程序	该代理程序备份 Active Directory 域服务的数据，并将安装在域控制器上。如果选择并在计算机上检测到应用程序，将安装它。
适用于 VMware 的代理程序 (Windows)	该代理程序备份 VMware 虚拟机，并将安装在对 vCenter 服务器具有网络访问权限的 Windows 计算机上。如果选择，将安装它。
适用于 Office 365 的代理程序	该代理程序会将 Microsoft 365 邮箱备份到本地目标，并将安装在 Windows 计算机上。如果选择，将安装它。
适用于 Oracle 的代理程序	该代理程序备份 Oracle 数据库，并将安装在运行 Oracle 数据库的计算机上。如果选择，将安装它。
安克诺斯数据保护软件监视器	该组件使用户可以在通知区域中监控正在运行任务的执行，并将安装在 Windows 计算机上。如果选择，将安装它。
命令行工具	安克诺斯数据保护软件 通过 acrocmd 实用程序支持命令行界面。acrocmd 不包含实际执行命令的任何工具。它仅向 安克诺斯数据保护软件 组件(代理程序和管理服务器)提供命令行界面。如果选择，将安装它。

可启动媒体生成器	该组件使用户可以创建可启动媒体，并将安装在 Windows 计算机上。

管理发现的计算机

在执行发现过程后，可以在**设备 > 不受控计算机**中找到所有发现的计算机。

本部分按所使用的发现方法分为几个子部分。计算机参数的完整列表如下所示(它可能因发现方法而有所不同)：

名称	说明
名称	计算机的名称。如果无法发现计算机的名称，将显示 IP 地址。
IP 地址	计算机的 IP 地址。
发现类型	用于检测计算机的发现方法。
组织单元	计算机所属的 Active Directory 中的组织单元。如果您在**不受控计算机 > 活动目录**中查看计算机列表，则将显示此列。
操作系统	计算机中安装的操作系统。

有一个**例外**部分，可以在其中添加在发现过程中必须跳过的计算机。例如，如果您不需要发现确切的计算机，可以将它们添加到此列表。

要将计算机添加到**例外**，请在列表中选择它，然后单击**添加到例外**。要从**例外**中删除计算机，请转到**不受控计算机 > 例外**、选择相应计算机，然后单击**从例外中删除**。

可以安装保护代理程序，并在 安克诺斯数据保护软件 中注册一批发现的计算机，方法是在列表中选择它们，然后单击**安装并注册**。打开的向导还让您可以将保护计划指派给一批计算机。

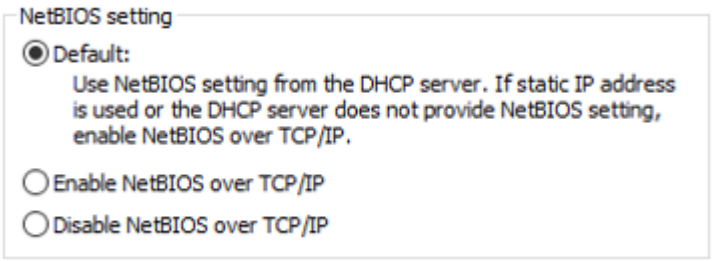
在保护代理程序安装在计算机上后，这些计算机将显示在**设备 > 装有代理程序的计算机**部分中。

要检查保护状态，请转到**仪表板 > 概述**，然后添加保护状态小组件或发现的计算机小组件。

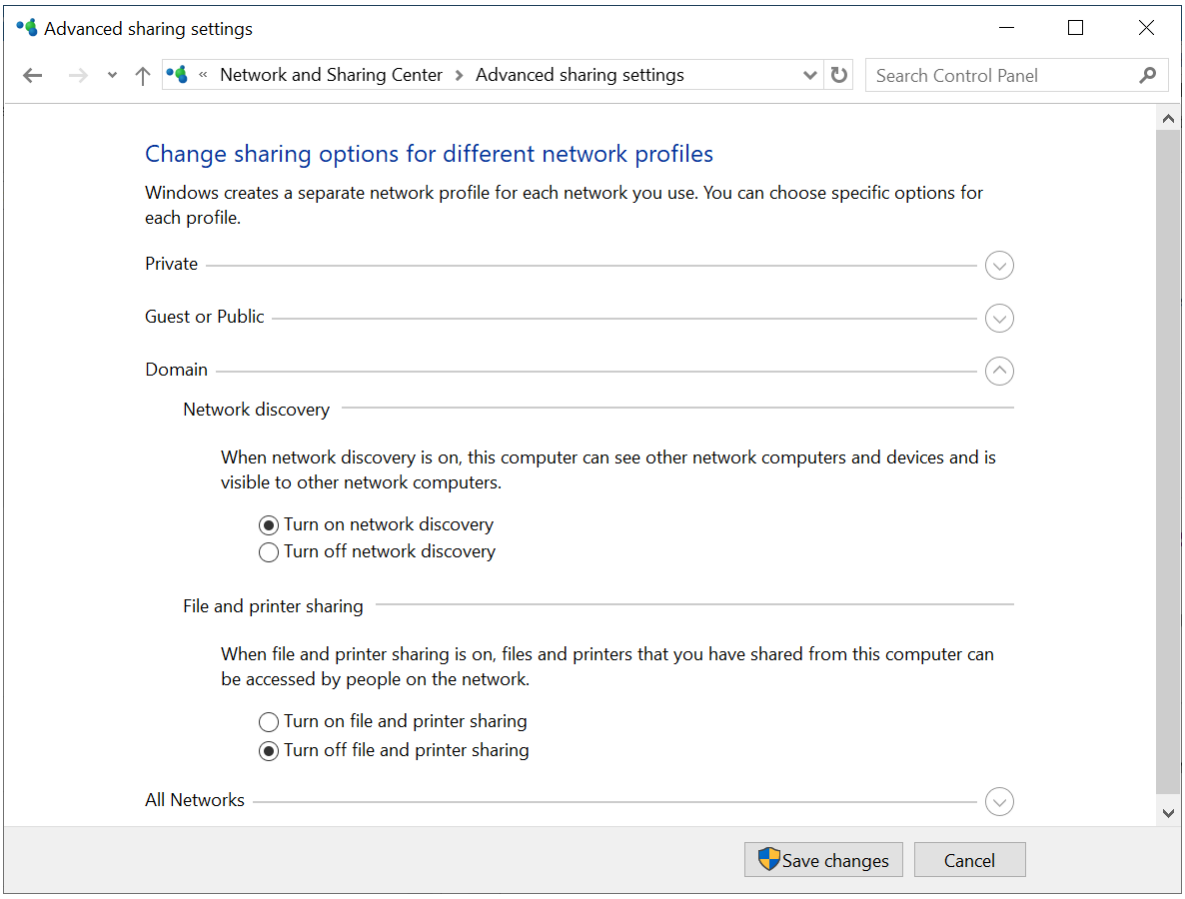
疑难解答

如果遇到与自动发现功能有关的任何问题，请尝试以下操作：

- 验证是否已启用基于 TCP/IP 的 NetBIOS 或将其设置为默认值。



- 在**控制面板 > 网络和共享中心 > 高级共享设置**中，打开网络发现。



- 验证**功能发现提供程序主机**服务是否正在执行发现的计算机上以及要发现的计算机上运行。
- 验证**功能发现提供程序主机**服务是否正在要发现的计算机上运行。

根据 OVF 模板部署适用于 VMware 的代理程序(虚拟设备)

在启动前

代理程序的系统要求

默认情况下，为虚拟设备指派 4 GB RAM 和 2 个 vCPU，这是最佳配置，足以应对大多数操作。如果备份流量带宽预期超过每秒 100 MB(例如，在 10 GBit 网络中)，我们建议将这些资源增加到 8 GB RAM 和 4 个 vCPU，以提高备份性能。

设备自带的虚拟磁盘占用空间不超过 6 GB。厚磁盘格式或精简磁盘格式无关紧要，它不影响设备性能。

注意
必须在 ESXi 主机上安装 vStorage API，才能启用虚拟机备份。请参阅 https://kb.acronis.com/content/14931。

我需要多少个代理程序?

即使一个虚拟设备能够保护整个 vSphere 环境，但最好的做法是每个 vSphere 群集(或每个主机，如果没有群集)部署一个虚拟设备。这样可以加快备份速度，因为此设备可以使用 HotAdd 传输来附加备份磁盘，从而将一个本地磁盘的备份流量转移到另一个磁盘。

通常虚拟设备和适用于 VMware 的代理程序可以同时使用，只要它们连接到同一个 vCenter 服务器，*或者*连接到不同的 ESXi 主机。对于一个代理程序直接连接到 ESXi，而另一个代理程序连接到管理此 ESXi 的 vCenter 服务器的情况要加以避免。

如果您有多个代理程序，我们建议不要使用本地连接的存储器(即，在添加到虚拟设备的虚拟磁盘上存储备份)。有关更多注意事项，请参阅"使用本地连接存储器"。

为代理程序禁用自动 DRS

如果将虚拟设备部署到 vSphere 群集，请确保对其禁用自动 vMotion。在群集 DRS 设置中，启用单个虚拟机自动化级别，然后将虚拟设备的**自动化级别**设置为**禁用**。

部署 OVF 模板

OVF 模板的位置

OVF 模板包含一个 .ovf 文件和两个 .vmdk 文件。

在本地部署中

完成安装管理服务器后，虚拟设备的 OVF 包位于以下文件夹：**%ProgramFiles%\Acronis\ESXAppliance**(在 Windows 中)或 **/usr/lib/Acronis/ESXAppliance**(在 Linux 中)。

在云部署中

1. 依次单击**所有设备** > **添加** > **VMware ESXi** > **虚拟设备 (OVF)**。
   Zip 存档下载到您的计算机。
2. 解压缩 .zip 存档。

部署 OVF 模板

1. 确保 OVF 模板文件可以从运行 vSphere Client 的计算机进行访问。
2. 启动 vSphere Client，然后登录到 vCenter 服务器。
3. 部署 OVF 模板。
   - 配置存储时，选择共享数据存储(如果存在)。厚磁盘格式或精简磁盘格式无关紧要，因为它不影响设备性能。
   - 在云部署中配置网络连接时，请确保选择允许 Internet 连接的网络，以便代理程序可以在云中正确注册自身。在本地部署中配置网络连接时，请确保选择包含管理服务器的网络。

配置虚拟设备

1. **启动虚拟设备**

   在 vSphere Client 中，显示**清查**、右键单击虚拟设备名称，然后依次选择**电源** > **接通电源**。选择**中控台**选项卡。

2. **代理服务器**

   如果在网络中启用了代理服务器：

   a. 若要启动命令外壳，请在虚拟设备 UI 中按 CTRL+SHIFT+F2。

   b. 使用文本编辑器打开文件 **/etc/Acronis/Global.config**。

   c. 请执行以下任一操作：

   - 如果要在代理程序安装期间指定代理服务器设置，请找到以下部分：

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

   - 否则，将上述各行复制并粘贴到文件中的 `<registry name="Global">...</registry>` 标记之间。

   d. 将 地址 替换为新代理服务器主机名称/IP 地址，将 端口 替换为端口号的十进制值。

   e. 如果代理服务器需要身份验证，请将 登录 和 密码 替换为代理服务器凭据。否则，从此文件中删除这些行。

   f. 保存文件。

   g. 在文本编辑器中打开文件 **/opt/acronis/etc/aakore.yaml**。

   h. 找到 **env** 部分或创建它，然后添加以下各行：

   ```
   env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
   ```

   i. 将 `proxy_login` 和 `proxy_password` 替换为代理服务器凭据，将 `proxy_address:port` 替换为代理服务器的地址和端口号。

   j. 运行 **reboot** 命令。

   否则，请跳过此步骤。

3. **网络设置**

   代理程序的网络连接通过使用动态主机配置协议 (DHCP) 自动配置。要更改默认配置，在 **eth0** 中的**代理程序选项**下，单击**更改**并指定所需的网络设置。

4. **vCenter/ESX(i)**

   在 **vCenter/ESX(i)** 中的**代理程序选项**下，单击**更改**，然后指定 vCenter 服务器名称或 IP 地址。代理程序将能够备份并恢复由 vCenter 服务器管理的任何虚拟机。

如果您未使用 vCenter 服务器，请指定要备份和恢复其虚拟机的 ESXi 主机的名称或 IP 地址。通常情况下，如果代理程序对由其自身主机管理的虚拟机进行备份，那么此备份运行会更快。

指定代理程序将用于连接到 vCenter 服务器或 ESXi 的凭据。建议您使用指派了**管理员**角色的帐户。否则，提供在 vCenter 服务器或 ESXi 上具有必要权限的帐户。

您可以单击**检查连接**以确保访问凭据正确。

5. **管理服务器**
   a. 在**代理程序选项**下的**管理服务器**中，单击**更改**。
   b. 在**服务器名称/IP**中，请执行以下任一操作：
      - 对于本地部署，选择**本地**。指定安装了管理服务器的计算机的主机名或 IP 地址。
      - 对于云部署，选择**云**。软件将显示网络安全保护服务地址。除外另有说明，否则请勿更改此地址。
   c. 在**用户名**和**密码**中，请执行以下任一操作：
      - 对于本地部署，指定管理服务器管理员的用户名和密码。
      - 对于云部署，为网络安全保护服务指定用户名和密码。代理程序和由代理程序管理的虚拟机将在此帐户下注册。
6. **时区**

   在**虚拟机**下的**时区**中，单击**更改**。选择您所在位置的时区以确保预定操作在正确的时间运行。
7. **[可选] 本地存储器**

   您可以将其他磁盘连接至虚拟设备，这样适用于 VMware 的代理程序即可备份至该本地连接的存储器。

   通过编辑虚拟机设置来添加磁盘，然后单击**刷新**。此时，**创建存储器**链接处于可用状态。单击此链接、选择磁盘，然后指定磁盘的标签。

正在部署适用于 Scale Computing HC3 的代理程序(虚拟设备)

在启动前

此设备是您在 Scale Computing HC3 群集中部署的预配置虚拟机。它包含的保护代理程序让您可以管理群集中所有虚拟机的网络安全保护。

代理程序的系统要求

部署虚拟设备时，可以在 vCPU 和 RAM 的不同组合之间进行选择。2 个 vCPU 和 4 GiB RAM 是最佳配置，足以应对大多数操作。如果备份流量带宽预期超过每秒 100 MB(例如，在 10 GBit 网络中)，我们建议将这些资源增加到 4 个 vCPU 和 8 GiB RAM，以提高备份性能。

设备自带的虚拟磁盘占用空间不超过 6 GB。

我需要多少个代理程序?

一个代理程序可以保护整个群集。如果需要分配备份流量带宽负载，可以在群集中放置多个代理程序。

如果在群集中放置多个代理程序，则虚拟机将自动在各代理程序之间平均分配，以便每个代理程序管理相同数量的计算机。

当各代理程序之中的负载不平衡达到 20% 时，将自动进行重新分配。例如，当添加或删除计算机或代理程序时，可能会发生此情况。例如，您想到需要更多的代理程序帮助处理吞吐量以及将额外的虚拟设备部署至群集。管理服务器会将最适合的计算机指定至新代理程序。将会减少旧代理程序的负载。当从管理服务器删除代理程序时，计算机被指定给分布在剩余代理程序中的代理程序。如果代理程序损坏或从 Scale Computing HC3 群集手动删除代理程序，则不会发生此情况。仅当从 安克诺斯数据保护软件 Web 界面删除此类代理程序时，才会开始重新分配。

您可以在以下位置查看自动分配结果：

- 在**所有设备**部分的每个虚拟机的**代理程序**列中
- 如果在**设置** > **代理程序**中选择某个代理程序，则在**详细信息**面板的**已指派虚拟机**部分中

部署虚拟设备

1. 登录到您的 安克诺斯数据保护软件 帐户。
2. 依次单击**设备** > **所有设备** > **添加** > **Scale Computing HC3**。
3. 选择要部署的虚拟设备数量：
4. 指定 Scale Computing HC3 群集的 IP 地址或主机名。
5. 指定在此群集中分配了 **VM 创建/编辑**角色的帐户的凭据。
6. 指定将用于临时存储虚拟设备映像文件的网络共享。至少需要 2GB 的可用空间。
7. 指定对此网络共享具有读写访问权限的帐户的凭据。
8. 单击**部署**。

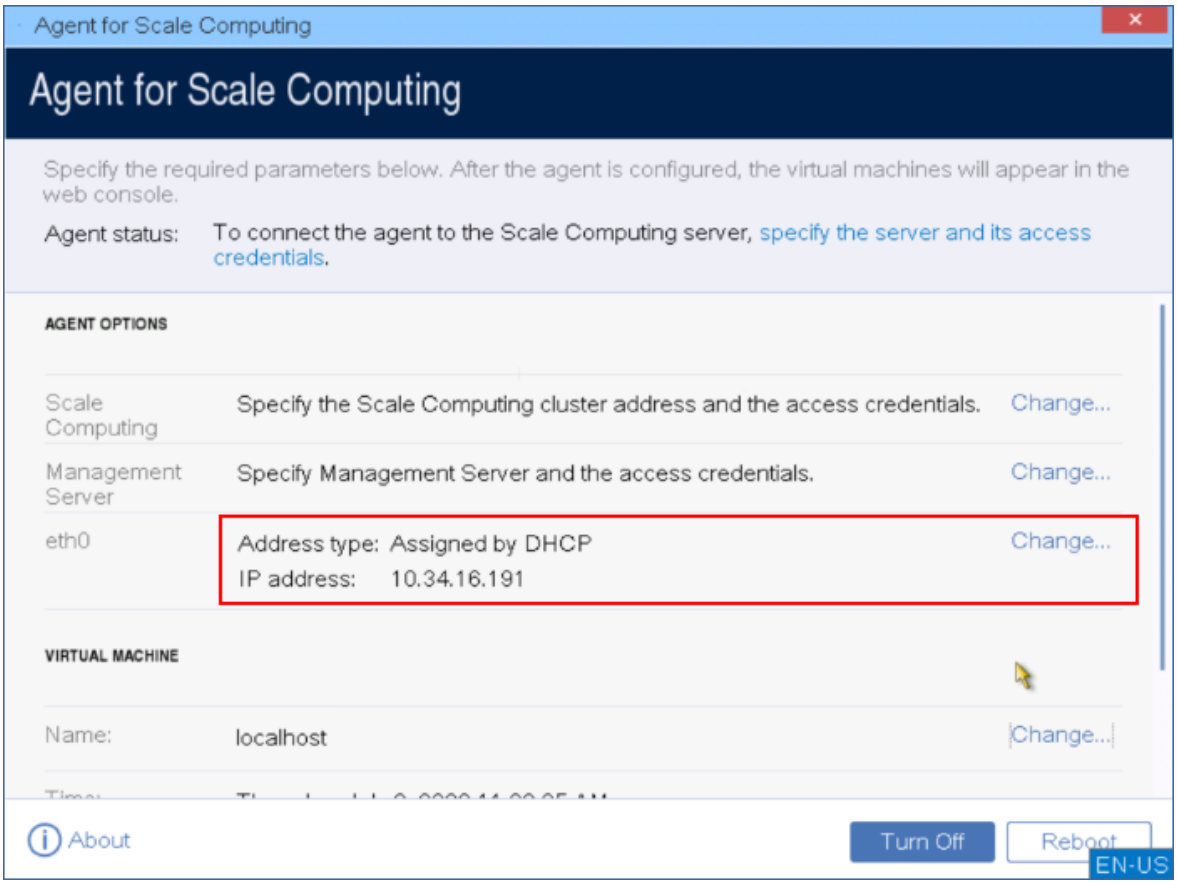
部署完成后，配置虚拟设备。

配置虚拟设备

部署虚拟设备后，需要对其进行配置，以便它可以访问将要保护的 Scale Computing HC3 群集和 安克诺斯数据保护软件 管理服务器。

若要配置虚拟设备

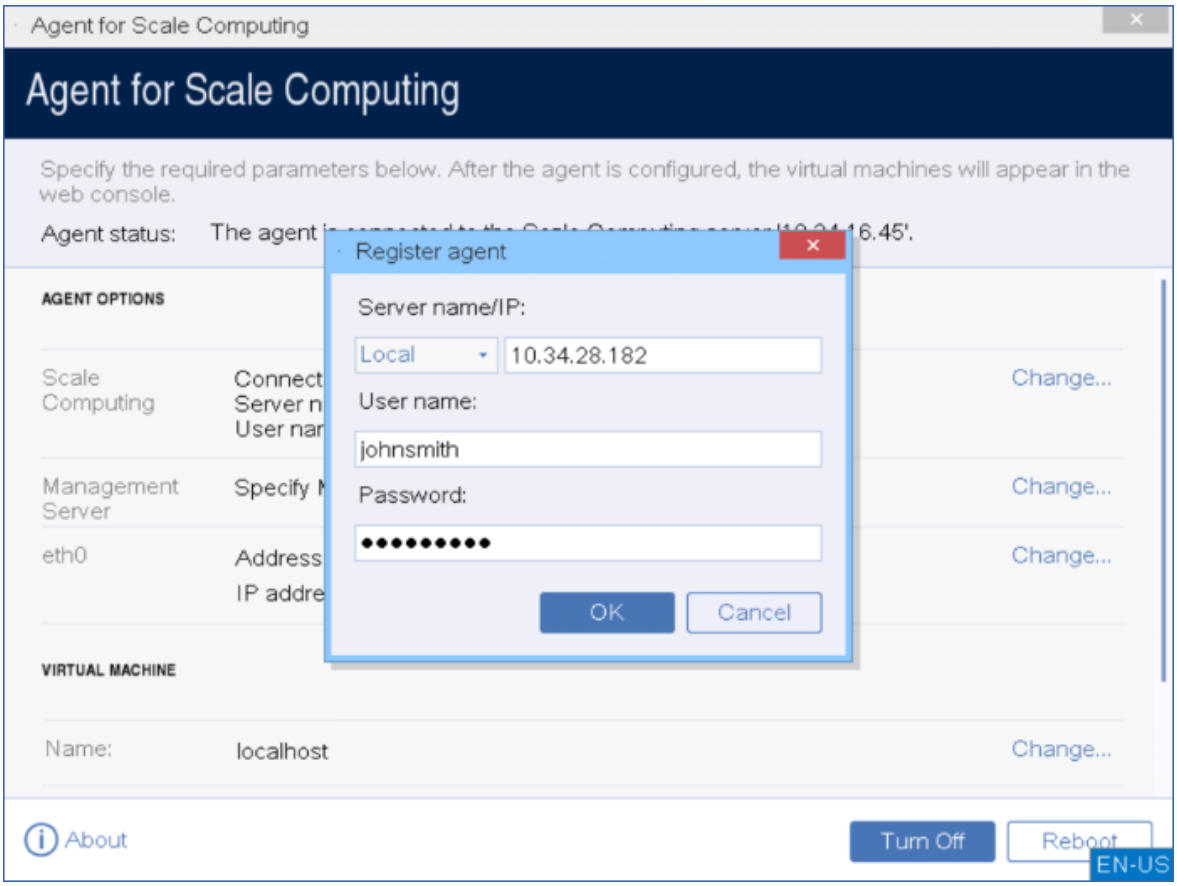
1. 登录到您的 Scale Computing HC3 帐户。
2. 选择包含需要配置的代理的虚拟机，然后单击**中控台**。
3. 配置设备的网络接口。可能有一个或多个接口要进行配置 - 具体取决于设备所使用的网络数量。确保自动指派的 DHCP 地址(如果有)在虚拟机所使用的网络内有效，或者手动指派它们。



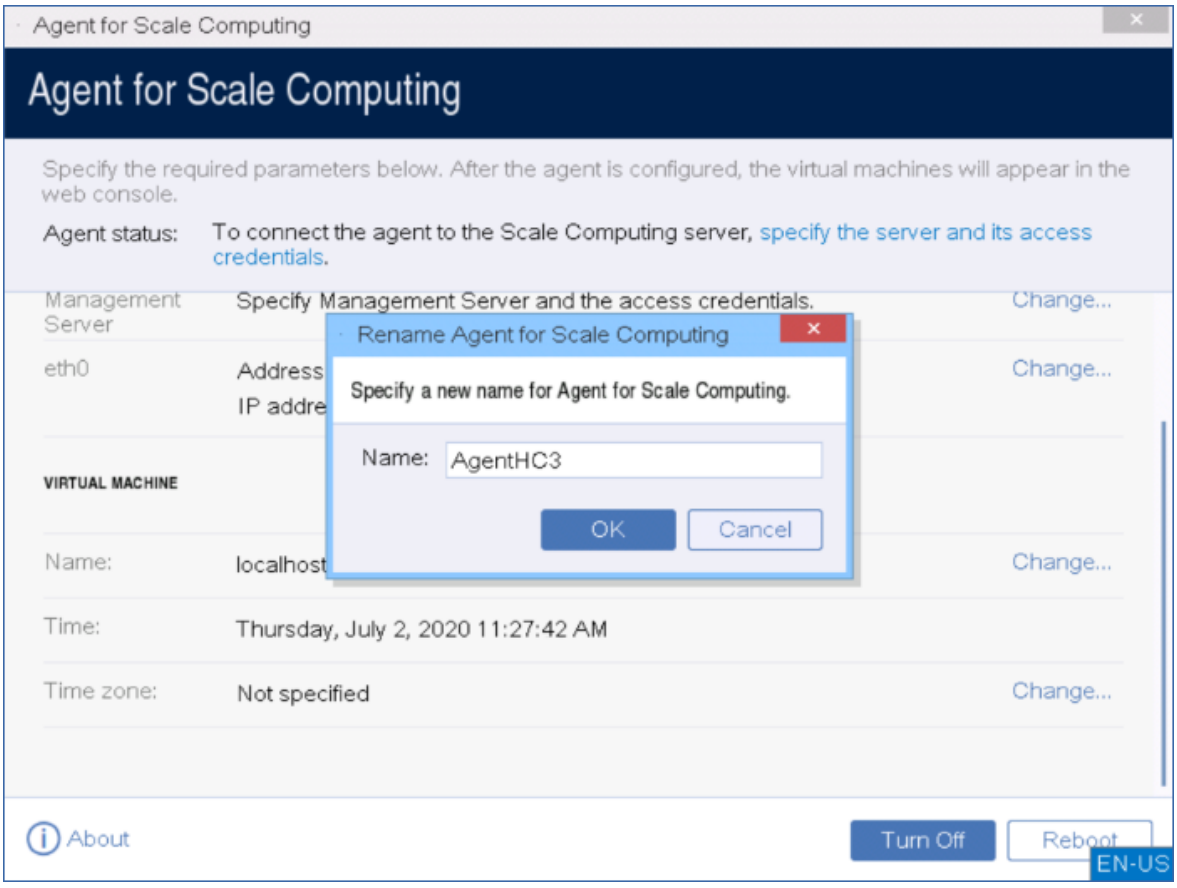
4. 指定 Scale Computing HC3 群集地址和凭据：
   - 群集的 DNS 名称或 IP 地址。
   - 在**用户名**和**密码**字段中，输入已分配适当角色的 Scale Computing HC3 帐户的凭据。

   您可以单击**检查连接**以确保访问凭据正确。

5. 指定 安克诺斯数据保护软件 管理服务器地址和用于访问它的凭据。



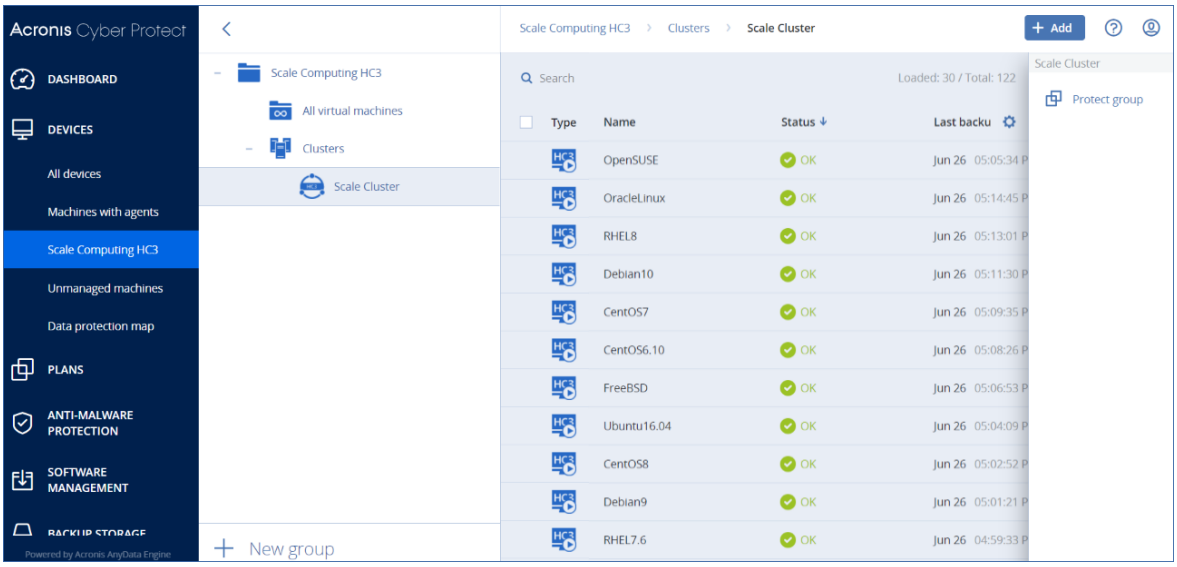
6. [可选] 为代理程序指定一个名称。该名称将显示在 安克诺斯数据保护软件 Web 中控台中。



7. [可选] 选择您所在位置的时区以确保预定操作在正确的时间运行。

保护 Scale Computing HC3 群集中的虚拟机

1. 登录到您的 安克诺斯数据保护软件 帐户。
2. 导航到**设备** > **Scale Computing HC3**> <您的群集>, 或者在**设备** > **所有设备**中找到您的计算机。
3. 选择所需计算机并为它们应用保护计划。



Scale Computing HC3 的代理程序 – 所需角色

本节介绍操作 Scale Computing HC3 虚拟机以及额外进行虚拟设备部署所需的角色。

操作	角色
备份虚拟机	备份 VM 创建/编辑 VM 删除
恢复到现有的虚拟机上	备份 VM 创建/编辑 VM 电源控制 VM 删除 群集设置
恢复至新虚拟机	备份 VM 创建/编辑 VM 电源控制 VM 删除 群集设置
虚拟设备部署	VM 创建/编辑

通过“组策略”部署代理程序

通过使用“组策略”，可在作为 Active Directory 域成员的计算机上集中安装（或部署）适用于 Windows 的代理程序。

在本部分里，您将了解如何设置“组策略”对象，以在整个域中或其组织单位中的计算机上部署适用于代理程序。

每当计算机登录到域时，所生成的“组策略”对象将确保该计算机上安装并注册了代理程序。

先决条件

在继续进行代理程序部署前，请确保：

- 您有一个带有控制器的活动目录域，并且该域控制器运行 Microsoft Windows Server 2003 或更高版本。
- 您是该域中的**域管理员**组成员。
- 您已下载 **Windows 中可供安装的所有代理程序**安装程序。下载链接在 Web 中控台中的**添加设备**页面上提供。

步骤 1:生成注册标记

注册标记会将您的身份信息传递给安装程序,而不会存储 安克诺斯数据保护软件 Web 中控台的登录名和密码。这使您能够在您的帐户下注册任意数量的计算机。为了更安全起见,标记的使用寿命有限。

生成注册标记的步骤

1. 使用应指派给计算机的帐户的凭据登录到 安克诺斯数据保护软件 Web 中控台。
2. 依次单击**所有设备** > **添加**。
3. 向下滚动到**注册标记**,然后单击**生成**。
4. 指定标记使用寿命,然后单击**生成标记**。
5. 复制标记或将其记录下来。如果您将来需要使用标记,请确保将其保存。
   可以单击**管理处于活动状态的标记**以查看和管理已生成的标记。请注意,出于安全原因,此表不会显示完整的标记值。

步骤 2:创建 .mst 转换并提取安装包

1. 在域中的任何计算机上以管理员身份登录。
2. 创建将包含安装包的共享文件夹。确保域用户可以访问共享文件夹,例如,通过为**所有人**保留默认共享设置。
3. 启动安装程序。
4. 单击**创建 .mst 和 .msi 文件用于无人参与安装**。
5. 查看或修改将添加到 .mst 文件的安装设置。在为管理服务器指定连接方法时,选择**使用注册标记**,然后输入已生成的标记。
6. 单击**继续**。
7. 在**将文件保存到**中,为已创建的文件夹指定路径。
8. 单击**生成**。

因此,将生成 .mst 转换,并且 .msi 和 .cab 安装包将提取到您创建的文件夹。

步骤 3:设置组策略对象

1. 以域管理员的身份登录域管理器;如果域中有多个域控制器,请以域管理员的身份登录到任一域控制器。
2. 如果您计划在组织单位中部署代理程序,请确保域中存在该组织单位。否则,请跳过此步骤。
3. 在**开始**菜单中,指向**管理工具**,然后单击 **Active Directory 用户和计算机**(在 Windows Server 2003 中)或**组策略管理**(在 Windows Server 2008 或更高版本中)。
4. 在 Windows Server 2003 中:
   - 右键单击域名或组织单元名称,然后单击**属性**。在对话框中单击**组策略**选项卡,然后单击**新建**。

   在 Windows Server 2008 或更高版本中:
   - 右键单击域名或组织单元名称,然后单击**在此域中创建 GPO,并在此处链接**。

5. 将新的“组策略”对象命名为**适用于 Windows 的代理程序**。
6. 打开**适用于 Windows 的代理程序**“组策路”对象以进行编辑，如下所示：
   - 在 Windows Server 2003 中，单击“组策略”对象，然后单击**编辑**。
   - 在 Windows Server 2008 或更高版本中的**组策略对象**下，右键单击“组策略”对象，然后单击**编辑**。
7. 在“组策略”对象编辑器管理单元中，展开**计算机配置**。
8. 在 Windows Server 2003 和 Windows Server 2008 中：
   - 展开**软件设置**。

   在 Windows Server 2012 或更高版本中：
   - 依次展开**策略** > **软件设置**。
9. 右键单击**软件安装**，然后指向**新建**，并单击**软件包**。
10. 选择您先前创建的共享文件夹中的代理程序 .msi 安装包，然后单击**打开**。
11. 在**部署软件**对话框中，单击**高级**，然后单击**确定**。
12. 在**修改**选项卡上，单击**添加**，然后选择您先前创建的 .mst 转换。
13. 单击**确定**关闭**部署软件**对话框。

正在更新虚拟设备

本地部署

要更新版本低于 15.24426 (发布于 2020 年 9 月) 的虚拟设备 (适用于 VMware 或 Scale Computing HC3 的代理程序)，请遵循 "更新代理程序"(第 159 页) 中的步骤。

要更新 15.24426 或更新版本的虚拟设备

1. 按照 http://kb.acronis.com/最新 中的描述下载更新包。
2. 在管理服务器计算机上的以下目录中保存该 `tar.bz` 文件：
   - Windows: `C:\Program Files\Acronis\VirtualAppliances\va-updates`
   - Linux: `/usr/lib/Acronis/VirtualAppliances/va-updates`
3. 在 安克诺斯数据保护软件 Web 中控台中，依次单击**设置** > **代理程序**。

   软件将显示计算机列表。虚拟设备过期的计算机将使用橙色感叹号进行标记。
4. 选择要更新虚拟设备的计算机。这些计算机必须处于联机状态。
5. 单击**更新代理程序**。
6. 选择部署代理程序
7. 指定目标计算机上具有管理权限的帐户的凭据。
8. 选择代理程序将用来访问管理服务器的名称或 IP 地址。

   默认情况下，服务器名称已选中。如果 DNS 服务器无法将该名称解析为 IP 地址，导致虚拟设备注册过程出错，则可能需要更改此设置。

更新进度显示在**活动**选项卡上。

注意
在更新过程中，任何正在进行的备份都将失败。

云部署

要获取如何在云部署中更新虚拟设备的信息，请参阅云文档中的 更新代理程序。

更新代理程序

先决条件

在 Windows 计算机上，安克诺斯数据保护软件 功能需要 Microsoft Visual C++ 2017 Redistributable。在更新代理程序之前，请确保已将上述软件安装在计算机上或先安装该软件。在安装后，可能需要重新启动。可以通过以下网址找到 Microsoft Visual C++ 可再发行程序包：https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows。

若要查找代理程序版本，请选择计算机，然后单击**详细信息**。

通过使用 安克诺斯数据保护软件 Web 中控台或以任何可用方式重复代理程序的安装，即可更新代理程序。要同时更新多个代理程序，请使用以下步骤。

使用 安克诺斯数据保护软件 Web 中控台更新代理程序

1. [仅在本地部署时] 更新管理服务器。
2. [仅在本地部署时] 确保带有管理服务器的计算机上具有安装包。有关具体步骤，请参阅"添加运行 Windows 的计算机">"安装包"。
3. 在 安克诺斯数据保护软件 Web 中控台中，依次单击**设置** > **代理程序**。
   软件将显示计算机列表。代理程序版本过期的计算机将使用橙色感叹号进行标记。
4. 选择要更新代理程序的计算机。计算机必须处于联机状态。
5. 单击**更新代理程序**。
6. 选择部署代理程序
7. 指定目标计算机上具有管理权限的帐户的凭据。
8. 选择代理程序将用于访问管理服务器的该服务器的名称或 IP 地址。
   默认情况下，服务器名称处于选中状态。如果您的管理服务器有多个网络接口，或者您遇到导致代理程序注册失败的 DNS 问题，则可能需要改为选择 IP 地址。
9. [仅在本地部署时] 更新进度显示在**活动**选项卡上。

注意
在更新过程中，任何正在进行的备份都将失败。

更新计算机上的 安克诺斯数据保护软件 定义

1. 依次单击**设置** > **代理程序**。
2. 选择要更新其上 安克诺斯数据保护软件 定义的计算机，然后单击**更新定义**。计算机必须处于联机状态。

要将"更新"角色指派给代理程序

1. 依次单击**设置** > **代理程序**。
2. 选择要向其指派"更新"角色的计算机、单击**详细信息**，然后在 **安克诺斯数据保护软件 定义**部分中启用**使用此代理程序来下载并分发修补程序和更新**。

要清除代理程序上的缓存数据

1. 依次单击**设置** > **代理程序**。
2. 选择要清除缓存数据(过时的更新文件和修补程序管理数据)的计算机，然后单击**"清除缓存"**。

升级到 Acronis 安克诺斯数据保护软件 15

可以通过以下方式将较早版本的产品升级到 Acronis 安克诺斯数据保护软件 15:

- 直接升级，无需卸载较早版本的产品。
  此选项仅适用于 Acronis Backup 12.5 Update 5(内部版本为 16180)及更高版本。
- 通过卸载较早版本的产品并安装 Acronis 安克诺斯数据保护软件 15 的最新副本。
  此选项适用于所有符合条件的产品。有关这些产品的详细信息，请参阅此知识库文章。

注意
我们建议您在升级之前先备份系统。如果升级失败，这将允许回滚到原始配置。

要开始升级，运行安装程序并按照屏幕上的说明进行操作。

Acronis 安克诺斯数据保护软件 15 中的管理服务器向后兼容，并支持 12.5 版代理程序。但是，这些代理程序不支持 安克诺斯数据保护软件 功能。

升级代理程序不会干扰现有的备份集及其设置。

卸载产品

如果您想要从计算机中删除个别产品组件，请运行安装程序、选择修改产品，然后取消选中要删除的组件。指向安装程序的链接位于**下载**页面(依次单击右上角的帐户图标 > **下载**)。

如果您想要从计算机中删除所有产品组件，请按照以下所述步骤操作。

警告!
在本地部署中，在选择要卸载的组件时要格外小心。

如果您错误地卸载了管理服务器，安克诺斯数据保护软件 web 中控台将失效，您将不再能够备份和恢复在此已卸载的管理服务器上注册的计算机。

在 Windows 中

1. 以管理员身份登录。
2. 转到**控制面板**，然后依次选择**程序和功能**(在 Windows XP 中为**添加或删除程序**) > **Acronis 安克诺斯数据保护软件** > **卸载**。
3. [可选]选中**删除日志和配置设置**复选框。

如果您要卸载代理程序并计划重新安装它，请不要选中此复选框。如果选中该复选框，可能会在 安克诺斯数据保护软件 Web 中控台中对该计算机进行复制，并且旧计算机的备份可能不会与新计算机关联。

4. 确认您的决定。

在 Linux 中

1. 以根用户身份运行 **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**。
2. [可选] 选中**清除所有产品痕迹(删除产品的日志、任务、保管库和配置设置)**复选框。

   如果您要卸载代理程序并计划重新安装它，请不要选中此复选框。如果选中该复选框，可能会在 安克诺斯数据保护软件 Web 中控台中对该计算机进行复制，并且旧计算机的备份可能不会与新计算机关联。
3. 确认您的决定。

在 macOS 中

1. 双击安装文件 (.dmg)。
2. 等待操作系统加载安装磁盘映像。
3. 在映像内，双击**卸载**。
4. 如果出现提示，请提供管理员凭据。
5. 确认您的决定。

删除适用于 VMware 的代理程序(虚拟设备)

1. 启动 vSphere Client，然后登录到 vCenter 服务器。
2. 如果虚拟设备已开启，请右键单击它，然后依次单击 **电源** > **关闭**。确认您的决定。
3. 如果虚拟设备在虚拟磁盘上使用本地连接存储器，而您想在该磁盘上保留数据，请执行以下步骤：

   a. 右键单击该虚拟设备，然后单击**编辑设置**。

   b. 选择具有存储器的磁盘，然后单击**移除**。在**移除选项**中，单击**从虚拟机移除**。

   c. 单击**确定**。

   执行步骤后，磁盘将保留在数据存储库中。可以将磁盘连接至其他虚拟设备。
4. 右键单击该虚拟设备，然后单击**从磁盘删除**。确认您的决定。

从 安克诺斯数据保护软件 web 中控台删除计算机

卸载代理程序后，将从管理服务器注销，并且安装了代理程序的计算机将从 安克诺斯数据保护软件 web 中控台自动删除。

但是，如果在此操作期间，与该管理服务器的连接中断(例如，由于网络问题)，代理程序可能被卸载，但此计算机可能仍然显示在 web 中控台中。在这种情况下，需要从Web 中控台中控台中手动删除计算机。

从 web 中控台中手动删除计算机

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **代理程序**。
2. 选择安装了代理程序的计算机。
3. 单击**删除**。

访问 安克诺斯数据保护软件 Web 中控台

要访问 安克诺斯数据保护软件 Web 中控台，请将登录页面地址输入 Web 浏览器地址栏中，然后按照以下所述登录。

本地部署

登录页面地址是安装管理服务器的计算机的 IP 地址或名称。

HTTP 和 HTTPS 协议在同一个 TCP 端口上均受支持，可在管理服务器安装过程中进行配置。默认端口为 9877。

可以配置管理服务器，以禁止通过 HTTP 访问 安克诺斯数据保护软件 Web 中控台，以及使用第三方 SSL 证书。

在 Windows 中

如果管理服务器安装在 Windows 中，则有两种方法可以登录到 安克诺斯数据保护软件 Web 中控台：

- 单击**登录**，以当前 Windows 用户身份登录。
  这是从安装了管理服务器的计算机登录的最简单方法。
  如果管理服务器安装在其他计算机上，则使用此方法时需满足以下条件：
  - 您用于登录的计算机位于与管理服务器相同的 Active Directory 域中。
  - 以域用户的身份登录。

  建议您为 Web 服务器配置集成式 Windows 身份验证。否则，浏览器将要求提供用户名和密码。但是，您可以禁用此选项。
- 单击**输入用户名和密码**，然后指定用户名和密码。

在任何情况下，您的帐户都必须位于管理服务器管理员的列表中。默认情况下，此列表包含运行管理服务器的计算机上的**管理员**组。有关详细信息，请参阅“管理员和单元”。

禁用“以当前 Windows 用户身份登录”选项。

1. 在安装管理服务器的计算机上，转到 `C:\Program Files\Acronis\AccountServer`。
2. 打开文件 **account_server.json** 进行编辑。
3. 导航到“connectors”部分，然后删除以下行：

```
{
"type":"sspi",
"name": "1 Windows Integrated Logon",
"id": "sspi",
"config": {}
},
```

4. 导航到“checksum”部分，然后按如下所示更改“sum”值：

```
"sum":"FWY/8e8C6c0AgNl0BfCrjgT4v2uj7RQNmaIYbwbjpzU="
```

5. 重新启动 Acronis 服务管理器服务，如“使用受信任的证书颁发机构颁发的证书”中所述。

在 Linux 中

如果管理服务器安装在 Linux 中，请指定位于管理服务器管理员列表中的帐户的用户名和密码。默认情况下，此列表仅包含运行管理服务器的计算机上的**根**用户。有关详细信息，请参阅“管理员和单元”。

云部署

登录页面地址为 https://backup.acronis.com/。用户名和密码是您 Acronis 帐户的用户名和密码。

如果您的帐户由备份管理员创建，则需要通过单击激活电子邮件中的链接来激活帐户并设置密码。

更改语言

登录后，单击右上角的帐户图标，即可更改 Web 界面的语言。

为 Web 服务器配置集成式 Windows 身份验证

如果从运行 Windows 的计算机或任何受支持的浏览器访问 安克诺斯数据保护软件 Web 中控台，则可以使用集成式 Windows 身份验证。

建议您为 Web 服务器配置集成式 Windows 身份验证。否则，浏览器将要求提供用户名和密码。

配置 Internet Explorer、Microsoft Edge、Opera 和 Google Chrome

如果运行浏览器的计算机与运行管理服务器的计算机位于相同的 Active Directory 域，请将中控台的登录页面添加至**本地内联网**站点列表中。

否则，请将中控台的登录页面添加至**受信任站点**列表中，并启用**使用当前用户名和密码自动登录**设置。

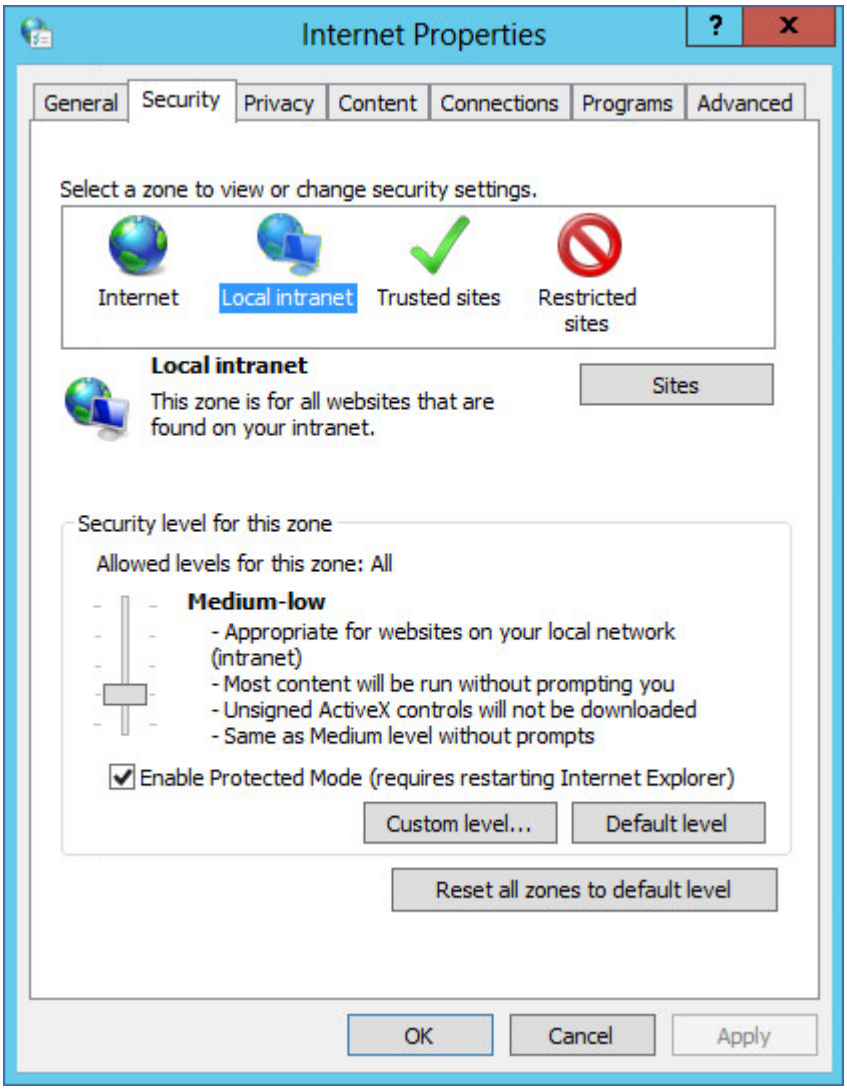
请参阅本部分下文中的逐步说明。由于这些浏览器使用的是 Windows 设置，因此还可以通过使用 Active Directory 域中的组策略进行配置.

配置 Mozilla Firefox

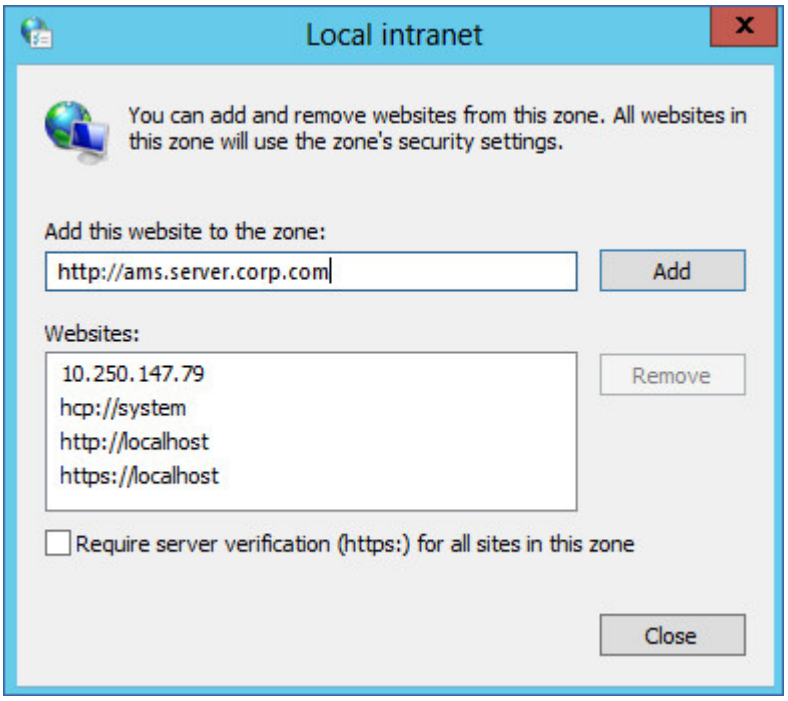
1. 在 Firefox 中，导航到 URL `about:config`，然后单击**我接受风险**按钮。
2. 在**搜索**字段，搜索 `network.negotiate-auth.trusted-uris` 首选项。
3. 双击该首选项，输入 安克诺斯数据保护软件 Web 中控台登录页面的地址。
4. 对 `network.automatic-ntlm-auth.trusted-uris` 首选项重复第 2-3 步。
5. 关闭 `about:config` 窗口。

将中控台添加至本地内联网站点列表

1. 转到**控制面板** > **Internet 选项**。
2. 在**安全**选项卡上，选择**本地内联网**。



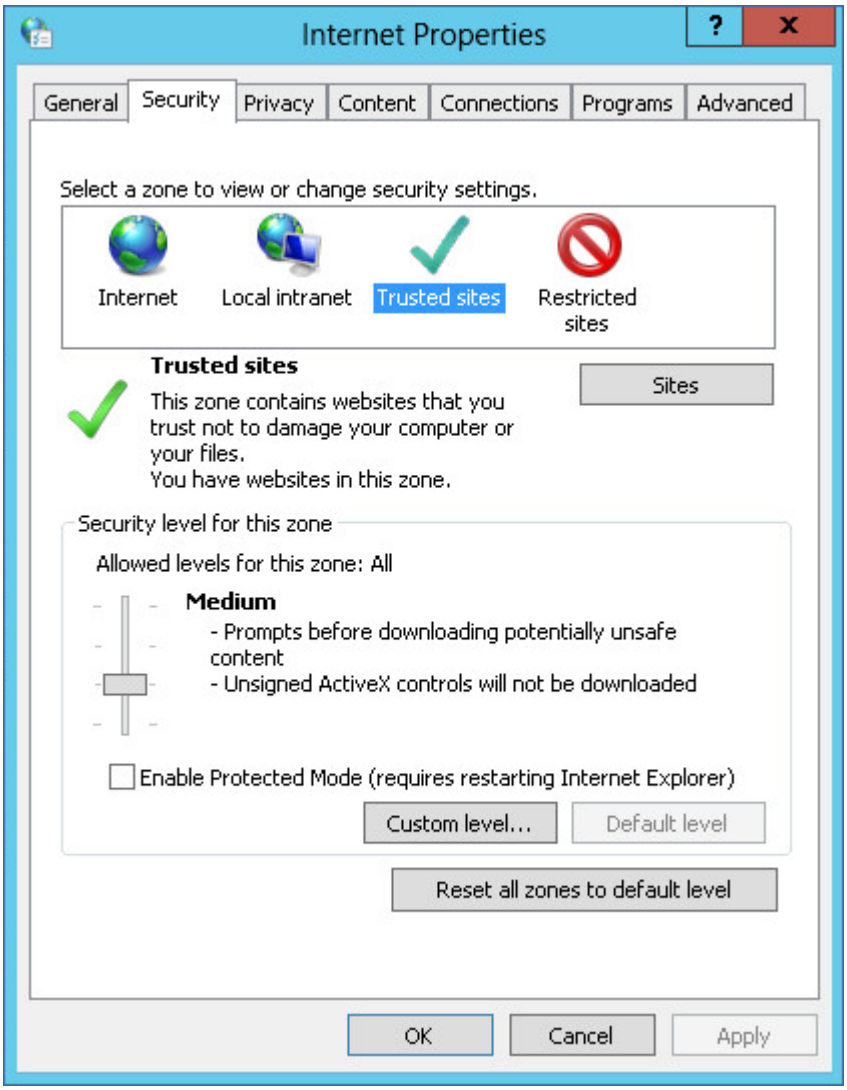
3. 单击**站点**。
4. 在**将此网站添加至区域**中，输入 安克诺斯数据保护软件 Web 中控台登录页面的地址，然后单击**添加**。



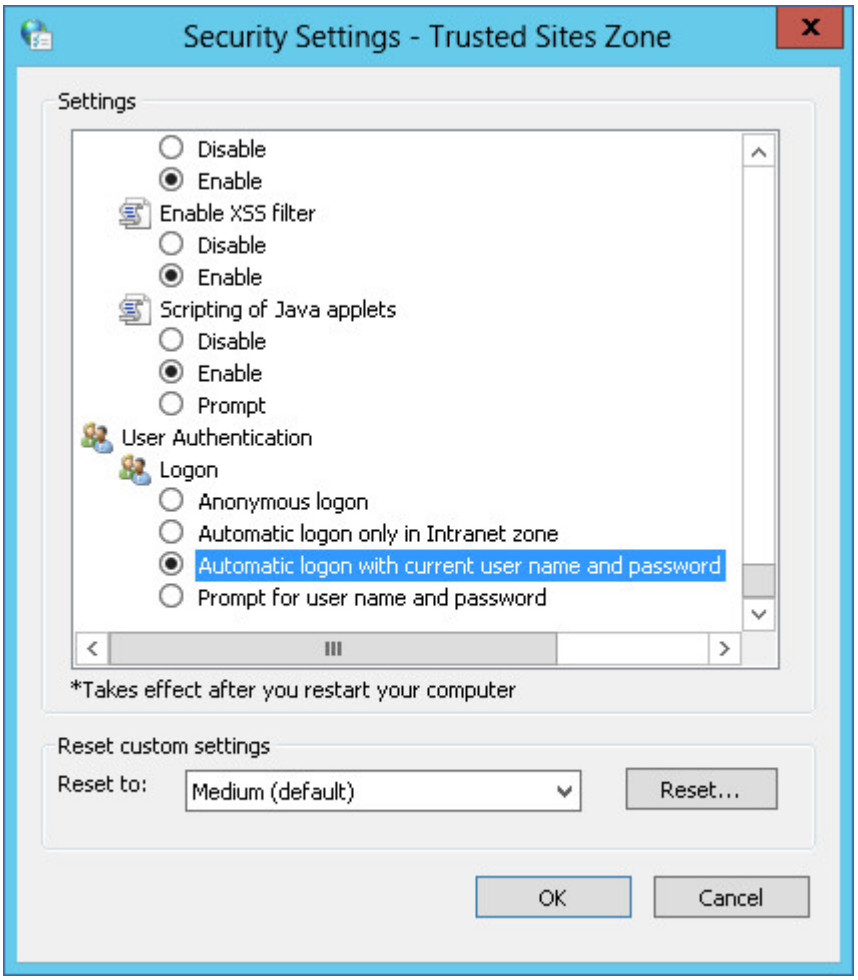
5. 单击**关闭**。
6. 单击**确定**。

将中控台添加至受信任的站点列表

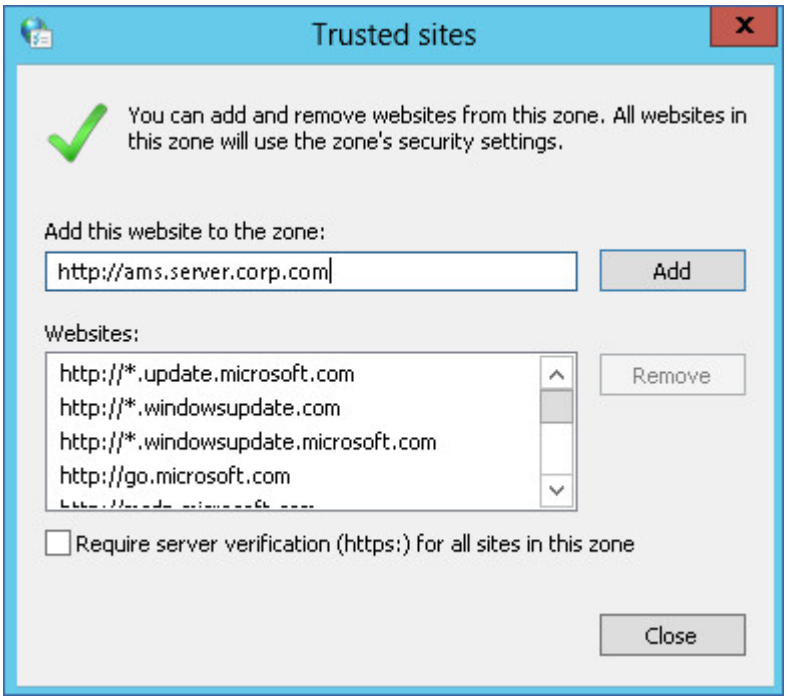
1. 转到**控制面板** > **Internet 选项**。
2. 在**安全**选项卡上，选择**受信任的站点**，然后单击**自定义级别**。



3. 在**登录**下，选择**使用当前用户名和密码自动登录**，然后单击**确定**。



4. 在**安全**选项卡上，仍然选择**受信任的站点**，然后单击**站点**。
5. 在**将此网站添加至区域**中，输入 安克诺斯数据保护软件 Web 中控台登录页面的地址，然后单击**添加**。



6. 单击**关闭**。
7. 单击**确定**。

仅允许与 Web 中控台建立 HTTPS 连接

出于安全原因，可以阻止用户通过 HTTP 协议访问 安克诺斯数据保护软件 Web 中控台，仅允许建立 HTTPS 连接。

仅允许与 Web 中控台建立 HTTPS 连接

1. 在运行管理服务器的计算机上，使用文本编辑器打开以下配置文件：
   - 在 Windows 中：`%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - 在 Linux 中：`/var/lib/Acronis/ApiGateway/api_gateway.json`
2. 找到以下部分：

```
"tls": {
  "auto_redirect" : false,
  "cert_file": "cert.pem",
```

3. 将“`auto_redirect`”值从 `false` 更改为 `true`。
   如果缺少“`auto_redirect`”行，请手动添加它：

```
"auto_redirect": true,
```

4. 保存 `api_gateway.json` 文件。

重要事项
请小心操作，切勿意外删除配置文件中的任何逗号、括号和引号。

5. 按如下所述，重新启动 Acronis 服务管理器服务。

在 Windows 中重新启动 Acronis 服务管理器服务

在 Windows 中

1. 在**开始**菜单中，单击**运行**，然后键入：**cmd**
2. 单击**确定**。
3. 运行以下命令：

```
net stop asm
net start asm
```

在 Linux 中

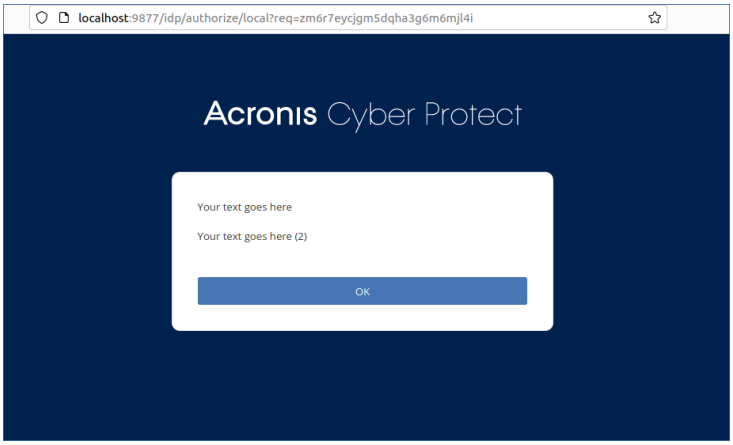
1. 打开**终端**。
2. 在任何目录中运行以下命令：

```
sudo service acronis_asm restart
```

将自定义消息添加到 Web 中控台

可以将自定义消息添加到 安克诺斯数据保护软件 Web 中控台。

此消息会在每次登录尝试之前显示。



先决条件

如果任何保护计划已应用于运行管理服务器的计算机，请确保自我保护功能已禁用。否则，您将无法编辑配置文件。

有关如何禁用或启用自我保护功能的详细信息，请参阅 "自我保护"(第 440 页)。

将自定义消息添加到 Web 中控台

在 Windows 中

1. 登录到装有管理服务器的计算机。您的帐户必须具有管理员权限。
2. 导航到 %Program Files%\Acronis\AccountServer。
3. [可选] 制作 AccountServer.zip 文件的备份副本。
4. 导航到 %Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale。
5. 解压缩与在 安克诺斯数据保护软件 Web 中控台中使用的语言相对应的 JSON 文件。例如，如果您使用英语，则解压缩 en.json 文件。

   注意
   为了能够编辑文件，必须对其进行解压缩，而不仅仅是通过双击来打开文件。

6. 打开解压缩的文件以进行编辑。可以使用文本编辑器，如“Notepad”或“Notepad++”。
7. 导航到以下行，然后在末尾处添加一个逗号：

   ```
   "APP_LOGINFORM_LOGIN_BUTTON":"Log in",
   ```

8. 在 "APP_LOGINFORM_LOGIN_BUTTON":"Log in" 行下，添加以下行：

   ```
   "APP_LOGINFORM_NOTICE": "<Type your custom message here>",
   ```

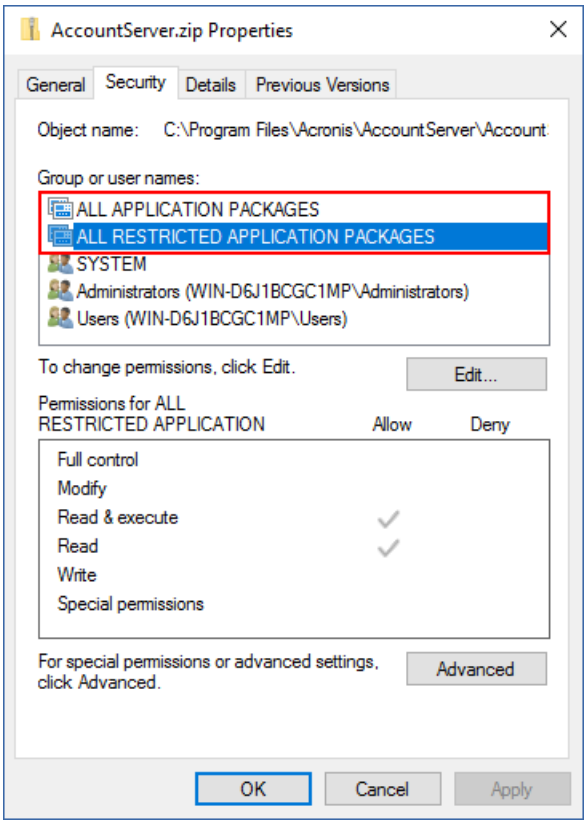
   ```
   "APP_LOGINFORM_IS_SCS": "true",
   ```

   ```
   "APP_LOGINFORM_OK_BUTTON":"OK"
   ```

   例如：

   ```
   16        "APP_LOGINFORM_SSPI_HINT": "Sign in as current Windows user",
   17        "APP_LOGINFORM_LOCAL_HINT": "Enter user name and password",
   18        "APP_ADVANCED_LICENSE_MISSING": "An Advanced license is missing",
   19        "APP_LOGINFORM_LOGOUT": "You logged out",
   20        "APP_LOGINFORM_LOGIN_BUTTON": "Log in",
   21        "APP_LOGINFORM_NOTICE": "Your text goes here /n Your text goes here (2) ",
   22        "APP_LOGINFORM_IS_SCS": "true",
   23        "APP_LOGINFORM_OK_BUTTON": "OK"
   24    }
   ```

9. 保存更改，然后将编辑后的 JSON 文件放回到 %Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale 中。
10. 右键单击 AccountServer.zip 文件，然后导航到**属性** > **安全**以验证所有应用程序包和所有受限制的应用程序包是否已添加在**组或用户名**(具有**读取**和**读取和执行**权限)下。



注意

如果缺少所有受限制的应用程序包，请从该列表中删除所有应用程序包，然后再次添加它。所有受限制的应用程序包会在添加所有应用程序包后自动显示。

11. 重新启动 **Acronis Service Manager 服务**，如 "重新启动 Acronis Service Manager 服务"(第 175 页) 中所述。

在 Linux 中

1. 登录到装有管理服务器的计算机。
2. 导航到 `/usr/lib/Acronis/AccountServer`。
3. 确保您拥有 `AccountServer.zip` 文件的写入权限。
4. [可选] 制作 `AccountServer.zip` 文件的备份副本。
5. 导航到 `/usr/lib/Acronis/AccountServer/static/locale`。
6. 解压缩与在 安克诺斯数据保护软件 Web 中控台中使用的语言相对应的 JSON 文件。例如，如果您使用英语，则解压缩 `en.json` 文件。
7. 打开解压缩的文件以进行编辑。
8. 导航到以下行，然后在末尾处添加一个逗号：

```
"APP_LOGINFORM_LOGIN_BUTTON":"Log in",
```

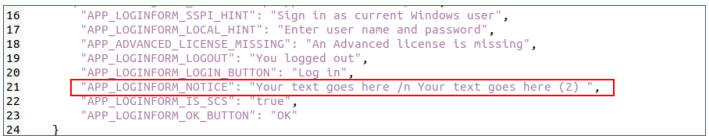
9. 在 `"APP_LOGINFORM_LOGIN_BUTTON":"Log in"` 行下，添加以下行：

```
"APP_LOGINFORM_NOTICE": "<Type your custom message here>",
```

```
"APP_LOGINFORM_IS_SCS": "true",
```

```
"APP_LOGINFORM_OK_BUTTON":"OK"
```

例如：



10. 保存更改，然后将编辑后的 JSON 文件放回到 `/usr/lib/Acronis/AccountServer/static/locale` 中。
11. 重新启动 **Acronis Service Manager 服务**，如 "重新启动 Acronis Service Manager 服务"(第 175 页) 中所述。

SSL 证书设置

本节介绍如何：

- 配置使用管理服务器生成的自签名安全套接层 (SSL) 证书的保护代理程序。
- 将由管理服务器生成的自签名安全套接层 (SSL) 证书更改为由受信任的证书颁发机构发布的证书，如 GoDaddy、Comodo 或 GlobalSign。如果进行上述更改，则管理服务器所使用的证书将在任何计算机上受信任。当使用 HTTPS 协议登录 安克诺斯数据保护软件 Web 中控台时，不会出现浏览器安全警报。

可以选择配置管理服务器，以通过将所有用户重定向到 HTTPS 来禁止通过 HTTP 访问 安克诺斯数据保护软件 Web 中控台。

使用自签名证书

要在 Windows 中配置保护代理程序

1. 在安装了代理程序的计算机上，打开注册表编辑器。
2. 找到以下注册表项：**HKEY_LOCAL_MACHINE\Software\Acronis\BackupAndRecovery\Settings\CurlOptions**。
3. 将 **VerifyPeer** 的值设置为 **0**。
4. 确保将 **VerifyPeer** 的值设置为 **0**。
5. 重启受控计算机服务 (MMS)：
   a. 在**开始**菜单中，单击**运行**，然后键入：**cmd**
   b. 单击**确定**。
   c. 运行以下命令：

```
net stop mms
net start mms
```

要在 Linux 中配置保护代理程序

1. 在安装了代理程序的计算机上，打开文件 **/etc/Acronis/BackupAndRecovery.config** for editing。
2. 导航至 **CurlOptions** 键并将 **VerifyPeer** 的值设置为 **0**。确保 **VerifyHost** 的值也设置为 **0**。
3. 保存编辑。
4. 通过在任意目录中执行以下命令来重新启动受控计算机服务 (MMS)：

```
sudo service acronis_mms restart
```

要在 macOS 中配置保护代理程序

1. 在安装了代理程序的计算机上，停止受控计算机服务 (MMS)。
   a. 转到**应用程序 > 实用程序 > 终端**
   b. 运行以下命令：

```
sudo launchctl stop acronis_mms
```

2. 打开文件 **/Library/Application Support/Acronis/Registry/BackupAndRecovery.config** 进行编辑。
3. 导航至 **CurlOptions** 键并将 **VerifyPeer** 的值设置为 **0**。确保 **VerifyHost** 的值也设置为 **0**。
4. 保存编辑。
5. 通过在终端运行以下命令，启动受控计算机服务 (MMS)。

```
sudo launchctl starts acronis_mms
```

使用受信任的证书颁发机构颁发的证书

若要配置 SSL 证书设置

1. 确保拥有以下各项：

如果使用证书和密钥文件	如果使用 PFX 文件
证书文件 (格式为 .pem)	PFX 文件
内含证书私钥的文件 (格式通常为 .key)	
私钥密码 (如果该密钥受密码保护)	PFX 文件的密码(如果该文件受密码保护)

2. 将该文件复制到运行管理服务器的计算机。
3. 在该计算机上，使用文本编辑器打开以下配置文件：
   - 在 Windows 中：`%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - 在 Linux 中：`/var/lib/Acronis/ApiGateway/api_gateway.json`
4. 找到以下部分：

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "",
```

5. 在 "cert_file" 行中的引号之间，指定证书文件或 PFX 文件的完整路径。
   例如：

操作系统	如果使用证书和密钥对	如果使用 .pfx 文件
Windows (注意正斜杠)	"cert_file":"C:/certificate/local-domain.ams.pem"	"cert_file":"C:/certificate/local-domain.ams.pfx"
Linux	"cert_file": "/home/user/local-domain.ams.pem"	"cert_file": "/home/user/local-domain.ams.pfx"

6. 在 "key_file" 行中的引号之间，指定私钥文件或包含证书密钥的 PFX 文件的完整路径。
   通常，PFX 文件包含证书及其密钥。在这种情况下，在 "key_file" 行中，指定与上一步相同的路径。
   例如：

操作系统	如果使用证书和密钥对	如果使用 .pfx 文件
Windows (注意正斜杠)	"key_file":"C:/certificate/private.key"	"cert_file":"C:/certificate/local-domain.ams.pfx"
Linux	"key_file": "/home/user/private.key"	"cert_file": "/home/user/local-domain.ams.pfx"

7. [可选] 如果私钥或 PFX 文件受密码保护，则在 "passphrase" 行中的引号之间，指定密码。
   例如："passphrase": "my password"

注意
如果 api_gateway.json 配置文件中缺少 "passphrase": ""，行，请手动添加它。
例如：

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "my password",
}
```

8. 保存 api_gateway.json 文件。

重要事项
请小心操作，切勿意外删除配置文件中的任何逗号、括号和引号。

9. 按如下所述，重新启动 Acronis 服务管理器服务。

重新启动 Acronis Service Manager 服务

在 Windows 中

1. 在**开始**菜单中，单击**运行**，然后键入：**cmd**
2. 单击**确定**。
3. 运行以下命令：

```
net stop asm
net start asm
```

在 Linux 中

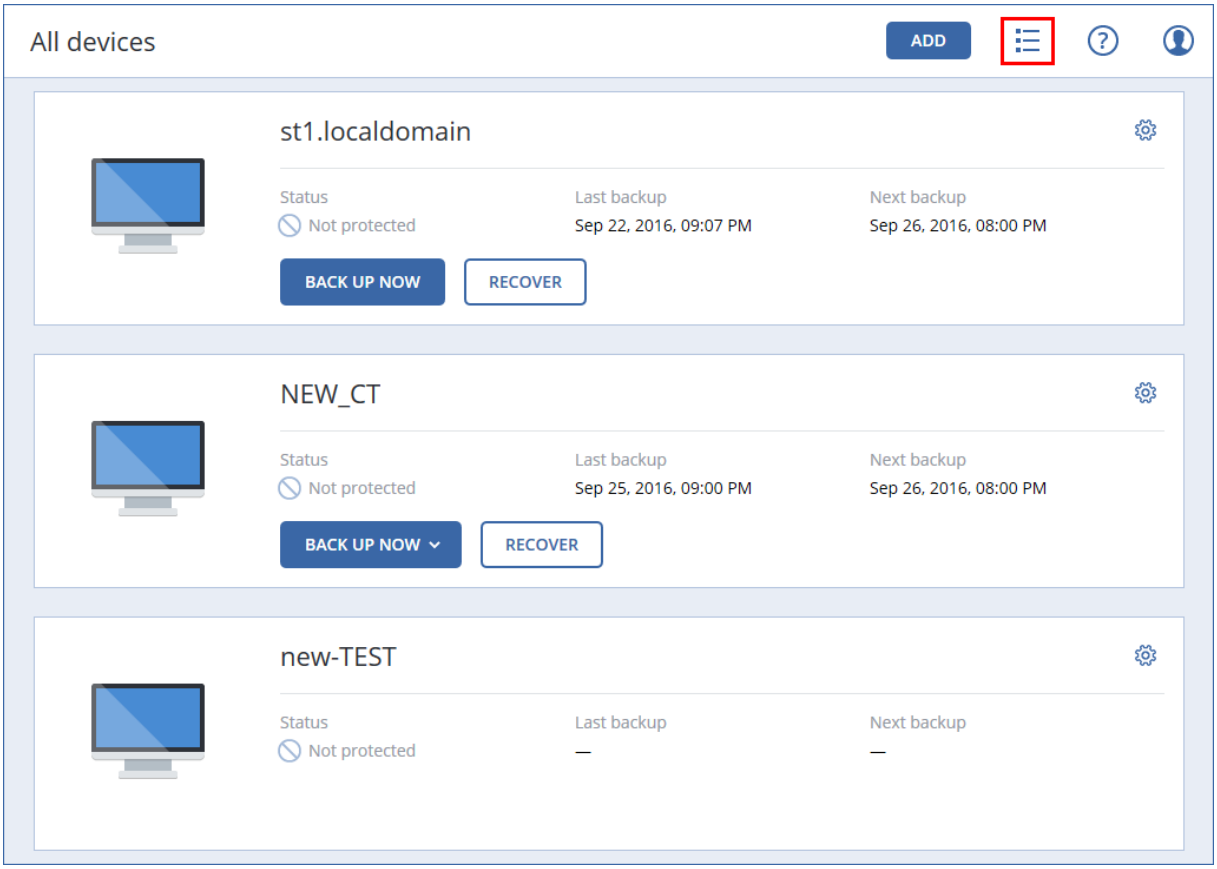
1. 打开**终端**。
2. 在任何目录中运行以下命令：

```
sudo service acronis_asm restart
```

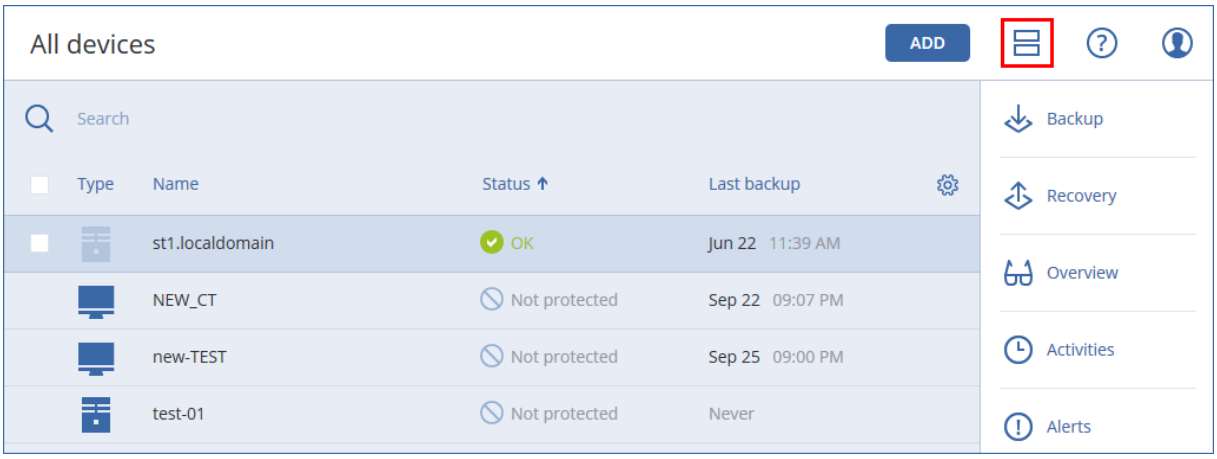
安克诺斯数据保护软件 Web 中控台视图

安克诺斯数据保护软件 Web 中控台有两种视图：简单视图和表视图。若要在视图之间切换，请单击右上角的相应图标。

简单视图支持少量计算机。



当计算机数量变大时，将自动启用表视图。



两种视图均提供对相同功能和操作的访问。本文档介绍从表视图访问操作。

当一台计算机联机或脱机时，该计算机在 安克诺斯数据保护软件 Web 中控台中的状态变化需要一些时间。

将每隔一分钟检查一次计算机状态。如果安装在此计算机上的代理程序并未在传输数据，并且连续五次检查都没有应答，则该计算机将显示为“脱机”。当计算机应答状态检查或开始传输数据时，该计算机将重新显示为“联机”。

保护计划和模块

保护计划是结合了多个数据保护模块的计划，其中包括

- 备份 - 让您可以将数据源备份到本地或云存储。
- 防病毒和反恶意软件保护 - 让您可以使用内置的反恶意软件解决方案检查计算机。
- URL 过滤 - 让您可以通过阻止访问恶意 URL 和要下载内容，来保护您的计算机免受来自 Internet 的威胁的影响。
- Windows Defender Antivirus - 让您可以管理 Windows Defender Antivirus 的设置来保护您的环境。
- Microsoft Security Essentials - 让您可以管理 Microsoft Security Essentials 的设置来保护您的环境。
- 漏洞评估 - 自动检查计算机上安装的 Microsoft 和第三方产品以查找漏洞，并向您提供有关漏洞的通知。
- 修补程序管理 - 让您可以在计算机上安装 Microsoft 和第三方产品的修补程序和更新，以修补发现的漏洞。
- 数据保护地图 - 让您可以发现数据，以便监控重要文件的保护状态。

保护计划让您可以全方位地保护数据源免受外部和内部威胁的影响。通过启用和禁用不同模块并设定模块设置，即可构建满足各种业务需求的灵活计划。

创建保护计划

保护计划可在其创建时或之后应用于多台计算机。当您创建一项计划时，系统会检查操作系统和设备类型(例如:工作站、虚拟机等)，并仅显示适用于您的设备的计划模块。

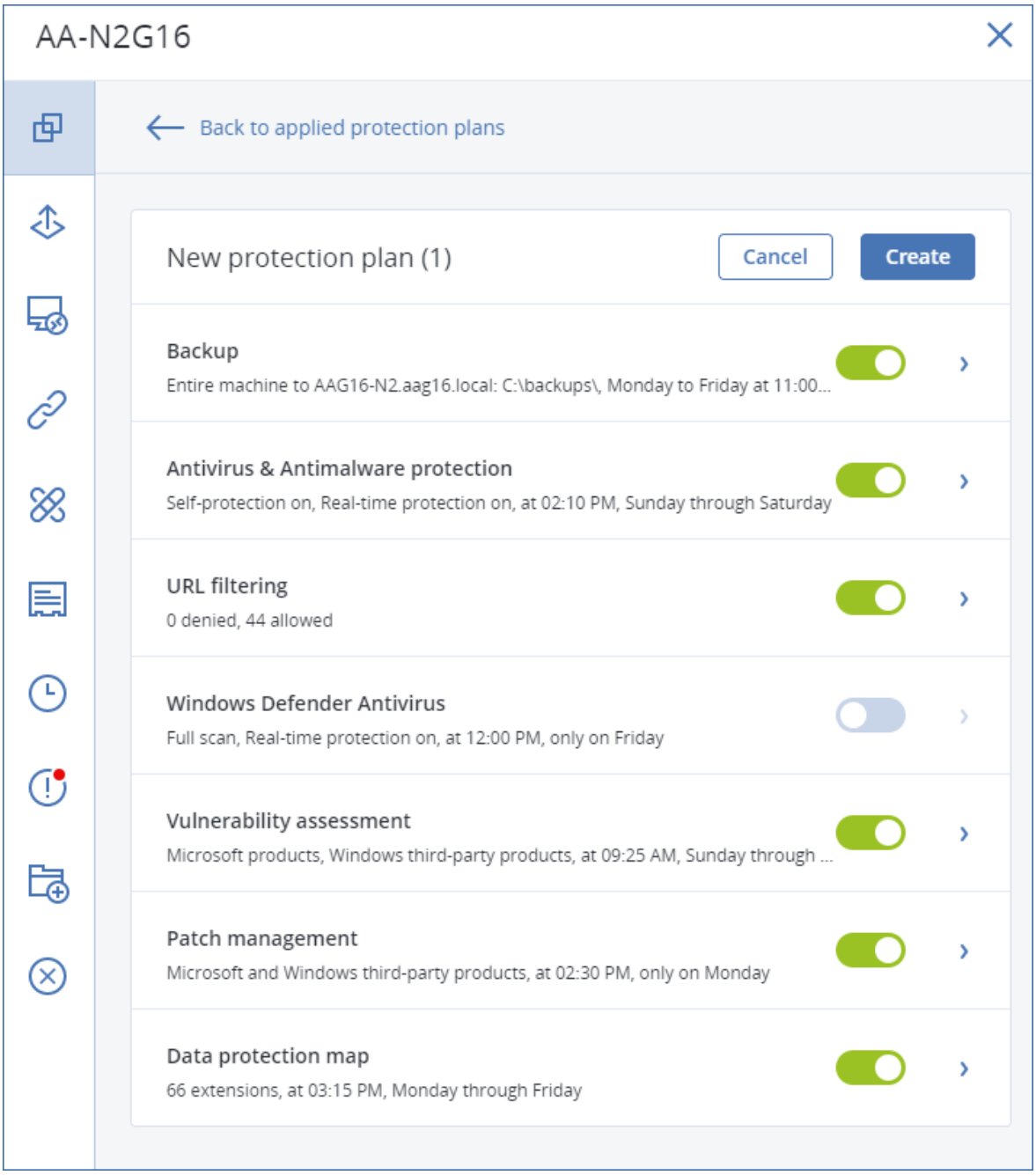
可以通过两种方式创建保护计划:

- 在**设备**部分中 - 选择要保护的一个或多个设备，然后为其创建计划。
- 在**计划**部分中 - 创建一个计划，然后选择要向其应用的计算机。

我们考虑使用第一种方式。

创建第一个保护计划

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设备** > **所有设备**。
2. 选择要保护的计算机。
3. 单击**"保护"**，然后单击**"创建计划"**。您将看到采用默认设置的保护计划。



4. [可选] 要修改保护计划名称，请单击名称旁边的铅笔图标。
5. [可选] 要启用或禁用计划模块，请单击模块名称旁边的开关。
6. [可选] 要配置模块参数，请单击保护计划的相应部分。
7. 准备就绪后，单击**创建**。

通过单击**立即运行**，即可手动执行“备份”、“防病毒和反恶意软件保护”、“漏洞评估”、“修补程序管理”和“数据保护地图”模块。

解决计划冲突

保护计划可以处于以下状态：

- **活动** - 计划已指派给设备并在设备上执行。
- **非活动** - 计划已指派给设备但处于禁用状态，不在设备上执行

将多个计划应用于设备

可以将多个保护计划应用于单个设备。结果是，您将在单个设备上指派一组不同的保护计划。例如，可以应用一个仅在该计划中启用了“防病毒和反恶意软件保护”模块的计划，而应用的另一个计划中仅包含“备份”模块。仅当保护计划中没有相交模块时，才能组合使用保护计划。如果在多个保护计划中启用了相同的模块，则必须解决它们之间的冲突。

解决计划冲突

计划与已应用的计划冲突

在一个或多个设备上创建新计划，但已应用的计划与新计划冲突时，可以通过以下方式之一来解决冲突：

- 创建新计划、应用它，然后禁用所有已应用的冲突计划。
- 创建新计划，然后禁用它。

在一个或多个设备上编辑计划，但已应用的计划与进行的更改冲突时，可以通过以下方式之一来解决冲突：

- 将更改保存到计划，然后禁用所有已应用的冲突计划。
- 将更改保存到计划，然后禁用它。

设备计划与组计划冲突

如果某个设备包含在已指派有组计划的一组设备中，并且您尝试为该设备指派新计划，则系统将要求您通过执行以下操作之一来解决冲突：

- 将设备从组中删除，然后为该设备应用新计划。
- 将新计划应用于整个组，或编辑当前组计划。

许可问题

设备上指派的配额必须适用于要执行、要更新或要应用的保护计划。要解决许可问题，请执行以下操作之一：

- 禁用指派的配额不支持的模块，然后继续使用保护计划。
- 手动更改指派的配额：转到**设备** > **<特定设备>** > **详细信息** > **服务配额**。然后吊销现有配额并指派新配额。

保护计划的操作

有关如何创建保护计划的信息，请参考“创建保护计划”。

保护计划的可用操作

可以执行以下保护计划的操作：

- 重命名计划
- 启用/禁用模块和编辑每个模块设置
- 启用/禁用计划

  禁用的计划将不会在应用该计划的设备上执行。

  对于打算以后使用相同计划保护同一设备的管理员来说，此操作很方便。该计划未从设备中吊销，要恢复保护，管理员只能重新启用该计划。
- 将计划应用于设备或设备组
- 吊销设备中的计划

  吊销的计划不会再应用于设备。

  对于不需要再次使用相同计划快速保护同一设备的管理员来说，此操作很方便。要恢复已吊销计划的保护，管理员必须知道该计划的名称、从可用计划列表中选择它，然后将该计划重新应用于所需设备。
- 导入/导出计划

  注意

  只能导入仅在 Acronis 安克诺斯数据保护软件 15 中创建的保护计划。使用旧版本创建的保护计划与 Acronis 安克诺斯数据保护软件 15 不兼容。
- 删除计划

应用现有保护计划

1. 选择要保护的计算机。
2. 单击**保护**。如果已将保护计划应用于选定计算机，请单击**添加计划**。
3. 该软件将显示以前创建的保护计划。
4. 选择所需的保护，然后单击**应用**。

编辑保护计划

1. 如果要编辑向所有计算机应用的保护计划，请选择这些计算机这些计算机之一。否则，选择要编辑保护计划的计算机。
2. 单击**保护**。
3. 选择要编辑的保护计划。
4. 单击保护计划名称旁边的省略号图标，然后单击**编辑**。
5. 要修改计划参数，请单击保护计划面板的相应部分。
6. 单击**保存更改**。
7. 要更改向所有计算机应用的保护计划，请单击**将更改应用于此保护计划**。否则，请单击**仅为选定设备创建新的保护计划**。

吊销计算机中的保护计划

1. 选择要从其中吊销保护计划的计算机。
2. 单击**保护**。
3. 如果已将多个保护计划应用于计算机，请选择要吊销的保护计划。
4. 单击保护计划名称旁边的省略号图标，然后单击**吊销**。

删除保护计划

1. 选择已应用要删除的保护计划的任何计算机。
2. 单击**保护**。
3. 如果已将多个保护计划应用于计算机，请选择要删除的保护计划。
4. 单击保护计划名称旁边的省略号图标，然后单击**删除**。
   结果是，保护计划从所有计算机中吊销，并从 Web 界面中完全删除。

备份

启用了备份模块的保护计划是一组规则，这些规则指定如何在给定计算机上保护给定数据。

保护计划可在其创建时或之后应用于多台计算机。

注意
在本地部署中，如果管理服务器上仅存在标准许可证，则保护计划无法应用于多个物理机。每个物理机必须具有自己的保护计划。

创建第一个启用备份模块的保护计划

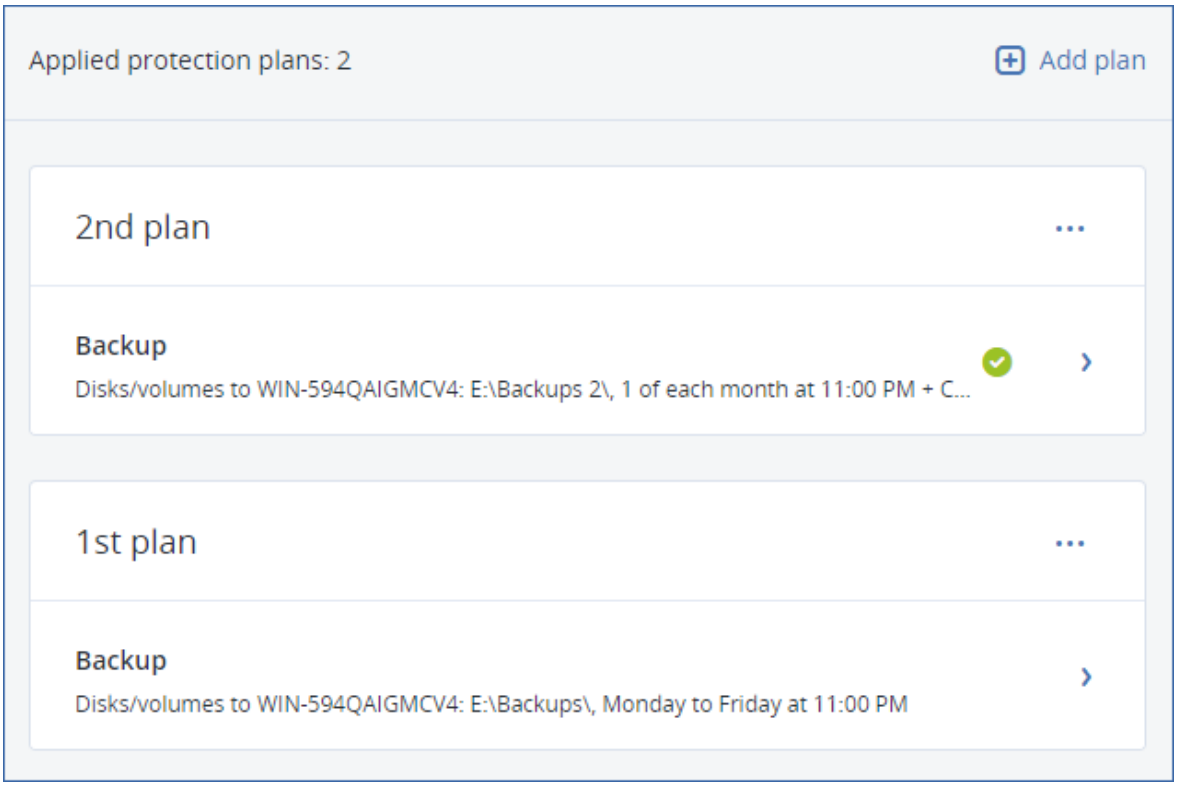
1. 选择要备份的计算机。
2. 单击**保护**。
   该软件将显示应用于计算机的保护计划。如果计算机尚未指派有任何计划，则将看到可以应用

的默认保护计划。可以根据需要调整设置并应用此计划，也可以创建新计划。

3. 要创建新计划，请单击**创建计划**。启用**备份**模块，然后展开设置。
4. [可选] 要修改保护计划名称，请单击默认名称。
5. [可选] 要修改备份模块参数，请单击保护计划面板的相应部分。
6. [可选] 要修改备份选项，请单击**备份选项**旁边的**更改**。
7. 单击**创建**。

应用现有保护计划

1. 选择要备份的计算机。
2. 单击**保护**。如果已将常用保护计划应用于选定计算机，请单击**添加计划**。
   该软件将显示以前创建的保护计划。



3. 选择要应用的保护计划。
4. 单击**应用**。

备份模块速查表

重要事项
本部分中所述的一些功能仅适用于本地部署。

下表总结了可用的备份模块参数。使用该表创建最符合您需求的保护计划。

备份内容	备份项目选择方法	备份位置	预定备份方案（不适用于云）	保留时间
磁盘/卷（物理机）	直接选择 策略规则 文件过滤器	云 本地文件夹 网络文件夹 SFTP 服务器*	始终增量（单个文件）* 始终完整	按备份存留时间（单规则/每备份集） 按备份数量 按备份的总大小*

		NFS* 安全区* 受控位置* 磁带设备*	每周完整，每日增量 每月完整、每周差异和每日增量备份 (GFS) 自定义 (F-D-I)	无限期保留
磁盘/卷（虚拟机）	策略规则 文件过滤器	云 本地文件夹 网络文件夹 SFTP 服务器* NFS* 受控位置* 磁带设备*		
文件（仅物理机）	直接选择 策略规则 文件过滤器	云 本地文件夹 网络文件夹 SFTP 服务器* NFS* 安全区* 受控位置* 磁带设备	始终完整 每周完整，每日增量 每月完整、每周差异和每日增量备份 (GFS) 始终增量（单个文件）* 自定义 (F-D-I)	
ESXi 配置	直接选择	本地文件夹 网络文件夹 SFTP 服务器 NFS*		
系统状态（仅适用于云部署）	直接选择	云 本地文件夹 网络文件夹	始终完整 每周完整，每日增量 自定义 (F-I)	

SQL 数据库	直接选择	云 本地文件夹 网络文件夹 受控位置* 磁带设备		
Exchange 数据库	直接选择			
Exchange 邮箱	直接选择	云 本地文件夹 网络文件夹 受控位置*	始终增量(单个文件)	
Microsoft 365 邮箱	直接选择			按备份存留时间(单规则/每备份集) 按备份数量 无限期保留

* 请参阅以下限制。

限制

SFTP 服务器和磁带设备

- 这些位置无法作为运行 macOS 的计算机的备份目标位置。
- 这些位置无法作为应用程序感知备份的目标位置。
- **始终增量(单个文件)**备份方案在备份到这些位置时不可用。
- **按备份的总大小**保留规则不可用于这些位置。

NFS

- 备份到 NFS 共享不可用于 Windows 中。
- 文件(物理机)的**始终增量(单个文件)**备份方案在备份到 NFS 共享时不可用。

安全区

- 无法在 Mac 上创建安全区。

受控位置

- 在以下情况下，已启用重复数据删除或加密的受控位置不可选为目标位置：
  - 如果备份方案设置为**始终增量(单个文件)**
  - 如果备份格式设置为**版本 12**
  - 运行 macOS 的计算机的磁盘级别备份
  - Exchange 邮箱和 Microsoft 365 邮箱的备份。
- **按备份的总大小**保留规则不可用于已启用重复数据删除的受控位置。

始终增量(单个文件)

- **始终增量(单个文件)**备份方案在备份到 SFTP 服务器或磁带设备时不可用。
- 仅当主备份位置位于 云时，才可以对文件(物理机)使用**始终增量(单个文件)**备份方案。

按备份的总大小

- 在以下情况下，**按备份的总大小**保留规则不可用：
  - 如果备份方案设置为**始终增量(单个文件)**
  - 当备份到 SFTP 服务器、磁带设备或已启用重复数据删除的受控位置时。

选择要备份的数据

选择整个计算机

整个计算机的备份是其所有不可移动磁盘的备份。

要配置此类备份，请在**要备份的内容**中，选择**整个计算机**。

重要事项
外部驱动器(例如，USB 闪存驱动器或 USB 硬盘驱动器)不会包括在**整个计算机**备份中。要备份这些驱动器，请配置**磁盘/卷**备份。有关磁盘备份的详细信息，请参阅 "选择磁盘/卷"(第 190 页)。

选择磁盘/卷

磁盘级备份以打包形式包含磁盘或卷的副本。您可以从磁盘级备份恢复个别磁盘、卷或文件。整个计算机的备份是其所有不可移动磁盘的备份。

注意
默认情况下，OneDrive 根文件夹不包含在备份操作中。如果选择备份特定的 OneDrive 文件和文件夹，将备份它们。在该设备上不可用的文件将在存档中有无效的内容。

有两种选择磁盘/卷的方式：直接在每台计算机上或使用策略规则。可以通过设置文件过滤器，将文件从磁盘备份中排除。

直接选择

直接选择仅适用于物理机。为了能够在虚拟机上直接选择磁盘和卷，必须在其来宾操作系统中安装保护代理程序。

1. 在**要备份的内容**中，选择**磁盘/卷**。
2. 单击**备份项目**。
3. 在**选择要备份的项目**中，选择**直接**。
4. 对于保护计划中包括的每台计算机，请选中要备份的磁盘或卷旁边的复选框。
5. 单击**完成**。

使用策略规则

1. 在**要备份的内容**中，选择**磁盘/卷**。
2. 单击**备份项目**。
3. 在**选择要备份的项目**中，选择**使用策略规则**。
4. 选择任意预定义规则、键入您自己的规则或将两者结合。

   策略规则将应用于保护计划中包括的所有计算机。如果当备份启动时未在计算机上找到满足至少一个规则的数据，则备份将在该计算机上失败。
5. 单击**完成**。

Windows、Linux 和 macOS 的规则

- [所有卷] 选择运行 Windows 的计算机上的所有卷和运行 Linux 或 macOS 的计算机上的所有已加载卷。

Windows 的规则

- 驱动器号 (例如 **C:**) 选择带有指定驱动器号的卷。
- [固定卷(物理机)] 选择物理机的所有卷 (可移动媒体除外)。固定卷包括 SCSI、ATAPI、ATA、SSA、SAS 和 SATA 设备上的卷以及 RAID 阵列上的卷。
- [启动+系统] 选择启动卷和系统卷。本组合是确保从备份恢复操作系统的最小数据集。
- [启动+系统磁盘(物理机)] 选择启动卷和系统卷所在磁盘上的所有卷。如果启动卷和系统卷不在同一磁盘上，则不会选择任何对象。此规则仅使用于物理机。
- [磁盘 1] 选择计算机的第一个磁盘，包括该磁盘上的所有卷。若要选择另一个磁盘，请键入相应的编号。

Linux 的规则

- `/dev/hda1` 选择第一个 IDE 硬盘上的第一个卷。
- `/dev/sda1` 选择第一个 SCSI 硬盘上的第一个卷。
- `/dev/md1` 选择第一个软件 RAID 硬盘。

要选择其他基本卷，请指定 `/dev/xdyN`，其中：

- “x”对应于磁盘类型
- “y”对应于磁盘号(a 对应第一个磁盘，b 对应第二个磁盘，以此类推)
- “N”是卷号。

要选择逻辑卷，请指定其在根帐户下运行 `ls /dev/mapper` 命令后显示的路径。例如：

```
[root@localhost ~]# ls /dev/mapper/
control vg_1-lv1 vg_1-lv2
```

此输出会显示属于卷组 **vg_1** 的两个逻辑卷 **lv1** 和 **lv2**。要备份这些卷，请输入：

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

macOS 的规则

- `[Disk 1]` 选择计算机的第一个磁盘，包括该磁盘上的所有卷。若要选择另一个磁盘，请键入相应的编号。

磁盘或卷备份存储什么内容?

磁盘或卷备份存储整个磁盘或卷**文件系统**，并包括操作系统启动所需的所有信息。从这样的备份可以恢复整个磁盘或卷，以及单个文件夹或文件。

启用**逐扇区(原始模式)**备份选项后，磁盘备份将存储所有磁盘扇区。可使用逐个扇区备份选项来备份具有无法识别或不支持的文件系统及其他专有数据格式的磁盘。

Windows

卷备份用于存储所选卷的所有文件和文件夹(包括隐藏和系统文件，不论其属性为何)、启动记录、文件配置表 (FAT)(如有)、带有主启动记录 (MBR) 的硬盘的根和零磁道。

磁盘备份用于存储所选磁盘的所有卷(包括诸如厂商的维护分区的隐藏卷)以及含有主启动记录的零磁道。

磁盘或卷备份(以及文件级备份)中*不*包括以下项目：

- 交换文件 (pagefile.sys) 和当计算机进入休眠状态时用于保留 RAM 内容的文件 (hiberfil.sys)。恢复后，将在相应的位置以零大小重新创建这些文件。
- 如果在操作系统下执行备份(与可启动媒体或在监控程序级别备份虚拟机不同)：
  - Windows 影存储。其路径在注册表值 **VSS Default Provider** 中确定，这可在注册表项 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup** 中找到。这意味着在从 Windows 7 开始的操作系统中，不会备份 Windows 还原点。
  - 如果启用**卷影复制服务 (VSS)**备份选项，则文件和文件夹在 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** 注册表项中指定。

Linux

卷备份会存储选定卷的所有文件和目录(不论其属性如何)、启动记录和文件系统超级区块。

磁盘备份会存储所有磁盘卷以及包含主启动记录的零磁道。

Mac

磁盘或卷备份会存储选定磁盘或卷的所有文件和目录，外加卷布局的描述。

排除以下项目：

- 系统元数据，如文件系统日志和 Spotlight 索引
- 垃圾
- Time Machine 备份

从物理角度看，Mac 上的磁盘和卷在文件级别备份。可以从磁盘和卷备份进行裸机恢复，但是逐扇区备份模式不可用。

选择文件/文件夹

文件级备份适用于由来宾操作系统中安装的代理程序备份的物理机和虚拟机。

文件级备份不足以进行操作系统恢复。如果您计划仅保护特定数据(例如，当前项目)，请选择文件备份。这将减少备份大小，从而节省存储空间。

注意
默认情况下，OneDrive 根文件夹不包含在备份操作中。如果选择备份特定的 OneDrive 文件和文件夹，将备份它们。在该设备上不可用的文件将在存档中有无效的内容。

有两种选择文件的方式：直接在每台计算机上或使用策略规则。每种方法都允许您通过设置文件过滤器进一步优化选择。

直接选择

1. 在**备份内容**中，选择**文件/文件夹**。
2. 单击**备份项目**。
3. 在**选择要备份的项目**中，选择**直接**。
4. 对于保护计划中包括的每台计算机：
   a. 单击**选择文件和文件夹**。
   b. 单击**本地文件夹**或**网络文件夹**。
      必须能够从选定的计算机访问共享。
   c. 浏览到所需的文件/文件夹或输入路径并单击箭头按钮。如果出现提示，请指定共享文件夹的用户名和密码。
      不支持使用匿名访问备份文件夹。
   d. 选择所需的文件/文件夹。
   e. 单击**完成**。

使用策略规则

1. 在**备份内容**中，选择**文件/文件夹**。
2. 单击**备份项目**。
3. 在**选择要备份的项目**中，选择**使用策略规则**。
4. 选择任意预定义规则、键入您自己的规则或将两者结合。

   策略规则将应用于保护计划中包括的所有计算机。如果当备份启动时未在计算机上找到满足至少一个规则的数据，则备份将在该计算机上失败。
5. 单击**完成**。

Windows 的选择规则

- 文件或文件夹的完整路径，例如 **D:\Work\Text.doc** 或 **C:\Windows**。
- 模板：
  - `[All Files]` 选择计算机所有卷上的所有文件。
  - `[All Profiles Folder]` 选择所有用户配置文件所在的文件夹（通常为 **C:\Users** 或 **C:\Documents and Settings**）。
- 环境变量：
  - `%ALLUSERSPROFILE%` 选择所有用户配置文件的公共数据所在的文件夹（通常为 **C:\ProgramData** 或 **C:\Documents and Settings\All Users**）。
  - `%PROGRAMFILES%` 选择 Program Files 文件夹（例如，**C:\Program Files**）。
  - `%WINDIR%` 选择 Windows 所在的文件夹（例如，**C:\Windows**）。

  您可以使用其他环境变量或环境变量和文本的组合。例如，若要选择 Program Files 文件夹中的 Java 文件夹，请键入：**%PROGRAMFILES%\Java**。

Linux 的选择规则

- 文件或目录的完整路径。例如，若要在 **/home/usr/docs** 上加载的卷 **/dev/hda3** 上备份 **file.txt**，请指定 **/dev/hda3/file.txt** 或 **/home/usr/docs/file.txt**。
  - `/home` 选择一般用户的主目录。
  - `/root` 选择根用户的主目录。
  - `/usr` 选择用户所有相关程序的目录。
  - `/etc` 选择系统配置文件的目录。
- 模板：
  - `[All Profiles Folder]` 选择 **/home**。这是所有用户配置文件默认情况下所在的文件夹。

macOS 的选择规则

- 文件或目录的完整路径。
- 模板：
  - `[All Profiles Folder]` 选择 **/Users**。这是所有用户配置文件默认情况下所在的文件夹。

示例：

- 若要在桌面上备份 **file.txt**，请指定 **/Users/<username>/Desktop/file.txt**，其中 <username> 是您的用户名。
- 若要备份所有用户的主目录，请指定 **/Users**。
- 若要备份安装了应用程序的目录，请指定 **/Applications**。

选择系统状态

系统状态备份适用于运行 Windows 7 及更高版本的计算机。

要备份系统状态，请在**备份内容**中选择**系统状态**。

系统状态备份由以下文件组成：

- 任务预定程序配置
- VSS 元数据存储
- 性能计数器配置信息
- MSSearch 服务
- 后台智能传输服务 (BITS)
- 注册表
- Windows 管理规范 (WMI)
- 组件服务类注册数据库

选择 ESXi 配置

ESXi 主机配置的备份可使您将 ESXi 主机恢复到裸机。此恢复在可启动媒体下执行。

在该主机上运行的虚拟机不包含在备份中。可以单独备份和恢复它们。

ESXi 主机配置的备份包括：

- 启动加载程序和主机的启动库分区。
- 主机状态(虚拟网络和存储的配置、SSL 密钥、服务器网络设置和本地用户信息)。
- 已安装或暂存在主机上的扩展和修补程序。
- 日志文件。

先决条件

- 必须在 ESXi 主机配置的**安全配置文件**中启用 SSH。
- 要备份 ESXi 配置，适用于 VMware 的代理程序使用 SSH 连接到 TCP 端口 22 上的 ESXi 主机。请确保您的防火墙不会阻止此连接。
- 您必须知道 ESXi 主机上的“根”帐户的密码。

限制

- VMware vSphere 7.0 不支持 ESXi 配置备份。
- 无法将 ESXi 配置备份到云存储。

选择 ESXi 配置

1. 单击**设备** > **所有设备**，然后选择要备份的 ESXi 主机。
2. 单击**备份**。
3. 在**要备份的内容**中，选择 **ESXi 配置**。
4. 在 **ESXi“根”密码**中，指定每台选定主机上的“根”帐户的密码，或者将相同的密码应用到所有主机。

连续数据保护 (CDP)

出于性能原因，通常按常规但时间较长的间隔执行备份。如果系统突然损坏，则上次备份和系统故障之间进行的数据更改将丢失。

连续数据保护功能让您可以连续备份预定备份之间选定数据的更改：

- 通过跟踪指定文件/文件夹中的更改
- 通过跟踪指定应用程序修改的文件的更改

可以从为备份选择的数据中选择要进行连续数据保护的特定文件。系统将备份这些文件的每一更改。可以将这些文件恢复至上次更改时间点。

当前，**连续数据保护**功能支持用于以下操作系统：

- Windows 7 及更高版本
- Windows Server 2008 R2 及更高版本

支持的文件系统：仅 NTFS，仅本地文件夹（不支持共享文件夹）。

连续数据保护选项与**应用程序备份**选项不兼容。

注意
不同版本的功能有所不同。您的许可证可能无法使用本文档中描述的某些功能。有关每个版本中所包含功能的详细信息，请参阅 Acronis 安克诺斯数据保护软件 15 版本比较（包括云部署）。

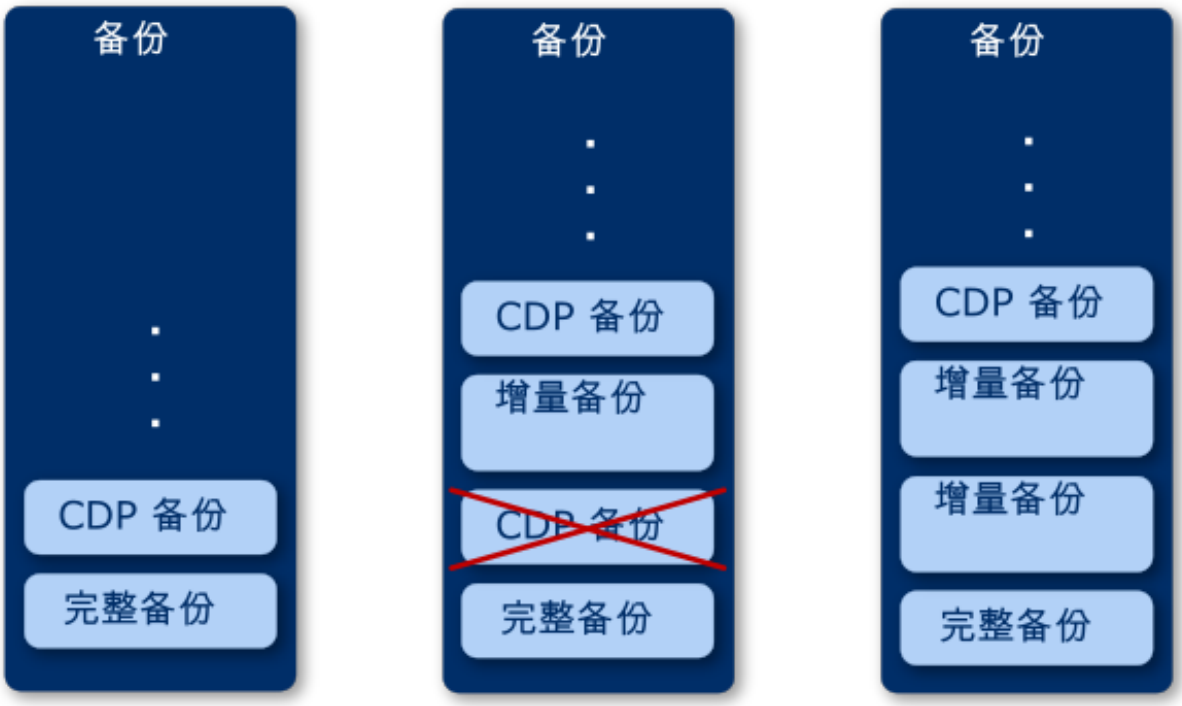
工作方式

让我们将连续创建的备份称为 CDP 备份。要创建 CDP 备份，必须预先创建完整备份或增量备份。

在启用备份模块和**连续数据保护**的情况下首次运行保护计划时，将首次创建完整备份。之后，将为选定或更改的文件/文件夹创建 CDP 备份。CDP 备份会始终包含您在最新状态下选择的数据。对选定文件/文件夹进行更改时，将不会创建新的 CDP 备份，而是将所有更改都记录到同一 CDP 备份中。

当开始预定的增量备份时，将放弃 CDP 备份，并在完成增量备份后创建新的 CDP 备份。

因此，CDP 备份始终保持为备份链中具有受保护文件/文件夹的最新实际状态的最新备份。



如果您已经有启用了备份模块的保护计划，并且决定启用**连续数据保护**，那么在启用该选项后将立即创建 CDP 备份，因为备份链已具有完整备份。

支持用于连续数据保护的数据源和目标

为了使连续数据保护能够正常工作，需要为以下数据源指定以下各项：

备份内容	要备份的项目
整台计算机	必须指定文件/文件夹或应用程序
磁盘/卷	必须指定磁盘/卷以及文件/文件夹或应用程序
文件/文件夹	必须指定文件/文件夹 可以指定应用程序(不强制)

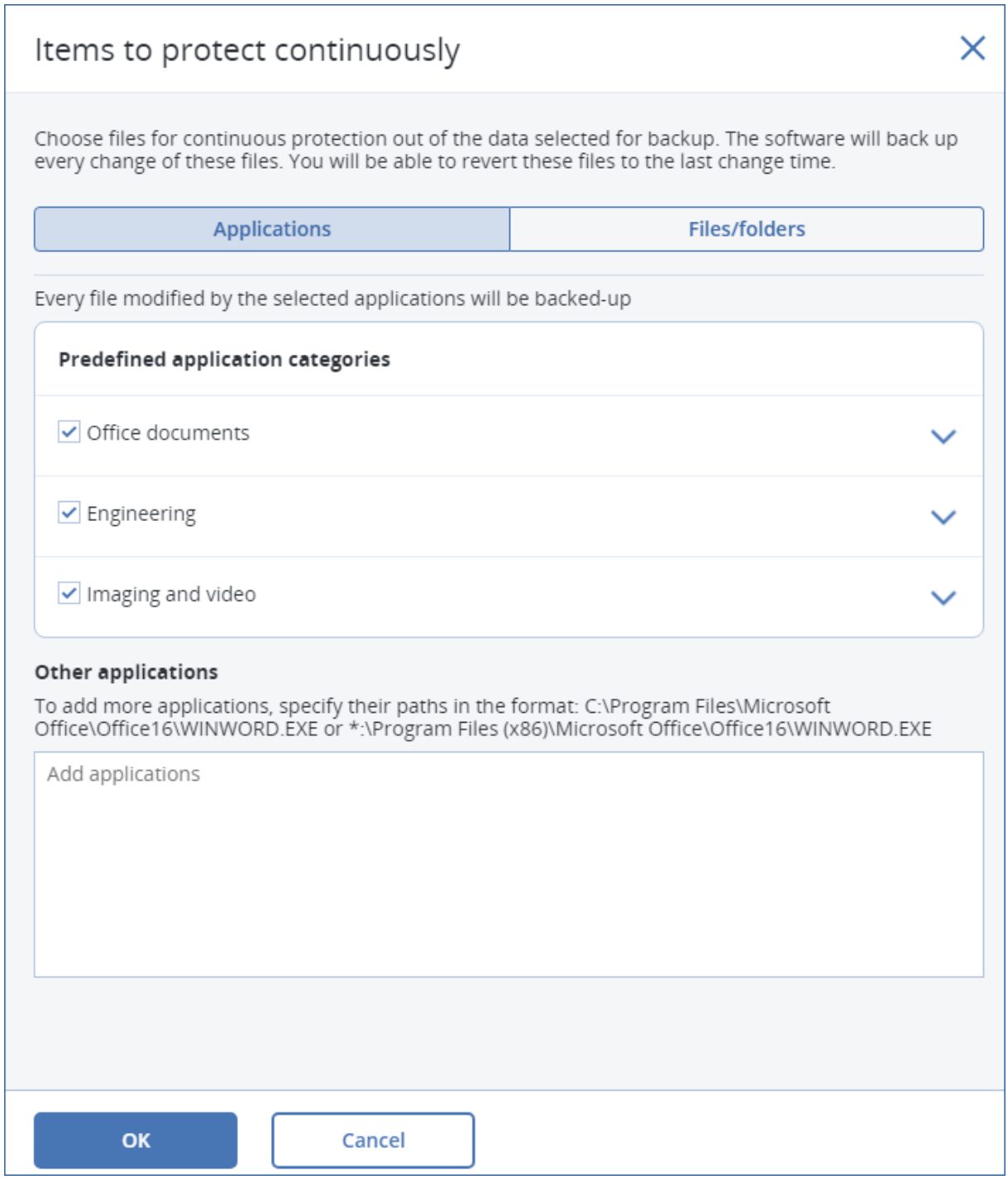
以下备份目标支持用于连续数据保护：

- 本地文件夹
- 网络文件夹

- 由脚本定义的位置
- 云存储
- Acronis Cyber Infrastructure

使用连续数据保护来保护设备

1. 在 安克诺斯数据保护软件 Web 中控台中，创建保护计划(具有已启用的**备份**模块)。
2. 启用**连续数据保护(CDP)**选项。
3. 指定**要连续保护的项目**：
   - **应用程序**(将备份选定应用程序修改的任何文件)。建议您使用此选项来通过“CDP 备份”保护 Office 文档。



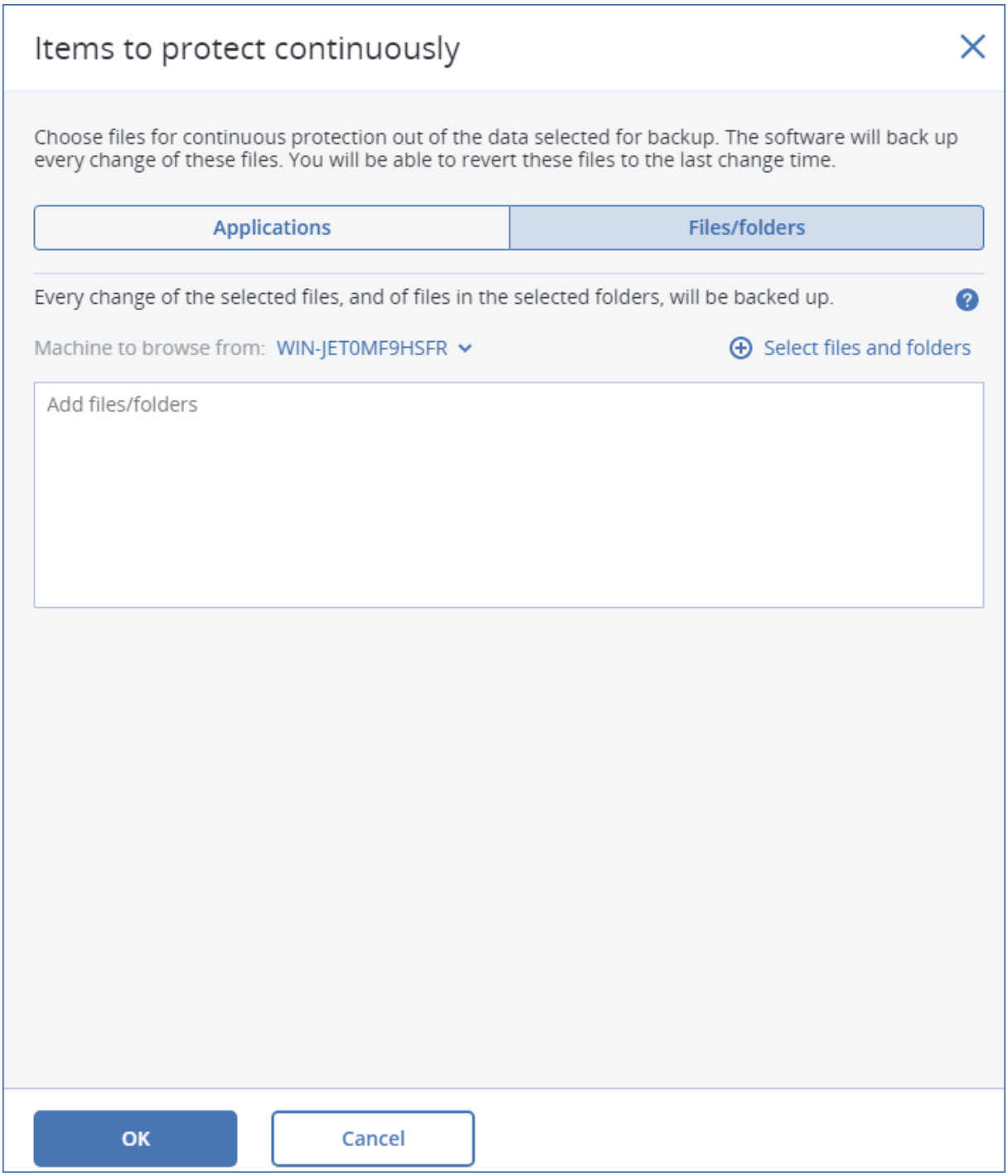
- 可以从预定义的类别中选择应用程序，也可以通过定义应用程序可执行文件的路径来指定其他应用程序。使用以下其中一种格式：

  `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`

  OR

  `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`

  - **文件/文件夹**（将备份指定位置中修改的任何文件）。建议您使用此选项来保护那些不断更改的文件和文件夹。



1. **要浏览的计算机** - 指定含有要选择用于连续数据保护的文件/文件夹的计算机。
   单击**选择文件和文件夹**，以选择指定计算机上的文件/文件夹。

   重要事项
   如果手动指定含有要连续备份的文件的文件夹，请使用掩码，例如：
   正确路径：D:\Data*
   不正确路径：D:\Data\

在文本字段中，还可以指定用于选择要备份的文件/文件夹的规则。有关如何定义规则的更多详细信息，请参阅“选择文件/文件夹”。准备就绪后，单击**完成**。

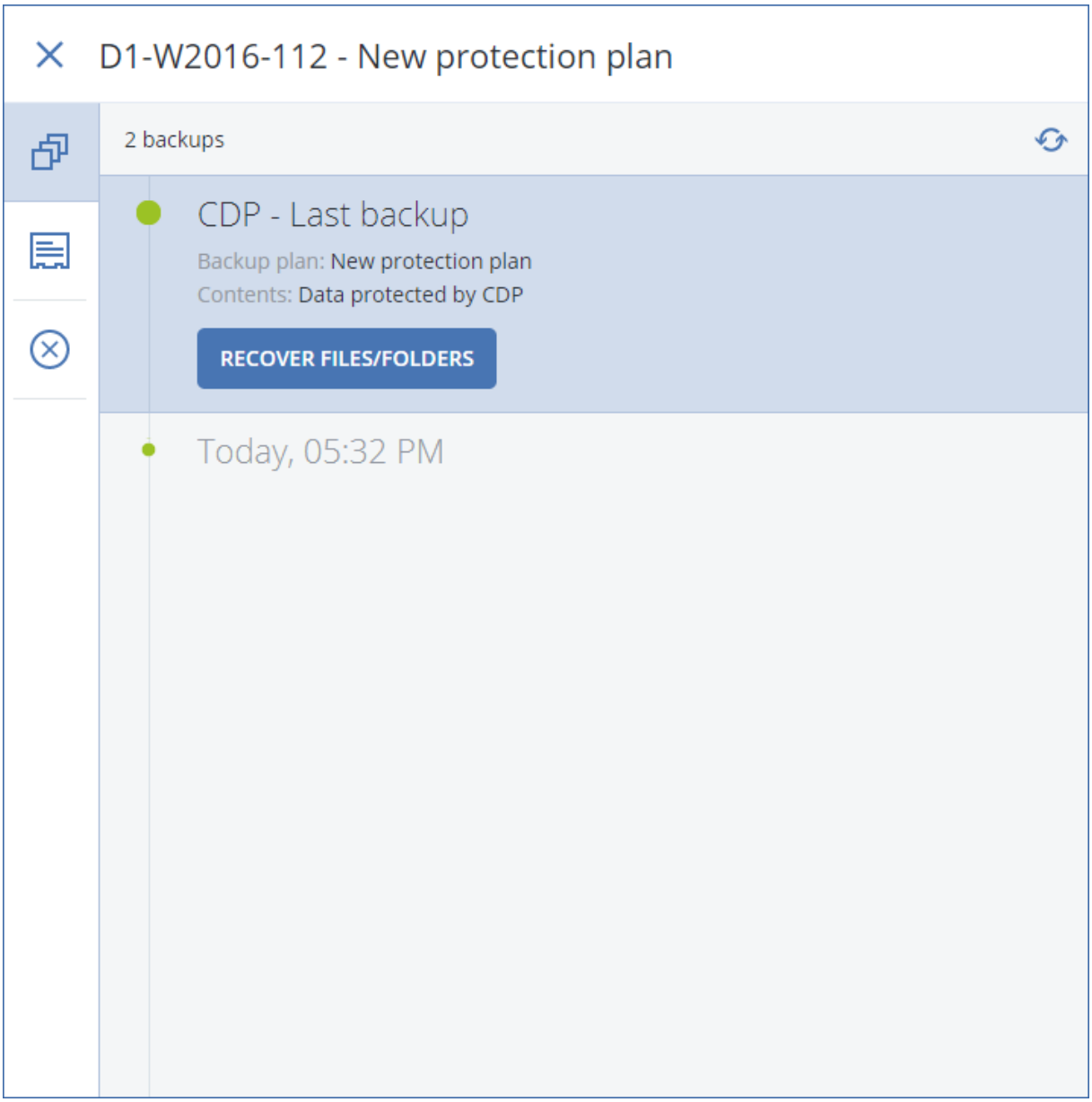
2. 单击**创建**。

结果是，已启用连续数据保护的保护计划将指派给选定的计算机。首次常规备份后，将连续创建带有 CDP 数据保护的最新副本的备份。将同时备份通过应用程序和文件/文件夹定义的数据。

根据为备份模块定义的保留策略，将保留连续备份的数据。

如何区分连续保护的备份

连续备份的备份具有 CDP 前缀。



如何将整个计算机恢复到最新状态

如果希望能够将整个计算机恢复到最新状态，可以在保护计划的备份模块中使用**连续数据保护 (CDP)** 选项。

可以从 CDP 备份中恢复整个计算机或文件/文件夹。在第一种情况下，将使整个计算机处于最新状态；在第二种情况下，将使文件/文件夹处于最新状态。

选择目标

重要事项
本部分中所述的一些功能仅适用于本地部署。

选择备份位置

1. 单击**备份位置**。
2. 请执行以下任一操作：
   - 选择一个之前使用过或预定义的备份位置
   - 单击**添加位置**，然后指定一个新的备份位置。

支持的位置

- **云存储**
  备份将存储在云数据中心中。
- **本地文件夹**
  如果选择了单台计算机，请浏览到选定计算机上的文件夹或键入文件夹路径。
  如果选择了多台计算机，请键入文件夹路径。备份将存储在每台选定物理机上或安装了适用于该虚拟机的代理程序的计算机上的此文件夹中。如果该文件夹不存在，将创建该文件夹。
- **网络文件夹**
  这是通过 SMB/CIFS/DFS 共享的文件夹。
  浏览到所需的共享文件夹，或者输入以下格式的路径：
  - 对于 SMB/CIFS 共享：`\\<主机名>\<路径>\` 或 `smb://<主机名>/<路径>/`
  - 对于 DFS 共享：`\\<完整 DNS 域名>\\<路径>`
    例如，`\\example.company.com\shared\files`

  然后，单击箭头按钮。如果出现提示，请指定共享文件夹的用户名和密码。通过单击文件夹名称旁边的钥匙图标，即可随时更改这些凭据。
  不支持使用匿名访问备份到文件夹。
- **Acronis Cyber Infrastructure**
  Acronis Cyber Infrastructure 可用作高度可靠的软件定义的存储，具有数据冗余和自动自我修复功能。可以将该存储配置为用于将备份存储在 Microsoft Azure 中或者与 S3 或 Swift 兼容的众多存储解决方案之一的网关。存储还可以采用 NFS 后端。有关详细信息，请参阅“关于 Acronis Cyber Infrastructure”。

重要事项
备份到 Acronis Cyber Infrastructure 不适用于 macOS 计算机。

- **NFS 文件夹**(适用于运行 Linux 或 macOS 的计算机)
  验证 nfs-utils 程序包是否已安装在装有适用于 Linux 的代理程序的 Linux 计算机上。
  浏览到所需的 NFS 文件夹, 或者输入以下格式的路径:
  `nfs://<主机名>/<导出的文件夹>:/<子文件夹>`
  然后, 单击箭头按钮。
  无法备份至受密码保护的 NFS 文件夹。
- **安全区**(如果它在每台选定的计算机上存在, 则可用)
  安全区 是备份计算机的磁盘上的安全分区。此分区必须在配置备份前手动创建。有关如何创建安全区 的信息以及其优点和限制信息, 请参阅"关于 安全区"。
- **SFTP**
  键入 SFTP 服务器名称或地址。支持以下表示法:
  `sftp://<服务器>`
  `sftp://<服务器>/<文件夹>`
  输入用户名和密码后, 可以浏览服务器文件夹。
  在任一表示法中, 还可以指定端口、用户名和密码:
  `sftp://<服务器>:<端口>/<文件夹>`
  `sftp://<用户名>@<服务器>:<端口>/<文件夹>`
  `sftp://<用户名>:<密码>@<服务器>:<端口>/<文件夹>`
  如果未指定端口号, 则使用端口 22。
  为其配置不带密码的 SFTP 访问的用户无法备份到 SFTP。
  不支持备份到 FTP 服务器。

高级存储选项

- **由脚本定义**(适用于运行 Windows 的计算机)
  可将每台计算机的备份存储在由脚本定义的文件夹中。该软件支持使用 JScript、VBScript 或 Python 3.5 编写的脚本。在部署保护计划时, 软件将在每台计算机上运行脚本。每台计算机的脚本输出都应是本地或网络文件夹路径。如果文件夹不存在, 系统将创建该文件夹(限制:使用 Python 编写的脚本无法在网络共享上创建文件夹) 。在**备份存储**选项卡上, 每个文件夹都显示为一个单独的备份位置。
  在**脚本类型**中, 选择脚本类型(**JScript**、**VBScript** 或 **Python**) , 然后导入或复制并粘贴该脚本。对于网络文件夹, 请指定具有读/写权限的访问凭据。
  示例:
  - 以下 **JScript** 脚本以 \\bkpsrv\<虚拟机> 格式输出计算机的备份位置:

```
WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject
("WScript.Network").ComputerName);
```

- 以下 **JScript** 脚本会在运行该脚本的计算机上的文件夹中输出备份位置：

  ```
  WScript.Echo("C:\\Backup");
  ```

  注意
  这些脚本中的位置路径区分大小写。因此，C:\Backup 和 C:\backup 会在 安克诺斯数据保护软件 Web 中控台中显示为不同的位置。此外，驱动器号也使用大写。

- 以下 **VBScript** 脚本以 \\bkpsrv\<虚拟机> 格式输出计算机的备份位置：

  ```
  WScript.Echo("\\bkpsrv\" + WScript.CreateObject("WScript.Network").ComputerName)
  ```

  因此，每台计算机的备份都将保存在服务器 **bkpsrv** 上的同名文件夹中。

- **存储节点**
  存储节点是一个服务器，旨在优化企业数据保护所需的各种资源（如公司的存储容量、网络带宽和生产服务器的 CPU 负载）的使用。此目标通过组织和管理作为企业备份（受控位置）的专用存储器的那些存储位置而实现。
  可以选择一个之前创建的位置，或通过单击**添加位置** > **存储节点**创建一个新位置。有关设置的信息，请参阅“添加受控位置”。
  系统可能会提示您为存储节点指定用户名和密码。安装存储节点的计算机上的以下 Windows 组的成员有权访问存储节点上的所有受控位置：
  - **管理员**
  - **Acronis ASN 远程用户**
    此组将在安装存储节点后自动创建。默认情况下，此组为空。可手动将用户添加到此组。
- **磁带**
  如果磁带设备连接至备份计算机或存储节点，则位置列表会显示默认磁带集区。此集区是自动创建的。
  可以选择默认集区，或通过单击**添加位置** > **磁带**创建一个新集区。有关集区设置的信息，请参阅“创建集区”。

关于 安全区

安全区 是备份计算机的磁盘上的安全分区。它可以存储此计算机的磁盘或文件的备份。

如果磁盘遇到物理故障，位于 安全区 中的备份可能会丢失。因此，安全区 不应是存储备份的唯一位置。在企业环境中，当普通位置暂时不可用或通过缓慢或繁忙的通道连接时，安全区 可视为用于备份的中间位置。

为什么使用 安全区？

安全区：

- 可将磁盘恢复至磁盘备份所在的同一磁盘。
- 提供具有成本效益且易用的方法，可保护数据免受软件故障、病毒侵袭、人工错误的影响。

- 无需使用独立的媒体或网络连接来备份或恢复数据。这对漫游用户尤为有用。
- 当使用备份的复制时，可充当主要目标位置。

限制

- 安全区 无法在 Mac 上进行组织。
- 安全区 是基本磁盘上的分区。它无法在动态磁盘上进行组织或创建为逻辑卷(由 LVM 管理)。
- 安全区 是使用 FAT32 文件系统格式化的。由于 FAT32 的文件大小限制为 4 GB，因此较大备份在保存到 安全区 时将进行拆分。这不会影响恢复过程和速度。

如何通过创建 安全区 转换磁盘

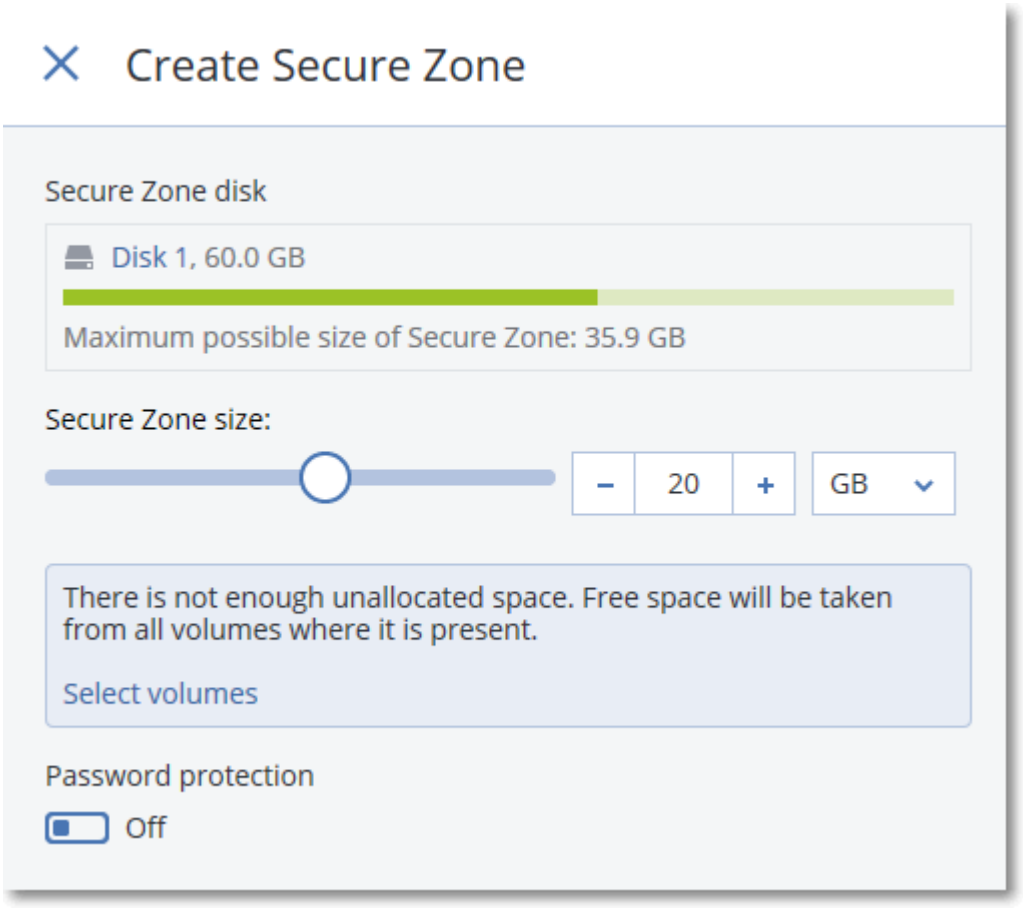
- 安全区 始终在硬盘的末尾区域进行创建。
- 如果在磁盘末尾没有未分配的空间或未分配空间不足，但是在卷之间有未分配的空间，则将会移动卷以便在磁盘的末尾区域增加更多的未分配空间。
- 当收集了所有的未分配空间，但空间仍然不足时，软件将使用您选择的卷上的可用空间，成比例降低卷的大小。
- 但是，在卷上应该有可用空间，这样操作系统和应用程序才能运行；例如创建临时文件。如果可用空间等于或低于卷总大小的 25%，软件将不会减少卷的大小。仅在磁盘上所有卷的可用空间都为 25% 或更低时，软件才会继续成比例减少卷大小。

上述情况表明，指定可能最大的 安全区 大小并不明智。最后所有卷上都没有可用空间，这将导致操作系统或应用程序工作不稳定，甚至无法启动。

重要事项
移动或调整系统启动所使用卷的大小将要求重新启动。

如何创建 安全区

1. 选择要创建 安全区 的计算机。
2. 依次单击**详细信息** > **创建 安全区**。
3. 在 **安全区 磁盘**下，单击**选择**，然后选择要创建安全区的硬盘(若有几个硬盘)。
   该软件会计算 安全区 的可能最大大小。
4. 输入 安全区 大小，或拖动滑块选择最小值和最大值之间的任何大小。
   最小大小约为 50 MB，视硬盘的几何参数而定。最大大小等于磁盘的未分配空间，加上磁盘的所有卷的总可用空间。
5. 如果所有未分配空间不足以容纳指定的大小，软件将从现有卷中获取可用空间。默认情况下，选择所有卷。如果要排除某些卷，请单击**选择卷**。否则，请跳过此步骤。



6. [可选] 启用**密码保护**开关并指定密码。
   需要密码才能访问位于 安全区 中的备份。备份到 安全区 不需要密码，除非备份是在可启动媒体下执行的。
7. 单击**创建**。
   软件将显示预期的分区布局。单击**确定**。
8. 等待软件创建 安全区。

现在，在创建保护计划时，即可在**备份位置**中选择 安全区。

如何删除 安全区

1. 选择附带 安全区 的计算机。
2. 单击**详细信息**。
3. 单击 **安全区** 旁边的齿轮图标，然后单击**删除**。
4. [可选] 指定将添加从区域释放的空间的卷。默认情况下，选择所有卷。
   将为选定卷平均分配空间。如果您未选择任何卷，释放的空间将成为未分配空间。
   调整系统启动使用的卷的大小将会要求重新启动。
5. 单击**删除**。

因此，将删除 安全区 以及其中存储的所有备份。

关于 Acronis Cyber Infrastructure

Acronis 安克诺斯数据保护软件 15 支持与 Acronis Cyber Infrastructure 3.5 更新 5 或更高版本集成。

备份到 Acronis Cyber Infrastructure 不适用于 macOS 计算机。

部署

为了使用 Acronis Cyber Infrastructure，请事先将它部署在裸机上。建议至少部署五台物理服务器，以便充分利用该产品。如果您只需要网关功能，可以使用一台物理或虚拟服务器，或者使用所需数量的服务器配置一个网关群集。

确保同步管理服务器和 Acronis Cyber Infrastructure 之间的时间设置。在部署过程中，可以配置 Acronis Cyber Infrastructure 的时间设置。默认启用通过网络时间协议 (NTP) 进行时间同步。

可以部署多个 Acronis Cyber Infrastructure 实例，并将它们注册在同一台管理服务器上。

注册

在 Acronis Cyber Infrastructure Web 界面中进行注册。Acronis Cyber Infrastructure 只可以在组织中由组织管理员进行注册。注册完成后，该存储即可供所有组织单位使用。可以将它作为备份位置添加到任何单位或组织。

在 Acronis 安克诺斯数据保护软件 界面中进行反向操作(注销)。依次单击**设置** > **存储节点**、单击所需的 Acronis Cyber Infrastructure，然后单击**删除**。

添加备份位置

每个 Acronis Cyber Infrastructure 实例上仅一个备份位置可以添加到单位或组织。以单位级别添加的位置可供该单位以及组织管理员使用。以组织级别添加的位置仅可供组织管理员使用。

在添加位置时，创建并输入其名称。如果您需要将现有位置添加到新的或不同的管理服务器，请选中**使用现有位置...**复选框，单击**浏览**，然后从列表中选择位置。

如果在管理服务器上注册了多个 Acronis Cyber Infrastructure 实例，则在添加位置时可以选择一个 Cyber Infrastructure 实例。

备份方案、操作和限制

无法从可启动媒体直接访问 Acronis Cyber Infrastructure。要使用 Acronis Cyber Infrastructure，请在管理服务器上注册媒体，然后通过 安克诺斯数据保护软件 Web 中控台管理它。

无法通过命令行接口访问 Acronis Cyber Infrastructure。

在可用备份方案和备份操作方面，Acronis Cyber Infrastructure 类似于云存储。唯一的不同是，可以在执行保护计划期间从 Acronis Cyber Infrastructure 中复制备份。

文档

可在 Acronis 网站上获得一整套 Acronis Cyber Infrastructure 文档。

预定

重要事项
本部分中所述的一些功能仅适用于本地部署。

时间表采用安装有代理程序的操作系统的时间设置(包括时区)。适用于 VMware 的代理程序(虚拟设备)的时区可以在代理程序的界面中进行配置。

例如,如果保护计划预定在 21:00 运行并应用于位于不同时区的多台计算机,则备份将于当地时间 21:00 在每台计算机上开始。

预定参数取决于备份目标。

当备份到云存储时

默认情况下,从周一到周五每天执行备份。您可以选择要运行备份的时间。

如果您要更改备份频率,请移动滑块,然后指定备份预定。

您可以预定按事件而不按时间进行备份。为此,请在时间表选择器中选择事件类型。有关详细信息,请参阅"按事件预定"。

重要事项
第一个备份是完整备份,这意味着它最耗时。所有后续备份都是增量备份,并且需要明显更少的时间。

当备份到其他位置时

您可以选择预定义的备份方案之一或创建自定义方案。备份方案是保护计划的一部分,包括备份预定和备份方法。

在**备份方案**中,选择以下内容之一:

- **始终增量(单个文件)**
  默认情况下,从周一到周五每天执行备份。您可以选择要运行备份的时间。
  如果您要更改备份频率,请移动滑块,然后指定备份预定。
  备份使用新的单文件备份格式[1]。
  当备份到磁带设备或 SFTP 服务器时,此方案不可用。

[1]一种新的备份格式,初始完整和后续增量备份使用此格式(而不是文件链)保存到单个 .tib 文件。此格式利用了增量备份方法的速度,同时避免了其主要劣势,即难以删除过期备份。软件将过期备份使用的块标记为"可用",并将新备份写入这些块。这导致清理速度极快,资源消耗最少。当备份到不支持随机存取读写的位置(例如,SFTP 服务器)时,单文件备份格式不可用。

- **始终完整**

  默认情况下，从周一到周五每天执行备份。您可以选择要运行备份的时间。

  如果您要更改备份频率，请移动滑块，然后指定备份预定。

  所有备份均为完整备份。
- **每周完整，每日增量**

  默认情况下，从周一到周五每天执行备份。您可以修改运行备份的一周中各天和时间。

  一周创建一次完整备份。所有其他备份均为增量备份。创建完整备份的天取决于**每周备份**选项（单击齿轮图标，然后依次单击**备份选项** > **每周备份**）。
- **每月完整、每周差异和每日增量备份 (GFS)**

  默认情况下，从周一到周五每天执行增量备份；每周六执行差异备份；每个月的第一天执行完整备份。您可以修改这些时间表和要运行备份的时间。

  此备份方案在保护计划面板上显示为**自定义**方案。
- **自定义**

  指定完整、差异和增量备份的预定。

  在备份 SQL 数据、Exchange 数据或系统状态时，差异备份不可用。

对于任何备份方案，您都可以预定按事件而不按时间进行备份。为此，请在时间表选择器中选择事件类型。有关详细信息，请参阅“按事件预定”。

其他预定选项

对于任何目标，您可以执行以下操作：

- 指定备份开始条件，确保只有在满足条件时才执行预定的备份。有关详细信息，请参阅“开始条件”。
- 为预定何时有效设定日期范围。选中**在日期范围内运行计划**复选框，然后指定日期范围。
- 禁用预定。当禁用预定时，将不应用保留规则，除非手动启动某个备份。
- 根据预定时间引入延迟。将随机选择每台计算机的延迟值，范围为从零到您指定的最大值。将多台计算机备份至网络位置时您可能要使用此设置，以免网络负荷过重。

  单击齿轮图标，然后依次单击**备份选项** > **预定**。选中**在时间窗口内分配备份开始时间**，然后指定最大延迟。将保护计划应用于计算机时会确定每台计算机的延迟值，并一直保留到编辑保护计划和更改最长延迟值为止。

  注意

  在云部署中，此选项默认启用，其中最大延迟设置为 30 分钟。在本地部署中，所有备份默认情况下直接按预定开始。

- 单击**显示更多**以访问以下选项：
  - **如果计算机已关闭，则在计算机启动时运行遗漏的任务**（默认禁用）
  - **在备份期间防止进入睡眠或休眠模式**（默认启用）

    此选项仅对运行 Windows 的计算机有效。
  - **从睡眠或休眠模式唤醒以启动预定备份**（默认禁用）

此选项仅对运行 Windows 的计算机有效。此选项在计算机关闭电源的情况下无效，即该选项未采用网络唤醒功能。

按事件预定

为保护计划设置时间表时，可以在时间表选择器中选择事件类型。一旦事件发生就会启动备份。

可选择以下其中一个事件：

- **自上次备份后的时间**
  这是距上次在同一个保护计划内成功完成备份的时间。您可以指定时间长度。

  注意
  由于预定基于成功的备份事件，因此，如果备份失败，则预定程序将不会再次运行作业，直到操作员手动运行相应计划并且该运行成功完成为止。

- **用户登录系统时**
  默认情况下，任何用户登录都会启动备份。您可以将任何用户更改为特定用户帐户。
- **用户注销系统时**
  默认情况下，任何用户注销都会启动备份。您可以将任何用户更改为特定用户帐户。

  注意
  系统关闭时备份将不会运行，因为关闭与注销不同。

- **系统启动时**
- **系统关闭时**
- **发生 Windows 事件日志事件时**
  您必须指定事件属性。

下表列出了 Windows、Linux 和 macOS 操作系统中各种数据的可用事件。

备份内容	自上次备份后的时间	用户登录系统时	用户注销系统时	系统启动时	系统关闭时	发生 Windows 事件日志事件时
磁盘/卷或文件(物理机)	Windows、Linux 和 macOS	Windows	Windows	Windows、Linux 和 macOS	Windows	Windows
磁盘/卷(虚拟机)	Windows 和 Linux	–	–	–	–	–
ESXi 配置	Windows 和 Linux	–	–	–	–	–
Microsoft	Windows	–	–	–	–	Windows

365 邮箱						
Exchange 数据库和邮箱	Windows	–	–	–	–	Windows
SQL 数据库	Windows	–	–	–	–	Windows

发生 Windows 事件日志事件时

您可以将备份预定为在其中一个事件日志(如**应用程序**、**安全**或**系统**日志)中记录了特定 Windows 事件时开始。

例如,您可能想设置这样一个保护计划:一旦 Windows 发现硬盘驱动器将要出现故障,就自动对数据进行紧急完整备份。

若要浏览事件和查看事件属性,请使用**计算机管理**中控台中的**事件查看器**管理单元。您必须是**管理员**组的成员才能打开**安全**日志。

事件属性

日志名称

指定日志的名称。从列表中选择标准日志名称(**应用程序**、**安全性**或**系统**),或者键入日志名称 - 例如:**Microsoft Office 会话**

事件源

指定事件源,通常用于指出导致事件发生的程序或系统组件 - 例如:**磁盘**。

包含指定字符串的任何事件源都将触发预定的备份。此选项不区分大小写。因此,如果指定字符串 **service**,则**服务控制管理器**和**时间服务**事件源都会触发备份。

事件类型

指定事件类型:**错误**、**警告**、**信息**、**审核成功**或**审核失败**。

事件 ID

指定事件编号,通常用于标识同一源的事件中特定类型的事件。

例如,当 Windows 发现磁盘上存在坏块时,会发生**错误**事件(其中事件源为**磁盘**,事件 ID 为 **7**);当磁盘尚不能访问时,会发生**错误**事件(其中事件源为**磁盘**,事件 ID 为 **15**)。

示例:'坏区块'紧急备份

硬盘上突然出现一个或多个坏区通常表示硬盘驱动很快会出现故障。假定您想要创建一个一旦发生此情况就会立即备份硬盘数据的保护计划。

在 Windows 发现硬盘上存在坏区时,它会将事件源为**磁盘**、事件编号为 **7** 的事件记录到**系统**日志中;事件类型为**错误**。

在创建此计划时，在**时间表**部分进行以下选择或输入：

- **日志名称**：**系统**
- **事件源**：**磁盘**
- **事件类型**：**错误**
- **事件 ID**：**7**

重要事项
要确保在即使存在坏块的情况下完成备份，必须将备份设置为忽略坏块。为此，在**备份选项**中，转至**错误处理**，然后勾选**忽略坏扇区**复选框。

开始条件

这些设置可增加预定程序的灵活性，使其可按照特定条件来执行备份。在存在多个条件的情况下，必须同时满足所有条件才允许启动备份。手动启动备份时，启动条件无效。

要访问这些设置，请在为保护计划设置时间表时，单击**显示更多**。

该条件(或多个条件中的一个)不满足时，预定程序的行为由备份开始条件备份选项定义。为了处理长时间不能满足条件，而进一步延迟备份会产生风险的情况，您可以设置时间间隔，在此时间间隔后无论条件是否满足，备份都将运行。

下表列出了 Windows、Linux 和 macOS 操作系统中各种数据的可用开始条件。

备份内容	磁盘/卷或文件(物理机)	磁盘/卷(虚拟机)	ESXi 配置	Microsoft 365 邮箱	Exchange 数据库和邮箱	SQL 数据库
用户空闲	Windows	–	–	–	–	–
备份位置所在的主机可用	Windows、Linux 和 macOS	Windows 和 Linux	Windows 和 Linux	Windows	Windows	Windows
用户已注销	Windows	–	–	–	–	–
符合时间间隔	Windows、Linux 和 macOS	Windows 和 Linux	–	–	–	–
节省电池	Windows	–	–	–	–	–

电量						
不在使用按流量计费的连接时启动	Windows	–	–	–	–	–
不在连接到以下 Wi-Fi 网络时启动	Windows	–	–	–	–	–
检查设备 IP 地址	Windows	–	–	–	–	–

用户空闲时

“用户空闲”表示计算机正在运行屏幕保护程序或该计算机已锁定。

示例

每天 21:00 在计算机上运行备份，最好在用户空闲时运行。如果到 23:00 用户仍处于活动状态，则直接运行备份。

- 预定：每天一次，每天运行。开始时间：**21:00**。
- 条件：**用户空闲**。
- 备份开始条件：**等待直至满足所有条件，但务必在 2** 小时后开始备份。

结果，

(1) 如果用户在 21:00 前进入空闲状态，则备份会在 21:00 开始。

(2) 如果用户在 21:00 到 23:00 之间进入空闲状态，则备份会在用户进入空闲状态后立即开始。

(3) 如果用户在 23:00 仍处于活动状态，则备份会在 23:00 开始。

备份位置所在的主机可用

“备份位置所在的主机可用”表示网络上指定用于存储备份的目标位置所在的计算机可用。

此条件对于网络文件夹、云存储和由存储节点管理的位置有效。

此条件不包括位置本身的可用性 - 仅限主机的可用性。例如，如果主机可用，但是此主机上的网络文件夹没有共享或者文件夹的凭据不再有效，则仍视为满足此条件。

示例

数据于每个工作日 21:00 备份到网络文件夹。如果文件夹所在的计算机当前不可用(例如，由于维护工作)，则您希望跳过备份并等待下一个工作日的预定启动。

- 预定：每天一次，周一到周五。开始时间：**21:00**。
- 条件：**备份位置所在的主机可用**。
- 备份开始条件：**跳过预定备份**。

结果：

(1) 如果到 21:00 时主机可用，则会立即开始备份。

(2) 如果到 21:00 时主机不可用，则在下一个工作日的主机可用时开始备份。

(3) 如果在工作日 21:00 时主机一直不可用，则永远不会开始备份。

用户已注销

可让您将备份执行延迟到所有用户都从 Windows 注销。

示例

在每个周五的 20:00 运行备份，最好在所有用户都注销后进行。如果其中一个用户在 23:00 仍处于登录状态，则将直接运行备份。

- 预定：每周一次，在周五进行。开始时间：**20:00**。
- 条件：**用户已注销**。
- 备份开始条件：**等待直至满足所有条件，但务必在 3** 小时后开始备份。

结果：

(1) 如果 20:00 所有用户都已注销，则备份将在 20:00 开始。

(2) 如果最后一位用户在 20:00 到 23:00 之间注销，则会在用户注销后立即开始备份。

(3) 如果任何用户在 23:00 仍处于登录状态，则备份会在 23:00 开始。

配合时间间隔时

将备份开始时间限制为指定时间间隔。

示例

一家公司使用同一网络附加存储上的不同位置来备份用户数据和服务器。工作日工作时间为 08:00 至 17:00。应在用户注销后立即备份用户数据，但备份时间不应早于 16:30。每天 23:00 对公司的服务器进行备份。所以，最好应在此时间前完成所有用户数据的备份以便释放网络带宽资源。假定备份用户数据所需时间不超过一小时，则最晚备份开始时间为 22:00。如果在指定时间间隔内用户仍处于登录状态或在其他时间注销，则不要备份用户数据，即跳过备份执行。

- 事件:**用户注销系统时**。指定用户帐户:**任何用户**。
- 条件:**符合时间间隔 16:30** 到 **22:00**。
- 备份开始条件:**跳过预定备份**。

结果:

(1) 如果用户在 16:30 和 22:00 之间注销,则会在用户注销后立即开始备份。

(2) 如果用户在其他时间注销,则会跳过备份。

节省电池电量

如果设备(笔记本电脑或平板电脑)未连接到电源,备份将受到阻止。视备份开始条件备份选项的值而定,跳过的备份也许会在设备连接到电源后开始。可使用以下选项:

- **不在使用电池时启动**
  仅在设备连接到电源时才开始备份。
- **如果电池电量高于以下值,则在使用电池时启动**
  如果设备连接到电源或者电池电量高于指定值,将开始备份。

示例

数据于每个工作日 21:00 进行备份。如果设备未连接到电源(例如,用户正参与时间较长会议),您希望跳过备份以节省电池电量,并等待直到用户将设备连接到电源。

- 预定:每天一次,周一到周五。开始时间:21:00。
- 条件:**节省电池电量**,**不在使用电池时启动**。
- 备份开始条件:**等待直至满足相关条件**。

结果:

(1) 如果到 21:00 时设备连接到电源,将立即开始备份。

(2) 如果到 21:00 时设备采用电池电源运行,将在设备连接到电源时开始备份。

不在使用按流量计费的连接时启动

如果在 Windows 中设备通过使用设置为按流量计费的连接接入 Internet,则备份会受到阻止(包括备份到本地磁盘)。有关 Windows 中按流量计费连接的详细信息,请参阅 https://support.microsoft.com/zh-cn/help/17452/windows-metered-internet-connections-faq。

作为阻止通过移动热点进行备份的额外措施,在启用**不在使用按流量计费的连接时启动**条件时,会自动启用**不在连接到以下 Wi-Fi 网络时启动**条件。默认指定以下网络名称:“android”、“phone”、“mobile”和“modem”。单击 X 符号即可从列表中删除这些名称。

示例

数据于每个工作日 21:00 进行备份。如果设备通过使用按流量计费连接接入 Internet(例如,用户正在出差),您希望跳过备份以节省网络流量并等待在下一个工作日预定开始备份。

- 预定：每天一次，周一到周五。开始时间：21:00。
- 条件：**不在使用按流量计费的连接时启动**。
- 备份开始条件：**跳过预定备份**。

结果：

(1) 如果到 21:00 时设备未使用按流量计费连接接入 Internet，将立即开始备份。

(2) 如果到 21:00 时设备使用按流量计费连接接入 Internet，将在下一个工作日开始备份。

(3) 如果在工作日 21:00 时设备始终使用按流量计费连接接入 Internet，将永远不会开始备份。

不在连接到以下 Wi-Fi 网络时启动

如果设备连接到任何指定的无线网络，备份会受到阻止（包括备份到本地磁盘）。您可以指定 Wi-Fi 网络名称，又称为服务集标识符 (SSID)。

限制将应用于其名称中包含子字符串形式的指定名称（不区分大小写）的所有网络。例如，如果指定“phone”作为网络名称，当设备连接到以下任何网络时，将不会开始备份：“John's iPhone”、“phone_wifi”或“my_PHONE_wifi”。

当设备使用手机热点接入 Internet 时，此条件对阻止备份非常有用。

作为阻止通过移动热点进行备份的额外措施，在启用**不在使用按流量计费的连接时启动**条件时，会自动启用**不在连接到以下 Wi-Fi 网络时启动**条件。默认指定以下网络名称：“android”、“phone”、“mobile”和“modem”。单击 X 符号即可从列表中删除这些名称。

示例

数据于每个工作日 21:00 进行备份。如果设备通过使用移动热点接入 Internet（例如，笔记本电脑在网络共享模式下实现连接），您希望跳过备份并等待在下一个工作日预定开始备份。

- 预定：每天一次，周一到周五。开始时间：21:00。
- 条件：**不在连接到以下网络时启动**，**网络名称**：<热点网络的 SSID>。
- 备份开始条件：**跳过预定备份**。

结果：

(1) 如果到 21:00 时计算机未连接到指定网络，将立即开始备份。

(2) 如果到 21:00 时计算机连接到指定网络，将在下一个工作日开始备份。

(3) 如果在工作日 21:00 时计算机始终连接到指定网络，将永远不会开始备份。

检查设备 IP 地址

如果任何设备 IP 地址在指定的 IP 地址范围之内或之外，则阻止备份（包括备份到本地磁盘）。可使用以下选项：

- **在 IP 范围以外时启动**
- **在 IP 范围以内时启动**

使用任一选项，可指定多个范围。仅支持 IPv4 地址。

此条件对身处海外的用户非常有用，可避免产生大数据传输费用。此外，可帮助阻止通过虚拟专用网络 (VPN) 连接进行备份。

示例

数据于每个工作日 21:00 进行备份。如果设备通过使用 VPN 隧道连接到公司网络（例如，用户在家工作），您希望跳过备份，并等待直至用户将设备带到办公室。

- 预定：每天一次，周一到周五。开始时间：21:00。
- 条件：**检查设备 IP 地址**，**在 IP 范围以外时启动**，**从**：<VPN IP 地址范围的起始地址>，**至**：<VPN IP 地址范围的结束地址>。
- 备份开始条件：**等待直至满足相关条件**。

结果：

(1) 如果到 21:00 时计算机 IP 地址不在指定范围中，将立即开始备份。

(2) 如果到 21:00 时计算机 IP 地址在指定范围中，将在该设备获取非 VPN IP 地址时立即开始备份。

(3) 如果在工作日 21:00 时计算机 IP 地址始终在指定范围中，将永远不会开始备份。

保留规则

重要事项
本部分中所述的一些功能仅适用于本地部署。

1. 单击**保留时间**。
2. 在**清理**中，选择以下选项之一：
   - **按备份存留时间**（默认）
     指定由保护计划创建的备份的保留时间。默认情况下，为每个备份集[1]单独指定保留规则。如果要为所有备份使用单个规则，请单击**为所有备份集切换至单个规则**。
   - **按备份数量**
     指定要保留的最大备份数。
   - **按备份的总大小**
     指定要保留的备份的最大总大小。
     此设置在采用**始终增量（单个文件）**备份方案时不可用，或者在备份到 SFTP 服务器或磁带设备时不可用。
   - **无限期地保留备份**
3. 选择开始清理的时间：

[1]一组可以应用个别保留规则的备份。对于自定义备份方案，备份集对应于备份方法（完整、差异和增量）。在所有其他情况下，备份集为“每月”、“每日”、“每周”和“每小时”。每月备份是一个月开始后创建的第一个备份。每周备份是在每周备份选项（单击齿轮图标，然后依次单击“备份选项”>“每周备份”）中所选日创建的第一个备份。如果每周备份是一个月开始后创建的第一个备份，则该备份视为每月备份。在此情况下，将在下周的所选日创建每周备份。除非每日备份符合每月备份或每周备份的定义，否则每日备份是某日开始后创建的第一个备份。除非每小时备份符合每月备份、每周备份或每日备份的定义，否则每小时备份是某个小时开始后创建的第一个备份。

- **备份后(默认)**
  创建新备份之后,将应用保留规则。
- **备份前**
  创建新备份之前,将应用保留规则。
  此设置在备份 Microsoft SQL Server 群集或 Microsoft Exchange Server 群集时不可用。

您需要了解的其他信息

- 在所有情况下都会保留保护计划创建的上一备份,除非配置保留规则以在开始新的备份操作之前清除备份并将要保留的备份数量设置为零。

  警告!
  如果通过这种方式应用保留规则来删除您拥有的唯一备份,那么在备份失败时,您将没有用于恢复数据的备份,原因是将没有可供使用的备份。

- 在覆盖磁带之前,不会删除存储在磁带上的备份。
- 如果每个备份都根据备份方案和备份格式存储为单独的文件,则在其所有从属(增量和差异)备份的存留时间到期之前,不能删除此文件。这需要额外空间用于存储推迟删除的备份。此外,备份存留时间、备份数或备份大小可能超出您指定的值。
  可以使用"备份合并"备份选项更改此行为。
- 保留规则是保护份计划的一部分。只要保护计划从计算机中吊销或删除,或者计算机本身从管理服务器中删除,它们就会停止作用于计算机的备份。如果您不再需要该计划创建的备份,请按照"删除备份"中所述的方法删除它们。

加密

我们建议您加密存储在云存储中的所有备份,尤其是在您的公司需要遵守法规时。

重要事项
如果您丢失或忘记密码,则无法恢复加密备份。

保护计划中的加密

要启用加密,请在创建保护计划时指定加密设置。在应用保护计划后,无法修改加密设置。要使用不同的加密设置,请创建新的保护计划。

指定保护计划中的加密设置

1. 在保护计划面板上,启用**加密**开关。
2. 指定并确认加密密码。
3. 选择以下加密算法之一:
   - **AES 128** - 备份将使用带 128 位密钥的高级加密标准 (AES) 算法进行加密。
   - **AES 192** - 备份将使用带 192 位密钥的 AES 算法进行加密。

- **AES 256** - 备份将使用带 256 位密钥的 AES 算法进行加密。

4. 单击**确定**。

作为计算机属性的加密

此选项面向处理多台计算机的备份的管理员。如果每台计算机都需要一个唯一的加密密码，或者无论保护计划的加密设置如何都需要对备份强制加密，请分别在每台计算机上保存加密设置。备份将使用带 256 位密钥的 AES 算法进行加密。

在计算机上保存加密设置会通过以下方式影响保护计划：

- **已应用于计算机的保护计划。**如果保护计划中的加密设置不同，备份将失败。
- **以后将应用于计算机的保护计划。**保存在计算机上的加密设置将覆盖保护计划中的加密设置。所有备份都将加密，即使在保护计划设置中禁用加密也是如此。

此选项可在运行适用于 VMware 的代理程序的计算机上使用。但是，如果您有多个连接到同一个 vCenter 服务器的适用于 VMware 的代理程序，请谨慎。必须为所有代理程序使用相同的加密设置，因为它们之间存在一种负载平衡。

保存加密设置之后，可以按照以下说明进行更改或重置。

重要事项
如果在此计算机上运行的保护计划已创建备份，则更改加密设置将导致此计划失败。若要继续备份，请创建新的备份计划。

在计算机上保存加密设置

1. 以管理员身份（在 Windows 中）或根用户身份（在 Linux 中）登录。
2. 运行以下脚本：
   - 在 Windows 中：<安装路径>**\PyShell\bin\acropsh.exe -m manage_creds --set-password** <加密密码>

     其中，<安装路径> 是保护代理程序的安装路径。默认情况下，该路径在云部署中为 **%ProgramFiles%\BackupClient**，在本地部署中为 **%ProgramFiles%\Acronis**。
   - 在 Linux 中：**/usr/sbin/acropsh -m manage_creds --set-password** <加密密码>

在计算机上重置加密设置

1. 以管理员身份（在 Windows 中）或根用户身份（在 Linux 中）登录。
2. 运行以下脚本：
   - 在 Windows 中：<安装路径>**\PyShell\bin\acropsh.exe -m manage_creds --reset**

     其中，<安装路径> 是保护代理程序的安装路径。默认情况下，该路径在云部署中为 **%ProgramFiles%\BackupClient**，在本地部署中为 **%ProgramFiles%\Acronis**。
   - 在 Linux 中：**/usr/sbin/acropsh -m manage_creds --reset**

通过使用 安克诺斯数据保护软件 监视器更改加密设置

1. 以管理员身份在 Windows 或 macOS 中登录。
2. 在通知区域 (Windows) 或菜单栏 (macOS) 中，单击 **安克诺斯数据保护软件 监视器**图标。

3. 单击齿轮图标。
4. 单击**加密**。
5. 请执行以下任一操作：
   - 选择**为此计算机设置特定密码**。指定并确认加密密码。
   - 选择**使用在保护计划中指定的加密设置**。
6. 单击**确定**。

加密的工作原理

AES 密码算法在密码块链接 (CBC) 模式下运行，并使用带有用户定义的大小 128、192 或 256 位的随机生成的密钥。密钥越大，程序加密备份所需的时间越长，数据安全性也越高。

随后加密密钥将使用 AES-256 进行加密，并将密码的 SHA-256 哈希作为密钥。密码本身并不存储在磁盘上的任何位置或备份中，密码哈希用于验证。有了这样的双层安全防护，备份数据会受到保护以防止未经授权的访问，但是若密码丢失，则无法恢复。

公证

公证让您能够证明文件在备份后仍是可信的且未经更改。建议在备份法律文档文件或需要证明真实性的其他文件时启用公证功能。

公证仅适用于文件级备份。将跳过具有数字签名的文件，因为不需要对这些文件进行公证。

在下列情况下，公证*不*可用：

- 如果备份格式设置为**版本 11**
- 如果备份目标为 安全区
- 如果备份目标为已启用重复数据删除或加密的受控位置

如何使用公证

要对备份所选的所有文件启用公证(具有数字签名的文件除外)，请在创建保护计划时启用**公证**开关。

配置恢复时，将使用特殊图标标记已公证文件，并且您还可以验证文件真实性。

工作方式

在备份期间，代理程序会计算备份文件的哈希代码，生成哈希树(根据文件夹结构)，将该树保存在备份中，然后将哈希树根发送到公证服务。该公证服务会将哈希树根保存在 Ethereum 块链数据库中，以确保该值不会更改。

验证文件真实性时，代理程序会计算该文件的哈希，然后将它与存储在备份内的哈希树中的哈希进行比较。如果这些哈希不匹配，该文件被视为不真实。否则，该文件真实性受哈希树保证。

为了验证哈希树本身未被破坏，代理程序会将哈希树根发送到公证服务。公证服务会将它与块链数据库中存储的根进行比较。如果哈希匹配，则所选文件的真实性得到保证。否则，软件会显示文件不真实的消息。

转换为虚拟机

重要事项
本部分中所述的一些功能仅适用于本地部署。

只有磁盘级别备份才提供转换为虚拟机选项。如果备份包括系统卷并包含操作系统启动所需的所有信息，则虚拟机可以自行启动。否则，您可以将其虚拟磁盘添加到其他虚拟机。

转换方法

- **定期转换**
  配置定期转换有两种方法：
  - **使转换成为保护计划的一部分**
    转换将在每次备份（如果针对主要位置进行配置）或每次复制（如果针对次要及后续位置配置）之后执行。
  - **创建单独的转换计划**
    此方法可让您指定一个单独的转换预定。
- **恢复至新虚拟机**
  此方法可让您选择要恢复的磁盘并调整每个虚拟磁盘的设置。此方法可用于执行一次转换或偶尔执行转换，例如，执行物理到虚拟迁移。

关于转换，您需要知道的内容

支持的虚拟机类型

将备份转换到虚拟机可以通过创建备份的同一个代理程序或通过其他代理程序来完成。

要执行到 VMware ESXi、Hyper-V 或 Scale Computing HC3 的转换，您分别需要 ESXi、Hyper-V 或 Scale Computing HC3 主机以及管理该主机的保护代理程序（适用于 VMware 的代理程序、适用于 Hyper-V 的代理程序或适用于 Scale Computing HC3 的代理程序）。

到 VHDX 文件的转换假定文件将作为虚拟磁盘连接到 Hyper-V 虚拟机。

下表总结了可以由代理程序创建的虚拟机类型：

VM 类型	适用于 VMware 的代理程序	适用于 Hyper-V 的代理程序	适用于 Windows 的代理程序	适用于 Linux 的代理程序	适用于 Mac 的代理程序	适用于 Scale Computing HC3 的代理程序
VMware ESXi	+	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–

VMware Workstation	+	+	+	+	–	–
VHDX 文件	+	+	+	+	–	–
Scale Computing HC3	–	–	–	–	–	+

限制

- 适用于 Windows 的代理程序、适用于 VMware 的代理程序 (Windows) 和适用于 Hyper-V 的代理程序无法转换存储在 NFS 上的备份
- 存储在 NFS 上或 SFTP 服务器上的备份无法在单独转换计划中转换。
- 存储在 安全区 中的备份只可以由在同一台计算机上运行的代理程序进行转换。
- 备份只能在单独的转换计划中转换为 Scale Computing HC3 虚拟机。
- 仅当包含 Linux 逻辑卷 (LVM) 的备份由适用于 VMware 的代理程序、适用于 Hyper-V 的代理程序和适用于 Scale Computing HC3 的代理程序创建并指向同一个虚拟机监控程序时，才可以对其进行转换。不支持跨虚拟机监控程序进行转换。
- 当 Windows 计算机的备份转换为 VMware Workstation 或 VHDX 文件时，生成的虚拟机从执行转换的计算机继承 CPU 类型。结果，相应的 CPU 驱动程序将安装在来宾操作系统上。如果在具有不同 CPU 类型的主机上开始，来宾系统将显示驱动程序错误。手动更新此驱动器。

定期转换到 ESXi 和 Hyper-V 与从备份运行虚拟机

这两个操作可在原始计算机出现故障的情况下，向您提供可以在数秒内启动的虚拟机。

定期转换会占用 CPU 和内存资源。虚拟机的文件会不断占用数据存储(存储) 上的空间。如果生产主机用于转换，这可能不切合实际。不过，虚拟机性能仅受限于主机资源。

在第二种情况下，仅当虚拟机正在运行时，才会消耗资源。只需用于保留对虚拟磁盘的更改的数据存储(存储) 空间。但是，虚拟机可能会缓慢运行，因为主机不会直接访问虚拟磁盘，但会与从备份中读取数据的代理程序进行通信。此外，虚拟机暂时可用。

在保护计划中转换为虚拟机

可从保护计划中存在的任何备份或复制位置配置转换为虚拟机。将在每次备份或复制之后执行转换。

关于先决条件和限制的信息，请参阅“关于转换需要知道的内容”。

在保护计划中设置转换为虚拟机

1. 确定要从哪个备份位置执行转换。
2. 在保护计划面板上，单击该位置下的**转换为 VM**。
3. 启用**转换**开关。
4. 在**转换为**中，选择目标虚拟机的类型。可选择以下其中一个选项：

- **VMware ESXi**
- **Microsoft Hyper-V**
- **VMware Workstation**
- **VHDX 文件**

5. 请执行以下任一操作：
   - 对于 VMware ESXi 和 Hyper-V：单击**主机**，选择目标主机，然后指定新计算机名称模板。
   - 对于其他虚拟机类型：在**路径**中，指定保存虚拟机文件和文件名称模板的位置。

   默认名称为 **[Machine Name]_converted**。
6. [可选] 单击**将执行转换的代理程序**，然后选择一个代理程序。

   该代理程序可能是要执行备份（默认）的代理程序，或是安装在其它计算机上的代理程序。如果选择后者，则必须将备份存储在共享位置（如网络文件夹），以便其他计算机可以访问这些备份。
7. [可选] 对于 VMware ESXi 和 Hyper-V，还可以执行以下操作：
   - 为 ESXi 单击**数据存储**或者为 Hyper-V 单击**路径**，然后为虚拟机选择数据存储（存储）。
   - 更改磁盘调配模式。VMware ESXi 的默认设置为**精简**，Hyper-V 的默认设置为**动态扩展**。
   - 单击 **VM 设置**以更改内存大小、处理器数量以及虚拟机的网络连接。
8. 单击**完成**。

如何常规转换到 VM 工作

定期转换的工作方式取决于您选择创建虚拟机的位置。

- **如果选择将虚拟机保存为一组文件：**每一次转换都将对该虚拟机从头开始重新创建。
- **如果选择在虚拟化服务器上创建虚拟机：**转换增量或差异备份时，软件会更新现有虚拟机，而不会重新创建虚拟机。这种转换通常较快。可以节省执行转换的主机的网络流量和 CPU 资源。如果不能更新该虚拟机，软件将重新创建该虚拟机。

以下为两种情况的详细描述。

如果选择将虚拟机保存为一组文件

首次转换的结果是将创建新的虚拟机。以后的每一次转换都将对该虚拟机进行重新创建。首先，将临时对旧计算机重命名。然后，将创建新虚拟机，它具有旧计算机的先前名称。若该操作成功，旧计算机将被删除。若该操作失败，新计算机将被删除，并且将为旧计算机指定其先前名称。这样，转换便始终以单个计算机结束。但是，转换过程中需要额外的存储空间来存储旧计算机。

如果选择在虚拟服务器上创建虚拟机

首次转换将创建新的虚拟机。后续转换按如下方式进行：

- 如果上次转换后存在*完整备份*，将从头开始重新创建该虚拟机（如本节前面所述）。
- 否则，将更新现有虚拟机来反应上次转换后的更改。如果不能更新（例如您已删除中间快照，参阅下文），将重新创建虚拟机。

中间快照

为能更新虚拟机，软件存储了多个中间快照。它们名为 **Backup...** 和 **Replica...**，应当予以保留。不需要的快照会自动删除。

最近的 **Replica...** 快照对应最近转换的结果。如果您想将虚拟机返回某个状态，可以转到该快照。例如，如果您使用了虚拟机，而现在想放弃所做的更改。

其他快照供软件内部使用。

复制

重要事项
本部分中所述的一些功能仅适用于本地部署。

此部分介绍备份复制，它是保护计划的一部分。有关创建单独的复制计划的信息，请参阅“脱离主机数据处理”。

如果您启用备份复制，则每个备份都将在创建后立即复制到另一个位置。如果未复制较早的备份（例如，网络连接中断），则软件还会复制在上次成功复制之后出现的所有备份。

已复制的备份不取决于原始位置中保留的备份，反之亦然。您可以从任何备份中恢复数据，无需访问其他位置。

用法示例

- **可靠的灾难恢复**
  进行现场存储备份（用于快速恢复）和异地存储备份（用于确保本地存储失败或自然灾难时的备份安全）。
- **使用云存储保护数据免受自然灾害**
  通过仅传输数据更改将备份复制到云存储中。
- **仅保留最新的恢复点**
  根据保留规则，从快速存储中删除较早的备份，防止过多使用昂贵的存储空间。

支持的位置

您可以从以下任意位置复制备份：

- 本地文件夹
- 网络文件夹
- 安全区
- SFTP 服务器
- 由存储节点管理的位置

您可以将备份复制*到*以下任意位置：

- 本地文件夹
- 网络文件夹
- 云存储

- SFTP 服务器
- 由存储节点管理的位置
- 磁带设备

启用备份复制

1. 在保护计划面板上，单击**添加位置**。
   仅当支持从上次选择的备份或复制位置进行复制时，**添加位置**控件才可用。
2. 指定要复制备份的位置。
3. [可选] 在**保留时间**中，更改所选位置的保留规则，如“保留规则”中所述。
4. [可选] 在**转换为 VM** 中，指定转换为虚拟机的设置，如“转换为虚拟机”中所述。
5. [可选] 单击齿轮图标 > **性能和备份窗口**，然后为所选位置设置备份窗口，如“性能和备份窗口”中所述。这些设置将定义复制性能。
6. [可选] 对要复制备份的所有位置重复第 1-5 步。最多支持五个连续位置，包括主要位置。

重要事项
如果在同一保护计划中启用备份和复制，请确保复制在下一次计划备份开始之前完成。如果复制仍在进行中，则计划备份将不会开始。例如，如果复制需要 26 小时才能完成，则每 24 小时运行一次的计划备份将不会开始。

为了避免出现这种依赖关系，请使用单独的备份复制计划。有关此特定计划的详细信息，请参阅 "备份复制"(第 302 页)。

使用高级许可证的注意事项

提示

您可以通过创建单独的复制计划，设置从云存储中复制备份。有关详细信息，请参阅 “脱离主机数据处理”。

限制条件

- 不支持将备份从存储节点管理的位置复制到本地文件夹。本地文件表示文件夹位于具有创建了该备份的代理程序的计算机上。
- 对于采用**版本 12** 备份格式的备份，不支持将备份复制*到*已启用重复数据删除的受控位置。

哪台计算机执行操作？

从任意位置复制备份由创建该备份的代理程序启动，由以下两者执行：

- 如果该位置*不*受存储节点管理，则由代理程序执行。
- 如果该位置受控，则由相应的存储节点执行。但是，将备份从受控位置复制到云存储是由创建该备份的代理程序执行。

如上所述，只有启动计算机的代理程序，才可以进行操作。

在受控位置之间复制备份

将备份从一个受控位置复制到另一个受控位置是由存储节点执行。

如果目标位置(可能在另一存储节点上)启用了重复数据删除,则源存储节点只发送目标位置中不存在的那些数据块。换言之,与代理程序相似,存储节点在源头执行重复数据删除。当您在地理上分开的存储节点之间复制数据时,这可节省网络流量。

手动启动备份

1. 选择具有至少一个已应用保护计划的计算机。
2. 单击**备份**。
3. 如果已应用多个保护计划,请选择相应保护计划。
4. 请执行以下任一操作:
   - 单击**立即运行**。系统会创建增量备份。
   - 如果备份方案中包括多个备份方法,则可以选择要使用的方法。单击**立即运行**按钮上的箭头,然后选择**完整**、**增量**或**差异**。

保护计划创建的第一个备份始终为完整备份。

备份进度显示在计算机的**状态**列中。

备份选项

重要事项
本部分中所述的一些功能仅适用于本地部署。

若要修改备份选项,请单击保护计划名称旁边的齿轮图标,然后单击**备份选项**。

备份选项的可用性

可用的备份选项集取决于:

- 代理程序运行的环境(Windows、Linux、macOS)。
- 要备份的数据类型(磁盘、文件、虚拟机、应用程序数据)。
- 备份目标(云存储、本地或网络文件夹)。

下表总结了备份选项的可用性。

	磁盘级别备份			文件级备份			虚拟机			SQL 和 Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Scale Compu	Windows

									ting	
警告	+	+	+	+	+	+	+	+	+	+
备份合并	+	+	+	+	+	+	+	+	+	-
备份文件名	+	+	+	+	+	+	+	+	+	+
备份格式	+	+	+	+	+	+	+	+	+	+
备份验证	+	+	+	+	+	+	+	+	+	+
块更改跟踪 (CBT)	+	-	-	-	-	-	+	+	+	+
群集备份模式	-	-	-	-	-	-	-	-	-	+
压缩级别	+	+	+	+	+	+	+	+	+	+
电子邮件通知	+	+	+	+	+	+	+	+	+	+
错误处理										
重新尝试 (如果发生错误)	+	+	+	+	+	+	+	+	+	+
处理时不显示消息和对话框 (无提	+	+	+	+	+	+	+	+	+	+

示模式)										
忽略损坏的扇区	+	-	+	+	-	+	+	+	+	-
如果在 VM 快照创建期间发生错误，则重新尝试	-	-	-	-	-	-	+	+	+	-
快速增量/差异备份	+	+	+	-	-	-	-	-	-	-
文件过滤器	+	+	+	+	+	+	+	+	+	-
文件级备份快照	-	-	-	+	+	+	-	-	-	-
日志截断	-	-	-	-	-	-	+	+	-	仅 SQL
LVM 快照	-	+	-	-	-	-	-	-	-	-
加载点	-	-	-	+	-	-	-	-	-	-
多卷快照	+	+	-	+	+	-	-	-	-	-
性能和备份窗	+	+	+	+	+	+	+	+	+	+

口										
物理数据装运	+	+	+	+	+	+	+	+	+	-
预/后命令	+	+	+	+	+	+	+	+	+	+
预/后数据捕获命令	+	+	+	+	+	+	+	-	-	+
SAN 硬件快照	-	-	-	-	-	-	+	-	-	-
预定										
在时间窗口内分配开始时间	+	+	+	+	+	+	+	+	+	+
限制同时运行的备份数量	-	-	-	-	-	-	+	+	+	-
逐扇区备份	+	+	-	-	-	-	+	+	+	-
分割	+	+	+	+	+	+	+	+	+	+
磁带管理	+	+	+	+	+	+	+	+	+	+
任务失败处理	+	+	+	+	+	+	+	+	+	+
任务	+	+	-	+	+	-	+	+	+	+

开始条件										
卷影复制服务(VSS)	+	-	-	+	-	-	-	+	-	+
适用于虚拟机的卷影复制服务(VSS)	-	-	-	-	-	-	+	+	+	-
每周备份	+	+	+	+	+	+	+	+	+	+
Windows事件日志	+	-	-	+	-	-	+	+	+	+

警告

未按指定连续天数成功备份

预设为:**已禁用**。

此选项确定在保护计划于指定时段内未成功执行备份时是否生成警告。除了失败的备份,还有未按预定运行的软件计数备份(缺少的备份)。

警告针对每台计算机生成并显示在**警告**选项卡上。

您可以指定在生成警告后,不进行备份的连续天数。

备份合并

此选项定义是在清理期间合并备份,还是删除整条备份链。

预设为:**已禁用**。

合并是将两个或更多后续备份组合为单个备份的过程。

如果启用此选项,应在清理期间删除的备份将与下一个从属备份(增量或差异)合并。

否则,在所有从属备份可删除之前,将保留该备份。这有助于避免可能的耗时合并,但需要额外的空间来存储推迟删除的备份。备份的存留时间或数量可能超出保留规则中指定的值。

重要事项
请注意合并只是一种删除方法，它不可替代删除操作。结果产生的备份将不包含出现在被删除备份中，但不出现在被保留的增量或差异备份中的数据。

如果存在以下任一种情况，此选项*无效*：

- 备份目标为磁带设备或云存储。
- 备份方案设置为**始终增量(单个文件)**。
- 备份格式设置为**版本 12**。

磁带上的备份不能合并。存储在云存储中的备份以及单个文件的备份(版本 11 和 12 格式)都始终会合并，因为其内部结构便于轻松快速进行合并。

但是，如果使用版本 12 格式，并且存在多个备份链(每个链存储在单独的 .tibx 文件中)，则仅能在最后一个链中进行合并。会将任何其他链整体删除，缩小到最小大小以保留元信息 (~12 KB) 的第一个链除外。需要此元信息才能确保同时进行读写操作期间的数据一致性。一旦应用了保留规则，包含在这些链中的备份即会从 GUI 中消失，尽管它们在整个链被删除之前一直物理上存在。

在所有其他情况下，延迟删除的备份在 GUI 中标记有垃圾桶图标 ( )。如果通过单击 X 符号删除此类备份，则会执行合并。仅当覆盖或擦除磁带时，该磁带上存储的备份才会从 GUI 中消失。

备份文件名

此选项定义保护计划创建的备份文件的名称。

当浏览备份位置时，可以在文件管理器中看见这些名称。

什么是备份文件?

每个保护计划都会在备份位置创建一个或多个文件，具体取决于所使用的备份方案和备份格式。下表列出了每个计算机或邮箱可以创建的文件。

	始终增量(单个文件)	**其他备份方案**
版本 11 备份格式	一个 TIB 文件和一个 XML 元数据文件	多个 TIB 文件和一个 XML 元数据文件(传统格式)
版本 12 备份格式	每个备份链一个 TIBX 文件(一个完整备份或差异备份，以及取决于前者的所有增量备份)	

所有文件都具有相同的名称，其中可能会(也可能不会)添加时间戳或序列号。可以在创建或编辑保护计划时定义此名称(称为备份文件名)。

注意
时间戳仅添加到版本 11 备份格式的备份文件名。

更改备份文件名之后，下一个备份会是完整备份，除非您指定同一台计算机上现有备份的文件名。如果是后者，将根据保护计划时间表创建完整备份、增量备份或差异备份。

请注意，可以为文件管理器无法浏览的位置设置备份文件名（例如云存储或磁带设备）。如果要在**备份存储**选项卡上查看自定义名称，这将很有意义。

可以在哪里查看备份文件名？

选择**备份存储**选项卡，然后选择备份组。

- 默认备份文件名显示在**详细信息**面板中。
- 如果设置非默认备份文件名，它将直接显示在**备份存储**选项卡的**名称**列中。

备份文件名的限制

- 备份文件名不能以数字结尾。

  在默认备份文件名中，为了防止文件名以数字结尾，文件名后附加了一个字母“A”。当创建自定义名称时，请务必确保其结尾不是数字。当使用变量时，文件名不得以变量结尾，因为变量可能会以数字结尾。
- 备份文件名不能包含以下符号：**()&?*$<>":\|/#**、行尾结束符号 **(\n)** 和制表符 **(\t)**。

默认备份文件名

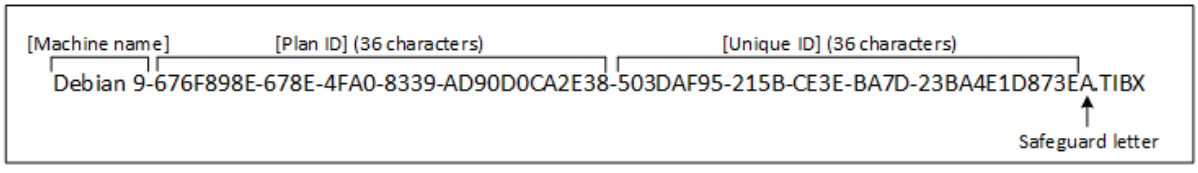
默认备份文件名为 `[Machine Name]-[Plan ID]-[Unique ID]A`。

邮箱备份的默认备份文件名为 `[Mailbox ID]_mailbox_[Plan ID]A`。

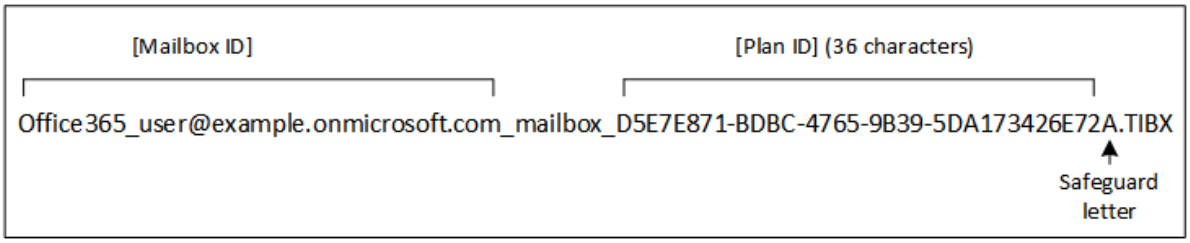
此文件名包含以下变量：

- `[Machine Name]` 对于所有类型的备份数据（Microsoft 365 邮箱除外），此变量会替换为计算机的名称（即 安克诺斯数据保护软件 Web 中控台中显示的相同名称）。对于 Microsoft 365 邮箱，此变量替换为邮箱用户的主体名称 (UPN)。
- `[Plan ID]` 此变量会替换为保护计划的唯一标识符。重命名计划时，此值不变。
- `[Unique ID]` 此变量会替换为所选计算机或邮箱的唯一标识符。计算机重命名或邮箱 UPN 改变时，此值不变。
- `[Mailbox ID]` 此变量会替换为邮箱 UPN。
- “A”是为防止文件名以数字结尾而在文件名后附加的一个安全字母。

下图显示默认备份文件名。



下图显示邮箱的默认备份文件名。



无变量的文件名

如果将备份文件名改为 MyBackup，则备份文件将如以下示例所示。两个示例都假设从 2016 年 9 月 13 日开始，预定在 14:40 进行每日增量备份。

对于具有**始终增量(单个文件)**备份方案的版本 12 格式：

```
MyBackup.tibx
```

对于具有其他备份方案的版本 12 格式：

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

对于具有 **始终增量(单个文件)** 备份方案的版本 11 格式：

```
MyBackup.xml
MyBackup.tib
```

对于具有其他备份方案的版本 11 格式：

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

使用变量

除了默认使用的变量之外，还可以使用 [Plan name] 变量，该变量会替换为保护计划的名称。

如果选择多台计算机或多个邮箱进行备份，则备份文件名必须包含 [Machine Name]、[Mailbox ID] 或 [Unique ID] 变量。

备份文件名与简化的文件名

通过使用纯文本和/或变量，可以构建与早期 Acronis 安克诺斯数据保护软件 版本中一样的文件名。但是，无法重新构建简化的文件名；在版本 12 中，除非使用单个文件格式，否则文件名将包含时间戳。

用法示例

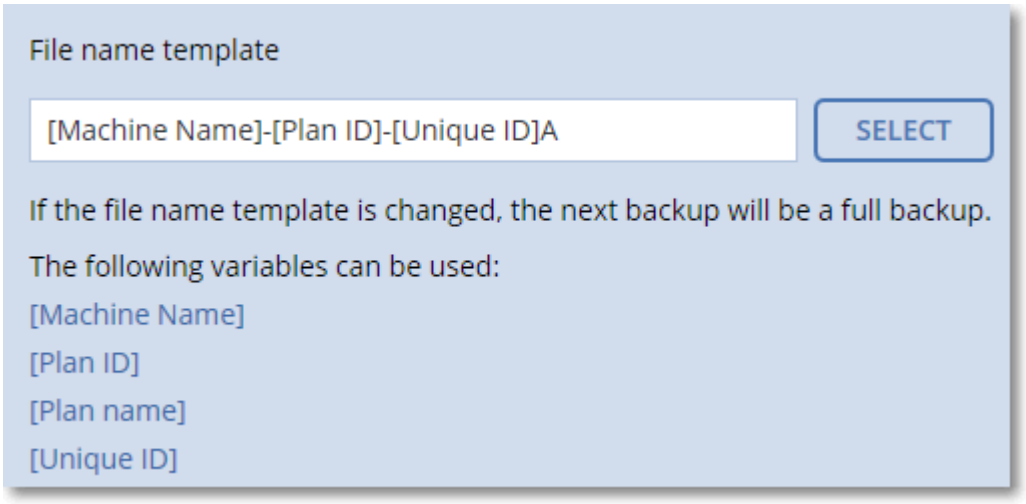
- **查看方便使用的文件名**

  当使用文件管理器浏览备份位置时，您会希望轻松识别备份。

- **继续现有备份序列**

  假定已将保护计划应用于一台计算机，并且您要从 安克诺斯数据保护软件 Web 中控台中删除该计算机或要卸载代理程序及其配置设置。在重新添加计算机或重新安装代理程序后，可以强制保护计划继续备份到相同备份或备份序列。为此，在保护计划的备份选项中，单击**备份文件名**，然后单击**选择**以选择所需的备份。

  浏览按钮可以显示在保护计划面板的**备份位置**部分选择的位置中的备份。该按钮无法浏览此位置之外的任何内容。



- **从之前的产品版本升级**

  如果在升级期间，保护计划未自动迁移，请重新创建计划并将其指向旧备份文件。如果只为备份选择了一台计算机，请单击**浏览**，然后选择所需的备份。如果为备份选择了多台计算机，请通过使用变量重新创建旧备份文件名。

注意
选择按钮仅适用于为单个设备创建并已应用的保护计划。

备份格式

此选项定义由保护计划创建的备份的格式。它仅适用于使用旧版备份格式版本 11 的保护计划。此时，您可以将其更改为新格式版本 12。此更改之后，该选项将无法访问。

此选项对邮箱备份*无效*。邮箱备份始终采用新格式。

预设为：**自动选择**。

可选择以下其中一个选项：

- **自动选择**

  将使用版本 12，除非保护计划向由较早版本的产品创建的备份附加备份。

- **版本 12**

  大多数情况下，建议针对快速备份和恢复使用新格式。每个备份链(一个完整备份或差异备份，以及取决于前者的所有增量备份)都会保存到单个 TIBX 文件中。

  对于此格式，**按备份的总大小**保留规则无效。
- **版本 11**

  为向后兼容保留的旧格式。您可向由较早版本的产品创建的备份附加备份。

  此外，如果要将完整备份、增量备份和差异备份作为单独的文件，请使用此格式(以及**始终增量(单个文件)**之外的任何备份方案)。

  如果备份目标(或复制目标)是启用了重复数据删除的受控位置或启用了加密的受控位置，则会自动选择此格式。如果将格式改为**版本 12**，备份将失败。

注意

无法使用备份格式版本 11 备份数据库可用性组 (DAG)。仅支持以版本 12 格式备份 DAG。

备份格式和备份文件

对于可以使用文件管理器浏览的备份位置(例如本地或网络文件夹)，备份格式决定了文件的数量及其扩展名。您可以使用备份文件名选项定义文件名。下表列出了每个计算机或邮箱可以创建的文件。

	始终增量(单个文件)	其他备份方案
版本 11 备份格式	一个 TIB 文件和一个 XML 元数据文件	多个 TIB 文件和一个 XML 元数据文件(传统格式)
版本 12 备份格式	每个备份链一个 TIBX 文件(一个完整备份或差异备份，以及取决于前者的所有增量备份)	

更改备份格式为版本 12 (TIBX)

如果将备份格式从版本 11(TIB 格式)更改为版本 12(TIBX 格式)：

- 下一个备份将是完整的。
- 在可以使用文件管理器浏览的备份位置(例如，本地或网络文件夹)中，将创建新的 TIBX 文件。新文件将具有原始文件的名称，附加有 **_v12A** 后缀。
- 保留规则和复制将仅应用于新备份。
- 旧备份不会被删除，并且会在**备份存储**选项卡上保持可用。可以手动删除它们。
- 旧的云备份将不会消耗**云存储**配额。
- 旧的本地备份将消耗**本地备份**配额，直到您手动删除它们。
- 如果备份目标(或复制目标)为已启用重复数据删除的受控位置，则备份将失败。

存档内重复数据删除

版本 12 的格式支持存档内重复数据删除。

存档内重复数据删除将使用客户端侧重复数据删除，并带来以下优势：

- 通过适用于任何数据类型的内置块级重复数据删除，显著减少了备份大小
- 高效处理硬链接，确保没有存储重复
- 基于哈希的区块划分

注意
默认情况下，将为所有 TIBX 格式的备份启用存档内重复数据删除。您不必在备份选项中启用它，也不能禁用它。

备份验证

验证是用于检查通过备份进行数据恢复之可行性的一种操作。如果启用此选项，则保护计划创建的每个备份都会在创建后立即进行验证。该操作由保护代理程序执行。

预设为：**已禁用**。

验证将计算可从备份恢复的每个数据块的校验和。唯一的例外是位于云存储中的文件级备份的验证。这些备份通过检查保存在备份中的元数据的一致性来进行验证。

验证是一个耗时的过程，即使对大小较小的增量或差异备份也是如此。这是因为该操作不仅验证备份本身包含的数据，还会验证通过选择备份可恢复的所有数据。此操作要求访问之前创建的备份。

虽然验证成功意味着成功恢复的可能性极高，但此程序并未检查影响恢复进程的所有因素。如果备份操作系统，建议您在可启动媒体下执行到备用硬盘驱动器的测试恢复，或者在 ESXi 或 Hyper-V 环境中从备份运行虚拟机。

块更改跟踪 (CBT)

此选项对运行 Windows 的虚拟机和物理机的磁盘级别备份有效。它还对于 Microsoft SQL Server 数据库和 Microsoft Exchange Server 数据库的备份有效。

预设为：**已启用**。

此选项可确定在执行增量或差异备份时是否使用块更改跟踪 (CBT)。

CBT 技术可加快备份过程。将在块级别上持续跟踪对磁盘或数据库内容的更改。当备份开始时，更改将立即保存到备份。

群集备份模式

这些选项对 Microsoft SQL Server 和 Microsoft Exchange Server 的数据库级别备份有效。

仅在选择对群集本身(Microsoft SQL Server Always On 可用性组 (AAG) 或 Microsoft Exchange Server 数据库可用性组 (DAG)) 而不是其中的单个节点或数据库进行备份时，这些选项才有效。如果选择群集中的单个项目，则备份将不是群集感知备份，只会备份项目的选定副本。

Microsoft SQL Server

此选项确定 SQL Server Always On 可用性组 (AAG) 的备份模式。若要使该选项有效，必须在所有 AAG 节点上安装适用于 SQL 的代理程序。有关备份 Always On 可用性组的更多信息，请参阅“保护

Always On 可用性组 (AAG)”。

预设为：**次要副本（如果可能）**。

可选择以下其中一个选项：

- **次要副本（如果可能）**
  如果所有次要副本都处于离线状态，将备份主要副本。备份主要副本可能会降低 SQL Server 的性能，但将备份处于最新状态的数据。
- **次要副本**
  如果所有次要副本都处于离线状态，备份将失败。备份次要副本不会影响 SQL 服务器性能，并可让您扩展备份窗口。然而，被动副本含有的信息可能不是最新的，因为这些副本经常设置为异步更新（延迟）。
- **主要副本**
  如果主要副本处于离线状态，备份将失败。备份主要副本可能会降低 SQL Server 的性能，但将备份处于最新状态的数据。

无论此选项的值是什么，为了确保数据库一致性，软件都会跳过在备份启动时*不*处于 **SYNCHRONIZED** 或 **SYNCHRONIZING** 状态的数据库。如果软件跳过所有数据库，则备份失败。

Microsoft Exchange Server

此选项确定 Exchange Server 数据库可用性组 (DAG) 的备份模式。若要使该选项有效，必须在所有 DAG 节点上安装适用于 Exchange 的代理程序。有关备份数据库可用性组的更多信息，请参阅“保护数据库可用性组 (DAG)”。

预设为：**被动副本（如果可能）**。

可选择以下其中一个选项：

- **被动副本（如果可能）**
  如果所有被动副本都处于离线状态，将备份主动副本。备份主动副本可能会降低 Exchange Server 的性能，但系统将备份处于最新状态的数据。
- **被动副本**
  如果所有被动副本都处于离线状态，备份将失败。备份被动副本不会影响 Exchange Server 性能，并允许您扩展备份窗口。然而，被动副本含有的信息可能不是最新的，因为这些副本经常设置为异步更新（延迟）。
- **主动副本**
  如果主动副本处于离线状态，备份将失败。备份主动副本可能会降低 Exchange Server 的性能，但系统将备份处于最新状态的数据。

无论此选项的值是什么，为了确保数据库一致性，软件都会跳过在备份启动时*不*处于 **HEALTHY** 或 **ACTIVE** 状态的数据库。如果软件跳过所有数据库，则备份失败。

压缩级别

此选项定义应用到要备份数据的压缩级别。可用级别包括：**无**、**正常**、**高**、**最大**。

预设为：**正常**。

较高的压缩级别意味着备份过程需要更长时间，但所产生的备份占用更少空间。当前，“高”和“最大”级别的作用类似。

最佳数据压缩级别视要备份数据的类型而定。例如，如果备份中包含本身已压缩好的文件（如 .jpg、.pdf 或 .mp3），即使选择最高压缩级别也无法明显减小备份大小。不过，.doc 或 .xls 等格式将会获得良好的压缩效果。

电子邮件通知

该选项可使您设置有关在备份期间发生的事件的电子邮件通知。

此选项仅在本地部署中可用。在云部署中，当创建帐户时，将为每个帐户配置设置。

预设为：**使用系统设置。**

可以使用系统设置，也可以使用仅特定于此计划的自定义值进行覆盖。按“电子邮件通知”中所述的方法配置系统设置。

重要事项
当更改系统设置时，使用系统设置的所有保护计划都会受影响。

在启用该选项之前，请确保已配置**电子邮件服务器**设置。

自定义保护计划的电子邮件通知

1. 选择**自定义此保护计划的设置**。
2. 在**收件人的电子邮件地址**字段中，键入目标电子邮件地址。您可以输入多个地址，但要用分号隔开。
3. [可选] 在**主题**中，更改电子邮件通知的主题。
   您可以使用下列变量：
   - `[Alert]` - 警报摘要。
   - `[Device]` - 设备名称。
   - `[Plan]` - 生成警报的计划的名称。
   - `[ManagementServer]` - 安装了管理服务器的计算机的主机名。
   - `[Unit]` - 计算机所属单位的名称。

   默认主题为 `[Alert]` **设备：** `[Device]` **计划：** `[Plan]`
4. 选中要接收相关通知的事件的复选框。您可以从备份期间发生的、按严重性排序的所有警告的列表中选择相应事件。

错误处理

这些选项可让您指定如何处理备份期间可能发生的错误。

如果发生错误，则重新尝试

预设为：**已启用。尝试次数：30.尝试间隔：30 秒。**

如果发生可恢复的错误，程序会重新尝试执行未成功的操作。您可以设置时间间隔和尝试次数。一旦操作成功或已执行指定尝试次数(以首先发生的为准)，尝试将停止。

例如，若网络上的备份目标位置变得不可用或无法到达，程序将每 30 秒尝试访问目标位置一次，但总次数不超过 30 次。一旦操作成功或已执行指定尝试次数(以首先发生的为准)，尝试将停止。

云存储

如果选择云存储作为备份目标，则选项值自动设置为**已启用**。**尝试次数：300**。**尝试间隔：30 秒**。

在这种情况下，实际尝试次数不受限制，但备份失败之前的超时计算方法如下：(300 秒 + **尝试间隔**) *(**尝试次数** + 1)。

示例：

- 使用默认值时，备份将在(300 秒 + 30 秒) *(300 + 1) = 99330 秒或约 27.6 小时后失败。
- 如果将**尝试次数**设置为 1 并将**尝试间隔**设置为 1 秒，则备份将在(300 秒 + 1 秒) *(1 + 1) = 602 秒或约 10 分钟后失败。

如果计算的超时超过 30 分钟，并且数据传输尚未开始，则实际超时将设置为 30 分钟。

处理时不显示消息和对话框(无提示模式)

预设为：**已启用**。

启用无消息模式后，程序将自动处理要求用户互动的情况(处理损坏的扇区除外，此项已定义为单独的选项)。如果操作必须有用户互动才能继续，则操作将失败。可在操作日志中找到操作的详细信息，包括错误(如果有)。

忽略损坏的扇区

预设为：**已禁用**。

如果禁用此选项，程序每次遇到坏扇区时，备份活动都将指派为**需要互动**状态。若要备份正在迅速损毁的磁盘上的有效信息，请启用忽略损坏的扇区。将备份剩余数据且您可加载生成的磁盘备份，并将有效文件解压至其他磁盘。

如果在 VM 快照创建期间发生错误，则重新尝试

预设为：**已启用。尝试次数：3。尝试间隔：5 分钟。**

当创建虚拟机快照失败时，程序将重新尝试执行未成功的操作。您可以设置时间间隔和尝试次数。一旦操作成功或已执行指定尝试次数(以首先发生的为准)，尝试将停止。

快速增量/差异备份

此选项对磁盘级增量和差异备份有效。

对于格式为 JFS、ReiserFS3、ReiserFS4、ReFS 或 XFS 文件系统的卷，此选项无效(始终禁用)。

预设为：**已启用**。

增量或差异备份仅会捕获数据更改。为加快备份进程，程序通过文件大小及其上次修改的日期/时间来确定文件是否有更改。如果禁用此功能，则程序会将整个文件内容与备份中存储的内容进行比较。

文件过滤器

通过使用文件过滤器，可以在备份中仅包括特定的文件和文件夹，也可以将特定的文件和文件夹排除备份。

除非另行说明，否则文件过滤器同时适用于磁盘级备份和文件级备份。

当应用于由 VMware 的代理程序、适用于 Hyper-V 的代理程序或适用于 Scale Computing 无代理模式备份的虚拟机上的动态磁盘(LVM 或 LDM 卷)时，文件过滤器无效。

启用文件过滤器

1. 在保护计划中，展开**备份**模块。
2. 在**备份选项**中，单击**更改**。
3. 选择**文件过滤器**。
4. 使用以下所述的任意选项。

包括或排除符合特定条件的文件

有两种以相反方式运作的选项。

- **仅备份符合以下条件的文件**
  示例：如果您选择备份整台计算机并在过滤器条件中指定 **C:\File.exe**，将仅备份此文件。

  注意
  如果在备份格式中选择了**版本 11** 并且备份目标不是云存储，则此过滤器对文件级备份无效。

- **请勿备份符合以下条件的文件**
  示例：如果您选择备份整台计算机并在过滤器条件中指定 **C:\File.exe**，将仅跳过此文件。

可以同时使用这两个选项。后一个选项优先于前一个选项，即，如果您在这两个字段中指定 **C:\File.exe**，将在备份期间跳过此文件。

条件

- **完整路径**
  指定文件或文件夹的完整路径，以驱动器号(备份 Windows 时)或根目录(备份 Linux 或 macOS 时)开头。
  在 Windows 和 Linux/macOS 中，可以在文件或文件夹路径中使用正斜杠(如 **C:/Temp/File.tmp** 中)。在 Windows 中，您还可以使用传统的反斜杠(如 **C:\Temp\File.tmp** 中)。

重要事项

如果在磁盘级别备份过程中未正确检测到备份计算机的操作系统，则完整路径文件过滤器将不起作用。对于排除过滤器，将显示一条警告。如果有包含过滤器，则备份将失败。

完整路径过滤器包括磁盘驱动器代号（在 Windows 中）或根目录（在 Linux 或 macOS）中。例如，文件完整路径可以是 **C:\Temp\File.tmp**。包含磁盘驱动器代号或根目录的过滤器 - 例如 **C:\Temp\File.tmp** 或 **C:\Temp*** - 将导致警告或失败。

不使用磁盘驱动器代号或根目录的过滤器（例如，**Temp*** 或 **Temp\File.tmp**）或以星号开头的过滤器（例如，***C:**）不会导致警告或失败。但是，如果未正确检测到备份计算机的操作系统，则这些过滤器也不起作用。

- **名称**

  指定文件或文件夹的名称，例如 **Document.txt**。将选择带有该名称的所有文件和文件夹。

条件不区分大小写。例如，通过指定 **C:\Temp**，您还将选择 **C:\TEMP**、**C:\temp** 等。

您可在条件中使用一个或多个通配符（*、** 和 ?）。无论是在完整路径内，还是在文件或文件夹名称中，均可使用这些字符。

星号 (*) 可替代文件名中的零个或多个字符。例如，条件 **Doc*.txt** 匹配 **Doc.txt** 和 **Document.txt** 等文件

[仅适用于**版本 12** 格式的备份] 双星号 (**) 替代文件名和路径中的零个或多个字符，包括斜杠字符。例如，条件 ****/Docs/**.txt** 匹配所有文件夹 **Docs** 的所有子文件夹中的所有 txt 文件。

问号 (?)仅替代文件名中的一个字符。例如，条件 **Doc?.txt** 匹配 **Doc1.txt** 和 **Docs.txt** 等文件，但不包括 **Doc.txt** 或 **Doc11.txt** 文件

排除隐藏的文件和文件夹

选择此复选框以跳过具有**隐藏**属性的文件和文件夹（对于 Windows 支持的文件系统）或是以句点 (.) 开头的文件和文件夹（对于 Linux 中的文件系统，如 Ext2 和 Ext3）。如果某个文件夹为隐藏文件夹，其中所有内容（包括未隐藏的文件）都将被排除。

排除系统文件和文件夹

此选项仅对 Windows 支持的文件系统有效。选中此复选框以跳过具有**系统**属性的文件和文件夹。如果某个文件夹具有**系统**属性，则其中所有内容（包括不含**系统**属性的文件）都将被排除。

注意

您可在文件/文件夹属性中或通过使用 attrib 命令查看文件或文件夹属性。有关详细信息，请参考 Windows 中的帮助和支持中心。

文件级备份快照

此选项仅对文件级备份有效。

此选项定义是逐个备份文件，还是创建即时数据快照。

注意
存储在网络共享中的文件总是逐个保存。

预设为：

- 如果仅为备份选择了运行 Linux 的计算机：**不创建快照。**
- 否则：**可能时创建快照。**

可选择以下其中一个选项：

- **可能时创建快照**
  若无法创建快照，则直接备份文件。
- **始终创建快照**
  使用快照可备份所有文件，包括使用独占访问权打开的文件。将在同一个时间点对文件进行备份。仅在这些因素至关重要时（即备份文件时不创建快照将无意义），选择此设置。若无法创建快照，备份操作将失败。
- **不创建快照**
  始终直接备份文件。尝试备份以独占访问权打开的文件将会产生读取错误。备份中的文件可能在时间上无连续性。

取证数据

计算机上可能由病毒、恶意软件和勒索软件执行的恶意活动。可能需要调查的另一种情况是其他程序窃取或更改计算机上的数据。此类活动可能需要进行调查，但仅当将数字证据保留在要调查的计算机上时才有可能。不幸的是，证据（文件、痕迹等）可能已删除，或者计算机可能不可用。

称为**取证数据**的备份选项让您可以收集可用于取证调查的数字证据。以下各项可以用作数字证据：未使用的磁盘空间的快照、内存转储以及正在运行的进程的快照。**取证数据**功能仅适用于整个计算机备份。

当前，**取证数据**选项仅适用于具有以下操作系统版本的 Windows 计算机：

- Windows 8.1，Windows 10
- Windows Server 2012 R2 – Windows Server 2019

注意
• 将具有备份模块的保护计划应用于计算机后，无法修改取证数据设置。要使用其他取证数据设置，请创建新的保护计划。
• 通过 VPN 连接到您网络并且无法直接访问 Internet 的计算机不支持具有取证数据收集的备份。

支持的带有取证数据的备份位置为：

- 云存储
- 本地文件夹

注意

1.仅支持通过 USB 连接的外部硬盘上的本地文件夹。

2.本地动态磁盘不支持用作取证备份的位置。

- 网络文件夹

带有取证数据的备份会自动进行公证。取证备份允许调查人员分析通常不包含在常规磁盘备份中的磁盘区域。

取证备份过程

系统在取证备份过程中将执行以下操作：

1. 收集原始内存转储和正在运行的进程的列表。
2. 自动将计算机重新启动到可启动媒体中。
3. 创建同时包含已占用空间和未分配空间的备份。
4. 公证备份的磁盘。
5. 重新启动进入实时操作系统并继续执行计划(例如，复制、保留、验证等)。

配置取证数据收集

1. 在安克诺斯数据保护软件 Web 中控台中，转到**设备** > **所有设备**。或者，可以从**计划**选项卡创建保护计划。
2. 选择相应设备，然后单击**保护**。
3. 在保护计划中，启用**备份**模块。
4. 在**要备份的内容**，选择**整个计算机**。
5. 在**备份选项**中，单击**更改**。
6. 找到**取证数据**选项。
7. 启用**收集取证数据**。系统将自动收集内存转储并创建正在运行的进程的快照。

注意

完整内存转储可能会包含敏感数据，例如密码。

8. 指定位置。
9. 单击**立即运行**以立即执行带有取证数据的备份，或者等到根据预定创建备份。
10. 转到**仪表板** > **活动**，验证是否已成功创建带有取证数据的备份。

结果，备份将包括取证数据，您将能够获取它们并进行分析。带有取证数据的备份会被标记，并可以在**备份存储** > **位置**中通过使用**仅限取证数据**选项从其他备份中过滤得到。

如何从备份中获取取证数据？

1. 在安克诺斯数据保护软件 Web 中控台中，转到**备份存储**，选择包含取证数据的备份的位置。
2. 选择带有取证数据的备份，然后单击**显示备份**。
3. 单击**恢复**以获取带有取证数据的备份。

- 要仅获取取证数据，请单击**取证数据**。
  系统将显示带有取证数据的文件夹。选择内存转储文件或任何其他取证文件，然后单击**下载**。
- 要恢复完整取证备份，请单击**整个计算机**。系统将在不使用启动模式的情况下恢复备份。因此，将可以检查磁盘是否未被更改。

可以将提供的内存转储与多个第三方取证软件一起使用，例如，通过访问 https://www.volatilityfoundation.org/ 将 Volatility Framework 用于进一步内存分析。

带有取证数据的备份的公证

为了确保带有取证数据的备份与生成的映像完全相同并且未遭篡改，备份模块会提供带有取证数据的备份的公证。

工作方式

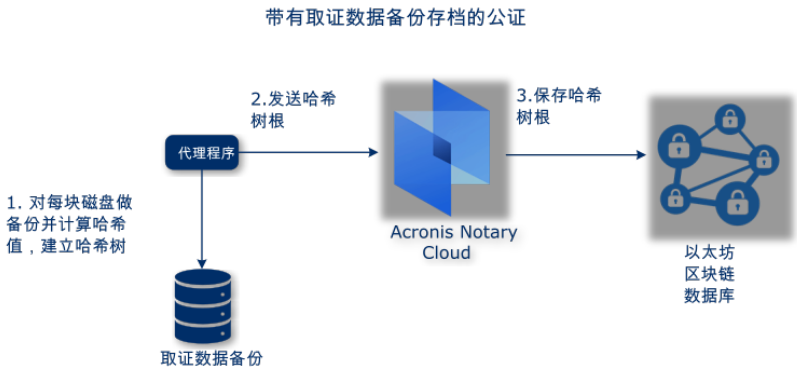
公证让您能够证明带有取证数据的磁盘在备份后仍是可信的且未经更改。

在备份期间，代理程序会计算备份磁盘的哈希代码、生成哈希树、将该树保存在备份中，然后将哈希树根发送到公证服务。该公证服务会将哈希树根保存在 Ethereum 块链数据库中，以确保该值不会更改。

验证带有取证数据的磁盘的真实性时，代理程序会计算该磁盘的哈希，然后将它与存储在备份内的哈希树中的哈希进行比较。如果这些哈希不匹配，该磁盘被视为不真实。否则，该磁盘真实性受哈希树保证。

为了验证哈希树本身未被破坏，代理程序会将哈希树根发送到公证服务。公证服务会将它与块链数据库中存储的根进行比较。如果哈希匹配，则所选磁盘的真实性得到保证。否则，软件会显示磁盘不真实的消息。

以下方案简要介绍了带有取证数据的备份的公证过程。



要手动验证经过公证的磁盘备份，可以获取它的证书，然后使用 tibxread 工具按照证书显示的验证步骤进行操作。

获取带有取证数据的备份的证书

要从中控台获取带有取证数据的备份的证书，请执行以下操作：

1. 转到**备份存储**，然后选择带有取证数据的备份。
2. 恢复整个计算机。
3. 系统会打开**磁盘映射**视图。
4. 单击磁盘的**获取证书**图标。
5. 系统将生成证书，并在浏览器中打开一个带有证书的新窗口。在证书下方，您会看到用于手动验证已公证的磁盘备份的说明。

用于获取备份的数据的工具“tibxread”

安克诺斯数据保护软件 会提供名为 tibxread 的工具，用于手动检查备份的磁盘完整性。该工具让您可以从备份中获取数据，并计算指定磁盘的哈希。该工具与以下组件一起自动安装：适用于 Windows 的代理程序、适用于 Linux 的代理程序和适用于 Mac 的代理程序。其位于以下位置：`C:\Program Files\Acronis\BackupAndRecovery`。

支持的位置为：

- 本地磁盘
- 无需使用凭据即可访问的网络文件夹 (CIFS/SMB)。
  如果网络文件夹受密码保护，可以使用操作系统工具将网络文件夹加载到本地文件夹，然后将本地文件夹用作该工具的来源。
- 云存储
  您应该提供 URL、端口和证书。可以从 Windows 注册表项或 Linux/Mac 计算机上的配置文件获得 URL 和端口。
  适用 Windows：

  ```
  HKEY_LOCAL_
  MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
  ult\<tenant_login>\FesUri
  ```

  适用 Linux：

  ```
  /etc/Acronis/BackupAndRecovery.config
  ```

  适用 macOS：

  ```
  /Library/Application Support/Acronis/Registry/BackupAndRecovery.config
  ```

  可以在以下位置中找到证书：
  适用 Windows：

  ```
  %allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
  ```

  适用 Linux：

  ```
  /var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

  适用 macOS：

  ```
  /Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

该工具具有以下命令：

- list backups
- list content
- get content
- calculate hash

list backups

列出备份中的恢复点。

概要：

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

选项

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

```
Output template:
```

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> – 备份 GUID。

<date> - 备份的创建日期。其格式为：DD.MM.YYYY HH24:MM:SS.默认采用本地时区(可以使用 --utc 选项进行更改) 。

输出示例：

```
GUID   Date   Date timestamp
----   ------ --------------
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

列出恢复点中的内容。

概要：

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

选项

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

输出模板：

```
Disk     Size   Notarization status
-------- ------ --------------------
<number> <size> <notarization_status>
```

<number> - 磁盘的标识符。

<size> - 以字节为单位的大小。

<notarization_status> - 可能的状态如下所示：未公证、已公证、下次备份。

输出示例：

```
Disk     Size   Notary status
-------- ------ --------------
1        123123465798 Notarized
2        123123465798 Notarized
```

get content

将恢复点中指定磁盘的内容写入到标准输出 (stdout)。

概要：

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

选项

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculate hash

使用 SHA-256 算法计算恢复点中指定磁盘的哈希，然后将它写入到 stdout。

概要：

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

选项

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

选项说明

选项	说明
--arc=BACKUP_NAME	可以从 Web 中控台的备份属性中获取的备份文件名。备份文件必须以扩展名 .tibx 进行指定。
--backup=RECOVERY_POINT_ID	恢复点标识符
--disk=DISK_NUMBER	磁盘号(与写入到“get content”命令的输出中的磁盘号相同)
--loc=URI	备份位置 URI。“--loc”选项的可能格式为: • 本地路径名称 (Windows) `c:/upload/backups` • 本地路径名称 (Linux) `/var/tmp` • SMB/CIFS `\\server\folder` • 云存储 `--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]` <IP_address> - 可以在 Windows 中的注册表项中找到它:HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri <path_to_certificate> - 用于访问 Cyber Cloud 的证书文件的路径。例如,在 Windows 中,该证书位于 `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<username>.crt`,其中 <username> 是用于访问 Cyber Cloud 的帐户名称。
--log=PATH	支持按指定的 PATH 写入日志(仅限本地路径,格式与 `--loc=URI` 参数相同)。日志记录级别为“DEBUG”。
--password=PASSWORD	备份的加密密码。如果不加密备份,请将该值保留为空。
--raw	在命令输出中隐藏标头(前两行)。在应解析命令输出时才会使用它。 不使用“`--raw`”的输出示例: `GUID Date Date timestamp` `---- ------ --------------` `516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865` `516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925` 使用“`--raw`”的输出:

	`` 516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865 516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925 ```
--utc	以 UTC 显示日期
--progress	显示操作的进度。 例如： ``` 1% 2% 3% 4% ... 100% ```

日志截断

此选项对 Microsoft SQL Server 数据库的备份和已启用 Microsoft SQL Server 应用程序备份的磁盘级备份有效。

此选项定义是否在成功备份后截断 SQL Server 事务日志。

预设为：**已启用**。

当启用此选项时，数据库只能恢复至此软件创建的备份的某个时间点。如果使用 Microsoft SQL Server 的本机备份引擎备份事务日志，则禁用此选项。您将能够在恢复后应用事务日志，从而将数据库恢复至任意时间点。

LVM 快照

此选项仅对物理机有效。

此选项对由 Linux 逻辑卷管理器 (LVM) 所管理卷的磁盘级备份有效。此类卷也称为逻辑卷。

此选项定义如何创建逻辑卷的快照。备份软件可自行完成此操作，也可以依赖 Linux 逻辑卷管理器 (LVM) 完成。

预设为：**通过备份软件**。

- **通过备份软件**。快照数据大部分保留在 RAM 中。备份更迅速，并且卷组中不需要有未分配的空间。因此，我们建议仅当您在备份逻辑卷遇到问题时才更改预设。
- **通过 LVM**。快照存储在卷组上的未分配空间。如果缺少未分配空间，则快照将由备份软件创建。

加载点

此选项仅对 Windows 中数据源的文件级备份有效，数据源包括已加载卷或群集共享卷。

此选项仅在备份层次结构高于加载点的文件夹时有效。(加载点是指逻辑上连接附加卷的文件夹。)

- 如果选择备份此类文件夹(父文件夹),并启用**加载点**选项,则位于已加载卷上的所有文件都会包含在备份中。如果禁用**加载点**选项,则备份中的加载点将为空。

  在父文件夹恢复过程中,加载点内容是否恢复取决于是否已启用恢复的**加载点**选项。
- 如果直接选择加载点,或者选择已加载卷中的文件夹,选定的文件夹将被视为普通文件夹。无论**加载点**选项的状态如何,都将备份普通文件夹;无论恢复的**加载点**选项状态如何,都将恢复普通文件夹。

预设为:**已禁用**。

注意

通过文件级备份来备份所需文件或整个卷,可以备份位于群集共享卷上的 Hyper-V 虚拟机。您只需关闭虚拟机,确保备份的状态一致。

示例

假定 **C:\Data1** 文件夹是已加载卷的加载点。该卷中包含文件夹 **Folder1** 和 **Folder2**。为数据的文件级备份创建一个保护计划。

如果选中卷"C"的复选框并启用**加载点**选项,则备份中的 **C:\Data1** 文件夹将包含 **Folder1** 和 **Folder2**。恢复备份数据时,请注意正确使用恢复的**加载点**选项。

如果选中卷"C"的复选框并禁用**加载点**选项,则备份中的 **C:\Data1** 文件夹将为空。

如果选中 **Data1**、**Folder1** 或 **Folder2** 文件夹的复选框,则选中的文件夹将包含在备份中作为普通文件夹,无论**加载点**选项的状态如何都是如此。

多卷快照

此选项对运行 Windows 或 Linux 的物理机备份有效。

此选项适用于磁盘级别备份。当文件级备份通过创建快照执行时,此选项也适用于文件级备份。("文件级备份快照"选项确定是否在文件级备份期间创建快照)。

此选项确定是同时还是逐个创建多个卷的快照。

预设为:

- 如果选择至少一个运行 Windows 的计算机用于备份:**已启用**。
- 如果未选择任何计算机(从**计划** > **备份**页开始创建保护计划时,可能会出现这种情况):**已启用**。
- 否则:**已禁用**。

如果启用此选项,则同时创建所有备份卷的快照。使用此选项对跨多个卷的数据(例如 Oracle 数据库)创建时间一致的备份。

如果禁用此选项,则逐个创建卷的快照。因此,如果数据跨多个卷,产生的备份可能不一致。

单击恢复

一键恢复允许用户自动恢复其计算机的最新磁盘备份。这可以是整台计算机的备份,也可以是这台计算机上特定磁盘或卷的备份。

管理员激活此功能后，即可在用户的计算机上使用 启动恢复管理器 访问此功能。管理员只能通过命令行界面执行此操作。要了解有关如何激活 启动恢复管理器 和一键恢复的更多信息，请参阅命令行参考。

一键恢复支持以下备份存储：

1. 安全区
2. 网络存储
3. 云存储

如果特定类型的存储不可用或其中没有磁盘备份，则会提示用户使用下一种存储类型。

如果存储中有多个包含磁盘备份的备份集（也称为*存档*），则一键恢复会选择上次更新的备份集。用户不能选择不同的备份集。

一键恢复支持以下操作：

- 从最新备份自动恢复
- 从自动选择的备份集中的特定备份（也称为*恢复点*）恢复

通过“一键恢复”恢复计算机

先决条件

- 管理员已在选定计算机上激活“一键恢复”。
- 选定计算机至少有一个磁盘备份。

恢复计算机

1. 重新启动要恢复的计算机。
2. 在重新启动期间，按 F11 键以进入 启动恢复管理器。
3. 选择所需的一键恢复选项：
   - 要自动恢复最新备份，请按键盘上的 1。
   - 要恢复上次更新备份集中的不同备份，请按键盘上的 2。
     - 要选择所需的备份（也称为*恢复点*），请按键盘上的相应数字。

图形用户界面会启动，然后消失。在没有它的情况下，恢复过程会继续。恢复完成后，计算机将重新启动。

性能和备份窗口

此选项使您能够设置一周中每小时的三个备份性能级别（高、低、禁止）之一。这样您可以定义何时允许备份开始和运行的时间窗口。高和低性能级别可根据进程优先级和输出速度进行配置。

此选项不可用于由云代理程序执行的备份，比如网站备份或位于云恢复站点上的服务器备份。

可以为保护计划中指定的每个位置分别配置此选项。要为复制位置配置此选项，请单击位置名称旁边的齿轮图标，然后单击**性能和备份窗口**。

此选项仅对备份和备份复制进程有效。备份后命令和包含在保护计划中的其他操作(验证、转换到虚拟机)都将运行而不管此选项如何。

预设为:**禁用**。

当禁用此选项时,通过以下参数允许备份随时运行(不管参数是否针对预设值进行了更改):

- CPU 优先级:**低**(在 Windows 中,对应于**正常以下**)。
- 输出速度:**无限制**。

当启用此选项时,根据为当前小时指定的性能参数允许或阻止预定的备份。在阻止备份时在某个小时的开始,备份进程将自动停止并生成警告。

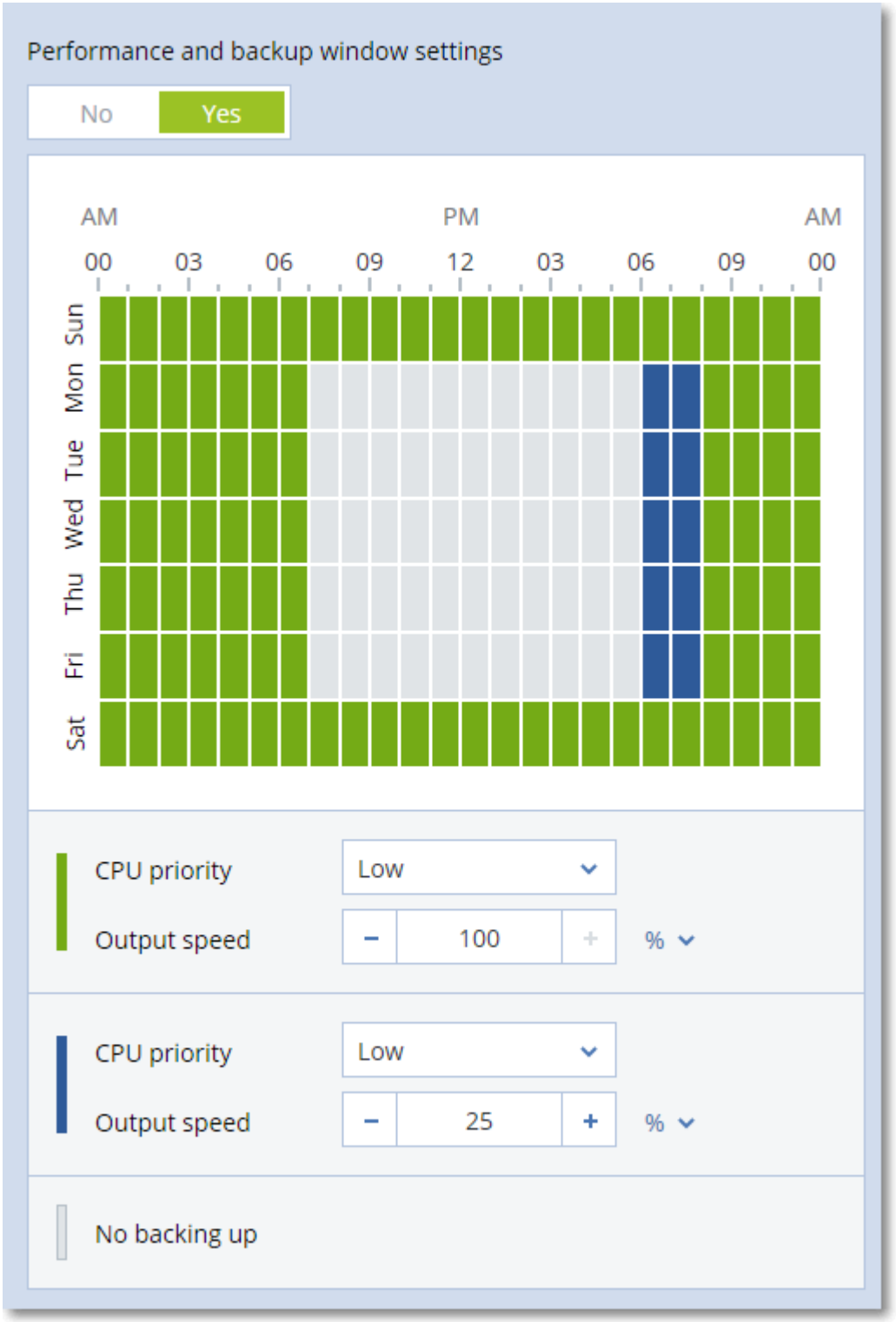
即使阻止了预定的备份,也可以手动启动备份。当允许备份时,它将使用最近小时的性能参数。

备份窗口

每个矩形代表一周中某天的某个小时。单击矩形以浏览以下状态:

- **绿色:**通过在下面绿色部分中指定的参数允许备份。
- **蓝色:**通过在下面蓝色部分中指定的参数允许备份。
  如果备份格式设置为**版本 11**,此状态不可用。
- **灰色:**阻止备份。

可以单击并拖动以便同时更改多个矩形的状态。



CPU 优先级

此参数定义操作系统中的备份进程的优先级。

可用设置包括：

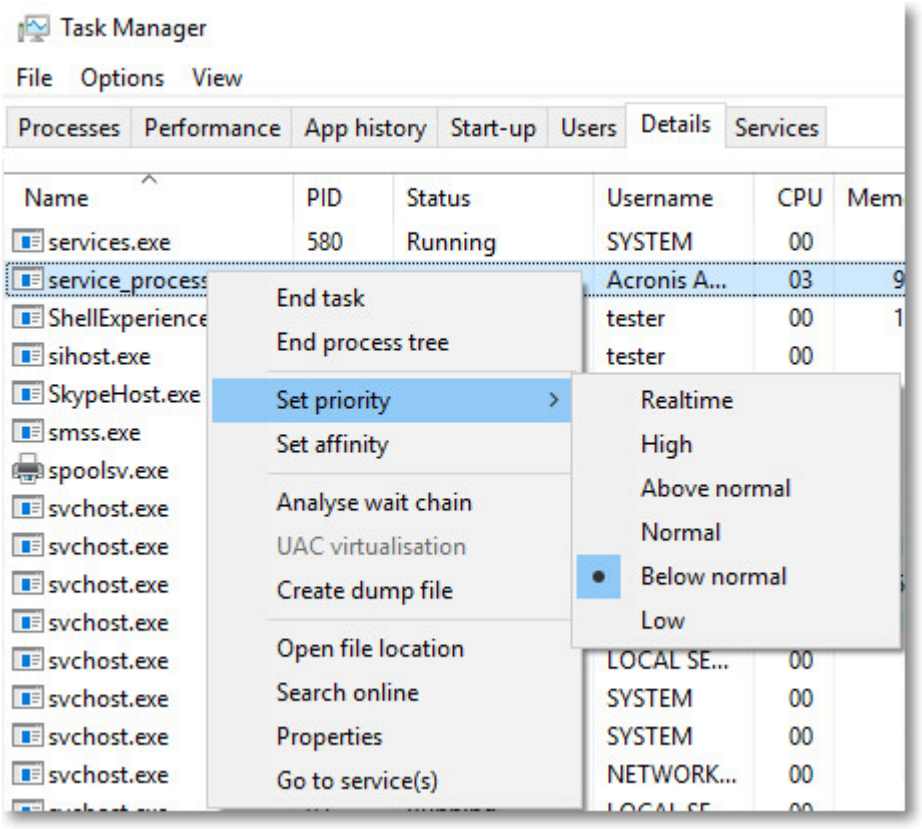
低 在 Windows 中，对应于 **正常以下**。

正常 在 Windows 中，对应于 **正常**。

高 - 在 Windows 中，对应于**高**。

系统中运行的进程的优先级决定分配给该进程的 CPU 使用量和系统资源。降低备份优先级，可释放出更多资源给其他应用程序。提高备份优先级，可加快备份进程，因为这将请求操作系统分配更多的资源（如 CPU 资源）至备份应用程序。不过，最终效果将取决于总 CPU 使用率，以及其他因素，如磁盘写入/读取速度或网络流量。

此选项在 Windows 中设置备份进程 (**service_process.exe**) 的优先级，以及在 Linux 和 OS X 中设置备份进程 (**service_process**) 的良好度。



备份期间的输出速度

此参数可使您限制硬盘写入速度（在备份至本地文件夹时）或通过网络传输备份数据的速度（在备份至网络共享或云存储时）。

启用此选项时，可以指定最大的允许输出速度：

- 以百分比形式表示目标硬盘的估计写入速度（在备份到本地文件夹时）或网络连接的估计最大速度（在备份到网络共享或云存储时）。
  此设置仅在代理程序在 Windows 中运行时有效。
- 单位为 KB/秒（针对所有目标）。

物理数据装运

如果备份目标是云存储并且备份格式设置为**版本 12**，则此选项有效。

此选项可用于由适用于 Windows 的代理程序、适用于 Linux 的代理程序、适用于 Mac 的代理程序、适用于 VMware 的代理程序和适用于 Hyper-V 的代理程序创建的磁盘级别备份和文件备份。不支持在可启动媒体下创建的备份。

此选项确定是否通过使用“物理数据装运”服务将保护计划创建的第一个完整备份发送到基于硬盘驱动器的云存储。后续增量备份可通过网络执行。

预设为：**已禁用**。

关于“物理数据装运”服务

“物理数据装运”服务 Web 界面仅适用于在本地部署中的组织管理员和云部署中的管理员。

有关使用“物理数据装运”服务和订单生成工具的详细说明，请参阅“物理数据装运管理员指南”。若要在“物理数据装运”服务 Web 界面中访问该文档，请单击问号图标。

物理数据装运过程的概述

1. 创建新的保护计划。在此计划中，启用**物理数据装运**备份选项。
   可以直接备份到驱动器，还可以备份到本地或网络文件夹，然后将备份复制/移动到驱动器。

   重要事项
   完成初始完整备份后，后续备份必须由同一保护计划执行。另一个保护计划（即使使用相同参数并针对同一台计算机）将需要另一个“物理数据装运”周期。

2. 在第一个备份完成后，使用“物理数据装运”服务 Web 界面来下载订单生成工具，并创建订单。
   要访问此 Web 界面，请执行以下任一操作：
   - 在本地部署中：登录到 Acronis 帐户，然后单击**物理数据装运**下的**转到追踪中控台**。
   - 在云部署中：登录到管理门户，依次单击**概述** > **使用情况**，然后单击**物理数据装运**下的**管理服务**。
3. 打包驱动器，然后将它们装运到数据中心。

   重要事项
   确保按照“物理数据装运管理员指南”中提供的打包说明进行操作。

4. 使用“物理数据装运”服务 Web 界面来跟踪订单状态。请注意，在初始备份上载到云存储之前，后续备份无法执行。

预/后命令

此选项让您可定义要在备份过程之前和之后自动执行的命令。

以下方案说明执行事前/事后命令的时间。

备份前命令	备份	备份后命令

事前/事后命令使用方法示例：

- 开始备份前，从磁盘中删除部分临时文件。
- 配置要在每次备份开始前启动的第三方防病毒产品。
- 选择性地将备份复制到其他位置。此选项可能非常有用，因为在保护计划中配置的复制会将每个备份都复制到后续位置。

此程序会在执行备份后命令之后执行复制。

此程序不支持互动命令，即需要用户输入的命令（如“pause”）。

备份前命令

若要指定备份程序开始前要执行的命令/批处理文件

1. 启用**在备份前执行命令**开关。
2. 在**命令...**字段中，键入命令或浏览并找到批处理文件。此程序不支持互动命令，即需要用户输入的命令（如“pause”）。
3. 在**工作目录**字段中，指定将执行命令/批处理文件所在目录的路径。
4. 在**参数**字段中，指定该命令的执行参数（如需要）。
5. 根据您要获得的结果，选择下表所述的相应选项。
6. 单击**完成**。

复选框	**选择**			
如果命令无法执行，备份将失败*	勾选	取消勾选	勾选	取消勾选
不要进行备份直至命令执行完毕	勾选	勾选	取消勾选	取消勾选
结果				
	预设 仅在命令成功执行后执行备份操作。如果命令无法执行，备份将失败。	执行命令后，无论命令执行成功与否，均会执行备份操作。	N/A	在执行命令时执行备份操作，无论命令执行结果如何。

*如果退出代码不等于 0，命令将视为失败。

备份后命令

若要指定在备份完成后要执行的命令/可执行文件

1. 启用**在备份后执行命令**开关。
2. 在**命令...**字段中，键入命令或浏览并找到批处理文件。

3. 在**工作目录**字段中，指定将执行命令/批处理文件所在目录的路径。
4. 在**参数**字段中，指定命令执行参数(如有必要)。
5. 如果成功执行命令对您极为重要，则选中**如果命令无法执行，备份将失败**复选框。如果退出代码不等于 0，命令将视为失败。如果命令执行失败，备份状态将设置为**错误**。
   如果未选中此复选框，则命令执行结果不会影响备份成功与否。可以通过浏览**活动**选项卡来跟踪命令执行结果。
6. 单击**完成**。

预/后数据捕获命令

此选项可让您定义在数据捕获(即创建数据快照)之前和之后要自动执行的命令。数据捕获将在备份过程开始时执行数据捕获。

以下方案说明执行数据捕获前/数据捕获后命令的时间。

<table>
<tr><td></td><td colspan="4"><---------- 备份 ----------></td><td></td></tr>
<tr><td>备份前命令</td><td>数据捕获前命令</td><td colspan="2">数据捕获</td><td>数据捕获后命令</td><td>备份后命令</td></tr>
</table>

如果已启用卷影复制服务选项，则命令执行与 Microsoft VSS 操作的顺序如下：

“数据捕获前”命令 -> VSS 暂停 -> 数据捕获 -> VSS 恢复 ->“数据捕获后”命令。

通过使用数据捕获前/数据捕获后命令，您可以暂停、恢复与 VSS 不兼容的数据库或应用程序。由于数据捕获只需数秒的时间，因此数据库或应用程序空闲时间将极短。

数据捕获前命令

若要指定数据捕获之前要执行的命令/批处理文件

1. 启用**在数据捕获前执行命令**开关。
2. 在**命令...**字段中，键入命令或浏览并找到批处理文件。此程序不支持互动命令，即需要用户输入的命令(如“pause”)。
3. 在**工作目录**字段中，指定将执行命令/批处理文件所在目录的路径。
4. 在**参数**字段中，指定该命令的执行参数(如需要)。
5. 根据您要获得的结果，选择下表所述的相应选项。
6. 单击**完成**。

复选框	**选择**			
如果命令无法执行，备份将失败*	勾选	取消勾选	勾选	取消勾选
不要进行数据捕获操作，直至	勾选	勾选	取消勾选	取消勾选

命令执行完毕				
结果				
	预设 仅在命令成功执行后执行备份操作。如果命令无法执行，备份将失败。	执行命令后，无论命令执行成功与否，均会执行备份操作。	N/A	在执行命令时执行备份操作，无论命令执行结果如何。

*如果退出代码不等于 0，命令将视为失败。

数据捕获后命令

若要指定数据捕获之前要执行的命令/批处理文件

1. 启用**在数据捕获后执行命令**开关。
2. 在**命令...**字段中，键入命令或浏览并找到批处理文件。此程序不支持互动命令，即需要用户输入的命令（如“pause”）。
3. 在**工作目录**字段中，指定将执行命令/批处理文件所在目录的路径。
4. 在**参数**字段中，指定该命令的执行参数（如需要）。
5. 根据您要获得的结果，选择下表所述的相应选项。
6. 单击**完成**。

复选框	选择			
如果命令无法执行，备份将失败*	勾选	取消勾选	勾选	取消勾选
不要进行备份直至命令执行完毕	勾选	勾选	取消勾选	取消勾选
结果				
	预设 仅在命令成功执行后执行备份操作。	执行命令后，无论命令执行成功与否，均会执行备份操作。	N/A	在执行命令时执行备份操作，无论命令执行结果如何。

*如果退出代码不等于 0，命令将视为失败。

SAN 硬件快照

此选项对 VMware ESXi 虚拟机的备份有效。

预设为：**已禁用**。

此选项可确定在执行备份时是否使用 SAN 快照。

如果此选项已禁用，则将从 VMware 快照读取虚拟磁盘内容。在整个备份期间将保留快照。

如果此选项已启用，则将从 SAN 快照读取虚拟磁盘内容。系统将创建 VMware 快照并使快照保持简洁，以使虚拟磁盘处于一致状态。如果无法从 SAN 快照读取，备份将失败。

在启用此选项之前，请检查并执行"使用 SAN 硬件快照"中列出的要求。

预定

此选项定义备份是按预定还是推迟启动，以及同时备份多少台虚拟机。

预设为：

- 本地部署：**严格按预定启动所有备份。**
- 云部署：**在时间窗口内分配备份开始时间。最长延迟时间：30 分钟。**

可选择以下其中一个选项：

- **严格按预定启动所有备份**

  物理机的备份将严格按预定启动。虚拟机将逐一进行备份。
- **在时间窗口内分配开始时间**

  物理机的备份将在与预定时间相比延迟的时间启动。将随机选择每台计算机的延迟值，范围为从零到您指定的最大值。将多台计算机备份至网络位置时您可能要使用此设置，以免网络负荷过重。将保护计划应用于计算机时会确定每台计算机的延迟值，并一直保留到编辑保护计划和更改最长延迟值为止。

  虚拟机将逐一进行备份。
- **限制同时运行的备份数量的方式**

  此选项仅在保护计划应用于多台虚拟机时才可用。此选项定义在执行给定保护计划时代理程序可以同时备份的虚拟机数量。

  如果根据保护计划，代理程序必须立即开始备份多台计算机，则该代理程序将选择 2 台计算机。(为了优化备份性能，代理程序将尝试匹配不同存储器上存储的计算机。)完成这 2 个备份其中任何一个后，代理程序将选择第 3 台计算机，依此类推。

  您可以选择代理程序可同步备份虚拟机的数量。最大值为 10。如果代理程序执行时间上重叠的多个保护计划，则会将其选项中指定的数量相加。可以限制代理程序可以同时备份的虚拟机总数，而无需考虑正在运行的保护计划数量。

  物理机的备份将严格按预定启动。

逐扇区备份

此选项仅对磁盘级备份有效。

此选项定义是否在物理级别上创建磁盘或卷的完全副本。

预设为：**已禁用**。

如果启用此选项，将备份所有磁盘或卷的扇区，包括未分配的空间和无数据的扇区。所生成的备份将与正在备份的磁盘大小相同(如果"压缩级别"选项设置为**"无"**)。当备份带有未识别或不受支持的文件系统的驱动器时，软件将自动切换到逐扇区模式。

注意
将无法从在逐扇区模式下创建的备份执行应用程序数据的恢复。

分割

此选项对于**始终完整**、**每周完整**，**每日增量**、**每月完整**、**每周差异和每日增量 (GFS)** 和**自定义**备份方案有效。

此选项可使您选择将大型备份分割为较小文件的方法。

预设为：**自动**。

可使用以下设置：

- **自动**
  如果备份超出文件系统所支持的最大文件大小，将分割该备份。
- **固定大小**
  输入所需的文件大小或从下拉列表中选择。

磁带管理

这些选项在备份目标为磁带设备时有效。

启用存储在磁带上的磁盘备份的文件恢复

预设为：**已禁用**。

如果选中此复选框，则每次备份时，软件会在已附加磁带设备的计算机的硬盘上创建辅助文件。只要这些辅助文件保持完好，就可以从磁盘备份进行文件恢复。当存储相应备份的磁带被擦除、删除或覆盖时，将自动删除这些文件。

辅助文件的位置如下：

- 在 Windows XP 和 Server 2003 中：**%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation**。
- 在 Windows 7 及更高版本的 Windows 中：**%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**。
- 在 Linux 中：**/var/lib/Acronis/BackupAndRecovery/TapeLocation**。

这些辅助文件占用的空间取决于相应备份中的文件数。对于包含约 20,000 个文件的磁盘的完整备份（典型工作站磁盘备份），辅助文件约占 150 MB。包含 250,000 个文件的服务器的完整备份可能产生约 700 MB 的辅助文件。因此，如果您确定不需要恢复个别文件，则可以清除此复选框以节省磁盘空间。

如果辅助文件在备份期间未创建或已删除，仍可以通过重新扫描存储备份的磁带来创建辅助文件。

每台计算机成功备份后将磁带移回插槽

预设为:**已启用**。

如果禁用此选项,则在完成使用磁带的操作后,该磁带仍会留在驱动器中。否则,软件会将磁带移回其在操作之前所在的插槽。根据保护计划,如果备份操作后紧跟其他操作(如备份验证或复制到其他位置),则磁带将在完成这些操作后移回到插槽。

如果同时启用了此选项和**每台计算机成功备份后弹出磁带**选项,则会弹出磁带。

每台计算机成功备份后弹出磁带

预设为:**已禁用**。

选中此复选框时,软件将在每台计算机成功备份后弹出磁带。根据保护计划,如果备份操作后紧跟其它操作(如备份验证或复制到另一位置),磁带将在完成这些操作后弹出。

创建完整备份时覆盖独立磁带驱动器中的磁带

预设为:**已禁用**。

此选项仅适用于独立磁带驱动器。启用此选项后,每次创建完整备份后都将覆盖插入驱动器的磁带。

使用以下磁带设备和驱动器

通过使用此选项,您可以指定要由保护计划使用的磁带设备和磁带驱动器。

无论是存储节点还是安装保护代理程序的计算机(或者两者兼有),磁带集区都包含附加到计算机的所有磁带设备的磁带存储节点。在将磁带集区选择用作备份位置后,可间接选择要将磁带设备附加到的计算机。默认情况下,可以通过附加到该计算机的任何磁带设备上的任何磁带驱动器将备份写入磁带。如果某些设备或驱动器丢失或不工作,保护计划将使用可用的设备或驱动器。

可以单击**仅所选设备和驱动器**,然后从列表中选择磁带设备和驱动器。通过选择整个设备,即可选择其所有驱动器。这意味着保护计划可以使用其中任何驱动器。如果所选设备或驱动器丢失或不工作并且未选择任何其他设备,则备份会失败。

通过使用此选项,可以控制多个代理程序执行到具有多个驱动器的大型磁带库的备份。例如,如果多个代理程序在同一个备份窗口期间备份其计算机,则备份大型文件服务器或文件共享可能不会开始,因为这些代理程序占用了所有驱动器。如果允许代理程序使用驱动器 2 和 3(假设),则驱动器 1 将为备份共享的代理程序保留。

多路数据流分用

预设为:**已禁用**。

多路数据流分用让您可以将数据从一个代理程序拆分为多个流,然后将这些流同时写入不同的磁带。这一功能可以加快备份速度,并且在代理程序的吞吐量高于磁带驱动器的吞吐量时特别有用。

仅当在**仅所选设备和驱动器**选项下选择多个磁带驱动器时，**多路数据流分用**复选框才可用。所选驱动器的数量等于代理程序中并发流的数量。如果备份开始时任何选定的驱动器都不可用，则该备份将失败。

要恢复带有多路数据流或兼有多路数据流及多路复用的备份，至少需要与用于创建该备份相同数量的驱动器。

无法更改现有保护计划的多路数据流分用设置。要使用其他设置或更改选定的磁带驱动器，请创建新的保护计划。

多路数据流分用可用于本地连接的磁带驱动器和连接到存储节点的磁带驱动器。

多路复用

预设为：**已禁用**。

多路复用让您可以将多个代理程序的数据流写入单个磁带。这一功能可以更好地利用快速磁带驱动器。默认情况下，多路复用因子（即，将数据发送到单个磁带的代理程序数量）设置为 2。可以将它提高到 10。

多路复用对于具有许多备份操作的大型环境很有用。它不会提高单个备份的性能。

为了在大型环境中实现最快的备份，需要分析代理程序、网络和磁带驱动器的吞吐量。然后，相应地设置多路复用因子，而无需过度多路复用。例如，如果代理程序提供数据的速率为 70 Mbit/s，磁带驱动器的写入速率为 250 Mbit/s，并且网络中不存在瓶颈，则将多路复用因子设置为 3。多路复用因子为 4 将导致过度多路复用且备份性能降低。通常，多路复用因子在 2 到 5 之间。

由于其结构，多路复用备份的恢复速度较慢。多路复用因子越大，恢复速度越慢。不支持同时恢复写入单个多路复用磁带的多个备份。

可以选择一个或多个特定磁带驱动器用于多路复用，也可以将多路复用选项与任何可用的磁带驱动器一起使用。多路复用不适用于本地连接的磁带驱动器。

无法更改现有保护计划的多路复用设置。要使用其他设置，请创建新的保护计划。

在保护计划中，可以如下组合多路数据流分用和多路复用：

- **同时清除多路数据流分用和多路复用选项。**
  每个代理程序将数据发送到单个磁带驱动器。
- **仅选择多路数据流分用选项。**
  每个代理程序同时将数据发送到至少两个磁带驱动器。
- **仅选择多路复用选项。**
  每个代理程序将数据发送到磁带驱动器，该磁带驱动器同时接受来自多个代理程序的流。磁带驱动器可以接受的最大流数量已在保护计划中设置，无法即时更改。
- **同时选择多路数据流分用和多路复用选项。**
  每个代理程序将数据发送到至少两个磁带驱动器，这些磁带驱动器同时接受来自多个代理程序的流。

磁带驱动器一次只能写入一种类型的备份(多路复用或非多路复用),具体取决于先启动的保护计划。

将磁带集区中所选的磁带集用于备份

预设为:**已禁用**。

一个集区内的磁带可分组为所谓的**磁带集**。

如果禁用此选项,则数据将在属于一个集区的所有磁带上进行备份。如果启用此选项,则您可以根据预定义或自定义规则分开备份。

- **针对每个使用单独的磁带集**(选择规则:**备份类型**、**设备类型**、**设备名称**、**该月的哪一天**、**星期几**、**月份**、**年**、**日期**)
  如果选择此变量,则您可以根据预定义规则安排磁带集。例如,您可以针对一周的每一天使用单独的磁带集,或者在单独的磁带集中存储每台计算机的备份。
- **为磁带集指定自定义规则**
  如果选择此变量,则指定您自己安排磁带集的规则。此规则可以包含以下变量:

变量语法	变量描述	可用值
[Resource Name]	每台计算机的备份将存储于单独的磁带集。	在管理服务器上注册的计算机的名称。
[Backup Type]	完整、增量和差异备份将存储于单独的磁带集。	full, inc, diff
[Resource Type]	每种类型计算机的备份将存储于单独的磁带集。	Server essentials, Server, Workstation, Physical machine, VMware Virtual Machine, Virtual-PC Virtual Machine, Virtual Server Virtual Machine, Hyper-V Virtual Machine, Parallels Virtual Machine, XEN Virtual Machine, KVM Virtual Machine, RHEV Virtual Machine, Parallels Cloud Virtual Machine
[Day]	一个月的每一天所创建的备份将存储于单独的磁带集。	01、02、03、...、31
[Weekday]	一周的每一天所创建的备份将存储于单独的磁带集。	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
[Month]	一年的每个月所创建的备份将存储于单独的磁带集。	January, February, March, April, May, June, July, August, September, October, November, December
[Year]	每年所创建的备份将存储于单独的磁带集。	2017、2018、...

- 例如，如果将规则指定为 [Resource Name]-[Backup Type]，则对于应用保护计划的每台计算机的每个完整备份、增量备份和差异备份，您都会有一个单独的磁带集。

您还可以为各个磁带指定磁带集。在这种情况下，软件会首先在磁带集值与保护计划中指定的表达式的值一致的磁带上写入备份。如有必要，将使用同一集区的其他磁带。之后，如果集区可补充，则将使用**可用磁带**集区的磁带。

例如，如果您为磁带 1 指定磁带集 Monday、为磁带 2 指定磁带集 Tuesday（以此类推），并在备份选项中指定 [Weekday]，则在该周的星期几将使用相应磁带。

任务失败处理

此选项决定保护计划预定执行失败时的程序行为。手动启动保护计划时，此选项无效。

如果启用此选项，程序将再次尝试执行保护计划。您可以指定尝试次数和尝试时间间隔。一旦尝试成功完成或已执行指定尝试次数（以首先发生的为准），程序将停止尝试。

预设为：**已禁用**。

任务开始条件

此选项在 Windows 和 Linux 操作系统下有效。

此选项决定任务即将开始（预定时间已到或时间表中指定的事件已发生），但条件（或多个条件之一）未满足时的程序行为。有关条件的更多信息，请参阅“开始条件”。

预设为：**等待至满足所有预定条件。**

等待直至满足所有预定条件

采用此设置后，预定程序开始监视条件，并会在条件满足时启动任务。如果一直不能满足条件，则任务将不会开始。

为了处理长时间不能满足条件，而进一步延迟任务会产生风险的情况，可以设置时间间隔，在此时间间隔后无论条件是否得到满足，任务都将运行。勾选**在此时间后务必运行任务**复选框，并指定时间间隔。任务将在条件满足或达到最长延迟时间后开始，以首先发生的为准。

跳过任务执行

任务的延迟可能是不可接受的，例如，您需要严格在指定时间执行任务。因此，合理的方案是跳过任务而非等待条件得到满足（尤其是当任务发生频率较高时）。

卷影复制服务 (VSS)

此选项仅对 Windows 操作系统有效。

此选项定义卷影复制服务 (VSS) 供应商是否必须通知 VSS 可感知的应用程序，备份即将开始。这确保了应用程序使用的所有数据的一致状态，特别是在备份软件创建数据快照时，确保所有数据库事务都已完成。而数据一致性则确保了应用程序可恢复至正确的状态，并在恢复后立即可用。

预设为：**已启用**。**自动选择快照提供程序**。

可选择以下其中一个选项：

- **自动选择快照提供程序**
  在硬件快照提供程序、软件快照提供程序和 Microsoft 软件卷影副本提供程序之间自动进行选择。
- **使用 Microsoft Software Shadow Copy Provider**
  我们建议您在备份应用程序服务器(Microsoft Exchange Server、Microsoft SQL Server、Microsoft SharePoint 或 Active Directory)时选择此选项。

如果数据库与 VSS 不兼容，请禁用此选项。快照创建速度更快，但在创建快照时无法保证尚未完成事务的应用程序的数据一致性。您可以使用数据捕获前/后命令来确保数据在一致的状态下进行备份。例如，指定暂停数据库并清除所有缓存的数据捕获前命令，以确保完成所有事务；并指定创建快照后恢复数据库运行的数据捕获后命令。

注意
如果启用此选项，则将不会备份在 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** 注册表项中指定的文件和文件夹。尤其是，系统将不备份离线 Outlook 数据文件 (.ost)，因为此注册表项的 **OutlookOST** 值中指定了这些文件。

启用 VSS 完整备份

如果启用此选项，则 Microsoft Exchange Server 和其他 VSS 感知应用程序(Microsoft SQL Server 除外)的日志将在每次成功执行完整、增量或差异磁盘级备份后截断。

预设为：**已禁用**。

请在下列情况下使此选项保持禁用状态：

- 如果您使用适用于 Exchange 的代理程序或第三方软件来备份 Exchange Server 数据。这是因为日志截断将会影响连续的事务日志备份。
- 如果您使用第三方软件备份 SQL Server 数据。原因是第三方软件会将最终磁盘级备份视为其"自身"完整备份。因此，SQL Server 数据的下一次差异备份将会失败。将一直无法进行备份，除非第三方软件创建下一个"自身"完整备份。
- 如果其他 VSS 感知应用程序正在计算机上运行，并且您由于任何原因需要保留日志。

启用此选项不会导致 Microsoft SQL Server 日志截断。若要在备份后截断 SQL Server 日志，请启用日志截断备份选项。

适用于虚拟机的卷影复制服务 (VSS)

此选项定义是否创建虚拟机的静止快照。若要创建静止快照，备份软件将通过使用 VMware Tools 或 Hyper-V Integration Services 在虚拟机内应用 VSS。

预设为：**已启用**。

如果启用此选项，在虚拟机中运行的所有 VSS 感知应用程序的事务都将在创建快照前完成。如果静止快照在“错误处理”选项中指定的重试次数后失败，并且应用程序备份处于禁用状态，则创建非静止快照。如果启用应用程序备份，备份将失败。

如果禁用此选项，将创建非静止快照。将在故障一致状态下备份虚拟机。我们建议您始终保持该选项启用，即使是不运行 VSS 感知应用程序的虚拟机。否则，在已捕获的备份中连文件系统的一致性也无法保证。

注意
该选项不会影响 Scale Computing HC3 虚拟机。对于这些虚拟机来说，是否停止运行取决于是否在虚拟机上安装了 Scale 工具。

每周备份

此选项决定“每周”在保留规则和备份方案中考虑哪些备份。“每周”备份是在一周开始后创建的第一个备份。

预设为：**周一**。

Windows 事件日志

此选项仅在 Windows 操作系统下有效。

此选项定义代理程序是否必须在 Windows 应用程序事件日志中记录备份操作的事件（要查看此日志，请运行 eventvwr.exe 或依次选择**控制面板** > **管理工具** > **事件查看器**）。您可以筛选要记录的事件。

预设为：**已禁用**。

恢复

恢复速查表

下表总结了可用的恢复方法。使用该表选择最符合您需求的恢复方法。

恢复内容	恢复方法
物理机(Windows 或 Linux)	使用 Web 界面 使用可启动媒体
物理机 (Mac)	使用可启动媒体
虚拟机(VMware、Hyper-V 或 Scale Computing HC3)	使用 Web 界面 使用可启动媒体
ESXi 配置	使用可启动媒体
文件/文件夹	使用 Web 界面 从云存储下载文件 使用可启动媒体 从本地备份提取文件
系统状态	使用 Web 界面
SQL 数据库	使用 Web 界面
Exchange 数据库	使用 Web 界面
Exchange 邮箱	使用 Web 界面
Microsoft 365 邮箱	使用 Web 界面
Oracle 数据库	使用 Oracle Explorer 工具

Mac 用户注意事项

- 从 10.11 El Capitan 开始，会对某些系统文件、文件夹和进程进行标记，以保护扩展的文件属性 com.apple.rootless。此功能称为系统完整性保护 (SIP)。受保护的文件包括预安装的应用程序和 /system、/bin、/sbin、/usr 中的大部分文件夹。

  受保护的文件和文件夹在操作系统下恢复时无法覆盖。如果需要覆盖受保护的文件，请执行可启动媒体下的恢复。
- 从 macOS Sierra 10.12 开始，通过“云中的存储”功能可将很少使用的文件移至 iCloud。如果这些文件占用空间较小，则继续留在文件系统上。将备份这些占用空间较小的文件，而不是保留原始文件。

当将占用文件恢复到原始位置时，它将与 iCloud 同步，并且原始文件可用。当将占用文件恢复到其他位置时，它不会同步，原始文件将不可用。

安全恢复

操作系统的备份映像可能已感染恶意软件，并可能重新感染正在恢复的计算机。

“安全恢复”功能让您可以通过在恢复过程中使用集成的反恶意软件扫描和“恶意软件删除”来防止感染再次发生。

限制：

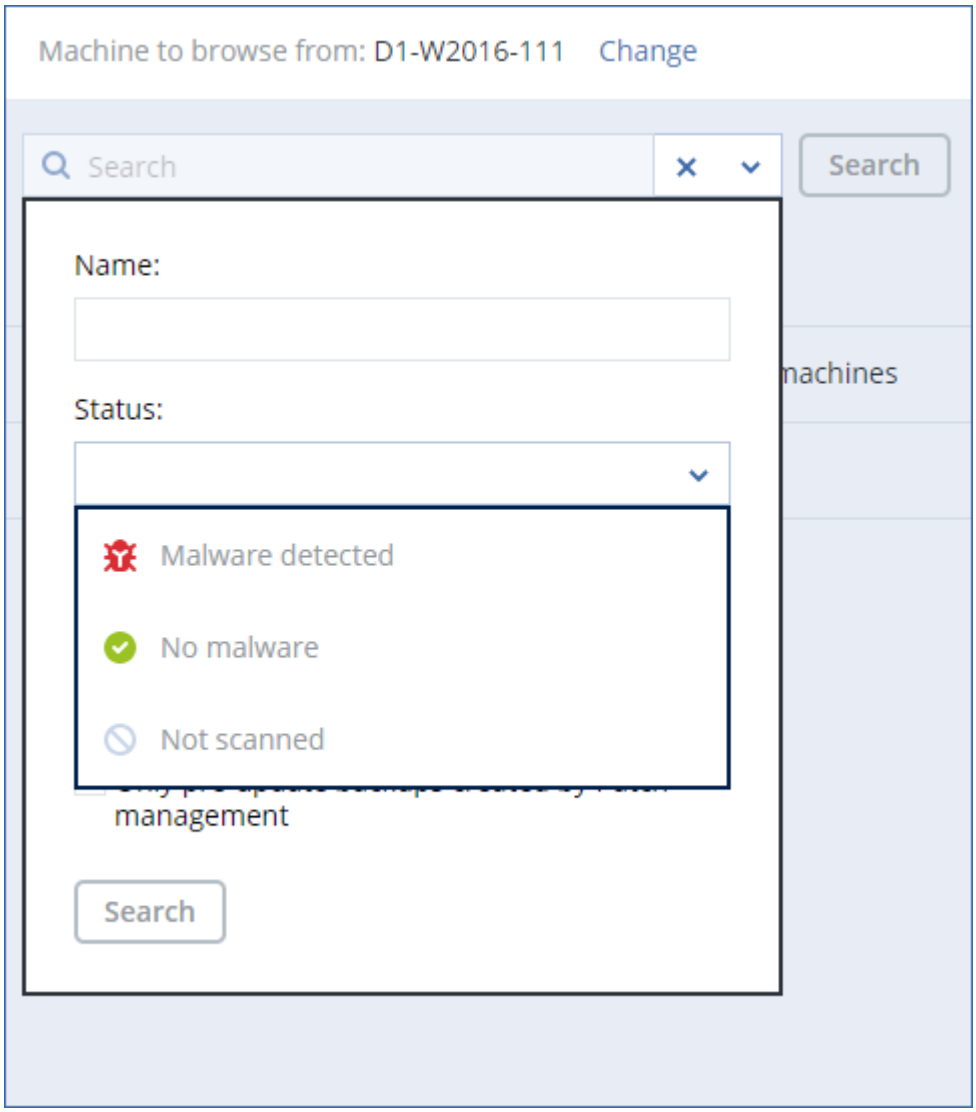
- “安全恢复”仅支持用于内部安装有适用于 Windows 的代理程序的 Windows 物理机或虚拟机。
- 仅支持类型为**“整台计算机”**或**“磁盘/卷”**的备份。
- 仅支持用于文件系统为 NTFS 的卷。非 NTFS 分区将在不执行反恶意软件扫描的情况下进行恢复。
- “安全恢复”不支持用于连续数据保护 (CDP) 备份。将基于上次常规备份恢复计算机，而不会使用 CDP 备份中的数据。要恢复 CDP 数据，请运行**文件/文件夹**恢复。

工作方式

如果在恢复过程中启用“安全恢复”选项，则系统将执行以下操作：

1. 扫描映像备份来查找恶意软件并标记被感染的文件。将为备份指派以下状态之一：
   - **无恶意软件** - 扫描过程中未在备份中发现恶意软件。
   - **检测到恶意软件** - 扫描过程中在备份中发现恶意软件。
   - **未扫描** - 未对备份进行扫描以查找恶意软件。
2. 将备份恢复到选定的计算机。
3. 删除检测到的恶意软件。

可以使用**状态**参数过滤备份。



创建可启动媒体

可启动媒体是一个 CD、DVD、USB 闪存驱动器或其他可移动媒体，可使您无需操作系统的帮助即可运行代理程序。可启动媒体的主要用途是恢复无法启动的操作系统。

我们强烈建议您在开始使用磁盘级备份后立即创建并测试可启动媒体。此外，每次保护代理程序发生重要更新后都重新创建该媒体也是良好的做法。

您可以使用相同的媒体恢复 Windows 或 Linux。要恢复 macOS，请在运行 macOS 的计算机上创建单独的媒体。

在 Windows 或 Linux 中创建可启动媒体

1. 下载可启动媒体 ISO 文件。要下载文件，请依次单击右上角的帐户图标 > **下载** > **可启动媒体**。
2. 请执行以下任一操作：
   - 使用 ISO 文件刻录 CD/DVD。
   - 通过使用 ISO 文件和网上提供的免费工具之一创建可启动 USB 闪存驱动器。

如果您需要启动 UEFI 计算机，请使用 ISO 到 USB 或 RUFUS；对于 BIOS 计算机，请使用 Win32DiskImager。在 Linux 中，使用 dd 实用工具较合理。

- 将 ISO 文件作为 CD/DVD 驱动器连接到要恢复的虚拟机。

您还可以使用可启动媒体生成器创建可启动媒体。

在 macOS 中创建可启动媒体

1. 在安装了适用于 Mac 的代理程序的计算机上，依次单击**应用程序** > **应急媒体生成器**。
2. 软件将显示连接的可启动媒体。选择要使其成为可启动媒体的媒体。

警告！
将擦除磁盘上的所有数据。

3. 单击**创建**。
4. 等待软件创建可启动媒体。

恢复计算机

恢复物理机

本部分介绍如何使用 安克诺斯数据保护软件 Web 中控台恢复物理机。

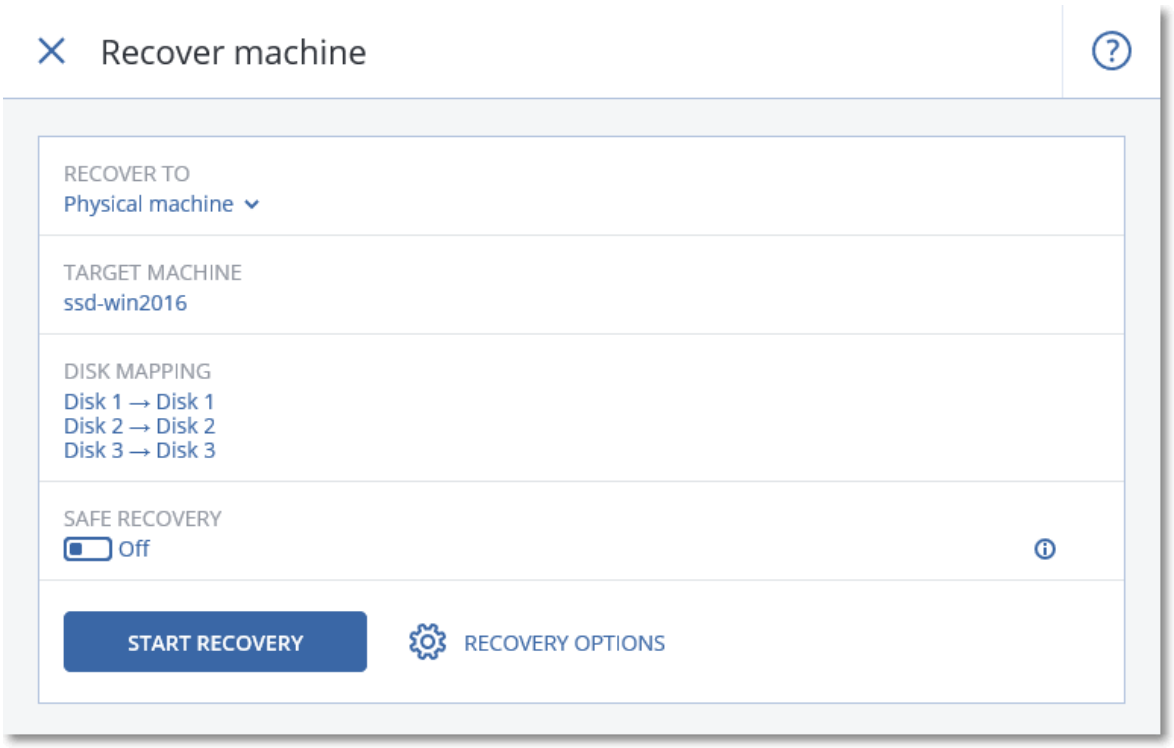
如果需要恢复以下任何内容，请使用可启动媒体，而不是 安克诺斯数据保护软件 Web 中控台：

- macOS 操作系统
- 将任何操作系统恢复至裸机或脱机计算机
- 逻辑卷（Linux 中逻辑卷管理器所创建的卷）的结构。媒体可让您自动重新创建逻辑卷结构。

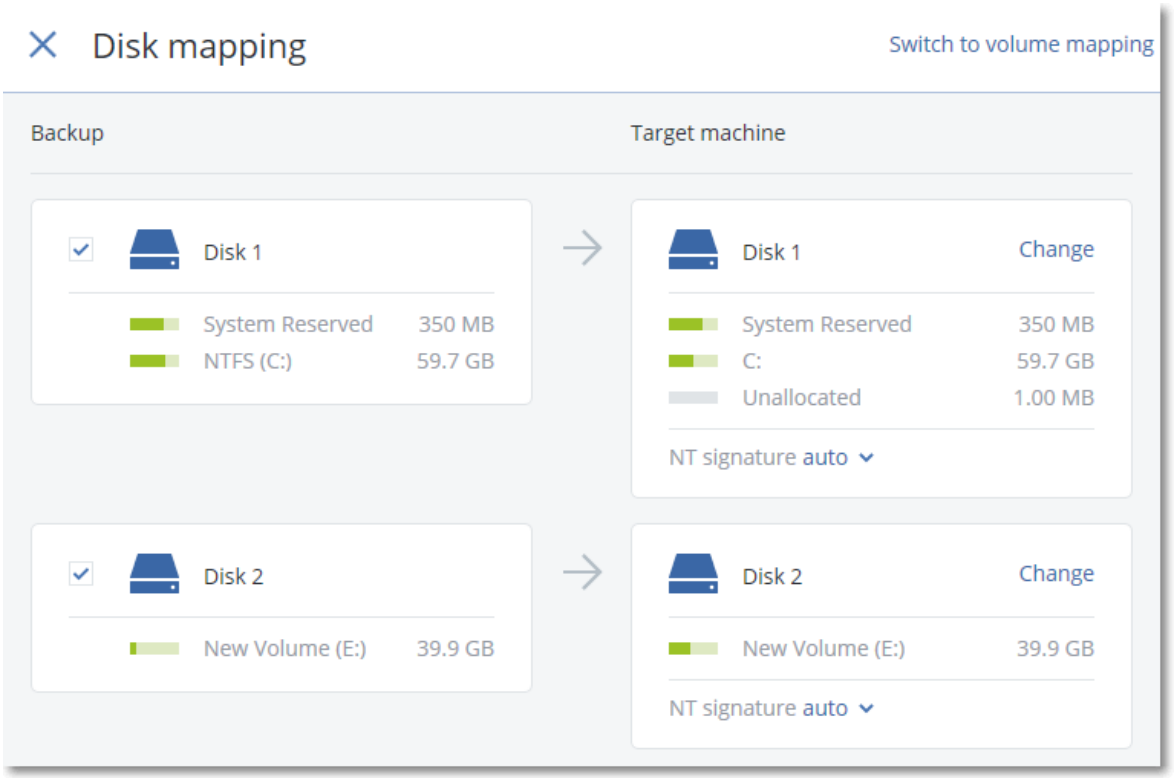
恢复操作系统和恢复使用 BitLocker 或 CheckPoint 加密的卷需要重新启动。有关详细信息，请参阅 "重新启动时恢复"（第 276 页）。

恢复至物理机

1. 选择已备份的计算机。
2. 单击**恢复**。
3. 选择恢复点。请注意，恢复点按位置过滤。
   如果计算机处于脱机状态，将不显示恢复点。请执行以下任一操作：
   - 如果备份位置是云或共享存储（即其他代理程序可以访问它），单击**选择计算机**，选择处于联机状态的目标计算机，然后选择恢复点。
   - 在备份存储选项卡上选择一个恢复点。
   - 按“使用可启动媒体恢复磁盘”中所述的方法恢复计算机。
4. 依次单击**恢复** > **整台计算机**。
   软件会将磁盘从备份自动映射到目标计算机的磁盘。
   若要恢复至另一台物理机，请单击**目标计算机**，然后选择处于联机状态的目标计算机。



5. 如果您对映射结果不满意，或者磁盘映射失败，请单击**磁盘映射**以手动重新映射磁盘。
   此外，在映射部分中，可以选择要恢复的个别磁盘或卷。可以使用右上角的**切换至...**链接，在恢复磁盘和卷之间切换。



6. [可选] 启用**安全恢复**开关来扫描备份中是否存在恶意软件。如果检测到恶意软件，将在备份中对该恶意软件进行标记并在恢复过程完成后立即删除它。
7. 单击**开始恢复**。

8. 确认要将磁盘覆盖为其备份版本。选择是否自动重新启动计算机。

恢复进度显示在**活动**选项卡上。

将物理机恢复到虚拟机

可以将物理机的备份恢复到虚拟机。

如果在您的环境中至少已安装一个相关目标虚拟机监控程序的代理程序并在管理服务器上注册，则可以恢复到虚拟机。例如，恢复到 VMware ESXi 需要在环境中安装适用于 VMware 的代理程序并在管理服务器上进行注册。

某些选项仅适用于云部署。

有关物理机到虚拟机迁移 (P2V) 的支持路径的详细信息，请参阅 "计算机迁移"(第 434 页)。

注意
无法将 macOS 物理机的备份恢复为虚拟机。

将物理机恢复为虚拟机

1. 选择已备份的计算机。
2. 单击**恢复**。
3. 选择恢复点。请注意，恢复点按位置过滤。
   如果计算机处于脱机状态，将不显示恢复点。请执行以下任一操作：
   - 如果备份位置是云或共享存储(即，其他代理程序可以访问它)，请单击**选择计算机**、选择处于联机状态的目标计算机，然后选择恢复点。
   - 在备份存储选项卡上选择一个恢复点。
   - 恢复计算机，如 "使用可启动媒体恢复磁盘和卷"(第 277 页) 中所述。
4. 依次单击**恢复** > **整台计算机**。
5. 在**恢复至**中，选择**虚拟机**。
6. 单击**目标计算机**。
   a. 选择虚拟机监控程序。

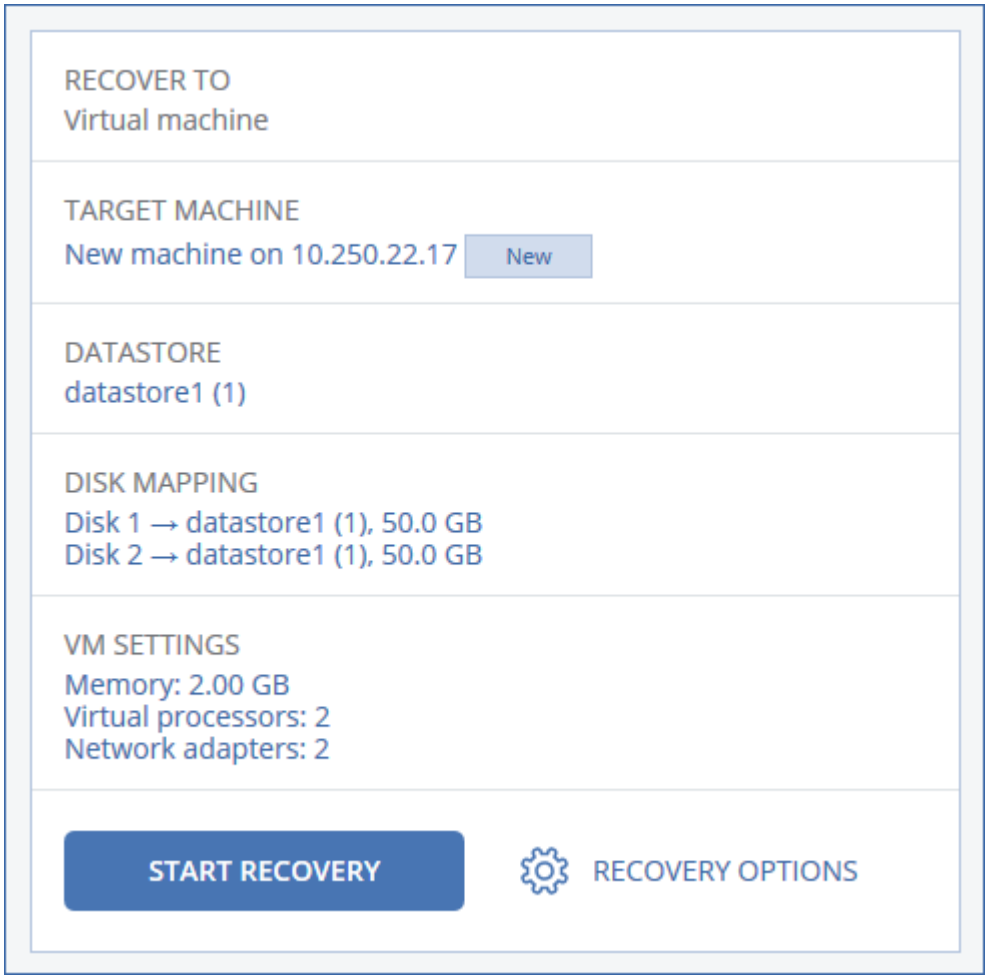
      注意
      该虚拟机监控程序的至少一个代理程序必须安装在您的环境中，并在管理服务器上进行注册。

   b. 选择恢复至新计算机还是现有计算机。由于新的计算机选项不需要目标计算机的磁盘配置与备份中的磁盘配置完全匹配，因此该选项优先。。
   c. 选择主机并指定新计算机名称，或选择现有目标计算机。
   d. 单击**确定**。
7. [对于 Virtuozzo Hybrid Infrastructure] 单击 **VM 设置**，然后选择**规格**。或者，可以更改虚拟机的内存大小、处理器数量和网络连接。
8. [可选] [当恢复到新计算机时] 配置所需的其他恢复选项：

- [不适用于 Virtuozzo Hybrid Infrastructure 和 Scale Computing HC3] 要为虚拟机选择数据存储，请针对 ESXi 单击**数据存储**、针对 Hyper-V 和 Virtuozzo 单击**路径**或针对 Red Hat Virtualization (oVirt) 单击**存储域**，然后为虚拟机选择数据存储（存储）。
- 要为每个虚拟磁盘选择数据存储（存储）、接口和调配模式，请单击**磁盘映射**。在映射部分中，可以选择要恢复的个别磁盘。

注意
如果正在恢复 Virtuozzo 容器或 Virtuozzo Hybrid Infrastructure 虚拟机，则无法更改这些设置。对于 Virtuozzo Hybrid Infrastructure，只能为目标磁盘选择存储策略。为此，选择所需的目标磁盘，然后单击**更改**。在打开的刀片中，单击齿轮图标、选择存储策略，然后单击**完成**。

- [适用于 VMware ESXi、Hyper-V、Virtuozzo 和 Red Hat Virtualization/oVirt] 要更改虚拟机的内存大小、处理器的数量和网络连接，请单击 **VM 设置**。



9. 单击**开始恢复**。
10. [当恢复到现有虚拟机时] 确认要覆盖磁盘。

恢复进度显示在**活动**选项卡上。

恢复虚拟机

可以将虚拟机的备份恢复到物理机或另一个虚拟机。

如果在您的环境中至少已安装一个相关目标虚拟机监控程序的代理程序并在管理服务器上注册，则可以恢复到虚拟机。例如，恢复到 VMware ESXi 需要在环境中安装适用于 VMware 的代理程序并在管理服务器上进行注册。

某些选项仅适用于云部署。

有关虚拟机到物理机 (V2P) 或虚拟机到虚拟机 (V2V) 迁移的支持路径的详细信息，请参阅 "计算机迁移"(第 434 页)。

注意
由于 Hyper-V 不支持 macOS，因此无法将 macOS 虚拟机恢复到 Hyper-V 主机。可以将 macOS 虚拟机恢复为在 Mac 硬件上安装的 VMware 主机。

重要事项
将另一台计算机恢复到虚拟机时，必须停止该虚拟机。默认情况下，该软件会在无提示的情况下停止计算机运行。在恢复完成后，必须手动启动计算机。可通过使用 VM 电源管理恢复选项（依次单击**恢复选项** > **VM 电源管理**），来更改默认行为。

恢复虚拟机

1. 请执行以下任一操作：
   - 选择备份计算机，单击**恢复**，然后选择恢复点。
   - 在备份存储选项卡上选择一个恢复点。
2. 依次单击**恢复** > **整台计算机**。
3. [当恢复到物理机时] 在**恢复到**中，选择**物理机**。
   仅当目标计算机的磁盘配置与备份中的磁盘配置完全匹配时，才可以恢复到物理机。如果是这种情况，请继续进行 "恢复物理机"(第 271 页) 中的第 4 步。否则，建议您使用可启动媒体执行虚拟机到物理机 (V2P) 迁移。
4. [可选] 默认情况下，选择原始计算机作为目标计算机。若要恢复至另一台虚拟机，请单击**目标计算机**，然后执行以下操作：
   a. 选择虚拟机监控程序。

      注意
      该虚拟机监控程序的至少一个代理程序必须安装在您的环境中，并在管理服务器上进行注册。

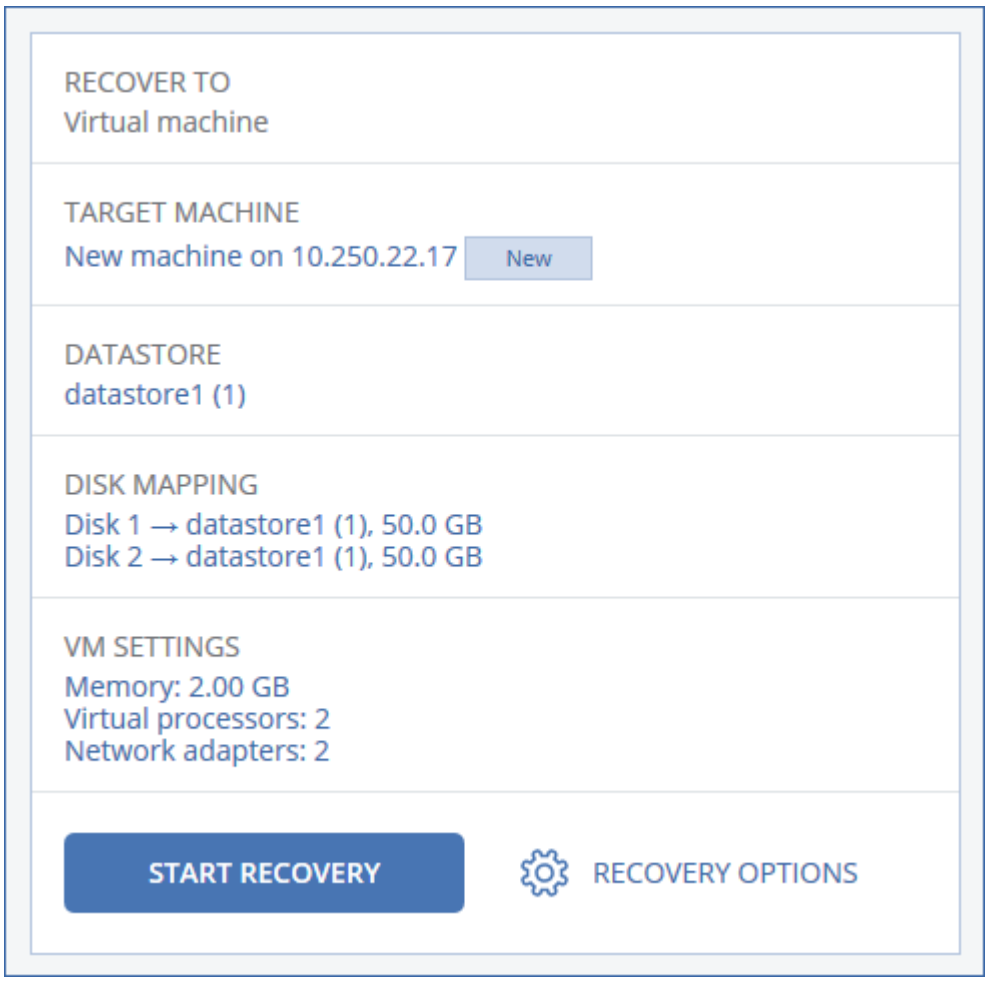
   b. 选择恢复至新计算机还是现有计算机。
   c. 选择主机，然后指定新的计算机名称，或者选择现有目标计算机。
   d. 单击**确定**。
5. [对于 Virtuozzo Hybrid Infrastructure] 单击 **VM 设置**，然后选择**规格**。或者，可以更改虚拟机的内存大小、处理器数量和网络连接。
6. [可选] [当恢复到新计算机时] 配置所需的其他恢复选项：
   - [不适用于 Virtuozzo Hybrid Infrastructure 和 Scale Computing HC3] 要为虚拟机选择数据存储，请针对 ESXi 单击**数据存储**、针对 Hyper-V 和 Virtuozzo 单击**路径**或针对 Red Hat

Virtualization (oVirt) 单击**存储域**，然后为虚拟机选择数据存储（存储）。

- 要为每个虚拟磁盘选择数据存储（存储）、接口和调配模式，请单击**磁盘映射**。在映射部分中，可以选择要恢复的个别磁盘。

  注意
  如果正在恢复 Virtuozzo 容器或 Virtuozzo Hybrid Infrastructure 虚拟机，则无法更改这些设置。对于 Virtuozzo Hybrid Infrastructure，只能为目标磁盘选择存储策略。为此，选择所需的目标磁盘，然后单击**更改**。在打开的刀片中，单击齿轮图标、选择存储策略，然后单击**完成**。

- [适用于 VMware ESXi、Hyper-V、Virtuozzo 和 Red Hat Virtualization/oVirt] 要更改虚拟机的内存大小、处理器的数量和网络连接，请单击 **VM 设置**。



7. 单击**开始恢复**。
8. [当恢复到现有虚拟机时] 确认要覆盖磁盘。

恢复进度显示在**活动**选项卡上。

重新启动时恢复

恢复以下内容时需要重新启动：

- 操作系统
- BitLocker 或 CheckPoint 加密的卷

重要事项
已备份的加密卷会恢复为未加密卷。

要求

- 恢复加密的卷需要在同一台计算机上有一个未加密的卷，并且该卷至少有 1 GB 的可用空间。否则，恢复将失败。
- 恢复加密的系统卷不需要任何其他的操作。要恢复加密的非系统卷，必须先将其锁定(例如，通过打开驻留在该卷上的文件)。否则，恢复将在不重新启动的情况下继续，并且 Windows 可能无法识别已恢复卷。

疑难解答

如果恢复失败且计算机重新启动后显示“无法从分区获取文件”错误，则禁用“安全启动”。有关如何执行此操作的详细信息，请参阅 Microsoft 文档中的禁用安全启动。

使用可启动媒体恢复磁盘和卷

有关如何创建可启动媒体的信息，请参阅 "创建可启动媒体"(第 270 页)。

使用可启动媒体恢复磁盘或卷

1. 通过使用可启动媒体启动目标计算机。
2. [仅适用于 macOS] 如果要将 APFS 格式的卷恢复到非原始计算机或裸机，请手动重新创建原始磁盘配置：
   a. 单击**磁盘实用工具**。
   b. 重新创建原始磁盘配置。有关说明，请参阅 https://support.apple.com/guide/disk-utility/welcome。
   c. 依次单击**磁盘实用工具 > 退出磁盘实用工具**。

   注意
   从 macOS 11 Big Sur 开始，无法备份和恢复系统卷。要恢复可启动 macOS 系统，需要恢复数据卷，然后在其上安装 macOS。
3. 单击**本地管理此计算机**或单击**应急可启动媒体**两次，具体取决于您要使用的媒体类型。
4. 如果在网络中启用代理服务器，请依次单击**工具 > 代理服务器**，然后指定代理服务器主机名/IP 地址和端口。否则，请跳过此步骤。
5. 在欢迎屏幕上，单击**恢复**。
6. 单击**选择数据**，然后单击**浏览**。
7. 指定备份位置：
   - 若要从云存储中恢复，请选择**云存储**。输入备份计算机分配到的帐户的凭据。

- 若要从本地或网络文件夹恢复，请浏览到**本地文件夹**或**网络文件夹**下的文件夹。

单击**确定**确认您的选择。

8. 选择要从其中恢复数据的备份。如果出现提示，请键入备份的密码。
9. 在**备份内容**中，选择**磁盘**或**卷**，然后选择要恢复的项目。单击**确定**确认您的选择。

   重要事项
   如果备份的计算机具有动态磁盘或逻辑卷 (LVM)，请选择**卷**。

10. 在**恢复位置**下，软件会将选定的磁盘自动映射到目标磁盘。
    如果映射不成功或者您对映射结果不满意，可以手动重新映射磁盘。

    注意
    更改磁盘布局可能会影响操作系统可启动性。请使用原始计算机的磁盘布局，除非您对成功完全有信心。

11. [仅适用于 macOS] 要将 APFS 格式的数据卷恢复为可启动 macOS 系统，请在 **macOS 安装**部分中，保持选中**在已恢复的 macOS 数据卷上安装 macOS** 复选框。
    恢复后，系统会重新启动，并且 macOS 安装会自动开始。需要 Internet 连接，安装程序才能下载必要文件。
    如果不需要将 APFS 格式的数据卷恢复为可启动系统，请清除**在已恢复的 macOS 数据卷上安装 macOS** 复选框。以后仍可以使该卷可启动，方法是在该卷上安装 macOS。
12. [仅适用于 Linux] 如果备份的计算机具有逻辑卷 (LVM) 并且要重新生成原始 LVM 结构：
    a. 确保目标计算机磁盘的数量和每个磁盘的容量都等于或大于原始计算机，然后单击**应用 RAID/LVM**。
    b. 复查卷结构，然后单击**应用 RAID/LVM** 创建卷结构。
    c. 确认选择。
13. [可选] 单击**恢复选项**来指定其他设置。
14. 单击**确定**来启动恢复。

使用异机还原

当恢复至不同硬件（包括 VMware 或 Hyper-V 平台）时，最新的操作系统会保持可启动状态。如果恢复的操作系统无法启动，请使用异机还原工具更新对于操作系统启动至关重要的驱动程序和模块。

异机还原适用于 Windows 和 Linux。

应用异机还原

1. 从可启动媒体启动计算机。
2. 单击**应用异机还原**。
3. 如果在计算机上安装了多个操作系统，请选择一个要应用异机还原的操作系统。
4. [仅限于 Windows] 配置其他设置。
5. 单击**确定**。

在 Windows 中应用异机还原

准备

准备驱动程序

在将异机还原应用到 Windows 操作系统之前，请确保您具有适用于新 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。驱动程序文件应带有 *.inf 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。

最佳做法是将您组织中使用的所有硬件的驱动程序存储在一个按设备类型或按硬件配置分类的存储库中。您可以在 DVD 或闪存驱动器上保留该存储库的副本；选取某些驱动程序并将其添加到可启动媒体中；为每个服务器创建包含必要驱动程序（和必要网络配置）的自定义可启动媒体。或者，您也可以在每次使用异机还原时仅指定该存储库的路径。

检查在可启动环境中对驱动程序的访问权限

确保在可启动媒体下工作时对带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。其位置在注册表值 **DevicePath** 中确定，该值可在注册表项 **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion** 中找到。此存储文件夹通常为 WINDOWS/inf。

异机还原将在指定文件夹的所有子文件夹中执行递归搜索，查找所有这些可用文件夹中最适用的 HAL 和 HDD 控制器驱动程序并将其安装到系统中。“异机还原”还会搜索网络适配器驱动程序，然后该“异机还原”功能会将所发现驱动程序的路径传送给操作系统。如果硬件具有多个网络接口卡，异机还原将尝试配置所有网络接口卡的驱动程序。

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。
- 您将系统迁移到了使用 SCSI 硬盘控制器的虚拟机。请使用与虚拟化软件捆绑在一起的 SCSI 驱动程序，或者从软件制造商网站下载最新版本的驱动程序。
- 如果自动驱动程序搜索不能帮助启动系统。

通过单击**添加驱动程序**指定合适的驱动程序。即使程序找到更适合的驱动程序，仍会安装在此处定义的驱动程序，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**。

如果异机还原未能在指定位置中找到兼容的驱动程序，将会显示有关问题设备的提示。请执行以下任一操作：

- 将驱动程序添加到之前指定的任何位置，然后单击**重试**。
- 如果忘记该位置，请单击**忽略**以继续该过程。如果结果不令人满意，请重新应用异机还原。在配置操作时，请指定必要驱动程序。

Windows 启动后，系统会初始化安装新硬件的标准程序。如果驱动程序具有 Microsoft Windows 签名，将以静默方式安装网络适配器驱动程序。否则，Windows 会要求确认是否安装未签名的驱动程序。

然后，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。

在 Linux 中应用异机还原

异机还原可应用到内核版本为 2.6.8 或更高版本的 Linux 操作系统。

当异机还原应用到 Linux 操作系统时，它将更新称为初始 RAM 磁盘 (initrd) 的临时文件系统。这可确保操作系统能够在新硬件上启动。

异机还原将新硬件的模块(包括设备驱动程序)添加到初始 RAM 磁盘。一般来说，它会在 **/lib/modules** 目录中查找必要的模块。如果异机还原未能找到所需的模块，它会将模块的文件名记录到日志中。

异机还原可能会修改 GRUB 启动加载程序的配置。这可能是必需的操作，例如，当新计算机具有的卷布局与原始计算机不同时，确保系统可启动性。

异机还原永远不会修改 Linux 内核。

还原至原始初始 RAM 磁盘

您可以还原至原始初始 RAM 磁盘(如有必要)。

初始 RAM 磁盘存储在计算机上的某个文件中。首次更新初始 RAM 磁盘之前，异机还原将其副本保存到同一目录中。该副本的名称为在原始文件名的基础上再后跟 **_acronis_backup.img** 后缀。如果运行异机还原多次(例如，已添加缺少的驱动程序后)，该副本将不会被覆盖。

若要还原至原始初始 RAM 磁盘，请执行以下任一操作：

- 相应地重命名副本。例如，运行如下所示的命令：

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- 在 **GRUB 启动加载程序配置**的 initrd 行中指定副本。

正在恢复文件

使用 Web 界面恢复文件

1. 选择原先包含要恢复的数据的计算机。
2. 单击**恢复**。
3. 选择恢复点。请注意，恢复点按位置过滤。

   如果选定的计算机是物理机并处于脱机状态，将不显示恢复点。请执行以下任一操作：
   - [推荐] 如果备份位置是云或共享存储(即其他代理程序可以访问它)，则单击**选择计算机**，选择处于联机状态的目标计算机，然后选择恢复点。
   - 在备份存储选项卡上选择一个恢复点。
   - 从云存储下载文件。
   - 使用可启动媒体。
4. 依次单击**恢复** > **文件/文件夹**。
5. 浏览到所需的文件夹或使用搜索功能获取所需文件和文件夹的列表。

   可以使用一个或多个通配符(* 和 ?)。有关使用通配符的更多详细信息，请参阅"文件过滤器"。

   注意
   对于存储在云存储中的磁盘级别备份，搜索功能不可用。
6. 选择要恢复的文件。
7. 如果要将文件另存为 .zip 文件，请单击**下载**，选择要将数据保存到的位置，然后单击**保存**。否则，请跳过此步骤。
8. 单击**恢复**。

   在**恢复至**中，您可以看到以下计算机之一：
   - 原先包含要恢复的文件的计算机(如果这台计算机上安装了代理程序)。
   - 安装了适用于 VMware 的代理程序、适用于 Hyper-V 的代理程序或适用于 Scale Computing HC3 的代理程序的计算机(如果文件来源于 ESXi、Hyper-V 或 Scale Computing HC3 虚拟机)。

   这是恢复的目标计算机。如有必要，您可以选择另一台计算机。
9. 在**路径**中，选择恢复目标位置。可选择以下其中一个选项：
   - 原始位置(当恢复至原始计算机时)
   - 目标计算机上的本地文件夹

     注意
     符号链接不受支持。
   - 可从目标计算机访问的网络文件夹。
10. 单击**开始恢复**。
11. 选择文件覆盖选项之一：
    - **覆盖现有文件**

- **覆盖现有文件(如果较旧)**
- **不覆盖现有文件**

恢复进度显示在**活动**选项卡上。

从云存储下载文件

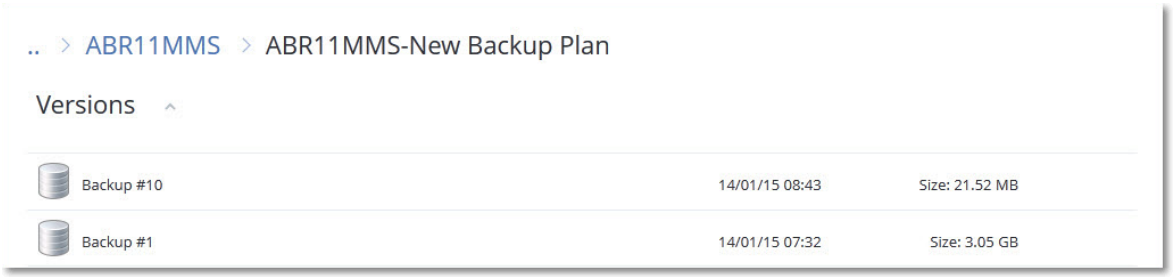
您可以浏览云存储、查看备份的内容和下载所需的文件。

限制

- 无法浏览系统状态、SQL 数据库和 Exchange 数据库的备份。
- 为获得更好的下载体验，每次下载不应超过 100 MB。若要快速从云中检索大量数据，请使用文件恢复步骤。

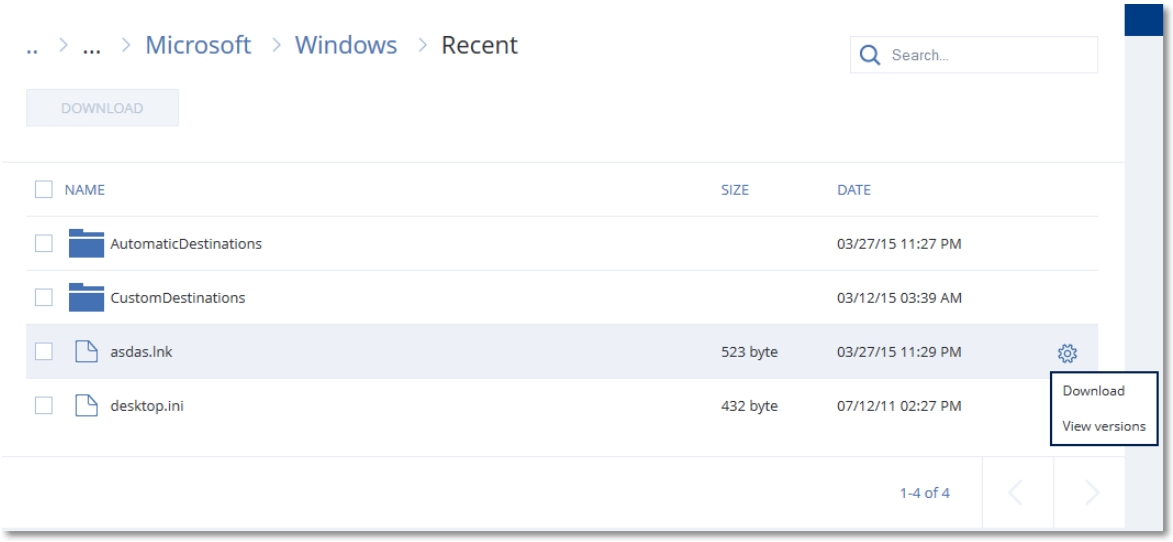
从云存储下载文件

1. 选择已备份的计算机。
2. 依次单击**恢复** > **更多恢复方法...** > **下载文件**。
3. 输入备份计算机分配到的帐户的凭据。
4. [当浏览磁盘级别备份时]在**版本**下，单击要从其中恢复文件的备份。



[当浏览文件级备份时]您可以在下一步中在位于选定文件右侧的齿轮图标下选择备份日期和时间。默认情况下，文件从最新的备份恢复。

5. 浏览到所需文件夹或使用搜索功能获取所需文件的列表。



6. 选中您需要恢复的项目对应的复选框，然后单击**下载**。

如果您选择单个文件，它将按原样下载。否则，所选数据将存档到 .zip 文件中。

7. 选择数据的保存位置，然后单击**保存**。

使用 Notary 服务验证文件真实性

如果在备份期间启用了公证，则您可以验证备份文件的真实性。

验证文件真实性

1. 如"使用 Web 界面恢复文件"部分的第 1-6 步或"从云存储下载文件"部分的第 1-5 步所述，选择相应文件。
2. 确保所选文件标记有以下图标：  。这意味着该文件是真实的。
3. 请执行以下任一操作：
   - 单击**验证**。
     软件会检查文件真实性并显示结果。
   - 单击**获取证书**。
     确认文件真实性的证书会在 Web 浏览器窗口中打开。该窗口还包含允许您手动验证文件真实性的说明。

使用 ASign 对文件签名

ASign 是一种服务，允许多个人以电子方式对备份文件进行签名。此功能仅适用于存储在云存储中的文件级备份。

一次只能对一个文件版本进行签名。如果该文件备份了多次，则您必须选择要签名的版本，将只对此版本进行签名。

例如，ASign 可用于以下文件的电子签名：

- 租赁协议
- 销售合同
- 资产购买协议
- 贷款协议
- 许可证
- 金融单据
- 保险单据
- 责任豁免书
- 医疗保健文档
- 研究论文
- 产品真实性证书
- 保密协议
- 报价书
- 保密协议
- 独立承包协议

在一个文件版本上签名

1. 如"使用 Web 界面恢复文件"部分的第 1-6 步所述，选择文件。
2. 确保在左侧面板中选择正确的日期和时间。
3. 单击**在此文件版本上签名**。
4. 为在其下存储备份的云存储帐户指定密码。帐户的登录名显示在提示符窗口中。
   ASign 服务界面在 Web 浏览器窗口中打开。
5. 通过指定其电子邮件地址来添加其他签名者。发送邀请后，无法添加或删除签名者，因此请确保列表中包含所有需要其签名的人。
6. 单击**邀请签名**以将邀请发送给签名者。
   每位签名者都会收到一封签名请求电子邮件。当所有请求的签名者对文件进行签名时，文件通过公证服务进行公证和签名。
   在每位签名者对文件进行签名时和整个进程完成时，您都会收到通知。您可以通过单击收到的任何电子邮件中的**查看详细信息**来访问 ASsign 网页。
7. 进程完成后，转到 ASign 网页并单击**获取文档**来下载包含以下内容的 .pdf 文档：
   - "签名证书"页面具有收集的签名。
   - 具有活动历史记录的"审核记录"页面：将邀请发送给签名者的时间、每位签名者对文件签名的时间等。

使用可启动媒体恢复文件

有关如何创建可启动媒体的信息，请参考"创建可启动媒体"。

使用可启动媒体恢复文件

1. 通过使用可启动媒体启动目标计算机。
2. 单击**本地管理此计算机**或单击**应急可启动媒体**两次，具体取决于您要使用的媒体类型。
3. 如果在网络中启用代理服务器，请依次单击**工具** > **代理服务器**，然后指定代理服务器主机名/IP 地址和端口。否则，请跳过此步骤。
4. 在欢迎屏幕上，单击**恢复**。
5. 单击**选择数据**，然后单击**浏览**。
6. 指定备份位置：
   - 若要从云存储中恢复，请选择**云存储**。输入备份计算机分配到的帐户的凭据。
   - 若要从本地或网络文件夹恢复，请浏览到**本地文件夹**或**网络文件夹**下的文件夹。

   单击**确定**确认您的选择。
7. 选择要从其中恢复数据的备份。如果出现提示，请键入备份的密码。
8. 在**备份内容**中，选择**文件夹/文件**。
9. 选择要恢复的数据。单击**确定**确认您的选择。
10. 在**恢复位置**下，指定某个文件夹。您可以选择禁止较新版本文件的覆盖或从恢复中排除某些文件。
11. [可选] 单击**恢复选项**来指定其他设置。
12. 单击**确定**来启动恢复。

注意

在 Linux 可启动媒体和 WinPE 可启动媒体下重新扫描和恢复时，磁带位置会占用大量空间，并且可能不适合 RAM。对于 Linux，您必须加载其他位置才能将数据保存到磁盘或共享。参见 Acronis Cyber Backup Advanced：更改 TapeLocation 文件夹 (KB 27445)。对于 Windows PE，目前没有解决方法。

从本地备份提取文件

您可以浏览备份内容，并提取所需文件。

要求

- 只能在 Windows 中通过文件资源管理器使用此功能。
- 保护代理程序必须安装在浏览备份的计算机上。
- 备份文件系统必须采用以下格式之一：FAT16、FAT32、NTFS、ReFS、Ext2、Ext3、Ext4、XFS 或 HFS+。
- 备份必须存储在本地文件夹或网络共享 (SMB/CIFS) 中。

从备份提取文件

1. 使用文件资源管理器浏览到备份位置。
2. 双击备份文件。文件名基于以下模板：
   <计算机名称> - <保护计划 GUID>
3. 如果备份已加密，则输入加密密码。否则，请跳过此步骤。
   文件资源管理器会显示恢复点。
4. 双击恢复点。
   文件资源管理器会显示备份数据。
5. 浏览到所需文件夹。
6. 将所需文件复制到文件系统上任意文件夹。

恢复系统状态

1. 选择要恢复系统状态的计算机。
2. 单击**恢复**。
3. 选择系统状态恢复点。请注意，恢复点按位置过滤。
4. 单击**恢复系统状态**。
5. 确认要将系统状态覆盖为其备份版本。

恢复进度显示在**活动**选项卡上。

恢复 ESXi 配置

若要恢复 ESXi 配置，您需要基于 Linux 的可启动媒体。有关如何创建可启动媒体的信息，请参考“创建可启动媒体”。

如果您要将 ESXi 配置恢复至非原始主机，并且原始 ESXi 主机仍然连接到 vCenter 服务器，请将此主机从 vCenter 服务器断开连接并删除它，以避免在恢复期间发生意外问题。如果您要将原始主机与恢复的主机一起保留，可以在恢复完成后添加它。

在该主机上运行的虚拟机未包含在 ESXi 配置备份中。可以单独备份和恢复它们。

恢复 ESXi 配置

1. 通过使用可启动媒体启动目标计算机。
2. 单击**本地管理此计算机**。
3. 在欢迎屏幕上，单击**恢复**。
4. 单击**选择数据**，然后单击**浏览**。
5. 指定备份位置：
   - 浏览到**本地文件夹**或**网络文件夹**下的文件夹。

   单击**确定**确认您的选择。
6. 在**显示**中，选择 **ESXi 配置**。
7. 选择要从其中恢复数据的备份。如果出现提示，请键入备份的密码。
8. 单击**确定**。
9. 在**要用于新数据存储的磁盘**中，执行以下操作：
   - 在**将 ESXi 恢复至**下，选择将恢复主机配置的磁盘。如果您要将配置恢复至原始主机，将默认选择原始磁盘。
   - [可选] 在**用于新数据存储**下，选择将创建新数据存储的磁盘。请谨慎选择，因为选定磁盘上的所有数据都将丢失。如果要在现有数据存储中保留虚拟机，请不要选择任何磁盘。
10. 如果选择新数据存储的任何磁盘，请选择**如何创建新数据存储**中的数据存储创建方法：**在每个磁盘上创建一个数据存储**或**在所有选定的 HDD 上创建一个数据存储**。
11. [可选] 在**网络映射**中，将备份中存在的虚拟交换机的自动映射结果更改为物理网络适配器。
12. [可选] 单击**恢复选项**来指定其他设置。
13. 单击**确定**来启动恢复。

恢复选项

若要修改恢复选项，请在配置恢复时单击**恢复选项**。

恢复选项的可用性

可用的恢复选项集取决于：

- 执行恢复的代理程序运行所在的环境（Windows、Linux、macOS 或可启动媒体）。
- 要恢复的数据类型（磁盘、文件、虚拟机、应用程序数据）。

下表总结了恢复选项的可用性。

	磁盘	文件	虚拟机	SQL 和 Exchange

	Windows	Linux	可启动媒体	Windows	Linux	macOS	可启动媒体	ESXi、Hyper-V、Scale Computing HC3	Windows
备份验证	+	+	+	+	+	+	+	+	+
启动模式	+	-	-	-	-	-	-	+	-
文件的日期和时间	-	-	-	+	+	+	+	-	-
错误处理	+	+	+	+	+	+	+	+	+
文件排除	-	-	-	+	+	+	+	-	-
Flashback	+	+	+	-	-	-	-	+	-
完整路径恢复	-	-	-	+	+	+	+	-	-
加载点	-	-	-	+	-	-	-	-	-
性能	+	+	-	+	+	+	-	+	+
预/后命令	+	+	-	+	+	+	-	+	+
SID 更改	+	-	-	-	-	-	-	-	-
VM 电源管理	-	-	-	-	-	-	-	+	-
"磁带管理"(第 292 页) > 使用磁盘缓存以加快恢复	-	-	-	+	+	+	-	-	-

Windows 事件日志	+	-	-	+	-	-	-	仅 Hyper-V	+
恢复后开机	-	-	-	-	-	-	+	-	-

备份验证

此选项定义在从备份恢复数据前，是否验证备份，以确保其未损坏。该操作由保护代理程序执行。

预设为：**已禁用**。

验证时，会计算备份中保存的每个数据块的校验和。唯一的例外是位于云存储中的文件级备份的验证。这些备份通过检查备份中所保存元信息的一致性来进行验证。

验证是一个耗时的过程，即使对大小较小的增量或差异备份也是如此。这是因为该操作不仅验证备份本身包含的数据，还会验证通过选择备份可恢复的所有数据。此操作要求访问之前创建的备份。

注意
验证适用于位于 Acronis 数据中心中的云存储，并由 Acronis 合作伙伴提供。

启动模式

此选项仅在从包含 Windows 操作系统的磁盘级别备份中恢复物理或虚拟机时有效。

您可用此选项，选择恢复后 Windows 将使用的启动模式（BIOS 或 UEFI）。如果原始计算机的启动模式不同于所选启动模式，软件将：

- 根据所选启动模式（适用于 BIOS 的 MBR、适用于 UEFI 的 GPT），初始化要将系统卷恢复到的磁盘。
- 调整 Windows 操作系统，使之能使用所选启动模式启动。

预设为：**如同在目标计算机上。**

可选择以下其中一个选项：

- **如同在目标计算机上**
  目标计算机上运行的代理程序检测到 Windows 当前所用的启动模式，并根据检测到的启动模式进行调整。
  除非应用以下所列限制，否则这是自动生成可启动系统的最安全值。由于**启动模式**选项在可启动媒体下不存在，因此媒体上的代理程序始终表现为似乎已选中该值。
- **如同在备份计算机上**
  目标计算机上运行的代理程序从备份中读取启动模式，并根据该启动模式进行调整。这可帮助您在其他计算机上恢复系统（即使该计算机使用其他启动模式），然后替换备份计算机中的磁盘。
- **BIOS**
  目标计算机上运行的代理程序进行调整以使用 BIOS。

- **UEFI**
  目标计算机上运行的代理程序进行调整以使用 UEFI。

更改设置后，将重复磁盘映射步骤。这需花费一些时间。

建议

如果需要在 UEFI 和 BIOS 之间转换 Windows：

- 恢复系统卷所在的整个磁盘。如果仅恢复现有卷之上的系统卷，则代理程序将无法正确初始化目标磁盘。
- 请记住，BIOS 不允许使用 2 TB 以上的磁盘空间。

限制

- 支持在 UEFI 和 BIOS 之间转换的系统：
  - 从 Windows 7 开始的 64 位 Windows 操作系统
  - 从 Windows Server 2008 SP1 开始，64 位 Windows Server 操作系统
- 如果备份存储在磁带设备上，则不支持在 UEFI 和 BIOS 之间转换。

如果不支持在 UEFI 和 BIOS 之间转换系统，则代理程序表现为好像**如同在备份计算机上**设置已选中。如果目标计算机同时支持 UEFI 和 BIOS，则需要手动启用与原始计算机对应的启动模式。否则，系统将不会启动。

文件的日期和时间

此选项仅在恢复文件时有效。

此选项定义是从备份恢复文件的日期和时间，还是为文件指定当前日期和时间。

如果启用此选项，将为文件指定当前日期和时间。

预设为：**已启用**。

错误处理

这些选项可让您指定如何处理恢复期间可能发生的错误。

如果发生错误，则重新尝试

预设为：**已启用。尝试次数：30.尝试间隔：30 秒。**

如果发生可恢复的错误，程序会重新尝试执行未成功的操作。您可以设置时间间隔和尝试次数。一旦操作成功或已执行指定尝试次数（以首先发生的为准），尝试将停止。

处理时不显示消息和对话框（无提示模式）

预设为：**已禁用**。

启动无消息模式后，程序将自动处理需要用户互动的情况(如有)。如果操作必须有用户互动才能继续，则操作将失败。可在操作日志中找到操作的详细信息，包括错误(如果有)。

如果通过重启进行恢复失败，则保存系统信息。

此选项对运行 Windows 或 Linux 的物理机的磁盘或卷恢复有效。

预设为：**已禁用**。

当启用此选项时，可以在本地磁盘(包括连接到目标计算机的闪存或HDD驱动器)或在可以保存日志、系统信息和故障转储文件的网络共享上指定一个文件夹。此文件将帮助技术支持人员识别问题。

文件排除

此选项仅在恢复文件时有效。

该选项定义了在恢复过程中要跳过的文件和文件夹，从而从恢复项目列表中排除。

注意
排除优先于要恢复的数据项选择。例如，如果您选择恢复 MyFile.tmp 文件并排除所有 .tmp 文件，将不会恢复 MyFile.tmp 文件。

文件级安全性

此选项仅在恢复 NTFS 格式卷的磁盘级和文件级备份中的文件时有效。

此选项定义是否随文件恢复文件的 NTFS 权限。

预设为：**已启用**。

您可以选择是恢复权限，还是让文件从其恢复到的文件夹继承其 NTFS 权限。

Flashback

在物理机和虚拟机(Mac 除外)上恢复磁盘和卷时，此选项有效。

如果启用此选项，仅恢复备份中的数据与目标磁盘数据之间的差异。这可加快数据恢复到备份时的相同磁盘，特别是在磁盘的卷布局尚未更改的情况下。数据在块级别上进行比较。

对于物理机，在块级别上比较数据的操作非常耗时。如果与备份存储的连接速度非常快，则恢复整个磁盘所需的时间少于计算数据差异的时间。因此，建议仅在与备份存储的连接速度非常慢的情况下启用该选项(例如，如果备份存储在云存储中或远程网络文件夹上)。

恢复物理机时，预设取决于备份位置：

- 如果备份位置为云存储，则预设为：**已启用**。
- 对于其他备份位置，预设为：**已禁用**。

恢复虚拟机时，预设为：**已启用**。

完整路径恢复

此选项仅对从文件级备份中恢复数据有效。

如果启用此选项，将在目标位置中重新创建文件的完整路径。

预设为：**已禁用**。

加载点

此选项仅对从 Windows 文件级备份中恢复数据有效。

启用此选项，即可恢复存储在已加载卷上并在启用加载点选项的情况下备份的文件和文件夹。

预设为：**已禁用**。

此选项仅在您为恢复选择的文件夹层次结构高于加载点的文件夹时有效。如果选择恢复加载点内的文件夹或加载点自身，则无论**加载点**选项值如何，都将恢复选定项目。

注意
请注意，如果恢复时未加载卷，数据将直接恢复到备份时作为加载点的文件夹。

性能

此选项定义操作系统中的恢复进程的优先级。

可用设置包括：**低**、**正常**I、**高**。

预设为：**正常**。

系统中运行的进程的优先级决定分配给该进程的 CPU 使用量和系统资源。降低恢复优先级，可释放出更多资源给其他应用程序。提高恢复优先级，可通过请求操作系统分配更多资源给执行恢复的应用程序，加速恢复进程。不过，最终效果将取决于总 CPU 使用率，以及其他因素，如磁盘 I/O 速度或网络流量。

预/后命令

此选项可让您定义在数据恢复之前和之后要自动执行的命令。

使用事前/事后命令的方法示例：

- 启动 **Checkdisk** 命令，以查找并修复文件系统逻辑错误、物理错误，或要在恢复开始前或恢复结束后启动的坏扇区。

此程序不支持互动命令，即需要用户输入的命令（如“pause”）。

如果恢复后重启，则恢复后的命令将不会执行。

恢复前命令

指定要在恢复程序开始之前执行的命令/批处理文件

1. 启用**在恢复前执行命令**开关。
2. 在**命令...**字段中，键入命令或浏览并找到批处理文件。此程序不支持互动命令，即需要用户输入的命令（如“pause”）。
3. 在**工作目录**字段中，指定将执行命令/批处理文件所在目录的路径。
4. 在**参数**字段中，指定该命令的执行参数（如需要）。
5. 根据您要获得的结果，选择下表所述的相应选项。
6. 单击**完成**。

复选框	**选择**			
如果命令无法执行，恢复将失败*	勾选	取消勾选	勾选	取消勾选
不要进行恢复操作直至命令执行完毕	勾选	勾选	取消勾选	取消勾选
结果				
	预设 仅在命令成功执行后执行恢复操作。如果命令无法执行，恢复将失败。	执行命令后即进行恢复操作，无论命令执行成功与否。	N/A	在执行命令的同时进行恢复操作，无论命令执行的结果如何。

*如果退出代码不等于 0，命令将视为失败。

恢复后命令

指定在恢复完成之后要执行的命令/可执行文件

1. 启用**在恢复后执行命令**开关。
2. 在**命令...**字段中，键入命令或浏览并找到批处理文件。
3. 在**工作目录**字段中，指定将执行命令/批处理文件所在目录的路径。
4. 在**参数**字段中，指定命令执行参数（如有必要）。
5. 如果成功执行命令对您极为重要，则选中**如果命令无法执行，恢复将失败**复选框。如果退出代码不等于 0，命令将视为失败。如果命令执行失败，恢复状态将设置为**错误**。

   如果未选中此复选框，则命令执行结果不会影响恢复成功与否。可以通过浏览**活动**选项卡来跟踪命令执行结果。
6. 单击**完成**。

注意
如果恢复后重启，则恢复后的命令将不会执行。

磁带管理

您可以使用以下磁带管理恢复选项。

使用磁带缓存以加快恢复

预设为：**已禁用**。

当您要从映像存档中恢复文件时，我们强烈建议您使用 **使用磁盘缓存以加快恢复** 选项。否则，恢复操作可能需要耗费大量时间。使用此选项后，磁带读取将按顺序执行，不会发生中断或倒带。

SID 更改

当恢复 Windows 8.1/Windows Server 2012 R2 或较早版本时，此选项有效。

当恢复至虚拟机的操作由适用于 VMware 的代理程序、适用于 Hyper-V 的代理程序或适用于 Scale Computing HC3 的代理程序执行时，此选项无效。

预设为：**已禁用**。

该软件可以为恢复的操作系统生成唯一的安全标识符（计算机 SID）。您只需使用此选项，即可确保依赖于计算机 SID 的第三方软件的可操作性。

Microsoft 官方并不支持针对已部署或已恢复的系统更改 SID。因此，使用此选项的风险由您自行承担。

VM 电源管理

当恢复至虚拟机的操作由适用于 VMware 的代理程序、适用于 Hyper-V 的代理程序或适用于 Scale Computing HC3 的代理程序执行时，这些选项有效。

开始恢复时关闭目标虚拟机

预设为：**已启用**。

如果计算机处于联机状态，则无法恢复至现有虚拟机，因此恢复开始时计算机会立刻自动关机。用户将中断与计算机的连接，未保存的数据将会丢失。

如果您想在恢复前手动关闭虚拟机，请取消勾选此选项的复选框。

恢复操作完成后接通目标虚拟机的电源

预设为：**已禁用**。

计算机从备份恢复至其他计算机上后，现有计算机的副本可能会在网络上出现。为安全起见，请在采取必要的预防措施后，手动开启恢复的虚拟机。

Windows 事件日志

此选项仅在 Windows 操作系统下有效。

此选项定义代理程序是否必须在 Windows 应用程序事件日志中记录恢复操作的事件(要查看此日志，请运行 eventvwr.exe 或依次选择**控制面板** > **管理工具** > **事件查看器**)。您可以筛选要记录的事件。

预设为：**已禁用**。

恢复后开机

在可启动媒体下运行时，此选项可用。

预设为：**已禁用**。

此选项可让您启动计算机至恢复的操作系统，而无需用户互动。

灾难恢复

此功能仅适用于 Acronis 安克诺斯数据保护软件 的云部署。有关此功能的详细说明，请参阅 https://www.acronis.com/support/documentation/DisasterRecovery/index.html#43224.html。

与备份有关的操作

备份存储选项卡

备份存储选项卡显示曾在管理服务器上注册的所有计算机的备份。这包括离线计算机和不再注册的计算机。

存储在共享位置(例如 SMB 或 NFS 共享)中的备份对具有该位置读取权限的所有用户可见。

在 Windows 中，备份文件继承其父文件夹的访问权限。因此，建议您限制此文件夹的读取权限。

在云存储中，用户仅有权访问自己的备份。在云部署中，管理员可以代表属于同一组及其子组的任何帐户查看备份。此帐户在**要从其浏览的计算机**中间接选择。**备份存储**选项卡显示曾在注册此计算机的相同帐户下注册的所有计算机的备份。

保护计划中使用的备份位置将自动添加到**备份存储**选项卡。若要将自定义文件夹(例如，可卸除的 USB 设备)添加到备份位置的列表，请单击**浏览**并指定文件夹路径。

警告！
请勿尝试手动编辑备份文件，因为这可能会导致文件损坏并使备份无法使用。另外，建议您导出备份或使用备份复制，而不是手动移动备份文件。

使用"备份存储"选项卡选择恢复点

1. 在**备份存储**选项卡上，选择存储备份的位置。
   软件将显示允许您的帐户在选定位置查看的所有备份。备份组合为组。组名称基于以下模板：
   <计算机名称> - <保护计划名称>
2. 选择要从其恢复数据的组。
3. [可选]单击**要从其浏览的计算机**旁边的**更改**，然后选择另一台计算机。某些备份只能由特定代理程序浏览。例如，您必须选择运行适用于 SQL 的代理程序的计算机来浏览 Microsoft SQL Server 数据库的备份。

   重要事项
   请注意，**要从其浏览的计算机**是从物理机备份恢复的默认目标。在选择恢复点并单击**恢复**后，仔细检查**目标计算机**设置，以确保要恢复至此特定计算机。若要更改恢复目标，请在**要从其浏览的计算机**中指定另一台计算机。

4. 单击**显示备份**。
5. 选择恢复点。

从备份加载卷

加载磁盘级备份上的卷可让您能够像访问物理磁盘一样访问卷。

在读写模式下加载卷可对备份内容进行修改，即保存、移动、创建、删除文件或文件夹，以及运行由一个文件组成的可执行程序。在此模式下，软件创建包含对备份内容所做的更改的增量备份。请注意，任何后续备份都不包含这些更改。

要求

- 只能在 Windows 中通过文件资源管理器使用此功能。
- 适用于 Windows 的代理程序必须安装在执行加载操作的计算机上。
- 备份的文件系统必须受到计算机正在运行的 Windows 版本的支持。
- 备份必须存储在本地文件夹、网络共享 (SMB/CIFS) 或安全区域中。

使用方案

- **共享数据**

  已加载卷可以通过网络轻松共享。
- **“Band aid”数据库恢复解决方案**

  从最近失败的计算机加载包含 SQL 数据库的卷。这将允许用户在失败的计算机恢复前访问数据库。此方法也可用于 Microsoft SharePoint 数据的粒度恢复，方法是使用 SharePoint 资源管理器。
- **脱机病毒清理**

  如果计算机受到感染，请加载其备份、使用防病毒程序清理它（或者查找没有感染的最新备份），然后从此备份中恢复计算机。
- **错误检查**

  如果卷大小经过调整的恢复失败了，原因可能是备份的文件系统出现错误。在读写模式下加载备份。然后使用 **chkdsk /r** 命令检查已加载卷是否有错误。在修复错误并且创建新的增量备份后，请从此备份中恢复系统。

从备份中加载卷

1. 使用文件资源管理器浏览到备份位置。
2. 双击备份文件。默认情况下，文件名基于以下模板：

   <计算机名称> - <保护计划 GUID>
3. 如果备份已加密，则输入加密密码。否则，请跳过此步骤。

   文件资源管理器会显示恢复点。
4. 双击恢复点。

   文件资源管理器会显示备份的卷。

   注意

   双击卷，以浏览其内容。您可以将文件和文件夹从备份复制到文件系统上的任何文件夹。
5. 右键单击要加载的卷，然后单击以下选项之一：

- **加载**

  注意
  在读写模式下只能加载存档(备份链)中的最后一个备份。

- **以只读模式加载**

6. 如果备份存储在网络共享上,请提供访问凭据。否则,请跳过此步骤。
   软件会加载选定的卷。第一个未使用的字母将分配给卷。

卸载卷

1. 使用文件资源管理器浏览到**计算机**(在 Windows 8.1 及更高版本上是**此电脑**)。
2. 右键单击已加载卷。
3. 单击**卸载**。
4. 如果卷在读写模式下加载,并且其内容已修改,请选择是否创建包含更改的增量备份。否则,请跳过此步骤。
   软件会卸载选定的卷。

验证备份

验证是用于检查通过备份进行数据恢复之可行性的一种操作。有关此操作的详细信息,请参阅 "验证"(第 303 页)。

验证备份

1. 选择备份的工作负载。
2. 单击**恢复**。
3. 选择恢复点。请注意,恢复点按位置过滤。
   如果工作负载处于脱机状态,将不会显示恢复点。请执行以下任一操作:
   - 如果备份位置是云或共享存储(即,其他代理程序可以访问它),请单击**选择计算机**、选择处于联机状态的目标工作负载,然后选择恢复点。
   - 在备份存储选项卡上,选择一个恢复点。有关此处备份的详细信息,请参阅 "备份存储选项卡"(第 296 页)。
4. 单击齿轮图标,然后单击**验证**。
5. 选择将执行验证的代理程序。
6. 选择验证方法。
7. 如果备份已加密,则提供加密密码。
8. 单击**开始**。

导出备份

导出操作将在指定的位置创建一个备份的自足副本。原备份就保持原样。导出操作可将特定的备份从增量和差异备份链中分离,以便实现快速恢复、写入可移动或可卸除媒体或其他用途。

导出操作的结果始终是完整备份。如果想要将整个备份链复制到不同位置并保留多个恢复点，请使用备份复制计划。

导出备份的备份文件名取决于备份格式选项的值：

- 对于具有任何备份方案的**版本12**格式，备份文件名与原始备份的文件名相同，除了序列号。如果来自同一个备份链的多个备份导出到相同位置，则四位序列号将附加到所有备份的文件名，除了第一个备份。
- 对于**版本 11**格式的**始终增量(单个文件)**备份方案，备份文件名精确匹配原备份的备份文件名。如果相同备份链的多个备份导出到相同位置，则每个导出操作将覆盖之前导出的备份。
- 对于具有其他备份方案的**版本 11**格式，备份文件名与原始备份的文件名相同，除了时间戳。导出备份的时间戳对应于执行导出时的时间。

导出的备份继承原备份的加密设置和密码。当导出加密备份时，必须指定密码。

导出备份

1. 选择已备份的计算机。
2. 单击**恢复**。
3. 选择恢复点。请注意，恢复点按位置过滤。

   如果计算机处于脱机状态，将不显示恢复点。请执行以下任一操作：
   - 如果备份位置是云或共享存储(即其他代理程序可以访问它)，单击**选择计算机**，选择处于联机状态的目标计算机，然后选择恢复点。
   - 在备份存储选项卡上选择一个恢复点。
4. 单击齿轮图标，然后单击**导出**。
5. 选择将执行导出的代理程序。
6. 如果备份已加密，则提供加密密码。否则，请跳过此步骤。
7. 指定导出目标。
8. 单击**开始**。

删除备份

警告！
删除某个备份时，也会永久删除其所有数据。无法恢复删除的数据。

删除存在于 安克诺斯数据保护软件 Web 中控台中且处于联机状态的计算机的备份

1. 在**所有设备**选项卡上，选择要删除其备份的计算机。
2. 单击**恢复**。
3. 选择要删除备份的位置。
4. 请执行以下任一操作：
   - 若要删除单个备份，请选择要删除的备份，单击齿轮图标，然后单击**删除**。
   - 若要删除选定位置中的所有备份，请单击**全部删除**。
5. 确认您的决定。

删除任意计算机的备份

1. 在**备份存储**选项卡上，选择要删除备份的位置。
   软件将显示允许您的帐户在选定位置查看的所有备份。备份组合为组。组名称基于以下模板：
   <计算机名称> - <保护计划名称>
2. 选择某个组。
3. 请执行以下任一操作：
   - 若要删除单个备份，请单击**显示备份**，选择要删除的备份，单击齿轮图标，然后单击**删除**。
   - 若要删除选定组，请单击**删除**。
4. 确认您的决定。

直接从云存储中删除备份

1. 登录到云存储，如"从云存储下载文件"中所述。
2. 单击要删除其备份的计算机的名称。
   该软件显示一个或多个备份组。
3. 单击对应要删除的备份组的齿轮图标。
4. 单击**删除**。
5. 确认操作。

“计划”选项卡

使用高级许可证，可以通过使用**计划**选项卡来管理保护计划和其他计划。

计划选项卡的每个部分都包含一个特定类型的所有计划。提供以下部分：

- 保护
- 备份扫描
- 备份复制
- 验证
- 清理
- 转换到 VM
- VM 复制
- 可启动媒体。本部分会显示为从可启动媒体启动的计算机所创建且只能应用于此类计算机的保护计划。

在每个部分中，可以创建、编辑、禁用、启用、删除、启动和监视计划的运行。

克隆和停止仅适用于保护计划。不同于从**设备**选项卡停止备份，停止某个保护计划会停止应用该计划的所有设备上的备份。如果在一个时间窗口内分配了多个设备的备份开始时间，则停止某个保护计划会停止正在运行的备份或阻止备份开始。

您还可以将一个计划导出到一个文件和导入之前导出的计划。

脱离主机数据处理

保护计划的大部分操作（如复制、验证和应用保留规则）都由执行备份的代理程序执行。这会给运行代理程序的计算机增加额外的工作负载，即使备份过程完成后也如此。

将反恶意软件扫描、复制、验证、清理和转换计划从保护计划中分离，可让您灵活处理以下操作：

- 选择其他代理程序执行这些操作
- 将这些操作预定在非高峰时段，以最大限度地减少网络带宽消耗
- 如果设置一个专用代理程序不在您的计划之内，则将这些操作挪到工作时间外执行

如果您使用的是存储节点，则在同一台计算机上安装专用代理程序是明智之选。

与备份和 VM 复制计划（使用运行代理程序的计算机的时间设置）不同，脱离主机数据处理计划根据管理服务器计算机的时间设置运行。

备份扫描计划

支持的位置

您可以在以下位置扫描备份中的恶意软件：**云存储**、**本地文件夹**、**网络文件夹**只有安装在扫描计算机上的代理程序才能访问**本地文件夹**位置。

有关备份扫描的更多详细信息，请参阅“备份的反恶意软件扫描”。

创建备份扫描计划

1. 在安克诺斯数据保护软件 Web 中控台中，依次单击**计划** > **备份扫描**。
2. 单击**创建计划**。
3. [可选] 若要修改计划名称，请单击默认名称旁边的铅笔图标。
4. 选择扫描代理程序。
5. 选择要扫描的备份位置或单个备份。
   您可以一次选择多个备份位置。要在一个计划中包含多个单个备份，需要逐个添加备份。
6. [如果选择了**云存储**或**网络文件夹**] 如果出现提示，请提供访问备份存储的凭据。
7. [如果选择了加密备份] 请提供备份的访问密码。如果已选定保管库或多个加密备份，那么可以指定一个密码。如果特定备份的密码错误，将显示警报。只有提供了正确密码的备份才会被扫描。
8. 配置扫描计划。
9. 准备就绪后，单击**创建**。

这样将创建备份扫描计划。

备份复制

支持的位置

下表总结了备份复制计划支持的备份位置。

备份位置	支持作为来源	支持作为目标
云存储	+	+
本地文件夹	+	+
网络文件夹	+	+
NFS 文件夹	–	–
安全区	–	–
SFTP 服务器	–	–
受控位置*	+	+
磁带设备	–	+

* 检查主题 "使用高级许可证的注意事项"(第 225 页) 中所述的限制。

创建备份复制计划

1. 单击**计划** > **备份复制**。
2. 单击**创建计划**。
   软件显示新的计划模板。
3. [可选] 若要修改计划名称，请单击默认名称。

4. 单击**代理程序**，然后选择将要执行复制的代理程序。
   您可选择有权访问源和目标备份位置的任何代理程序。
5. 单击**要复制的项目**，然后选择此计划将复制的备份。
   使用右上角的**位置/备份**开关，即可在选择备份和选择全部位置之间切换。
   如果所选备份已加密，则所有备份必须使用相同的加密密码。对于使用不同加密密码的备份，请创建单独的计划。
6. 单击**目标位置**，然后指定目标位置。
7. [可选] 在**复制方法**中，选择要复制的备份。可选择以下其中一个选项：
   - **所有备份**(默认)
   - **仅完整备份**
   - **仅上次备份**
8. [可选] 单击**时间表**，然后更改时间表。
9. [可选] 单击**保留规则**，然后按照"保留规则"中所述，指定目标位置的保留规则。
10. 如果在**要复制的项目**中选择的备份已加密，则启用**备份密码**开关，然后提供加密密码。否则，请跳过此步骤。
11. [可选] 若要修改计划选项，请单击齿轮图标。
12. 单击**创建**。

验证

验证是用于检查通过备份进行数据恢复之可行性的一种操作。

备份位置验证可验证该位置中存储的所有备份。

工作方式

验证计划提供了两种验证方法。如果选择这两种方法，将连续执行相应操作。

- **计算备份中保存的每个数据块的校验和**
  有关通过计算校验和进行验证的详细信息，请参阅"备份验证"。
- **从备份运行虚拟机**
  此方法仅适用于包含操作系统的磁盘级别备份。要使用此方法，您需要 ESXi 或 Hyper-V 主机以及管理该主机的保护代理程序(适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序)。
  代理程序从备份运行虚拟机，然后连接至 VMware 工具或 Hyper-V 检测信号服务，以确保操作系统已成功启动。如果连接失败，代理程序会每两分钟尝试一次连接，共可尝试五次。如果所有尝试均失败，则验证失败。
  与验证计划和已验证备份的数量无关，执行验证的代理程序每次运行一个虚拟机。只要验证结果变得清晰，代理程序就会删除该虚拟机并运行下一个虚拟机。

如果验证失败，您可以在**概述**选项卡的**活动**部分上深入了解详细信息。

支持的位置

下表总结了验证计划支持的备份位置。

备份位置	计算校验和	运行 VM
云存储	+	+
本地文件夹	+	+
网络文件夹	+	+
NFS 文件夹	–	–
安全区	–	–
SFTP 服务器	–	–
受控位置	+	+
磁带设备	+	–

创建新的验证计划

1. 单击**计划** > **验证**。
2. 单击**创建计划**。
   软件显示新的计划模板。
3. [可选] 若要修改计划名称，请单击默认名称。
4. 单击**代理程序**，然后选择将要执行验证的代理程序。
   如果要通过从备份运行虚拟机来执行验证，则选择适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序。否则，选择在管理服务器上注册并有权访问备份位置的任何代理程序。
5. 单击**要验证的项目**，然后选择此计划将验证的备份。
   使用右上角的**位置/备份**开关，即可在选择备份和选择全部位置之间切换。
   如果所选备份已加密，则所有备份必须使用相同的加密密码。对于使用不同加密密码的备份，请创建单独的计划。
6. [可选] 在**验证内容**中，选择要验证的备份。可选择以下其中一个选项：
   - **所有备份**
   - **仅上次备份**
7. [可选] 单击**验证方法**，然后选择以下任意方法：
   - **校验和验证**
     软件将计算备份中保存的每个数据块的校验和。
   - **作为虚拟机运行**
     该软件将从每个备份运行虚拟机。
8. 如果选择**作为虚拟机运行**：
   a. 单击**目标计算机**，然后选择虚拟机类型（ESXi 或 Hyper-V）、主机和计算机名称模板。
      默认名称为 **[Machine Name]_validate**。
   b. 为 ESXi 单击**数据存储**或者为 Hyper-V 单击**路径**，然后为虚拟机选择数据存储。
   c. [可选] 更改磁盘调配模式。
      VMware ESXi 的默认设置为**精简**，Hyper-V 的默认设置为**动态扩展**。

d. [可选] 单击 **VM 设置**以更改虚拟机的内存大小和网络连接。
默认情况下，虚拟机未连接到网络，虚拟机的内存大小等于原始计算机的内存大小。

注意
始终启用**VM 检测信号**开关，以通过从备份运行虚拟机来验证来宾操作系统中的虚拟机监控程序工具（VMware Tools 或 Hyper-V Integration Services）报告的虚拟机的检测信号状态。此开关是为将来版本设计的，因此无法与之交互。

9. [可选] 单击**预定**，然后更改预定。
10. 如果在**要验证的项目**中选择的备份已加密，则启用**备份密码**开关，然后提供加密密码。否则，请跳过此步骤。
11. [可选] 要修改计划选项，请单击齿轮图标。
12. 单击**创建**。

清理

清理是一项根据保留规则删除过时备份的操作。

支持的位置

清理计划支持除 NFS 文件夹、SFTP 服务器和 安全区 之外的所有备份位置。

创建新的清理计划

1. 单击**计划** > **清理**。
2. 单击**创建计划**。
软件显示新的计划模板。
3. [可选] 若要修改计划名称，请单击默认名称。
4. 单击**代理程序**，然后选择将要执行清理的代理程序。
您可以选择有权访问备份位置的任何代理程序。
5. 单击**要清理的项目**，然后选择此计划将清理的备份。
使用右上角的**位置/备份**开关，即可在选择备份和选择全部位置之间切换。
如果所选备份已加密，则所有备份必须使用相同的加密密码。对于使用不同加密密码的备份，请创建单独的计划。
6. [可选] 单击**时间表**，然后更改时间表。
7. [可选] 单击**保留规则**，然后按照"保留规则"中所述，指定保留规则。
8. 如果在**要清理的项目**中选择的备份已加密，则启用**备份密码**开关，然后提供加密密码。否则，请跳过此步骤。
9. [可选] 若要修改计划选项，请单击齿轮图标。
10. 单击**创建**。

转换为虚拟机

您可以为转换到虚拟机创建单独的计划，并手动或按预定运行此计划。

关于先决条件和限制的信息，请参阅“关于转换需要知道的内容”。

为转换到虚拟机创建计划

1. 单击**计划** > **转换为 VM**。
2. 单击**创建计划**。
   软件显示新的计划模板。
3. [可选] 若要修改计划名称，请单击默认名称。
4. 在**转换为**中，选择目标虚拟机的类型。可选择以下其中一个选项：
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**
   - **VHDX 文件**

   注意
   要保存存储空间，每个到 VHDX 文件的转换都会覆盖在以前的转换期间创建的目标位置中的 VHDX 文件。

5. 请执行以下任一操作：
   - [对于 VMware ESXi、Hyper-V 和 Scale Computing HC3] 单击**主机**、选择目标主机，然后指定新的计算机名称模板。
   - [对于其他虚拟机类型] 在**路径**中，指定保存虚拟机文件和文件名称模板的位置。

   默认名称为 **[Machine Name]_converted**。
6. 单击**代理程序**，然后选择将执行转换的代理程序。
7. 单击**要转换的项目**，然后选择此计划将转换为虚拟机的备份。
   使用右上角的**位置/备份**开关，即可在选择备份和选择全部位置之间切换。
   如果所选备份已加密，则所有备份必须使用相同的加密密码。对于使用不同加密密码的备份，请创建单独的计划。
8. [仅适用于 VMware ESXi 和 Hyper-V] 为 ESXi 单击**数据存储**或者为 Hyper-V 单击**路径**，然后为虚拟机选择数据存储(存储) 。
9. [仅适用于 VMware ESXi 和 Hyper-V] 选择磁盘调配模式。VMware ESXi 的默认设置为**精简**，Hyper-V 的默认设置为**动态扩展**。
10. [可选] [对于 VMware ESXi、Hyper-V 和 Scale Computing HC3] 单击 **VM 设置**以修改虚拟机的内存大小、处理器数量或网络连接。
11. [可选] 单击**时间表**，然后更改时间表。
12. 如果在**要转换的项目**中选择的备份已加密，则启用**备份密码**开关，然后提供加密密码。否则，请跳过此步骤。
13. [可选] 若要修改计划选项，请单击齿轮图标。
14. 单击**创建**。

可启动媒体

重要事项
本部分中所述的一些功能仅适用于本地部署。

可启动媒体

可启动媒体是允许在基于 Linux 的环境中或 Windows 预安装环境 (WinPE) 中运行保护代理程序的物理媒体(CD、DVD、USB 闪存驱动器或计算机 BIOS 支持用作启动设备的其他可移动媒体) , 而无需操作系统的帮助。

可启动媒体最常用于:

- 恢复无法启动的操作系统
- 访问和备份损坏的系统中幸存的数据
- 在裸机部署操作系统
- 在裸机上创建基本或动态卷
- 逐个扇区备份采用不支持的文件系统的磁盘
- 离线备份任何由于访问受限、被正运行的应用程序锁定或其他任何原因而无法在线备份的数据。

还可以通过使用 Acronis PXE 服务器、Windows 部署服务 (WDS) 或远程安装服务 (RIS) 的网络启动, 来启动计算机。具有已上载可启动组件的这些服务器也可以视作一种可启动媒体。您可使用同一向导创建可启动媒体或配置 PXE 服务器或 WDS/RIS。

创建可启动媒体还是下载现成可用的可启动媒体?

使用"可启动媒体生成器", 您可以为 Windows, Linux 或 macOS 计算机创建自己的可启动媒体("基于 Linux"或"基于 WinPE") 。对于功能齐全的可启动媒体, 您需要指定 Acronis 安克诺斯数据保护软件 许可号。如果没有此密钥, 可启动媒体将只能执行恢复操作。

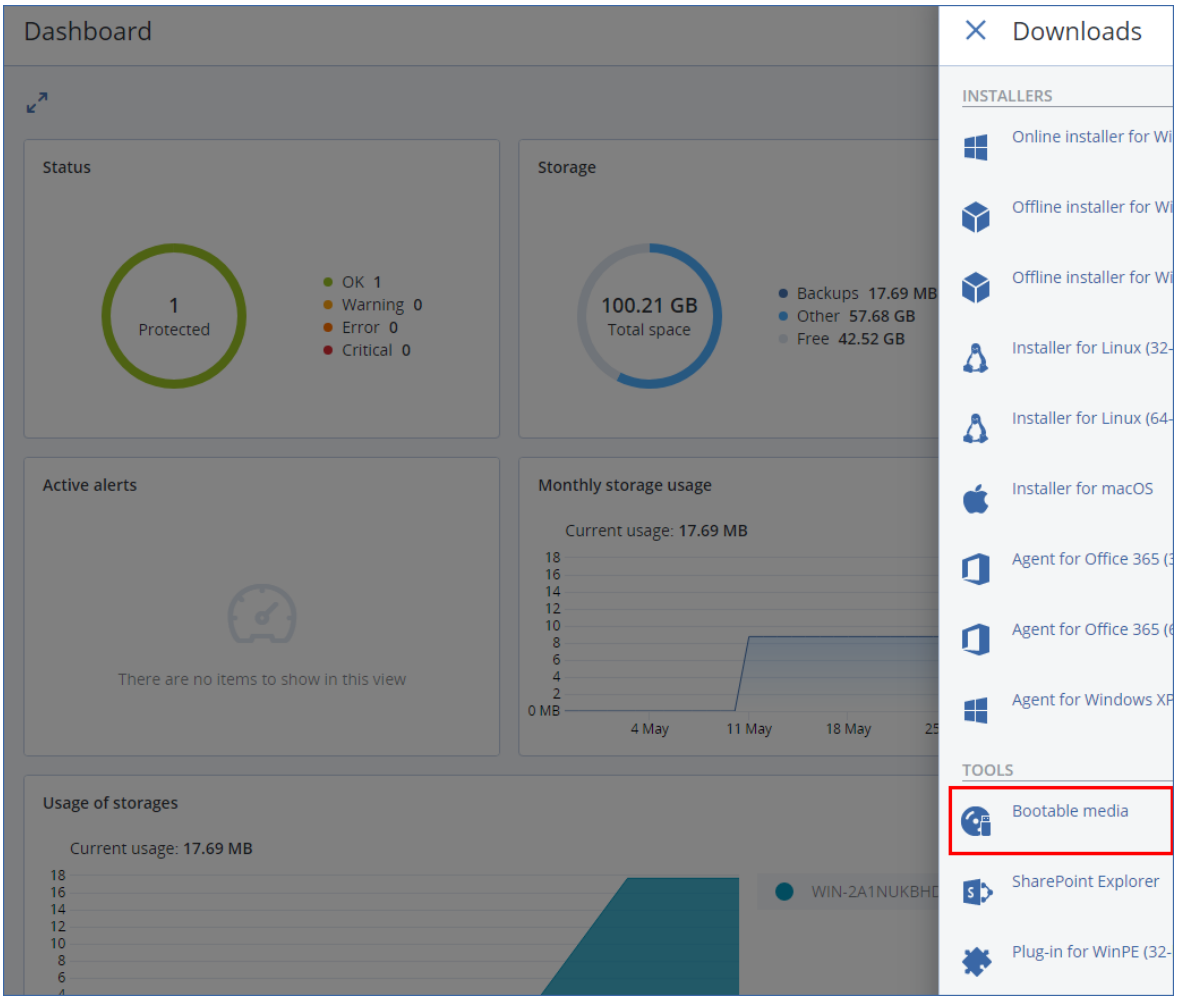
注意
可启动媒体不支持混合驱动器。

另外, 您可以下载现成可用的可启动媒体(仅基于 Linux) 。仅可使用下载的可启动媒体来进行恢复操作和访问 Acronis Universal Restore。您不能备份数据、验证或导出备份、管理磁盘或对其使用脚本。下载的可启动媒体不适用于 macOS 计算机。

注意
现成可用的可启动媒体不支持存储节点、磁带位置和 SFTP 位置。如果要在本地部署中使用这些存储位置, 则必须使用可启动媒体生成器创建自己的可启动媒体。请参阅 https://kb.acronis.com/content/61566。

下载现成可用的可启动媒体

1. 在安克诺斯数据保护软件 Web 中控台中，单击右上角的帐户图标，然后单击**下载**。
2. 选择 **可启动媒体**。



您可以将下载的 ISO 文件刻录到 CD/DVD 上，或者使用网上提供的免费工具之一创建可启动 USB 闪存驱动器。如果您需要启动 UEFI 计算机，请使用 ISO 到 USB 或 RUFUS；对于 BIOS 计算机，请使用 Win32DiskImager。在 Linux 中，使用 dd 实用工具较合理。

如果安克诺斯数据保护软件 Web 中控台不可访问，可以从 Acronis 客户门户中的帐户下载现成可用的可启动媒体：

1. 转到 https://account.acronis.com。
2. 找到 Acronis 安克诺斯数据保护软件，然后单击**下载**。
3. 在打开的页面上，找到**其他下载**，然后单击**可启动媒体 ISO (适用于 Windows 和 Linux)**。

是基于 Linux 还是基于 WinPE 的可启动媒体

基于 Linux

基于 Linux 的可启动媒体包含基于 Linux 内核的可启动保护代理程序。代理程序可在任何个人计算机兼容的硬件上启动并执行操作，包括裸机和带有已损坏的或不支持文件系统的计算机。在安克

诺斯数据保护软件 Web 中控台，可以采用本地或远程方式配置和控制操作。

基于 Linux 的媒体支持的硬件列表可在以下知识库文章中找到：http://kb.acronis.com/content/55310。

基于 WinPE

基于 WinPE 的可启动媒体包含一个称为 Windows 预安装环境 (WinPE) 的大小最小 Windows 系统和适用于 WinPE 的 Acronis 插件（即可在预安装环境中运行的改版保护代理程序）。

WinPE 被证明是用于含有各种硬件的较大环境中最方便的启动解决方案。

优点：

- 与使用基于 Linux 的可启动媒体相比，在 Windows 预安装环境中使用 Acronis 安克诺斯数据保护软件 可提供更多功能。在启动 PC 兼容硬件进入 WinPE 后，不仅可以使用保护代理程序，还可以使用 PE 命令和脚本以及已添加到 PE 中的其他插件。
- 基于 PE 的可启动媒体有助于克服某些与 Linux 相关的可启动媒体问题，如仅支持特定的 RAID 控制器或特定级别的 RAID 阵列。基于 WinPE 2.x 及更高版本的媒体允许动态加载必要的设备驱动程序。

限制：

- 基于 4.0 之前 WinPE 版本的可启动媒体无法在使用统一可扩展固件接口 (UEFI) 的计算机上启动。
- 当使用基于 PE 的可启动媒体启动计算机时，您无法选择光学媒体，例如 CD、DVD 或蓝光光盘 (BD)，作为备份目标。

可启动媒体生成器

可启动媒体生成器是一个用于创建可启动媒体的专用工具。仅适用于本地部署。

当安装管理服务器时，会默认安装可启动媒体生成器。您可以分别在运行 Windows 或 Linux 的任意计算机上安装媒体生成器。支持的操作系统与相应的代理程序一致。

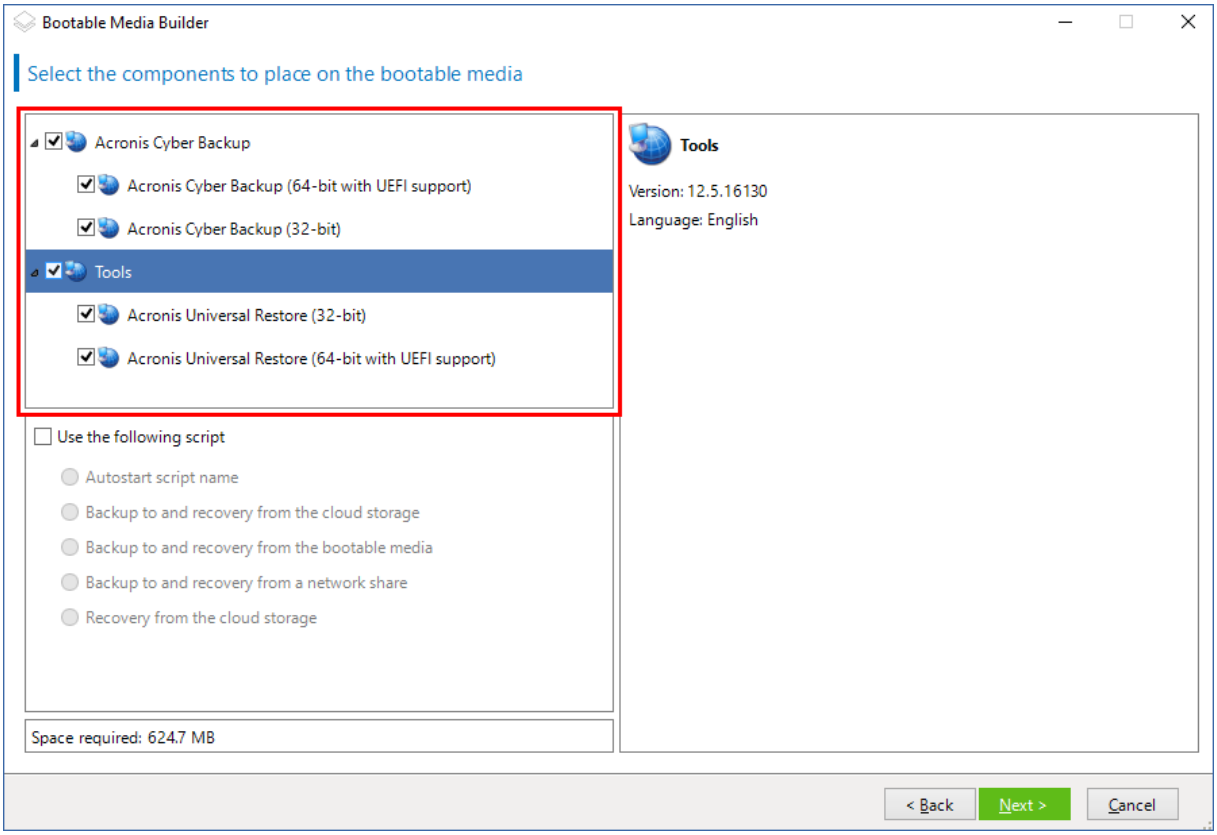
为什么要使用媒体生成器？

可用于在 安克诺斯数据保护软件 Web 中控台中进行下载的现成可用的可启动媒体仅可用于恢复。此媒体以 Linux 内核为基础。不同于 Windows PE，它不允许在运行时插入自定义驱动程序。

- 该媒体生成器使您能够创建带有备份功能的基于 Linux 或基于 WinPE 的自定义、功能齐全的可启动媒体。
- 除了创建物理可启动媒体之外，您还可以将其组件上载到 Windows 部署服务 (WDS)，然后使用网络启动。
- 现成可用的可启动媒体不支持存储节点、磁带位置和 SFTP 位置。如果要在本地部署中使用这些存储位置，则必须使用可启动媒体生成器创建自己的可启动媒体。请参阅 https://kb.acronis.com/content/61566。

32 位还是 64 位?

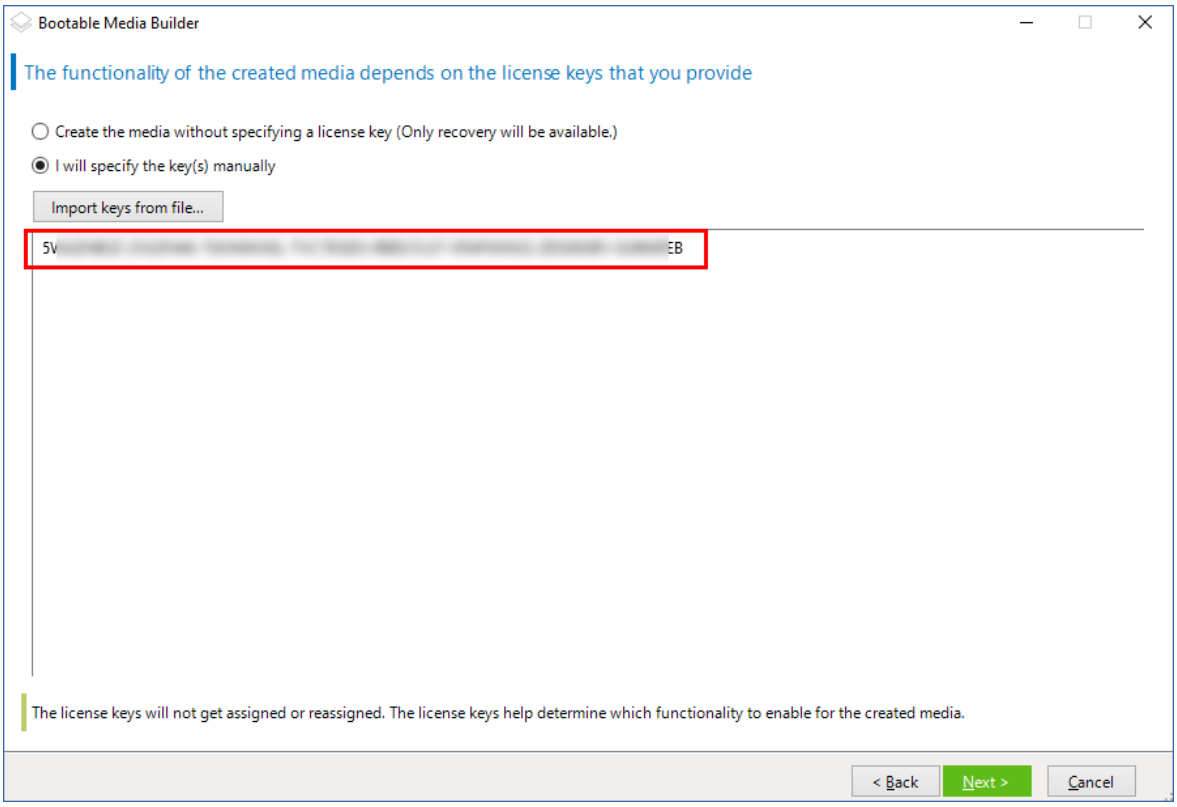
可启动媒体生成器创建包含 32 位和 64 位组件的媒体。在大多数情况下，您需要使用 64 位媒体来启动使用统一可扩展固件接口 (UEFI) 的计算机。



基于 Linux 的可启动媒体

若要创建基于 Linux 的可启动媒体，请执行以下操作：

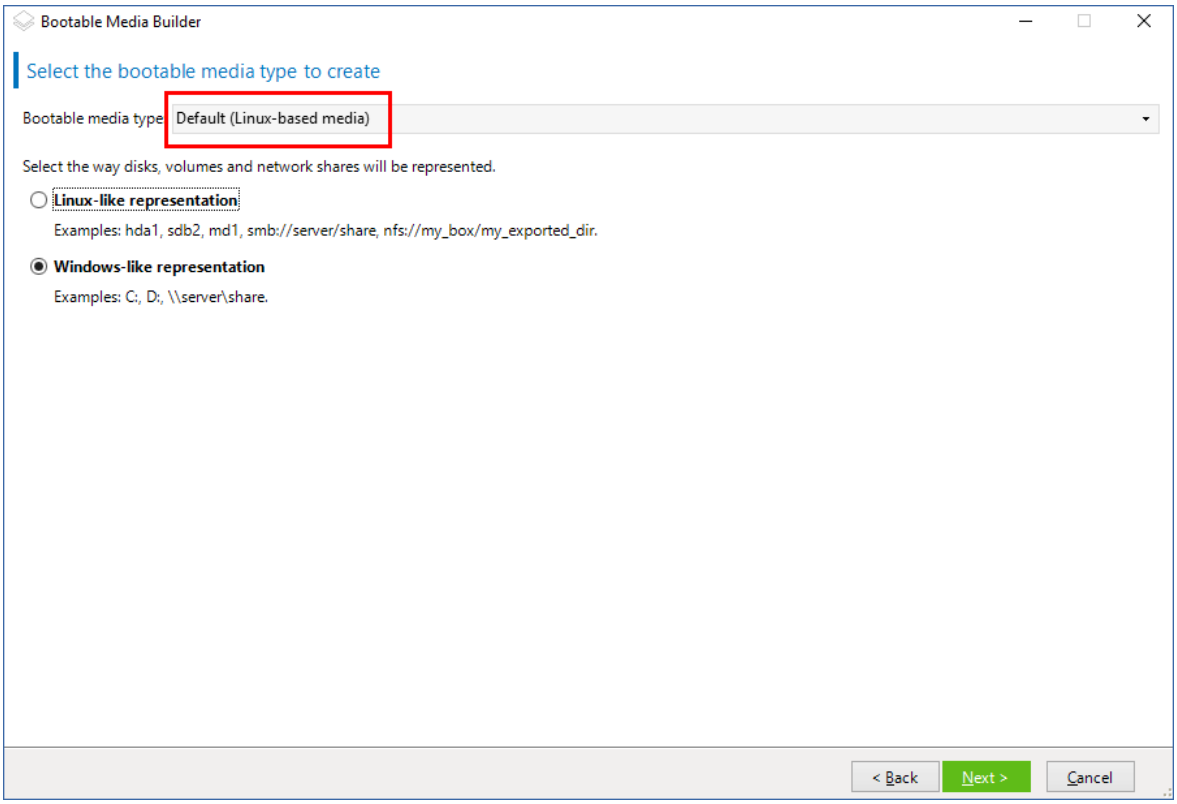
1. 启动**可启动媒体生成器**。
2. 要创建功能齐全的可启动媒体，请指定一个 Acronis 安克诺斯数据保护软件 许可号。此许可号用于确定哪些功能将包含在可启动媒体中。不会有任何计算机的许可证被吊销。
   如果不指定许可号，则生成的可启动媒体只能用于恢复操作。



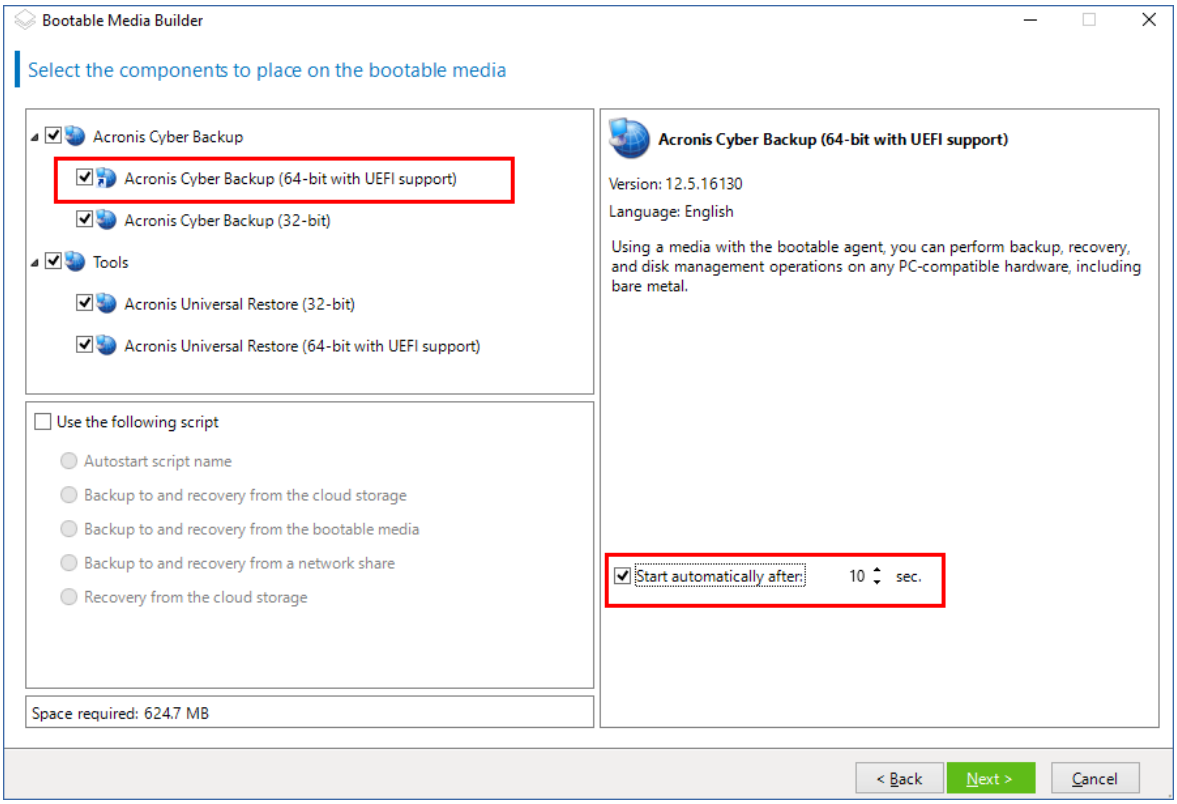
3. 选择**可启动媒体类型：默认（基于 Linux 的媒体）**。

   选择卷和网络资源的显示方式：

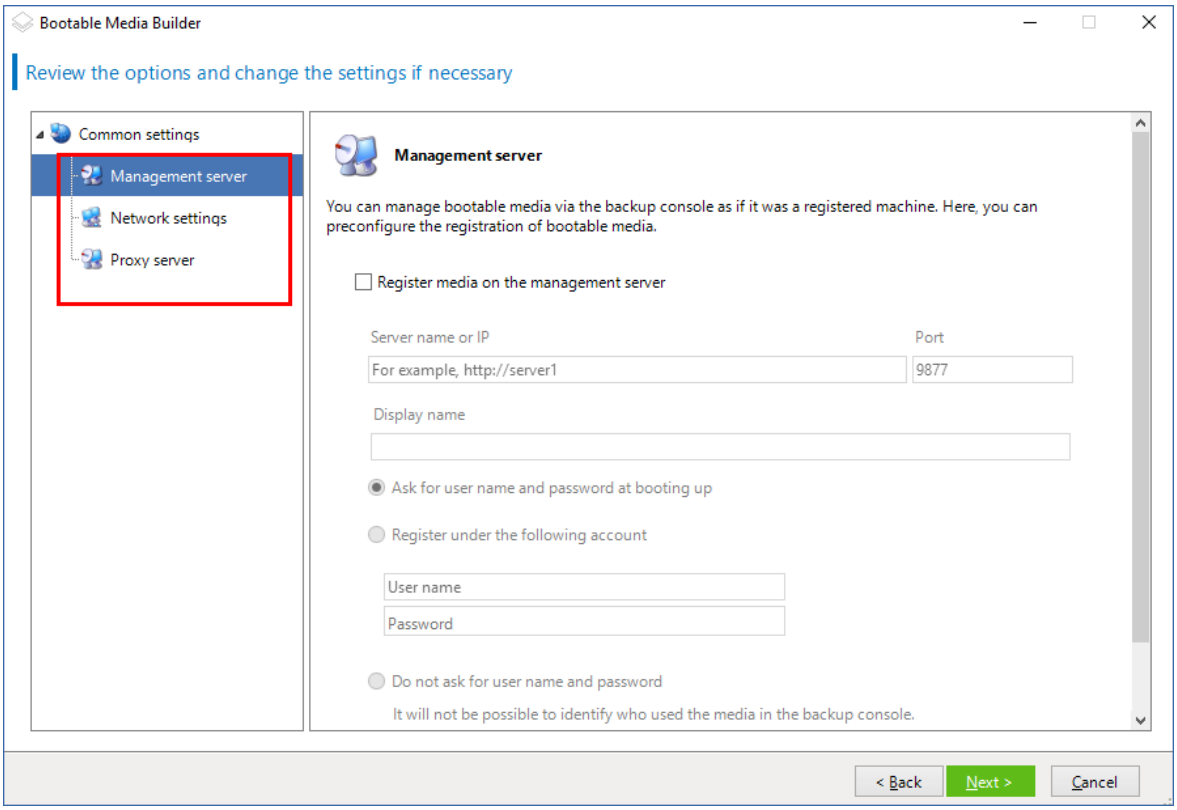
   - 采用 Linux 格式卷处理的媒体将卷显示为 hda1 和 sdb2 等。在开始恢复之前，它会尝试重建 MD 设备和逻辑 (LVM) 卷。
   - 采用 Windows 格式卷处理的媒体将卷显示为 C:和 D:。它提供对动态 (LDM) 卷的访问。



4. [可选] 指定 Linux 内核的参数。请用空格分隔多个参数。
   例如，要在每次媒体启动时能够为可启动代理程序选择显示模式，请键入：**vga=ask**
   有关可用参数的详细信息，请参阅内核参数。
5. [可选] 选择将在可启动媒体中使用的语言。
6. 选择要置于媒体上的组件：Acronis 安克诺斯数据保护软件 可启动代理程序和/或 Universal Restore（如果计划在不同硬件上还原系统）。
   使用可启动代理程序可在任何与计算机兼容的硬件，包括裸机上，进行备份、恢复和磁盘管理操作。
   异机还原使您能够启动恢复到不同硬件或虚拟机的操作系统。该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、母板或芯片集）的驱动程序。
7. [可选] 指定启动菜单的超时时间间隔以及在超时时自动启动的组件。要执行此操作，请单击左上窗格中所需的组件，然后设置其时间间隔。在从 WDS/RIS 启动时，这可以完成无人参与的现场操作。
   如果此设置未配置，加载程序将会等待用户选择是启动操作系统（如果存在）还是组件。



8. [可选] 如果要实现可启动代理程序操作自动化，请选中**使用以下脚本**复选框。然后，选择其中一个脚本并指定脚本参数。
9. [可选] 选择如何在启动时在管理服务器上注册媒体。有关注册设置的更多信息，请参阅"管理服务器"。



10. [可选] 指定网络设置：要指定给计算机网络适配器的 TCP/IP 设置。有关详细信息，请参阅 "网络设置"(第 323 页) 。
11. [可选] 指定网络端口：可启动代理监听传入连接的 TCP 端口。
12. [可选] 如果在网络中启用了代理服务器，请指定其主机名/IP 地址和端口。
13. 选择媒体类型。您可以：
    - 创建 ISO 映像。然后您可以将其刻录到 CD/DVD；使用它创建可启动 USB 闪存驱动器；或将其连接到虚拟机。
    - 创建 ZIP 文件。
    - 将所选组件上载到 Acronis PXE 服务器。
    - 将所选组件上载到 WDS/RIS。
14. [可选] 添加异机还原要使用的 Windows 系统驱动程序。仅当异机还原添加到媒体并且选择了 WDS/RIS 之外的媒体时，才会显示该窗口。
15. 如果出现系统提示，请指定 WDS/RIS 的主机名/IP 地址和凭据，或者指定媒体 ISO 文件的路径。
16. 在摘要窗口中查看您的设置，然后单击**继续**。

内核参数

此窗口允许您指定 Linux 内核的一个或多个参数。当可启动媒体启动时，会自动应用这些参数。

当使用可启动媒体遇到问题时，通常会使用这些参数。一般情况下，您可以将此字段留空。

您也可以通过在启动菜单中按 F11 来指定这些参数。

参数

若要指定多个参数，请用空格将其分开。

acpi=off

禁用高级配置和电源接口 (ACPI)。当特定的硬件配置遇到问题时，您可能想要使用此参数。

noapic

禁用高级可编程中断控制器 (APIC)。当特定的硬件配置遇到问题时，您可能想要使用此参数。

vga=ask

提示可启动媒体的图形用户界面将使用的视频模式。若无 **vga** 参数，系统会自动检测视频模式。

vga= *mode_number*

指定可启动媒体的图形用户界面将使用的视频模式。模式编号由 *mode_number* 以十六进制格式给出，例如：**vga=0x318**

与模式编号对应的屏幕分辨率和颜色数可能因计算机而异。建议您先使用 **vga=ask** 参数来选择 *mode_number* 的值。

quiet

加载 Linux 内核时禁止显示启动消息，并在加载内核后启动管理中控台。

此参数在创建可启动媒体时隐式指定，但您可以在启动菜单中删除此参数。

没有此参数，将显示所有启动消息，后跟命令指示符。要从命令提示符启动管理中控台，请运行以下命令：**/bin/product**

nousb

禁止加载 USB（通用串行总线）子系统。

nousb2

禁用 USB 2.0 支持。USB 1.1 设备仍可使用此参数。此参数允许您在 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）。

nodma

禁止所有 IDE 硬盘驱动器的直接内存访问 (DMA)。防止内核在某些硬件上冻结。

nofw

禁用 FireWire (IEEE1394) 接口支持。

nopcmcia

禁用 PCMCIA 硬件检测。

nomouse

禁用鼠标支持。

module_name **=off**

禁用由 *module_name* 提供其名称的模块。例如，要禁用 SATA 模块，请指定：**sata_sis=off**

pci=bios

强制使用 PCI BIOS，不直接访问硬件设备。如果计算机上有一个非标准 PCI 主机桥，则可使用此参数。

pci=nobios

禁止使用 PCI BIOS，仅允许使用直接硬件访问方式。若可启动媒体无法启动（可能由 BIOS 引起），可以使用此参数。

pci=biosirq

使用 PCI BIOS 调用来获得中断路由表。若内核无法分配中断请求 (IRQ) 或在主板上发现次要 PCI 总线，可使用此参数。

这些调用可能在某些计算机上无法正常工作，但这是获得中断路由表的唯一方式。

LAYOUTS=en-US, de-DE, fr-FR, ...

指定在可启动媒体的图形用户界面中可使用的键盘布局。

如果没有此参数，则只可使用两个布局："美式英语"和与媒体的启动菜单中所选语言相对应的布局。

可以指定以下任意布局：

比利时语：**be-BE**

捷克语：**cz-CZ**

英语：**en-GB**

美式英语：**en-US**

法语：**fr-FR**

法语（瑞士）：**fr-CH**

德语：**de-DE**

德语（瑞士）：**de-CH**

意大利语：**it-IT**

波兰语：**pl-PL**

葡萄牙语：**pt-PT**

葡萄牙语（巴西）：**pt-BR**

俄语：**ru-RU**

塞尔维亚语（西里尔语）：**sr-CR**

塞尔维亚语（拉丁语）：**sr-LT**

西班牙语：**es-ES**

在可启动媒体下工作时，可使用 CTRL + SHIFT 来循环显示可用布局。

可启动媒体中的脚本

如果您希望可启动媒体执行一组确定的操作，则在可启动媒体生成器中创建媒体时可以指定一个脚本。每次媒体启动时，都会运行此脚本，而不是显示用户界面。

您可以选择预定义的脚本之一或遵循以下脚本约定创建自定义脚本。

预定义脚本

可启动媒体生成器提供以下预定义脚本：

- 备份到云存储和从云存储恢复 (**entire_pc_cloud**)
- 备份到可启动媒体和从可启动媒体恢复 (**entire_pc_local**)
- 备份到网络共享和从网络共享恢复 (**entire_pc_share**)
- 从云存储恢复 (**golden_image**)

脚本可在安装了可启动媒体生成器的计算机的以下目录中找到：

- 在 Windows 中：**%ProgramData%\Acronis\MediaBuilder\scripts**
- 在 Linux 中：**/var/lib/Acronis/MediaBuilder/scripts/**

备份到云存储和从云存储恢复

此脚本可将计算机备份到云存储，或从此脚本在云存储中创建的最近备份恢复该计算机。开始时，脚本将提示用户在备份、恢复和启动用户界面之间进行选择。

在可启动媒体生成器中，指定以下脚本参数：

1. 云存储的用户名和密码。
2. [可选] 脚本将用于加密或访问备份的密码。

备份到可启动媒体和从可启动媒体恢复

此脚本可将计算机备份到可启动媒体，或从此脚本在相同媒体中创建的最近备份恢复该计算机。开始时，脚本将提示用户在备份、恢复和启动用户界面之间进行选择。

在可启动媒体生成器中，可以指定脚本将用于加密或访问备份的密码。

备份到网络共享和从网络共享恢复

此脚本可将计算机备份到网络共享，或从其位于网络共享的最近备份恢复该计算机。开始时，脚本将提示用户在备份、恢复和启动用户界面之间进行选择。

在可启动媒体生成器中，指定以下脚本参数：

1. 网络共享路径。
2. 网络共享的用户名和密码。
3. [可选] 备份文件名。默认值为**自动备份**。如果您希望脚本将备份附加到现有备份，或者从采用非默认名称的备份恢复，则将默认值更改为此备份的文件名称。

   查找备份文件名

   a. 在安克诺斯数据保护软件 Web 中控台中，转到**备份存储** > **位置**。
   b. 选择网络共享（如果共享未列出，请单击**添加位置**）。
   c. 选择备份。
   d. 单击**详细信息**。文件名显示在**备份文件名**下方。
4. [可选] 脚本将用于加密或访问备份的密码。

从云存储恢复

此脚本将从位于云存储中的最近备份恢复该计算机。开始时，脚本将提示用户指定以下各项：

1. 云存储的用户名和密码。
2. 密码（如果备份已加密）。

建议您在此云存储帐户下仅存储一台计算机的备份。否则，如果另一台计算机的备份比当前计算机的备份更新，脚本将选择那台计算机的备份。

自定义脚本

重要事项
创建自定义脚本需要 Bash 命令语言和 JavaScript 对象表示法 (JSON) 的知识。如果您不熟悉 Bash，则 http://www.tldp.org/LDP/abs/html 是学习的好地方。在 http://www.json.org 中将提供 JSON 规范。

脚本文件

脚本必须位于安装了可启动媒体生成器的计算机的以下目录中：

- 在 Windows 中：**%ProgramData%\Acronis\MediaBuilder\scripts**
- 在 Linux 中：**/var/lib/Acronis/MediaBuilder/scripts/**

脚本必须包括至少三个文件：

- **<script_file>.sh** - 一个带 Bash 脚本的文件。创建该脚本时，仅使用有限的 shell 命令集，该命令集可在 https://busybox.net/downloads/BusyBox.html 中找到。也可以使用以下命令：
  - `acrocmd` - 备份和恢复的命令行实用程序
  - `product` - 启动可启动媒体用户界面的命令

  此文件和脚本包含（例如，通过使用 dot 命令）的任何其他文件必须位于 **bin** 子文件夹中。在脚本中，将其他文件路径指定为 **/ConfigurationFiles/bin/<some_file>**。
- **autostart** - 启动 **<script_file>.sh** 的文件。文件内容必须如下：

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - 一个包含以下内容的 JSON 文件：
  - 要在可启动媒体生成器中显示的脚本名称和描述。
  - 要通过可启动媒体生成器配置的脚本变量的名称。
  - 将在可启动媒体生成器中显示的每个变量的控制参数。

Autostart.json 的结构

顶级对象

配对		必需	描述
名称	值类型		
displayName	字串	是	要在可启动媒体生成器中显示的脚本名称。
description	字串	否	要在可启动媒体生成器中显示的脚本描述。
timeout	编号	否	启动该脚本前启动菜单的超时（以秒为单位）。如果未指

			定配对，超时将为 10 秒。
variables	对象	否	要通过可启动媒体生成器配置的 **<script_file>.sh** 的任何变量。 此值应为一组以下配对：一个变量的字串标识符与该变量的对象（参见下表）。

变量对象

配对		必需	描述
名称	值类型		
displayName	字串	是	**<script_file>.sh** 中使用的变量名称。
type	字串	是	可启动媒体生成器中显示的控件类型。此控件用于配置变量值。 有关所有支持的类型，请参见下表。
description	字串	是	显示在可启动媒体生成器中控件上方的控件标签。
default	string，如果 type 是 string、multiString、password 或 enum number，如果 type 是 number、spinner 或 checkbox	否	控件的默认值。如果未指定配对，则默认值将为空字串或零，视控件类型而定。 复选框的默认值可以为 0（取消勾选状态）或 1（勾选状态）。
order	编号 （非负）	是	可启动媒体生成器中的控件顺序。此值越高，控件相对于 **autostart.json** 中定义的其他控件的位置越低。初始值必须为 0。
min （仅适用于 spinner）	编号	否	选值框中选值控件的最小值。如果未指定配对，则该值将为 0。
max （仅适用于 spinner）	编号	否	选值框中选值控件的最大值。如果未指定配对，则该值将为 100。
step （仅适用于	编号	否	选值框中选值控件的步进值。如果未指定配对，则该值将为 1。

spinner)			
items (仅适用于 enum)	字串阵列	是	下拉列表的值。
required (适用于 string、multiString、password 和 enum)	编号	否	指定控件值可以为空 (0) 或不可以为空 (1)。如果未指定配对，则控件值可以为空。

控件类型

名称	说明
string	单行不受限文本框用于输入或编辑短字串。
multiString	多行不受限文本框用于输入或编辑长字串。
password	单行不受限文本框用于安全地输入密码。
number	单行仅限数值文本框用于输入或编辑数值。
spinner	单行仅限数值文本框用于输入或编辑数值，有一个选值控件，也称为选值框。
enum	标准下拉列表，有一组固定的预定值。
checkbox	复选框，有两种状态 - 取消勾选状态或勾选状态。

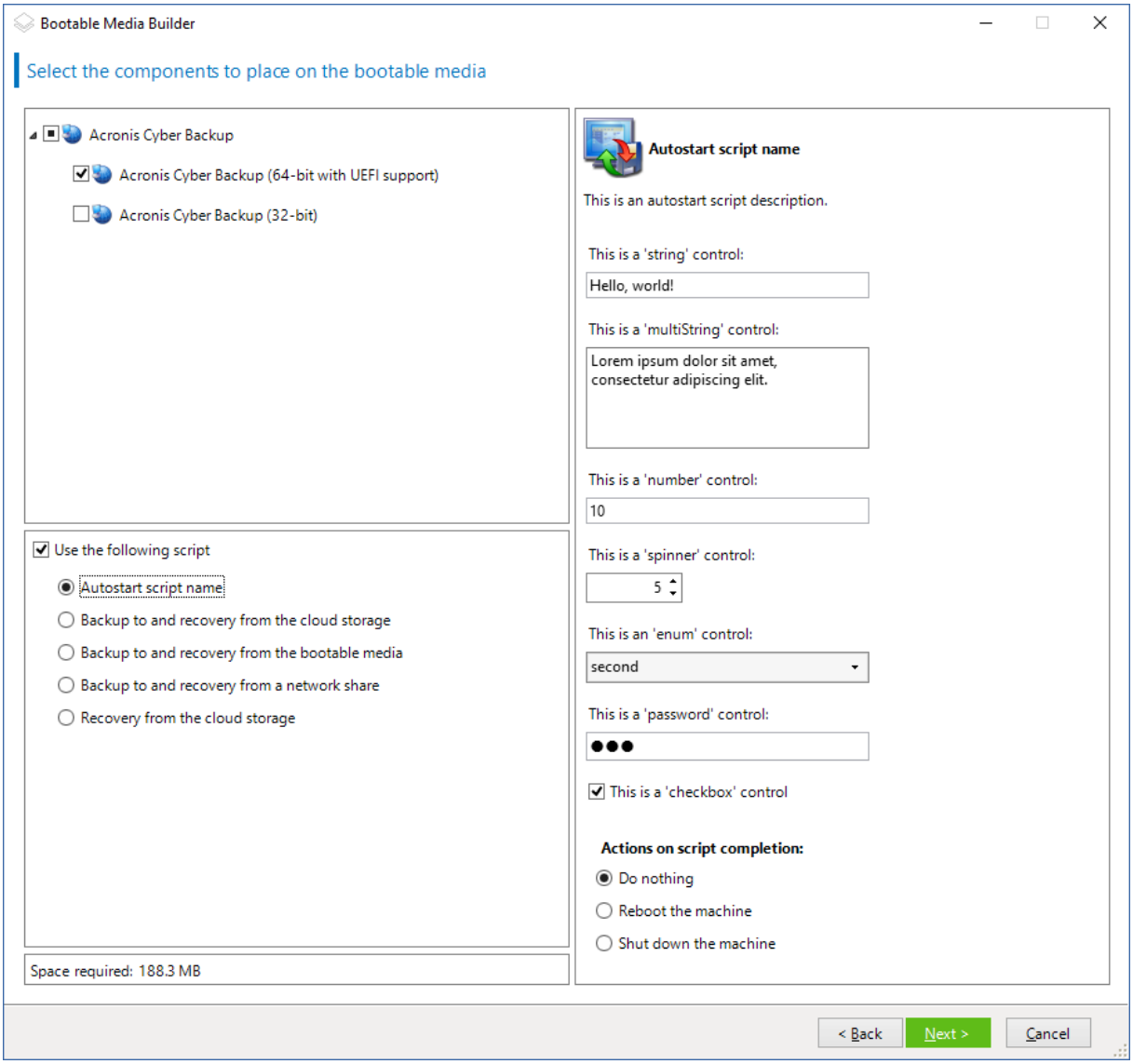
下面的 **autostart.json** 示例包含可用于配置 **<script_file>.sh** 变量的所有可能的控件类型。

```
{
        "displayName":"Autostart script name",
        "description":"This is an autostart script description.",
        "variables": {
                "var_string": {
                        "displayName":"VAR_STRING",
                        "type":"string", "order": 1,
                        "description":"This is a 'string' control:", "default": "Hello, world!"
                },
                "var_multistring": {
                        "displayName":"VAR_MULTISTRING",
```

```
        "type":"multiString", "order": 2,
        "description":"This is a 'multiString' control:",
        "default":"Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
    },
    "var_number": {
        "displayName":"VAR_NUMBER",
        "type":"number", "order": 3,
        "description":"This is a 'number' control:", "default": 10
    },
    "var_spinner": {
        "displayName":"VAR_SPINNER",
        "type":"spinner", "order": 4,
        "description":"This is a 'spinner' control:",
        "min":1, "max": 10, "step": 1, "default": 5
    },
    "var_enum": {
        "displayName":"VAR_ENUM",
        "type":"enum", "order": 5,
        "description":"This is an 'enum' control:",
        "items": ["first", "second", "third"], "default": "second"
    },
    "var_password": {
        "displayName":"VAR_PASSWORD",
        "type":"password", "order": 6,
        "description":"This is a 'password' control:", "default": "qwe"
    },
    "var_checkbox": {
        "displayName":"VAR_CHECKBOX",
        "type":"checkbox", "order": 7,
        "description":"This is a 'checkbox' control", "default":1
    }
```

```
        }
}
```

这是其在可启动媒体生成器中的表现形式。



管理服务器

在创建可启动媒体时，您可以选择在管理服务器上预配置媒体注册。

注册媒体让您可以将媒体作为注册计算机以通过 安克诺斯数据保护软件 Web 中控台进行管理。除了方便远程访问，这还让管理员能够跟踪在可启动媒体下执行的所有操作。操作都记录在**活动**中，因此可以查看何人何时开始操作。

如果没有预配置注册，在从媒体启动计算机后仍然可以注册媒体。

在管理服务器上预配置注册

1. 勾选**在管理服务器上注册媒体**复选框。
2. 在**服务器名称或 IP** 中，指定安装了管理服务器的计算机的主机名或 IP 地址。可以使用以下其中一种格式：
   - http://<服务器>。例如 http://10.250.10.10 或 http://server1
   - <IP 地址>。例如 10.250.10.10
   - <主机名>。例如 server1 或 server1.example.com
3. 在**端口**中，指定要用于访问管理服务器的端口。默认值为 9877。
4. 在**显示名称**中，指定该计算机在 安克诺斯数据保护软件 Web 中控台中显示的名称。若此字段留为空白，则显示名称将设置为以下其中一种：
   - 如果之前在管理服务器上注册了该计算机，则其将拥有相同的名称。
   - 否则，将使用该计算机的完全限定域名 (FQDN) 或 IP 地址。
5. 选择将用于在管理服务器上注册媒体的帐户。可使用以下选项：
   - **在启动时请求提供用户名和密码**

     每次从媒体启动计算机时都必须提供凭据。

     对于成功的注册，帐户必须位于管理服务器管理员（**设置** > **帐户**）的列表中。在 安克诺斯数据保护软件 Web 中控台中，根据给予指定帐户的权限，媒体将显示在组织下或特定单位下。

     在可启动媒体界面中，可以通过单击**工具** > **在管理服务器上注册媒体**，更改用户名和密码。
   - **使用以下帐户注册**

     每次从媒体启动计算机时，会自动注册计算机。

     您指定的帐户必须位于管理服务器管理员（**设置** > **帐户**）的列表中。在 安克诺斯数据保护软件 Web 中控台中，根据给予指定帐户的权限，媒体将显示在组织下或特定单位下。

     在可启动媒体界面中，*无法*更改注册参数。

网络设置

创建可启动媒体时，您可选择预配置将由可启动代理程序使用的网络连接。下列参数可预配置：

- IP 地址
- 子网掩码
- 网关
- DNS 服务器
- WINS 服务器

当可启动代理程序在计算机上启动时，该配置将应用于计算机的网络接口卡 (NIC)。若尚未预配置设置，代理程序将使用 DHCP 自动配置。当可启动代理程序在计算机上运行时，您也可以手动配置网络设置。

预配置多个网络连接

您可为多达 10 个网络接口卡预配置 TCP/IP 设置。为确保为每个 NIC 指定适合的设置，在相应服务器上创建将被自定义的媒体。当您在向导窗口中选择一个现有 NIC 时，其设置被选中保存在该媒体上。每个现有 NIC 的 MAC 地址也将保存在该媒体上。

除 MAC 地址外，您可更改任何设置；或在必要时为不存在的 NIC 配置设置。

当可启动代理程序在服务器上启动，它将检索可用 NIC 的列表。此列表按 NIC 占用的插槽排序：最接近处理器的位于顶部。

可启动代理程序为每个已知的 NIC 指定适合的设置，通过其 MAC 地址识别 NIC。在配置包含已知 MAC 地址的 NIC 后，将从上部未指定的 NIC 开始为剩余的 NIC 指定您为不存在的 NIC 所指定的设置。

您可为任何计算机自定义可启动媒体，而不仅限于在之上创建了媒体的计算机。若要进行此操作，根据它们在该计算机上的插槽顺序配置 NIC：NIC1 占用最接近处理器的插槽，NIC2 位于下一个插槽，依此类推。当可启动代理程序在该计算机上启动时，它将无法找到具有已知 MAC 地址的 NIC 并将采用与您所使用的相同顺序配置 NIC。

示例

可启动代理程序可使用其中一个网络适配器通过生产网络与管理中控台通信。可为此连接进行自动配置。用于恢复的可更改大小的数据可通过第二个 NIC 传输，使用静态 TCP/IP 设置的方式包括在专用的备份网络中。

网络端口

创建可启动媒体时，可以选择预配置可启动代理程序监听来自 acrocmd 实用工具的传入连接的网络端口。可用选项有：

- 默认端口
- 目前使用的端口
- 新端口（输入端口号）

若该端口尚未预配置，代理程序将使用端口 9876。

供异机还原使用的驱动程序

在创建可启动媒体时，您可以选择将 Windows 驱动程序添加到媒体中。异机还原将使用这些驱动程序来启动迁移到相异硬件的 Windows。

您能够配置异机还原，以便：

- 在媒体中搜索最适合目标硬件的驱动程序
- 获取您从媒体明确指定的大容量存储驱动程序。如果目标硬件具有用于硬盘的特定大容量存储控制器（如 SCSI、RAID 或光纤通道适配器），则必须使用该功能。

驱动程序将置于可启动媒体上的可见 Drivers 文件夹中。这些驱动程序不会加载到目标计算机 RAM 中，因此在整个异机还原操作过程中媒体必须保持插入或连接状态。

当您创建可移动媒体或其 ISO 或可拆卸媒体（如闪存驱动器）时，可以使用将驱动程序添加到可启动媒体的方式。驱动程序无法上载到 WDS/RIS。

您只能通过添加 INF 文件或包含此类文件的文件夹，以组的形式将驱动程序添加到列表中。您将无法从 INF 文件中选择单独的驱动程序，但媒体生成器会显示文件内容以为您提供相关信息。

若要添加驱动程序，请执行以下操作：

1. 单击**添加**，然后浏览到 INF 文件或包含 INF 文件的文件夹。
2. 选择 INF 文件或文件夹。
3. 单击**确定**。

您只能通过删除 INF 文件，以组的形式从列表中删除驱动程序。

若要删除驱动程序，请执行以下操作：

1. 选择 INF 文件。
2. 单击**删除**。

基于 WinPE 的可启动媒体

可启动媒体生成器提供了将 Acronis 安克诺斯数据保护软件 与 WinPE 相集成的两种方法：

- 使用该插件从头创建 PE ISO。
- 将 Acronis 插件添加到 WIM 文件，以供将来使用（手动创建 ISO、将其他工具添加到映像等）。

您可以创建基于 WinRE 的 PE 映像，而无需任何其他准备，也可以在安装 Windows 自动安装工具包 (AIK) 或 Windows 评估和部署工具包 (ADK) 后创建 PE 映像。

基于 WinRE 的 PE 映像

以下操作系统支持创建基于 WinRE 的映像：

- Windows 7（32 位和 64 位）
- Windows 8、8.1、10（32 位和 64 位）
- Windows Server 2012、2016、2019（64 位）

PE 映像

安装 Windows 自动安装工具包 (AIK) 或 Windows 评估和部署工具包 (ADK) 后，可启动媒体生成器支持基于以下任何内核的 WinPE 分发：

- Windows Vista (PE 2.0)
- Windows Vista SP1 和 Windows Server 2008 (PE 2.1)
- 带或不带 Windows 7 SP1 (PE 3.1) 增补包的 Windows 7 (PE 3.0)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE for Windows 10)

可启动媒体生成器支持 32 位和 64 位 WinPE 分发。32 位 WinPE 分发也可在 64 位硬件上运行。但是，您需要通过 64 位分发来启动使用统一可扩展固件接口 (UEFI) 的计算机。

基于 WinPE 4 和更高版本的 PE 映像大约需要 1 GB 的 RAM 才能正常工作。

注意
磁盘管理功能不可用于基于 Windows PE 4.0 和更高版本的可启动媒体。因此，磁盘管理支持 Windows 7 和更早的操作系统。如需在 Windows 8 和更高版本上执行磁盘管理操作，您需要安装 Acronis Disk Director。有关详细信息，请参阅此知识库文章：
https://kb.acronis.com/content/47031。

准备：WinPE 2.x 和 3.x

为了能够创建或修改 PE 2.x 或 3.x 映像，请在安装了 Windows 自动安装工具包 (AIK) 的计算机上安装可启动媒体生成器。如果您没有带 AIK 的计算机，请按以下所示进行准备：

准备带 AIK 的计算机

1. 下载并安装 Windows 自动安装工具包。
   适用于 Windows Vista (PE 2.0) 的自动安装工具包 (AIK)：
   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=en
   适用于 Windows Vista SP1 和 Windows Server 2008 (PE 2.1) 的自动安装工具包 (AIK)：
   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=en
   适用于 Windows 7 (PE 3.0) 的自动安装工具包 (AIK)：
   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=en
   适用于 Windows 7 SP1 (PE 3.1) 的自动安装工具包 (AIK) 补充：
   http://www.microsoft.com/download/en/details.aspx?id=5188
   您可以单击上述链接找到安装的系统要求。
2. [可选] 将 WAIK 刻录到 DVD 或复制到闪存驱动器。
3. 从该工具包安装 Microsoft .NET Framework(NETFXx86 或 NETFXx64，视您的硬件而定)。
4. 从该工具包安装 Microsoft Core XML (MSXML) 5.0 或 6.0 分析器。
5. 从该工具包安装 Windows AIK。
6. 在同一计算机上安装可启动媒体生成器。

建议您熟悉一下 Windows AIK 提供的帮助文档。要访问文档，请从“开始”菜单中选择 **Microsoft Windows AIK -> 文档**。

准备：WinPE 4.0 和更高版本

为了能够创建或修改 PE 4 或更高版本映像，请在已安装 Windows 评估和部署工具包 (ADK) 的计算机上安装可启动媒体生成器。如果您没有带 ADK 的计算机，请按以下所示进行准备：

准备带 ADK 的计算机

1. 下载评估和部署工具包的安装程序。

   适用于 Windows 8 (PE 4.0) 的评估和部署工具包 (ADK): http://www.microsoft.com/en-us/download/details.aspx?id=30652。

   适用于 Windows 8.1 (PE 5.0) 的评估和部署工具包 (ADK): http://www.microsoft.com/en-US/download/details.aspx?id=39982。

   适用于 Windows 10 (PE for Windows 10) 的评估和部署工具包 (ADK): https://msdn.microsoft.com/en-us/windows/hardware/dn913721%28v=vs.8.5%29.aspx。

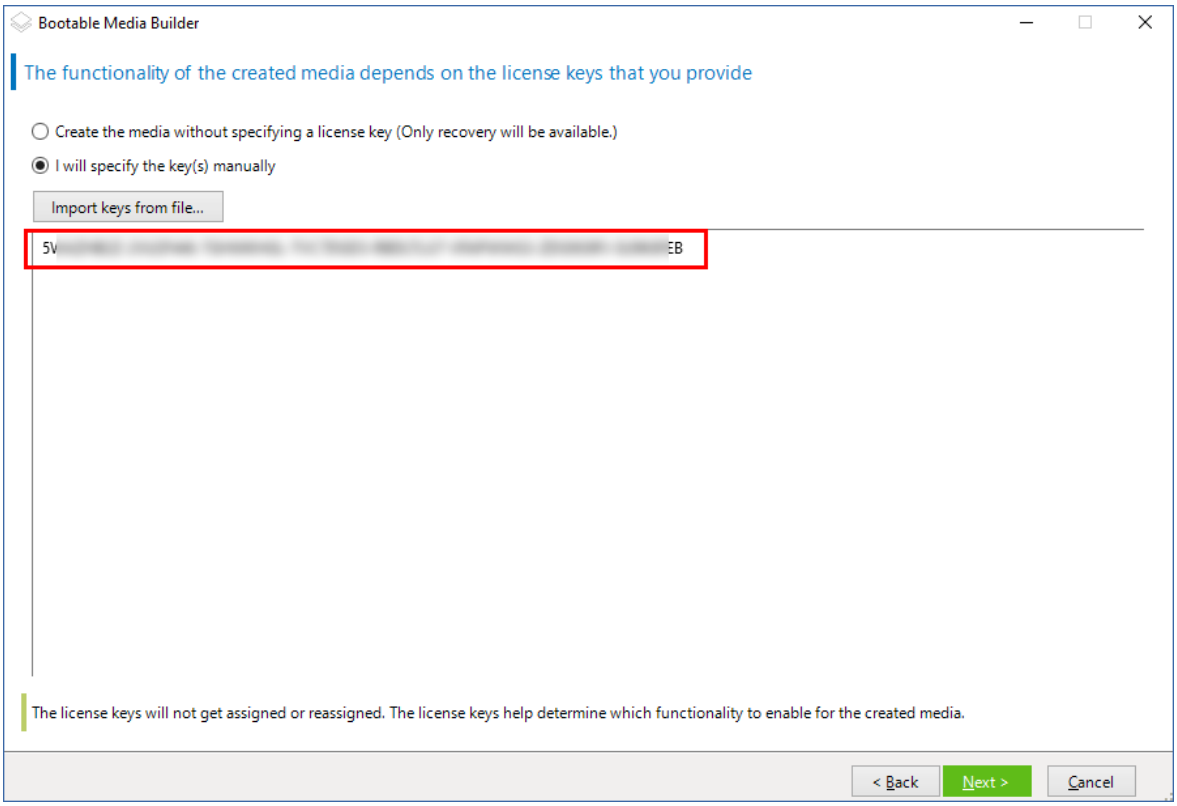
   您可以单击上述链接找到安装的系统要求。
2. 在计算机上安装评估和部署工具包。
3. 在同一计算机上安装可启动媒体生成器。

将 Acronis 插件添加到 WinPE

要将 Acronis 插件添加到 WinPE，请执行以下操作：

1. 启动可启动媒体生成器。
2. 要创建功能齐全的可启动媒体，请指定一个 Acronis 安克诺斯数据保护软件 许可号。此许可号用于确定哪些功能将包含在可启动媒体中。不会有任何计算机的许可证被吊销。

   如果不指定许可号，则生成的可启动媒体只能用于恢复操作。



3. 选择**可启动媒体类型：Windows PE** 或**可启动媒体类型：Windows PE(64 位)**。启动使用统一可扩展固件接口 (UEFI) 的计算机需要 64 位媒体。

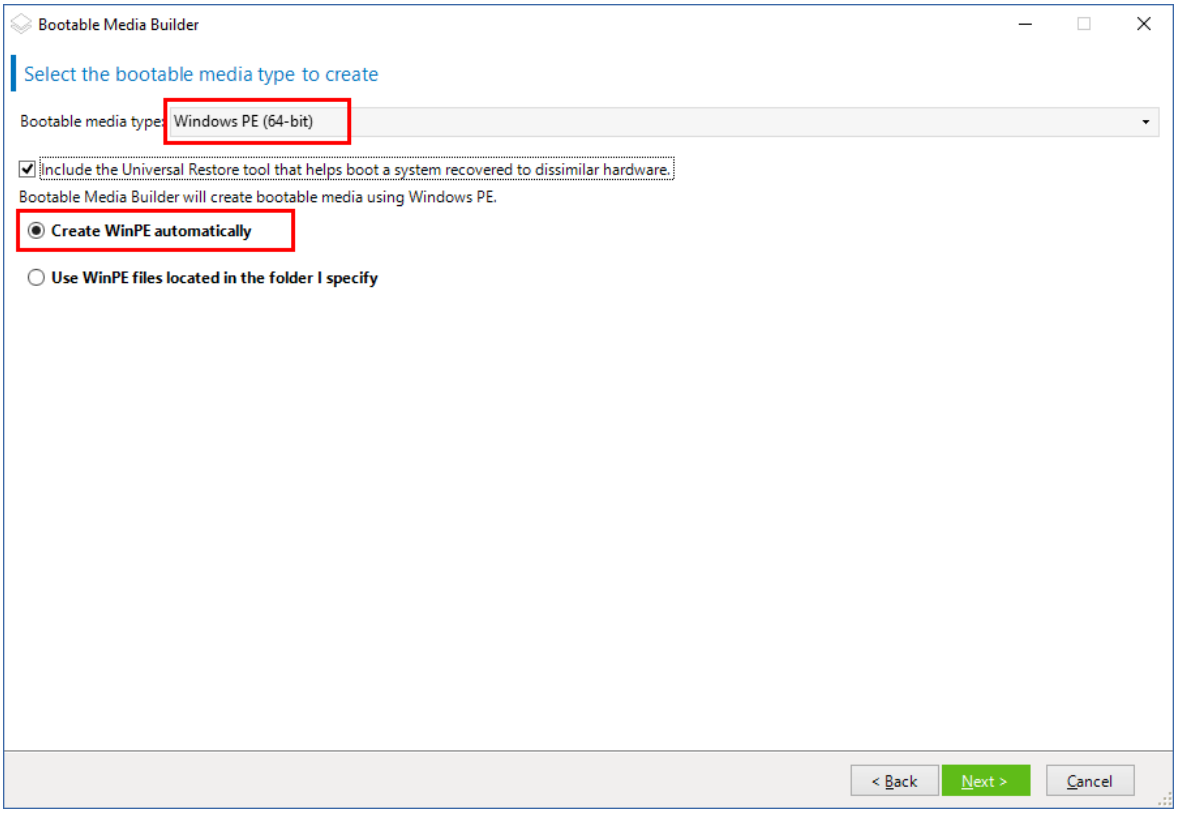
   如果您已选择**可启动媒体类型：Windows PE**，请首先执行以下操作：

   - 单击**下载用于 WinPE(32 位) 的插件**。
   - 将插件保存到 **%PROGRAM_FILES%\Acronis\BootableComponents\WinPE32**。

如果您计划将某个操作系统恢复至不同硬件或虚拟机，并希望确保系统的可启动性，请选中**包括异机还原工具...**复选框。

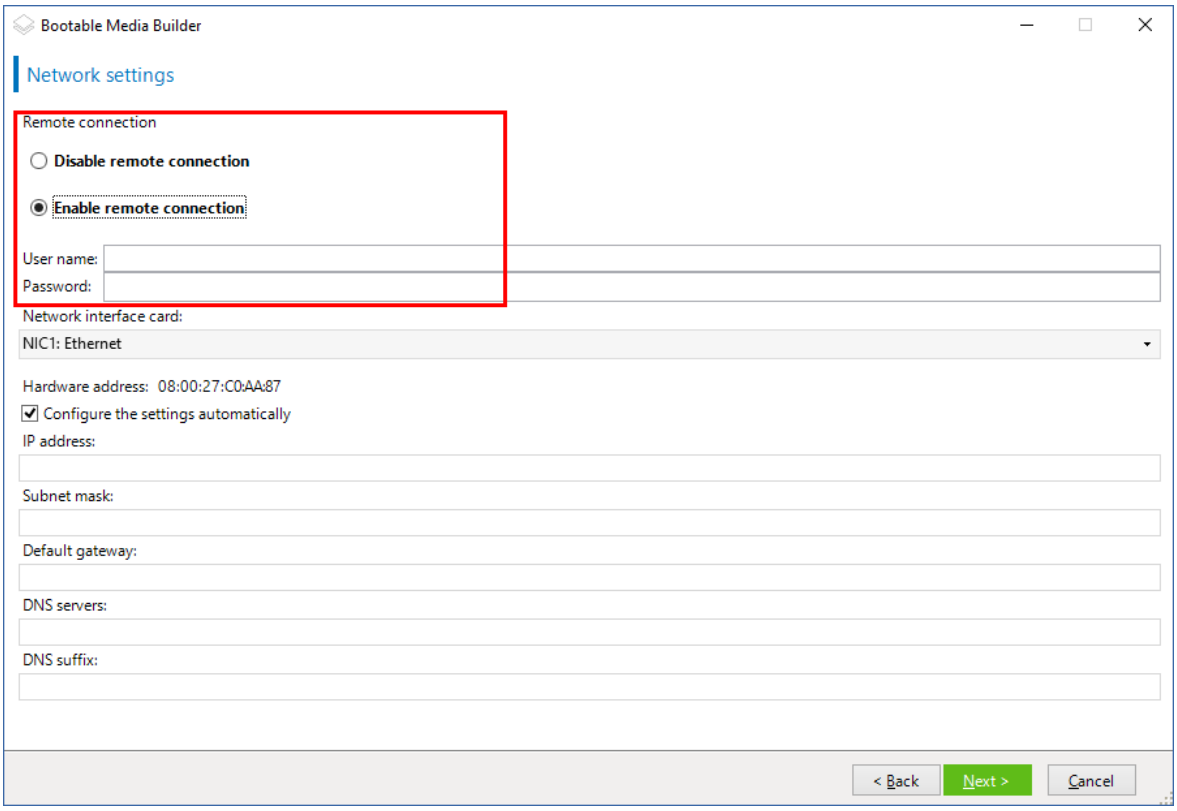
4. 选择**自动创建 WinPE。**

   软件将运行相应的脚本并继续前进到下一个窗口。



5. 选择将在可启动媒体中使用的语言。
6. 选择是启用还是禁用与从该媒体启动的计算机的远程连接。如果启用，请输入要在命令行中指定的用户名和密码(如果 acrocmd 实用工具在其他计算机上运行)。您也可以将这些字段留空，然后可以通过命令行界面进行远程连接，而无需凭据。

   当从 安克诺斯数据保护软件 Web 中控台在管理服务器上注册媒体时，也需要使用这些凭据。



7. 为计算机网络适配器指定网络设置，或选择 DHCP 自动配置。

注意
网络设置仅适用于 Acronis 安克诺斯数据保护软件 15 Advanced 和 Acronis 安克诺斯数据保护软件 15 Backup Advanced 许可证。有关详细的功能比较，请参阅本知识库文章。

8. [可选] 选择如何在启动时在管理服务器上注册媒体。有关注册设置的更多信息，请参阅"管理服务器"。
9. [可选] 指定要添加到 Windows PE 的 Windows 驱动程序。
   计算机启动进入 Windows PE 后，驱动程序可以帮助您访问备份所在的设备。如果使用 32 位 WinPE 分发，请添加 32 位驱动程序，如果使用 64 位 WinPE 分发，请添加 64 位驱动程序。
   此外，在配置适用于 Windows 的异机还原时，您还能指向添加的驱动程序。对于异机还原，请添加 32 位或 64 位驱动程序，具体取决于您计划恢复 32 位还是 64 位 Windows 操作系统。
   若要添加驱动程序，请执行以下操作：
   - 单击**添加**，然后指定相应 SCSI、RAID、SATA 控制器、网络适配器、磁带机或其他设备必备的 .inf 文件的路径。
   - 对于您要在生成的 WinPE 媒体中包含的每个驱动程序重复该步骤。
10. 选择您是要创建 ISO 或 WIM 映像，还是将媒体上载到服务器(WDS 或 RIS)。
11. 指定所生成映像文件的完整路径(包括文件名)，或者指定服务器并提供用于访问该服务器的用户名和密码。
12. 在摘要窗口中查看您的设置，然后单击**继续**。
13. 使用第三方工具将 .ISO 刻录到 CD 或 DVD，或准备一个可启动的闪存驱动器。

当计算机启动进入 WinPE 后，代理程序将自动启动。

若要从将要生成的 WIM 文件创建 PE 映像(ISO 文件):

- 替换包含新创建的 WIM 文件的 Windows PE 文件夹中的默认 boot.wim 文件。对于上述示例,请键入:

```
copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- 使用 **Oscdimg** 工具。对于上述示例,请键入:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

警告!
请勿复制并粘贴此示例。请手动键入命令,否则会失败。

有关自定义 Windows PE 2.x 和 3.x 的详细信息,请参阅"Windows 预安装环境用户指南(Winpe.chm)"。有关自定义 Windows PE 4.0 以及更高版本的信息可以在 Microsoft TechNet 库中找到。

连接到从媒体启动的计算机

一旦计算机从可启动媒体启动,计算机终端将显示一个启动窗口,带有从 DHCP 获得的或根据预配置值设置的 IP 地址。

配置网络设置

若要更改当前会话的网络设置,请在启动窗口中单击**配置网络**。随后显示的**网络设置**窗口将允许您配置计算机的每个网络界面卡 (NIC) 的网络设置。

在计算机重新启动之后,在会话期间进行的更改将会丢失。

添加 VLAN

在**网络设置**窗口中,可以添加虚拟局域网 (VLAN)。如果您需要访问包含在特定 VLAN 中的备份位置,请使用此功能。

VLAN 主要用于将局域网划分为多个段。连接至交换机的 *access* 端口的 NIC 始终可以访问在端口配置中指定的 VLAN。仅当您在网络设置中指定 VLAN 时,连接至交换机的 *trunk* 端口的 NIC 才可以访问端口配置中允许的 VLAN。

允许通过 trunk 端口访问 VLAN

1. 单击**添加 VLAN**。
2. 选择可以访问包括所需 VLAN 的局域网的 NIC。
3. 指定 VLAN 标识符。

单击**确定**之后,新的条目会出现在网络适配器列表中。

如果需要删除某个 VLAN,请单击所需的 VLAN 条目,然后单击**删除 VLAN**。

本地连接

若要直接操作从可启动媒体启动的计算机，请在启动窗口中单击**在本地管理此计算机**。

远程连接

若要远程连接媒体，请按照"在管理服务器上注册媒体"中所述在管理服务器上注册此媒体。

在管理服务器上注册媒体

注册可启动媒体让您可以将媒体作为注册计算机以通过 安克诺斯数据保护软件 Web 中控台进行管理。这适用于所有可启动媒体，无需考虑启动方式(物理媒体、启动恢复管理器、Acronis PXE 服务器、WDS 或 RIS)。但是，无法注册在 macOS 中创建的可启动媒体。

只有在管理服务器上添加了至少一个 Acronis 安克诺斯数据保护软件 高级许可证的情况下，才可以注册媒体。

可以从媒体 UI 注册媒体。

可以在可启动媒体生成器的管理服务器选项中预配置注册参数。如果预配置了所有注册参数，则媒体将自动显示在 安克诺斯数据保护软件 Web 中控台中。如果预配置了某些参数，则以下过程中的某些步骤可能不可用。

从媒体 UI 注册媒体

媒体可以使用可启动媒体生成器下载或创建。

从媒体 UI 注册媒体

1. 从媒体启动计算机。
2. 请执行以下任一操作：
   - 在启动窗口中，在**管理服务器**下，单击**编辑**。
   - 在可启动媒体界面中，单击**工具** > **在管理服务器上注册媒体**。
3. 在**注册位置**中，指定安装了管理服务器的计算机的主机名或 IP 地址。可以使用以下其中一种格式：
   - `http://`<服务器>。例如 `http://10.250.10.10` 或 `http://server`
   - <IP 地址>。例如 `10.250.10.10`
   - <主机名>。例如 `server` 或 `server.example.com`
4. 在**用户名**和**密码**中，提供位于管理服务器管理员(**设置** > **帐户**)列表中的帐户的凭据。在 安克诺斯数据保护软件 Web 中控台中，根据给予指定帐户的权限，媒体将显示在组织下或特定单位下。
5. 在**显示名称**中，指定该计算机在 安克诺斯数据保护软件 Web 中控台中显示的名称。若此字段留为空白，则显示名称将设置为以下其中一种：
   - 如果之前在管理服务器上注册了该计算机，则其将拥有相同的名称。

- 否则，将使用该计算机的完全限定域名 (FQDN) 或 IP 地址。

6. 单击**确定**。

对可启动媒体的本地操作

通过可启动媒体进行的操作与在运行的操作系统下执行的备份和恢复操作类似。区别如下：

1. 在具有类似 Windows 的卷表示形式的可启动媒体下，卷的驱动器号与在 Windows 中相同。在 Windows 中没有驱动器号的卷（如系统保留卷）按照它们在磁盘上的顺序自由分配代号。
   如果可启动媒体无法在计算机上检测到 Windows 或检测到多个，所有卷（包括没有驱动器号的卷）都将按照它们在磁盘上的顺序分配代号。因此，卷号可能与 Windows 中显示的不同。例如，可启动媒体下的 D: 盘可能对应的是在 Windows 中的 E: 盘。

   注意
   我们建议您为卷指定一个唯一名称。

2. 具有类似 Linux 的卷表示形式的可启动媒体会将本地磁盘和卷显示为尚未加载 (sda1, sda2...)。
3. 使用可启动媒体创建的备份具有简化文件名。只有使用标准文件命名方法将名称添加到现有存档，或者目标不支持简化文件名时，才会为备份分配标准名称。
4. 具有类似 Linux 的卷表示形式的可启动媒体无法将备份写入 NTFS 格式的卷。如果要写入备份，请切换到具有类似 Windows 的卷表示形式的媒体。如需切换可启动媒体的卷表示，请依次单击**工具** > **更改卷表示形式**.
5. 任务无法排程。如果您需要重复一项操作，则需要重新配置。
6. 日志的存留时间仅限于当前会话。您可将整个日志或筛选的日志条目保存到一个文件。
7. 集中式保管库未在**存档**窗口的文件夹树中显示。
   要访问受管保管库，请在**路径**字段中键入以下字符串：
   bsp://node_address/vault_name/
   要访问不受控的集中式保管库，请键入保管库文件夹的完整路径。
   输入访问凭据后，您将在保管库中看到存档列表。

设置显示模式

通过基于 Linux 的可启动媒体启动计算机时，系统会根据硬件配置（监视器和图形卡规格）自动检测显示视频模式。如未能正确检测到视频模式，将执行以下操作：

1. 在启动菜单中，按 F11。
2. 在命令行中，输入以下命令：**vga=ask**，然后继续启动。
3. 从支持的视频模式列表中，键入编号（如：**318**）选择合适的视频模式然后按 **ENTER**。

如果您不希望每次从指定硬件配置上的媒体启动时均执行此步骤，请重新创建可启动媒体，方法是将适当的模式编号（在本例中为 **vga=0x318**）输入 **内核参数** 窗口中。

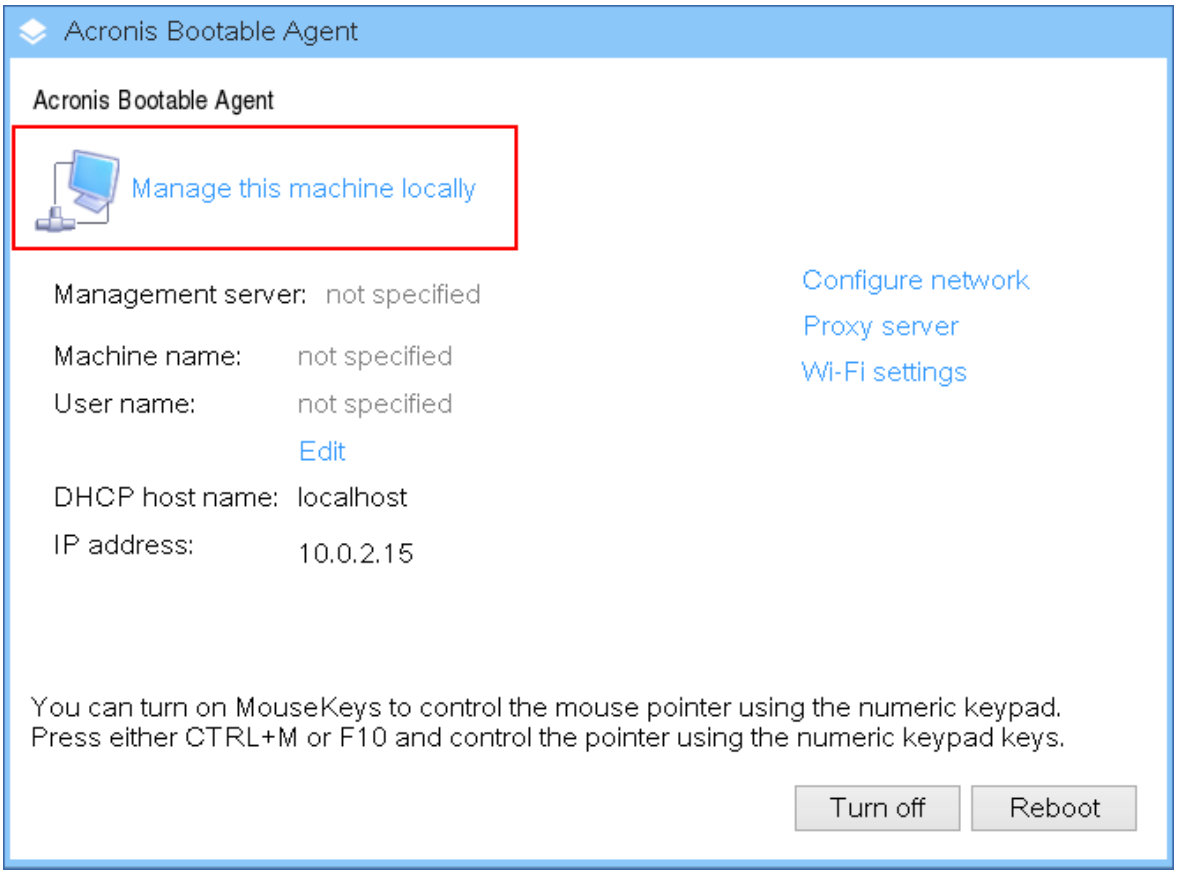
带本地可启动媒体的备份

只能使用由可启动媒体生成器创建的可启动媒体，并通过使用 Acronis 安克诺斯数据保护软件 许可号来备份数据。有关如何创建可启动媒体的信息，请参考“创建可启动媒体”。有关如何创建可启动媒体的更多信息，请分别参考基于 Linux 的可启动媒体或 基于 Windows-PE 的可启动媒体。

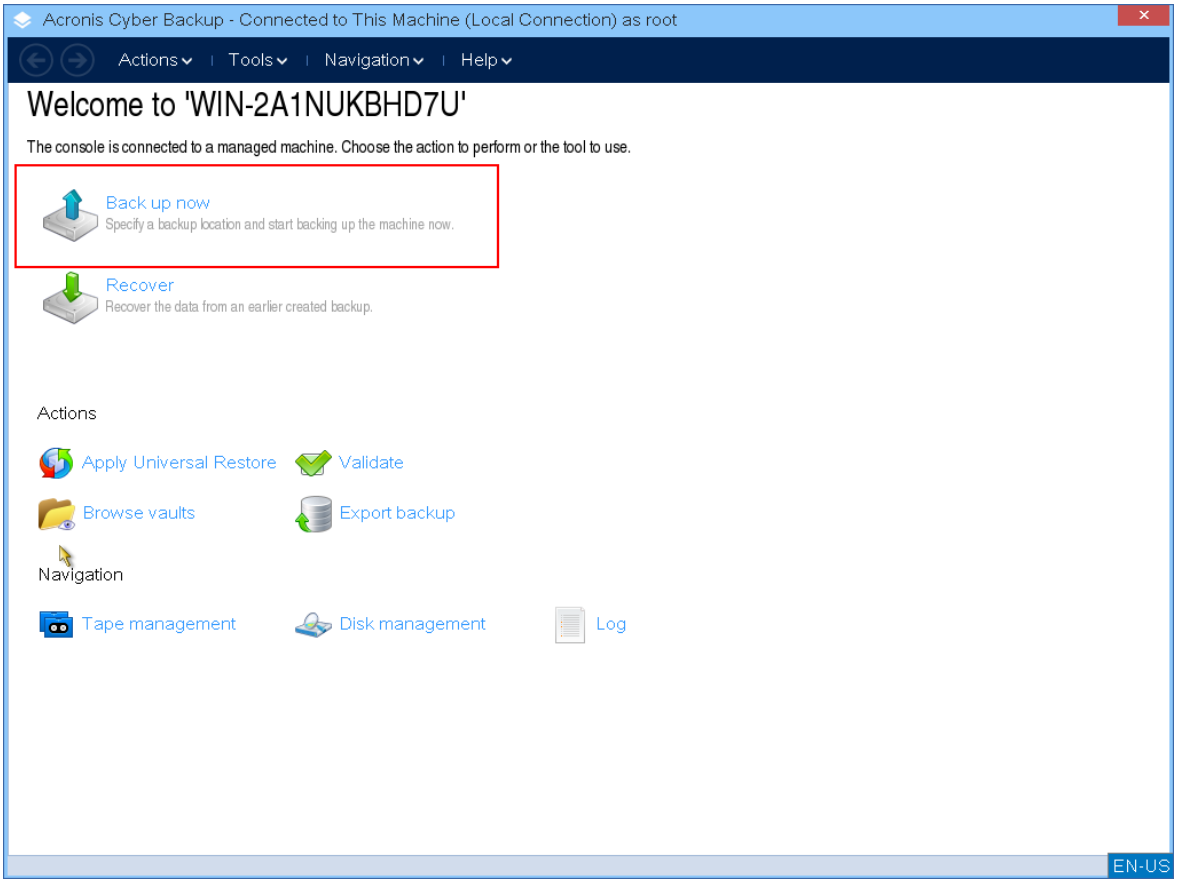
在可启动媒体下备份数据

1. 从 Acronis 可启动应急媒体启动。

2. 如需备份本地计算机，单击**本地管理此计算机**。有关远程连接的更多信息，请参考在管理服务器上注册媒体。



3. 单击**立即备份**。

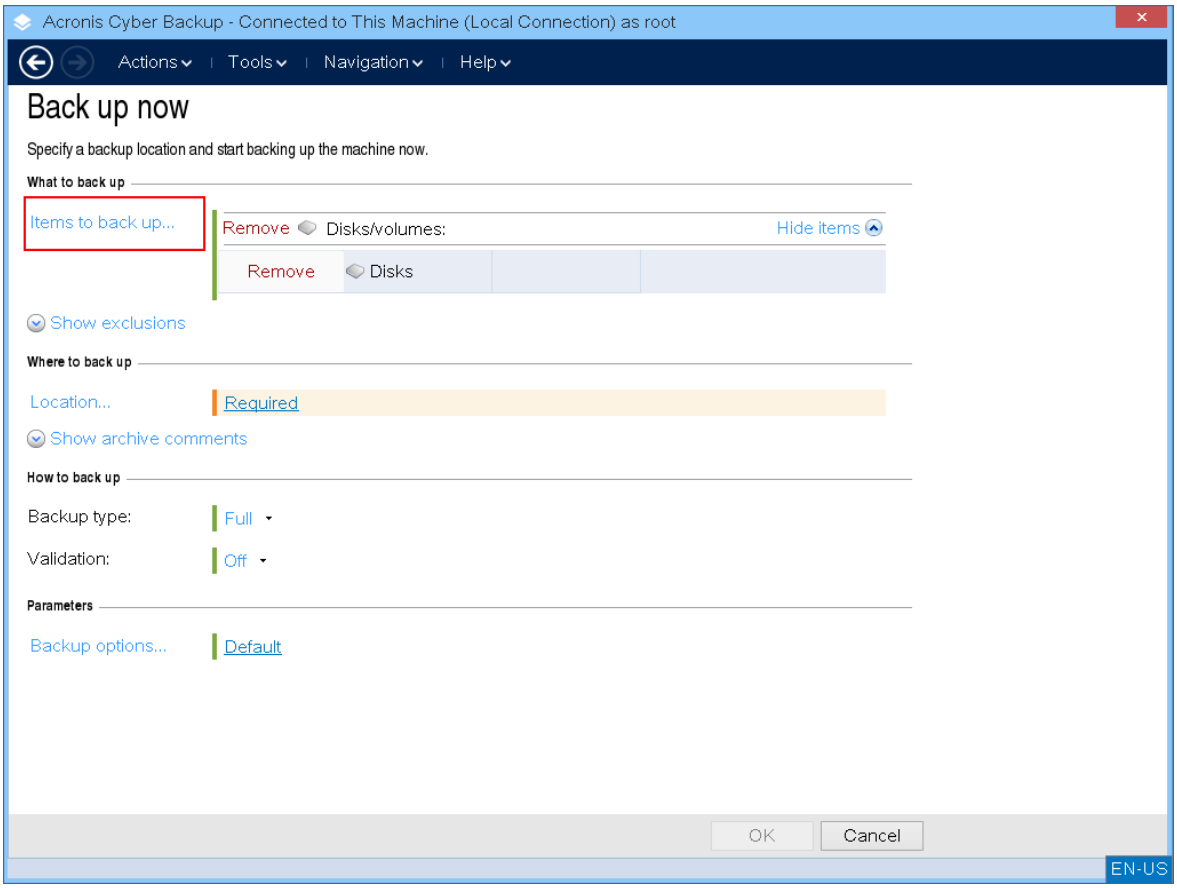


4. 默认情况下，计算机的所有不可移动磁盘均被自动选中用于备份。如需更改要备份的数据，请单击**要备份的项目**，然后选择所需的磁盘或卷。

   选择要备份的数据后，您可能会看到以下消息："*不能直接选择此计算机。该计算机上安装有旧的代理程序版本。请使用政策规则选择用于备份的计算机。*"这是一个可以安全地忽略的 GUI 问题。选择要备份的单独的磁盘或卷。

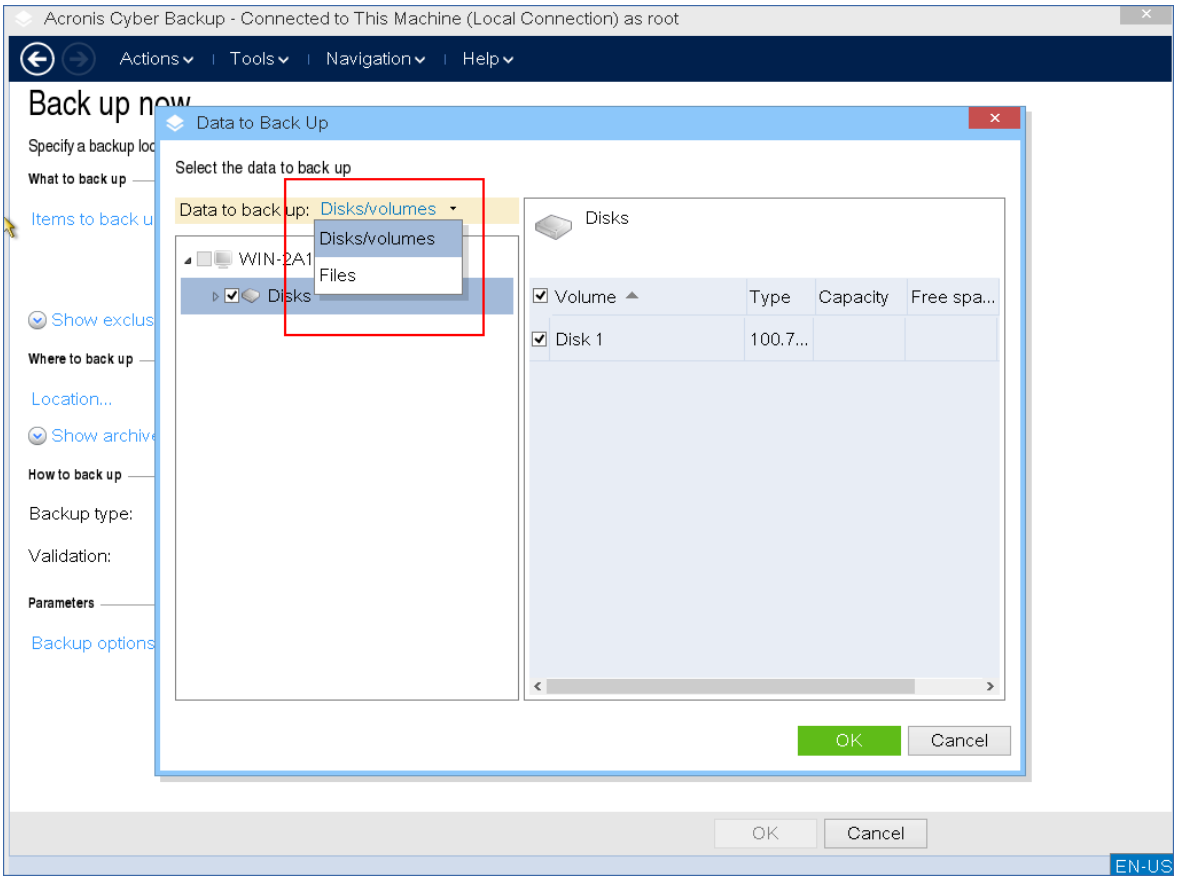
   注意

   使用基于 Linux 的可启动媒体，您可能会看到与 Windows 中不同的驱动器号。尝试通过大小或标签来标识所需的驱动器或分区。

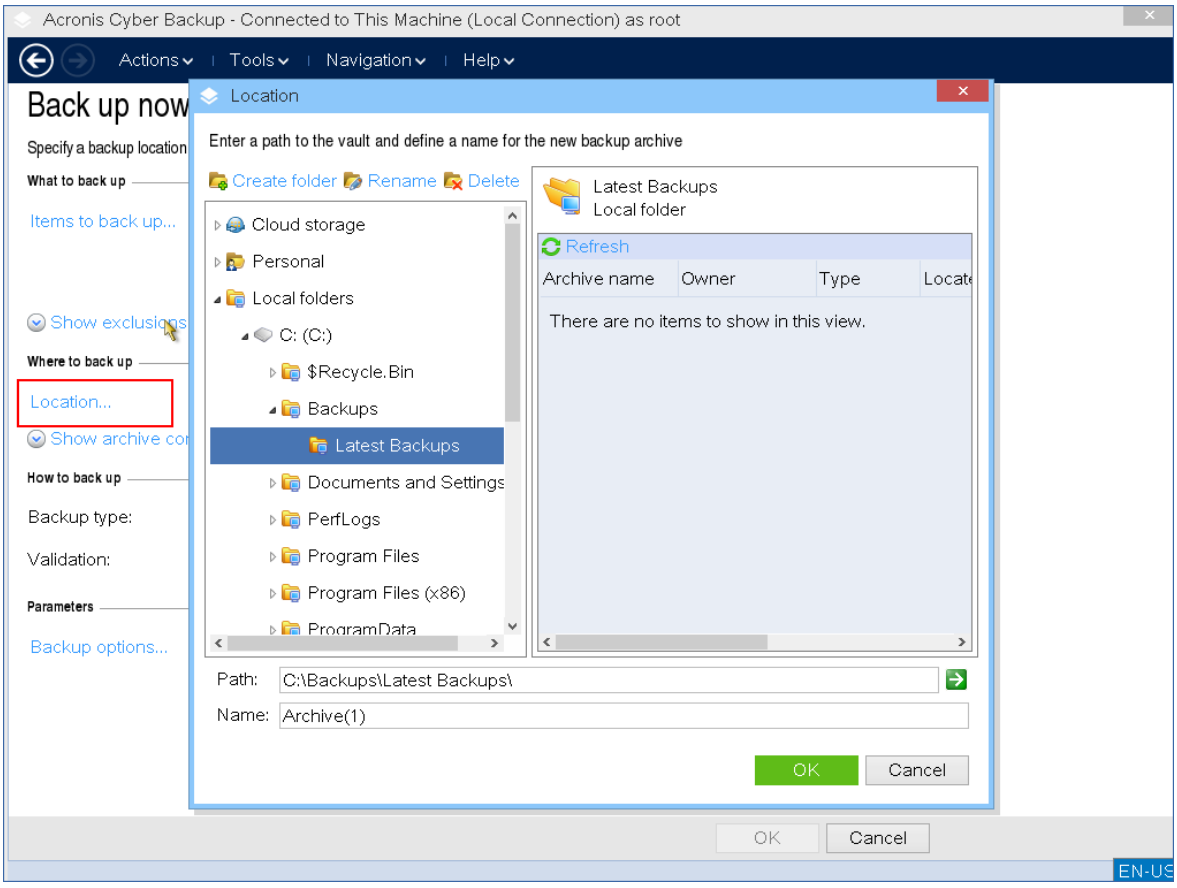


5. 如果需要备份文件或文件夹而不是磁盘，请切换至**要备份的数据**中的**文件**。

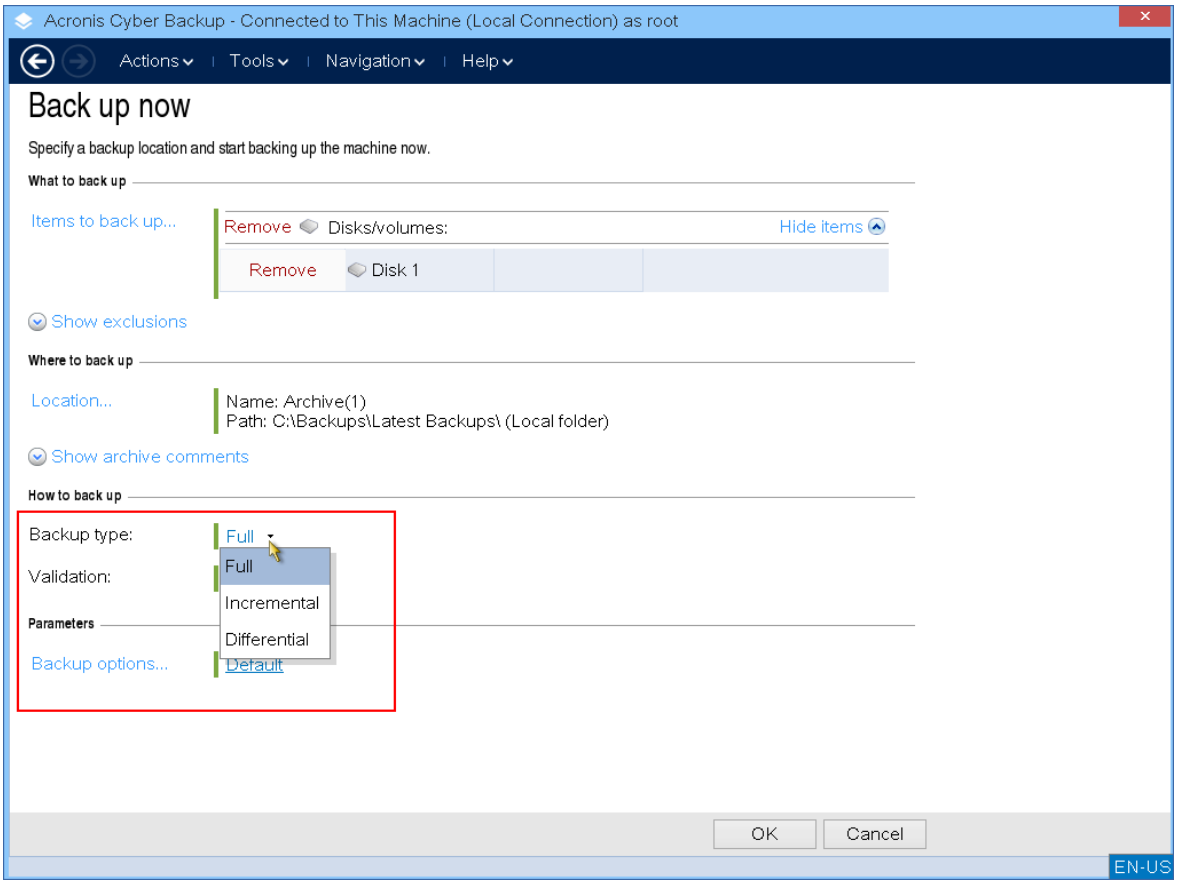
   可启动媒体下只有磁盘/分区和文件/文件夹备份可用。其他类型的备份(如数据库备份)仅在运行的操作系统下可用。



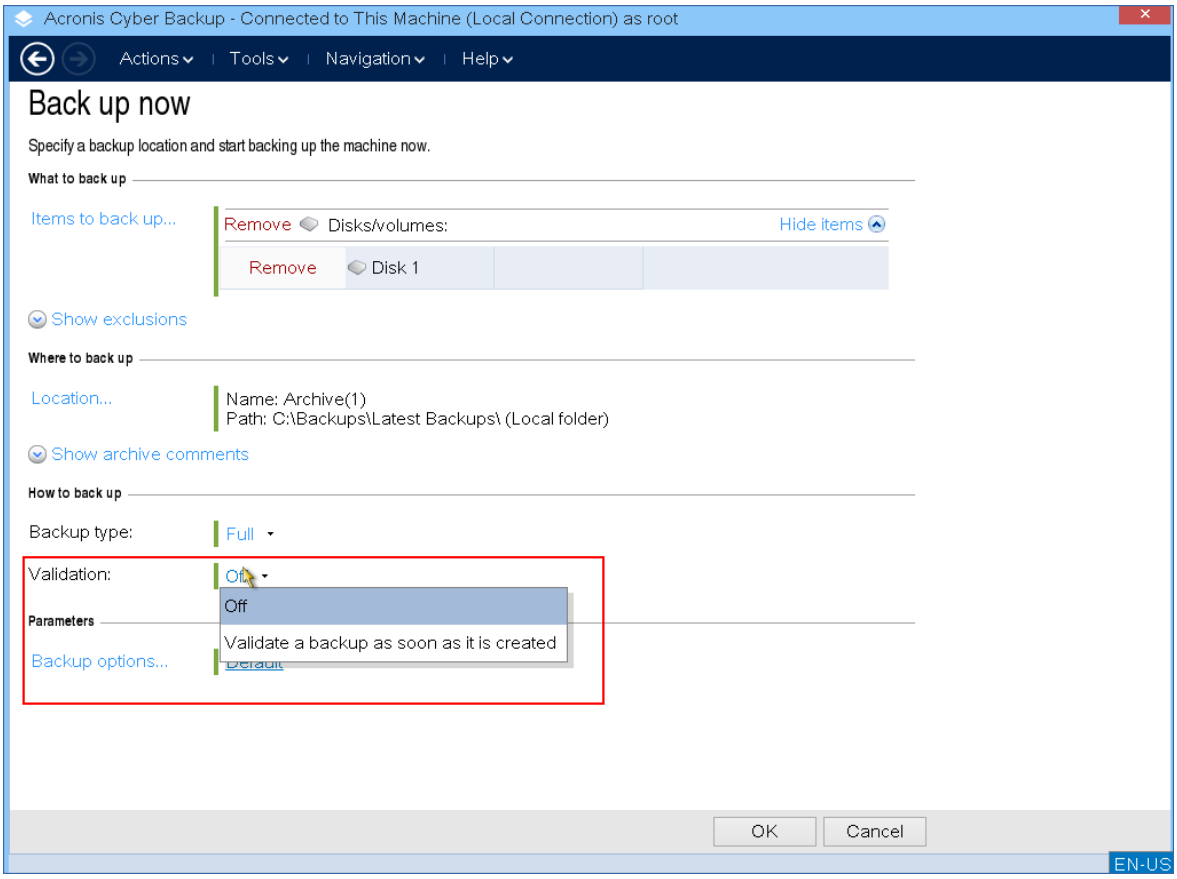
6. 单击 **位置**，然后选择要保存备份的位置。



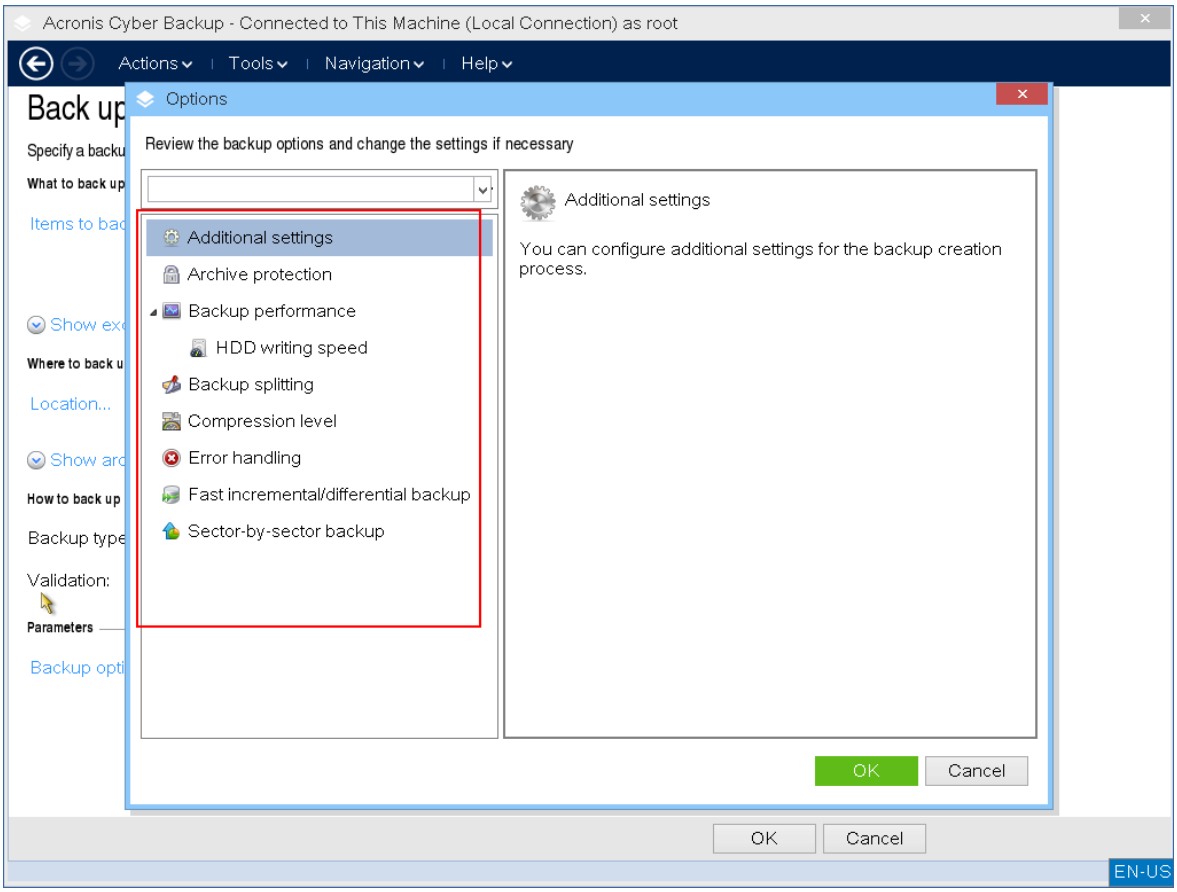
7. 为备份选择位置并命名。
8. 指定备份类型。如果这是此位置的第一次备份，则将创建完整备份。如果继续备份链，可以选择**增量**或**差异**，以节省空间。有关备份类型的详细信息，请参阅 https://kb.acronis.com/content/1536。



9. [可选]如果要验证备份文件，请选择**创建备份时验证备份**。



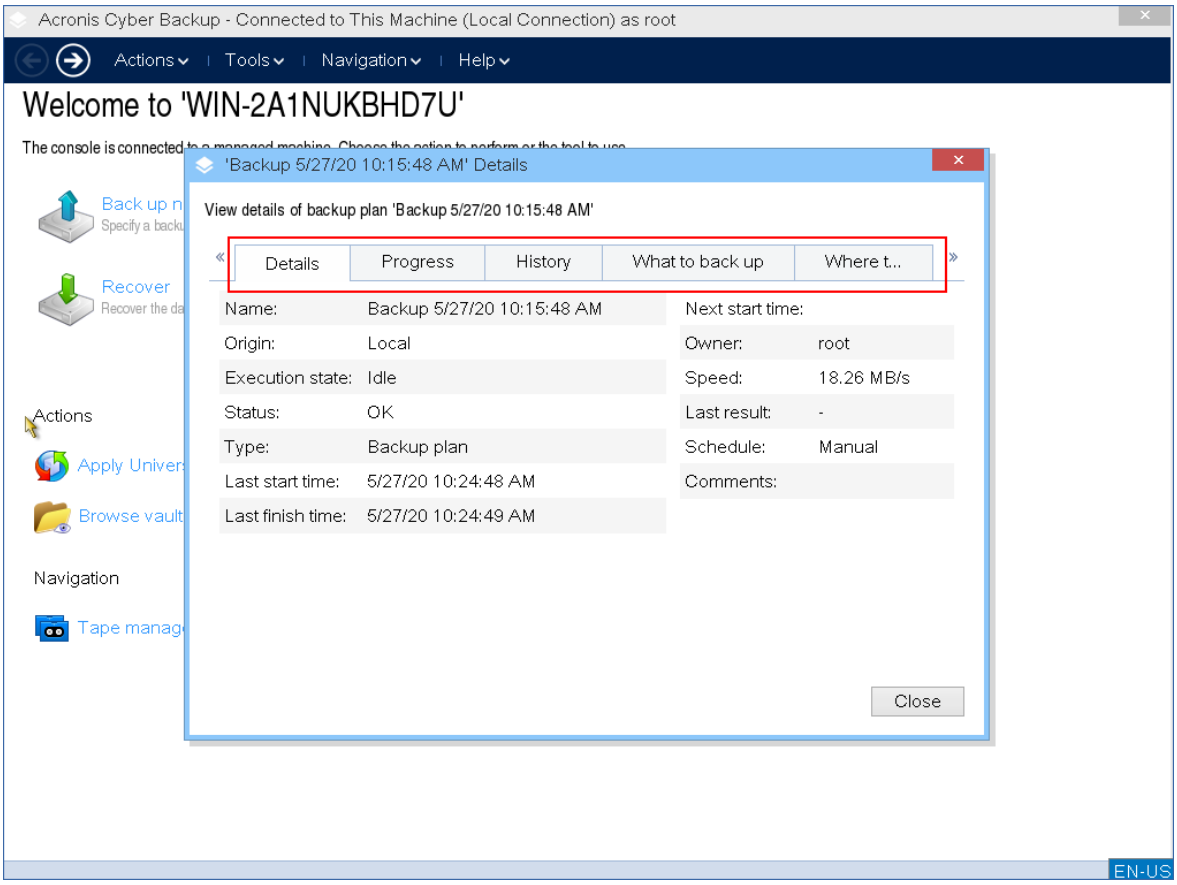
10. [可选]指定可能需要的备份选项 – 例如备份文件的密码、备份拆分或错误处理。



11. 单击**确定**开始备份。

    可启动媒体从磁盘读取数据，将其压缩为.tib文件，然后将该文件写入所选位置。这一操作不会创建磁盘快照，因为没有正在运行的应用程序。

12. 您可以在出现的窗口中检查备份任务状态和有关备份的其他信息。

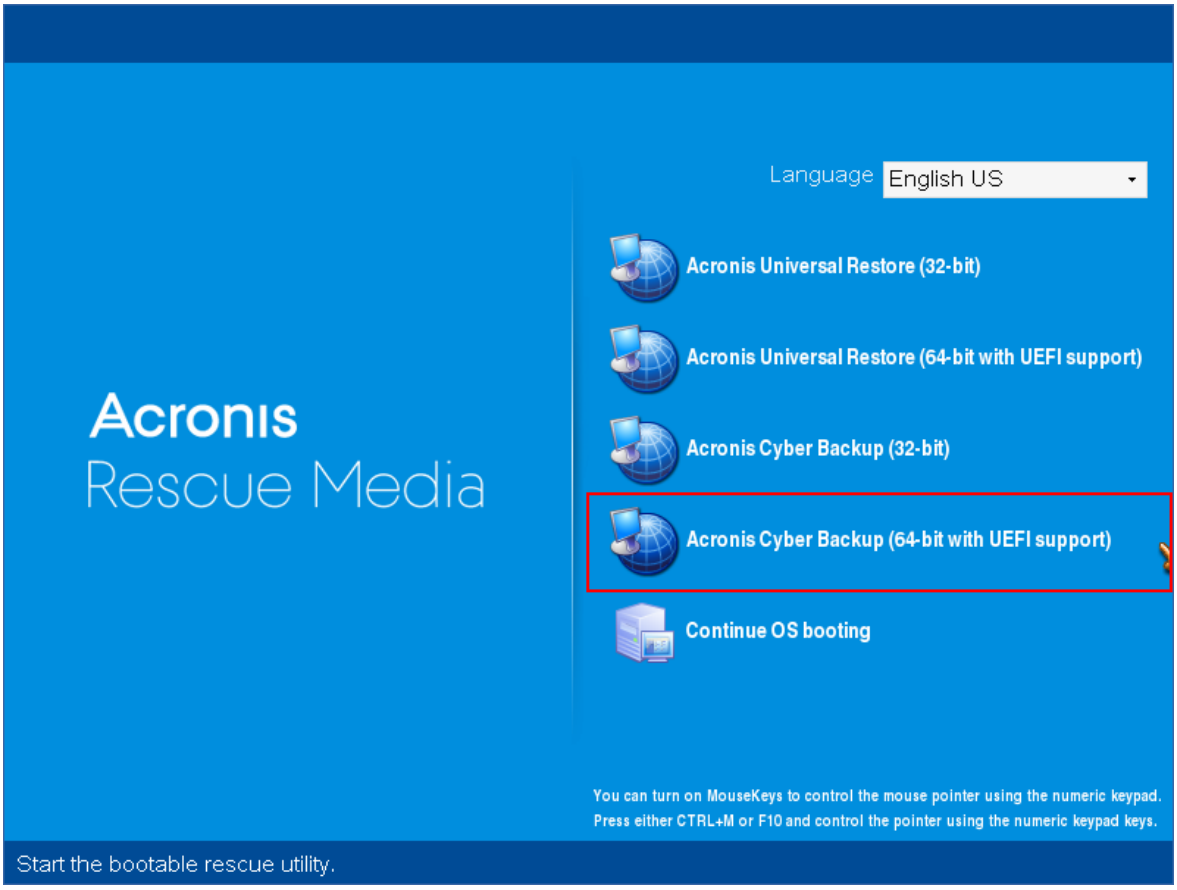


本地使用可启动媒体恢复

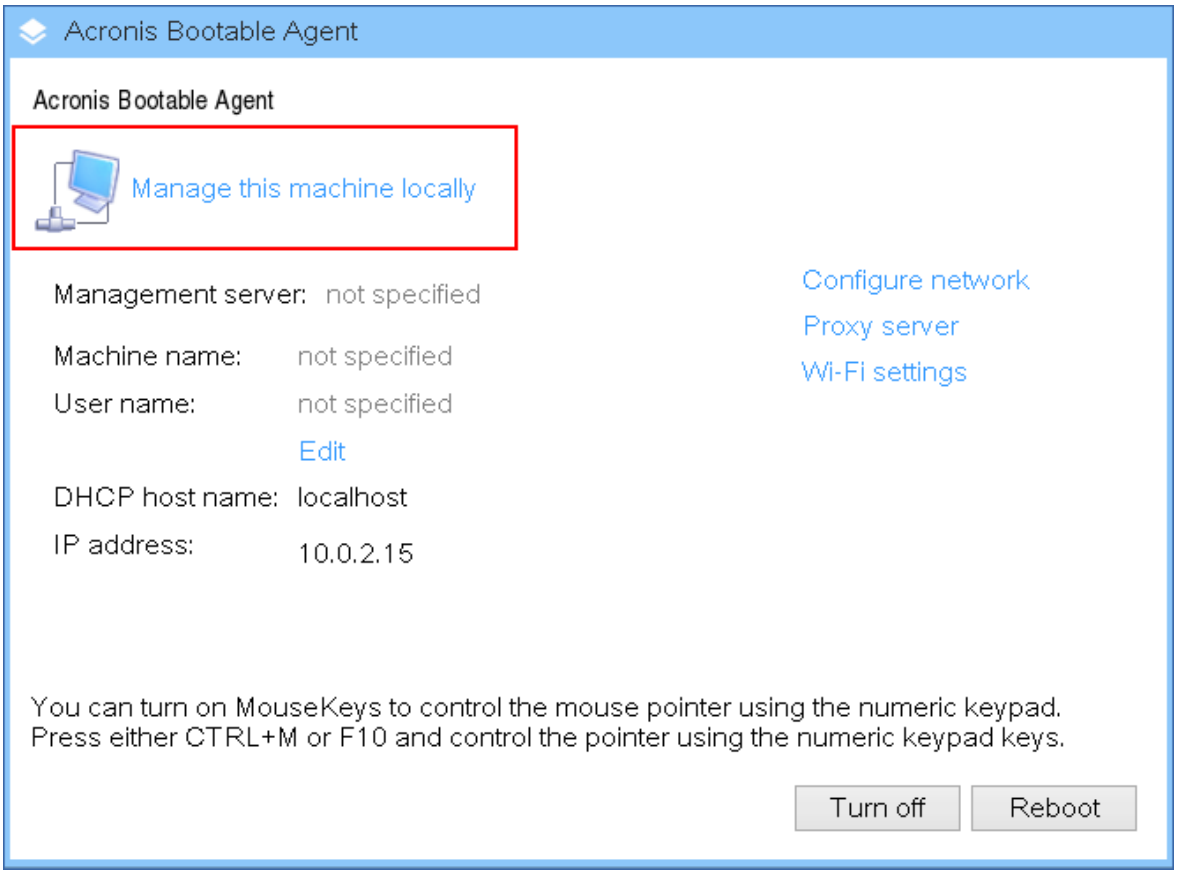
恢复操作在使用 Bootable Media Builder 创建的可启动媒体和下载的现成可启动媒体中都可用。

在可启动媒体下恢复数据

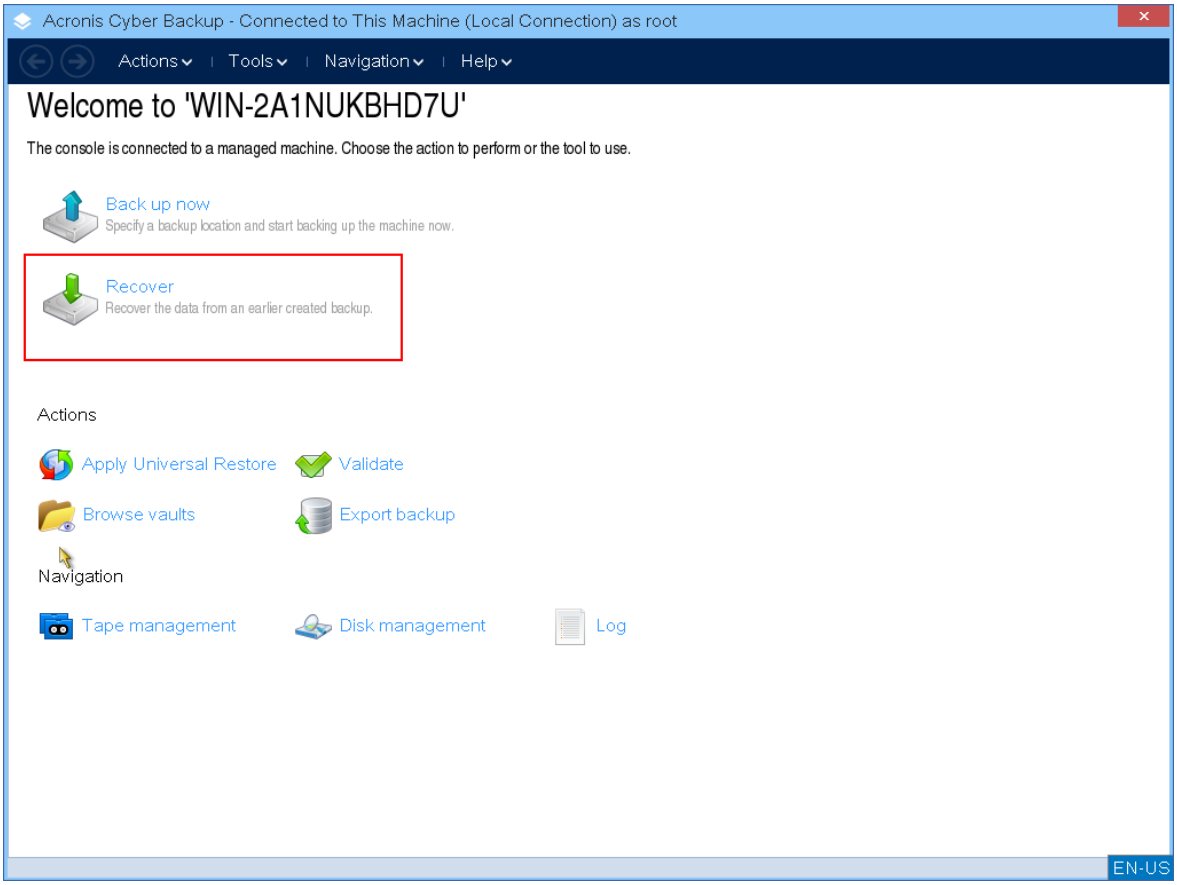
1. 从 Acronis 可启动应急媒体启动。



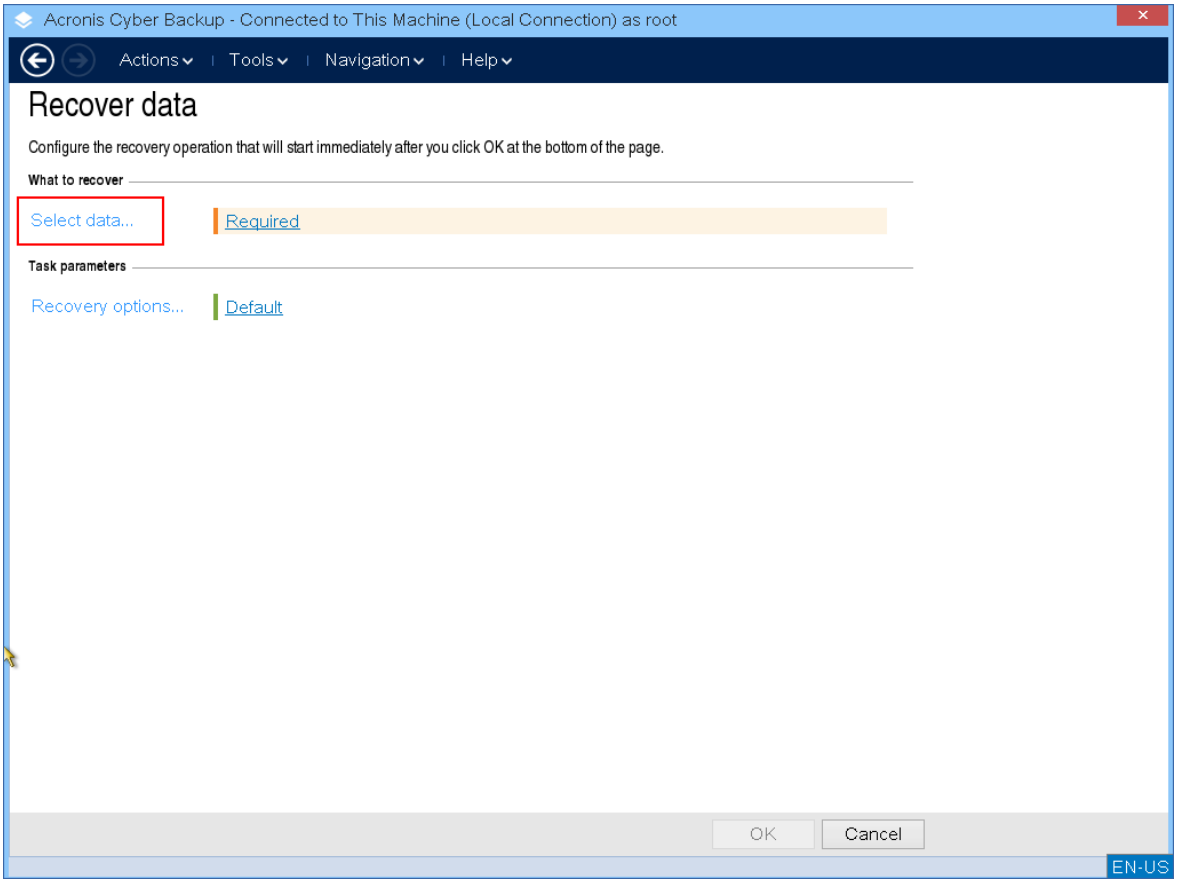
2. 要将数据恢复到本地计算机，请单击**在本地管理此计算机**。有关远程连接的更多信息，请参考在管理服务器上注册媒体。



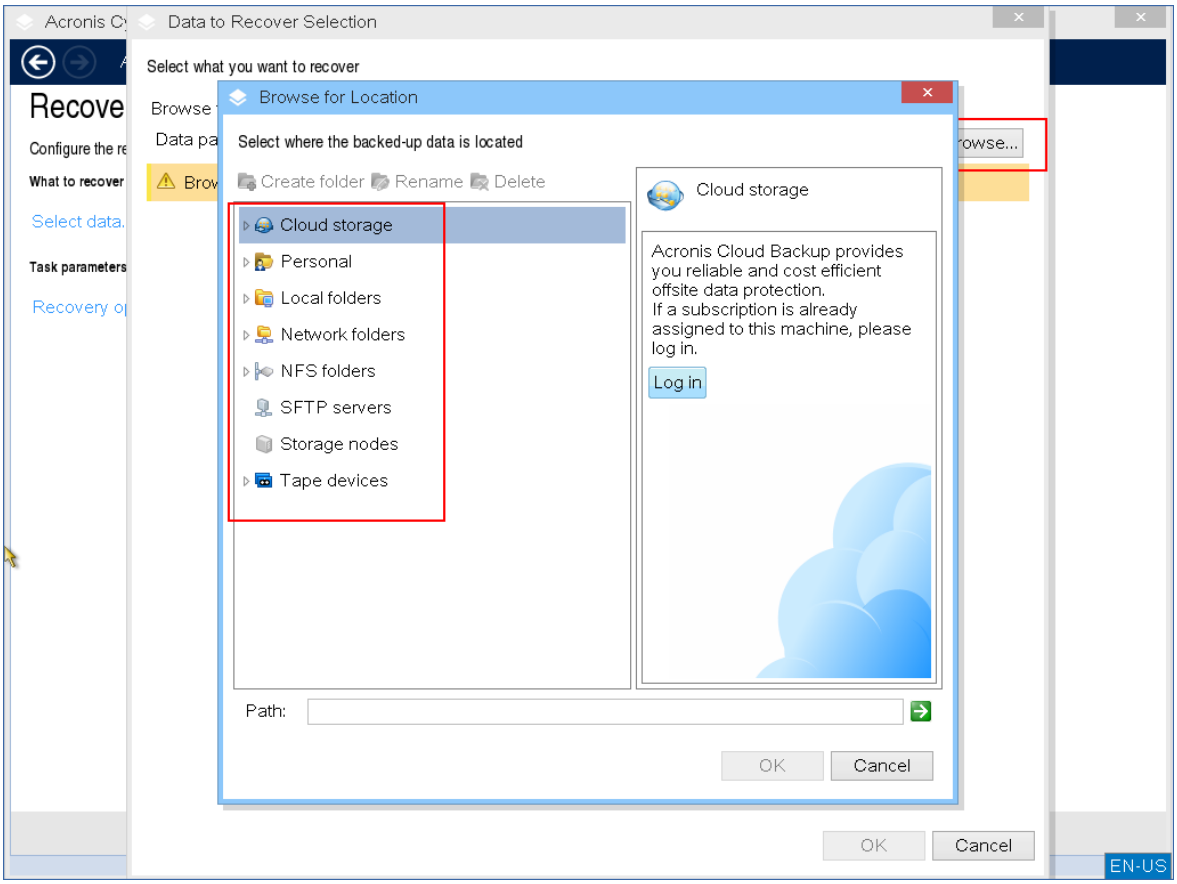
3. 单击**恢复**。



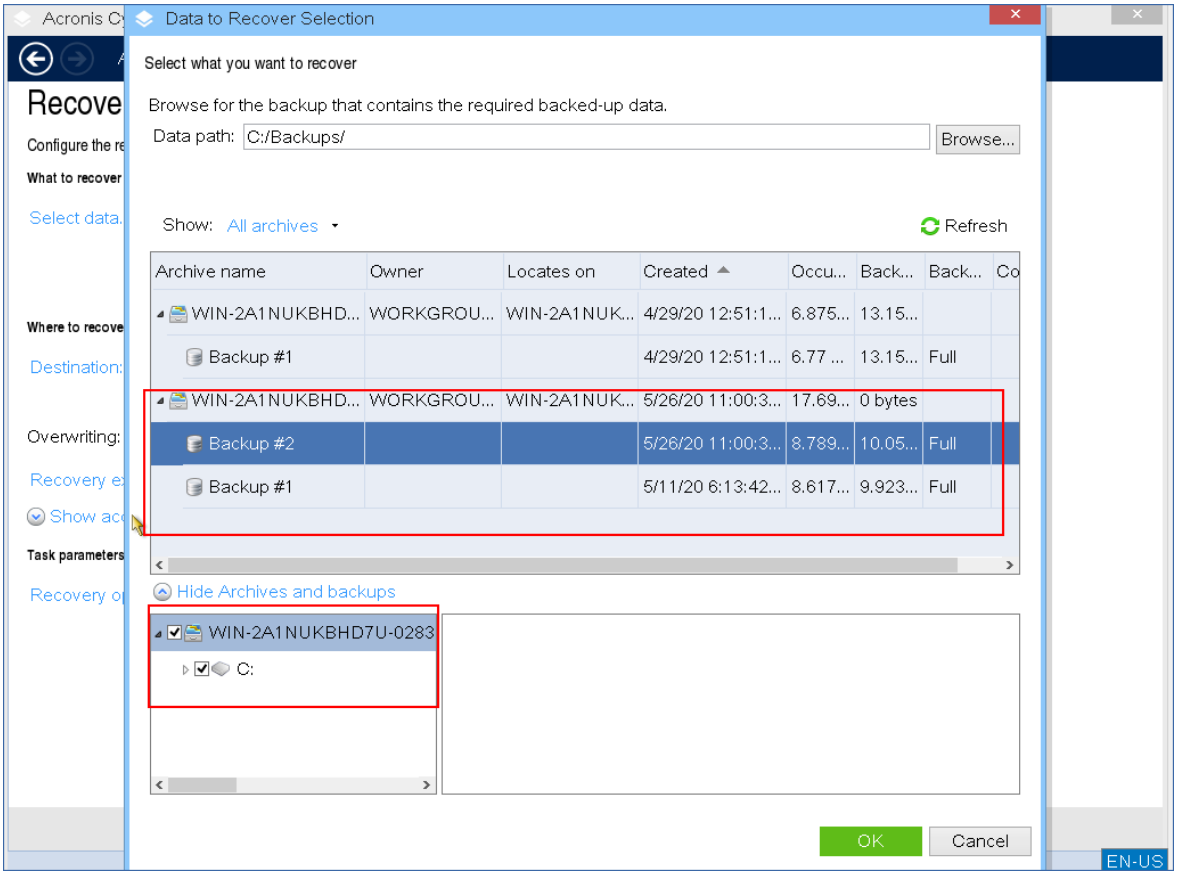
4. 在**恢复内容**下，单击**选择数据**。



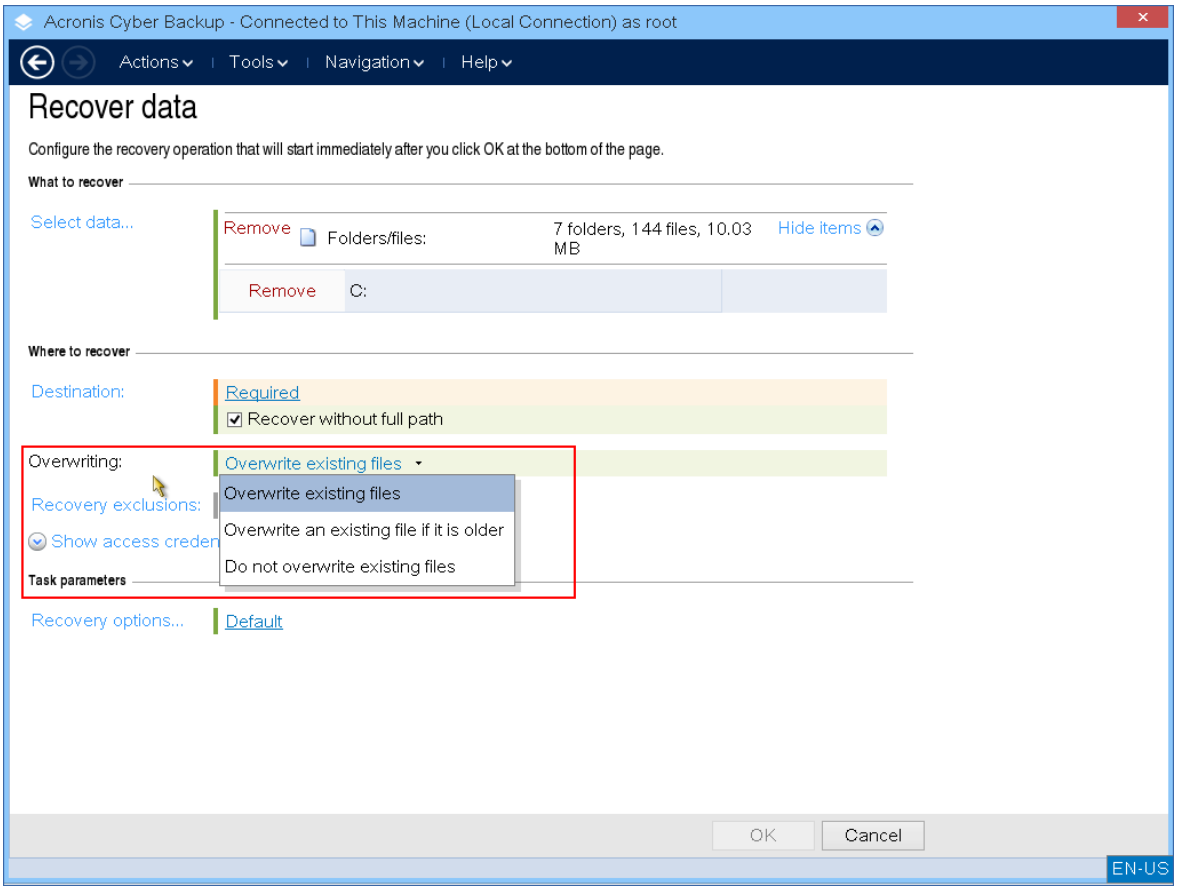
5. 单击**浏览**并选择备份位置。



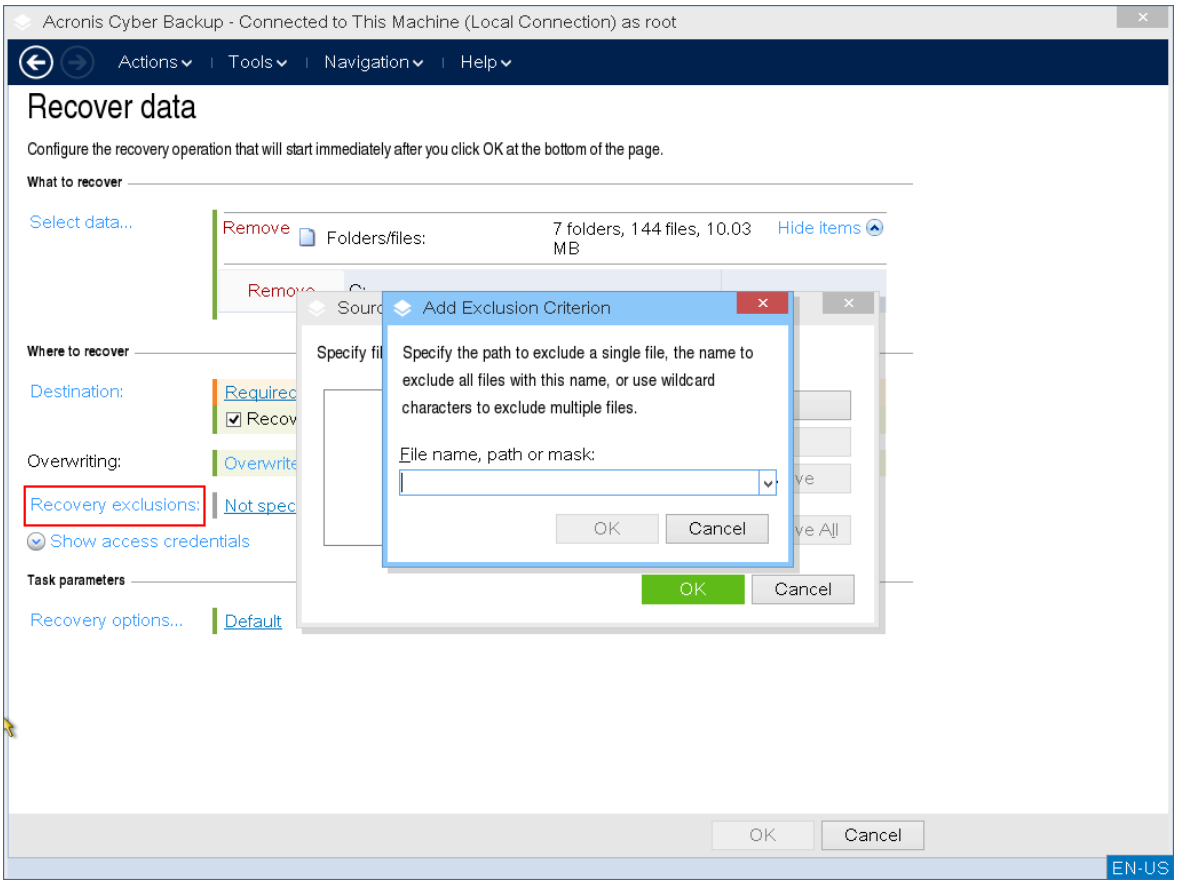
6. 选择要从中恢复的备份文件。



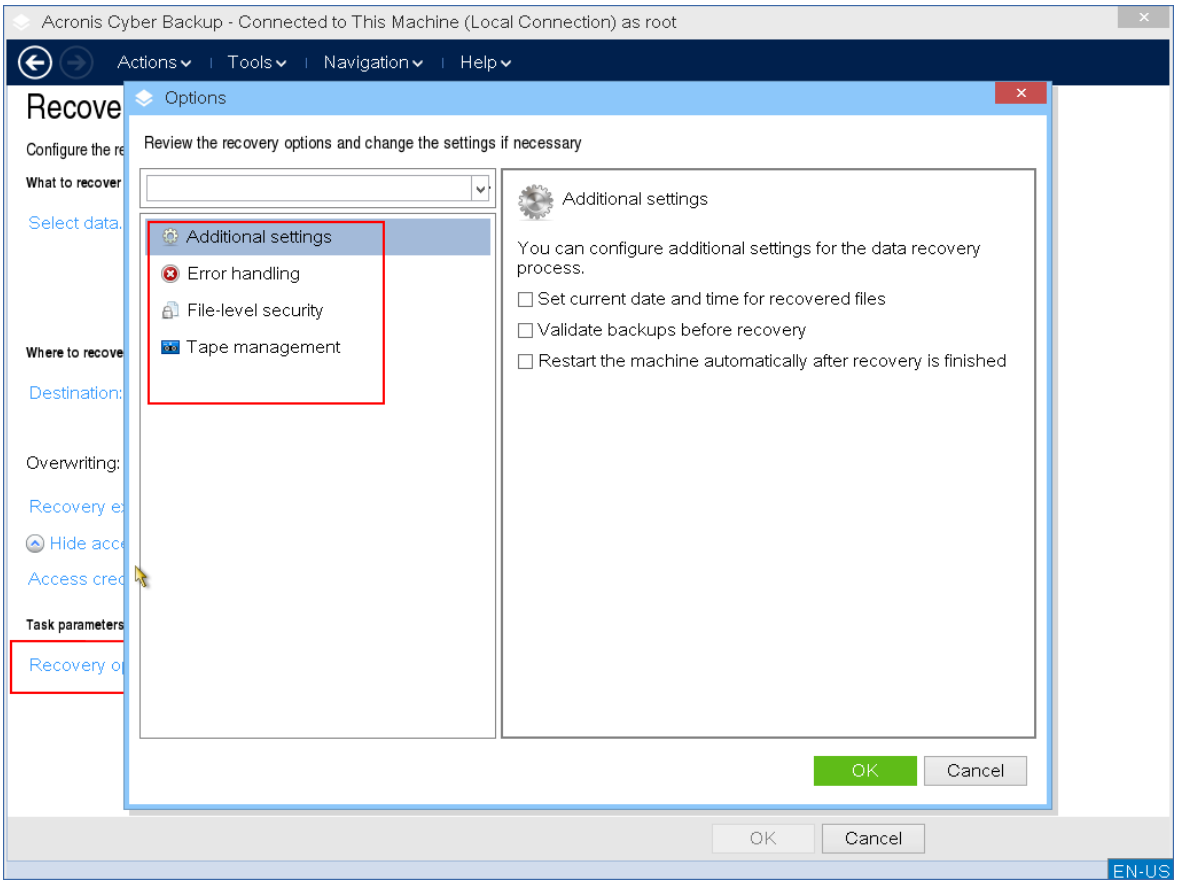
7. 在左下角窗格中，选择要恢复的驱动器/卷（或文件/文件夹），然后单击 **OK**。
8. [可选]配置覆盖规则。



9. [可选]配置恢复排除。



10. [可选]配置恢复选项。



11. 检查您的设置是否正确，然后单击 **OK**。

注意
要将数据恢复到不同硬件，必须使用 Acronis Universal Restore。当备份位于 Acronis 安全区 中时，Acronis Universal Restore 不可用。

带可启动媒体的磁盘管理

使用 Acronis 可启动媒体，可以准备磁盘/卷配置，以恢复使用 Acronis 安克诺斯数据保护软件 备份的卷映像。

有时在卷经过备份并且其映像被放置于安全存储中之后，计算机磁盘配置可能由于 HDD 更换或硬件丢失而发生更改。在这类情况下，您可重新创建必需的磁盘配置，以便将卷映像"按原样"或通过变更您认为必需的磁盘或卷结构完全恢复。

请采取所有必要的预防措施来避免可能的数据丢失。

重要事项
在磁盘和卷上进行的所有操作都有一定的数据损坏的风险。必须非常小心地在系统、可启动或数据卷上执行操作，以免在启动过程中或硬盘数据存储时出现任何可能的问题。
对硬盘和卷进行操作需要花费一定的时间，在这一过程中，断电、无意关闭计算机或意外按下"重启"按钮都可能导致卷损坏和数据丢失。

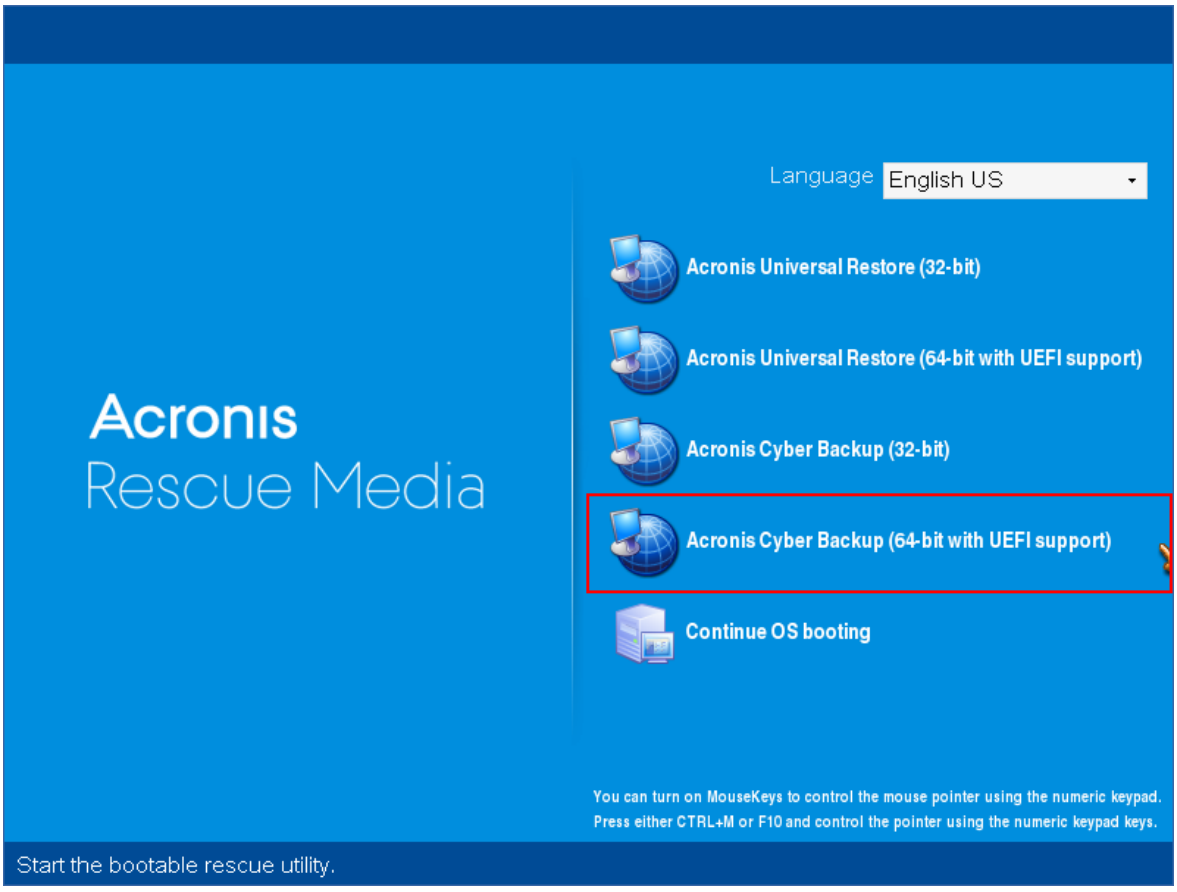
可在裸机、无法启动的计算机或非 Windows 系统的计算机上执行磁盘管理操作。您需要使用可启动媒体生成器创建的可启动媒体，并通过使用您的 Acronis 安克诺斯数据保护软件 许可号。有关如何创建可启动媒体的信息，请参考“创建可启动媒体”。有关如何创建可启动媒体的更多信息，请分别参考基于 Linux 的可启动媒体或 基于 Windows-PE 的可启动媒体。

注意

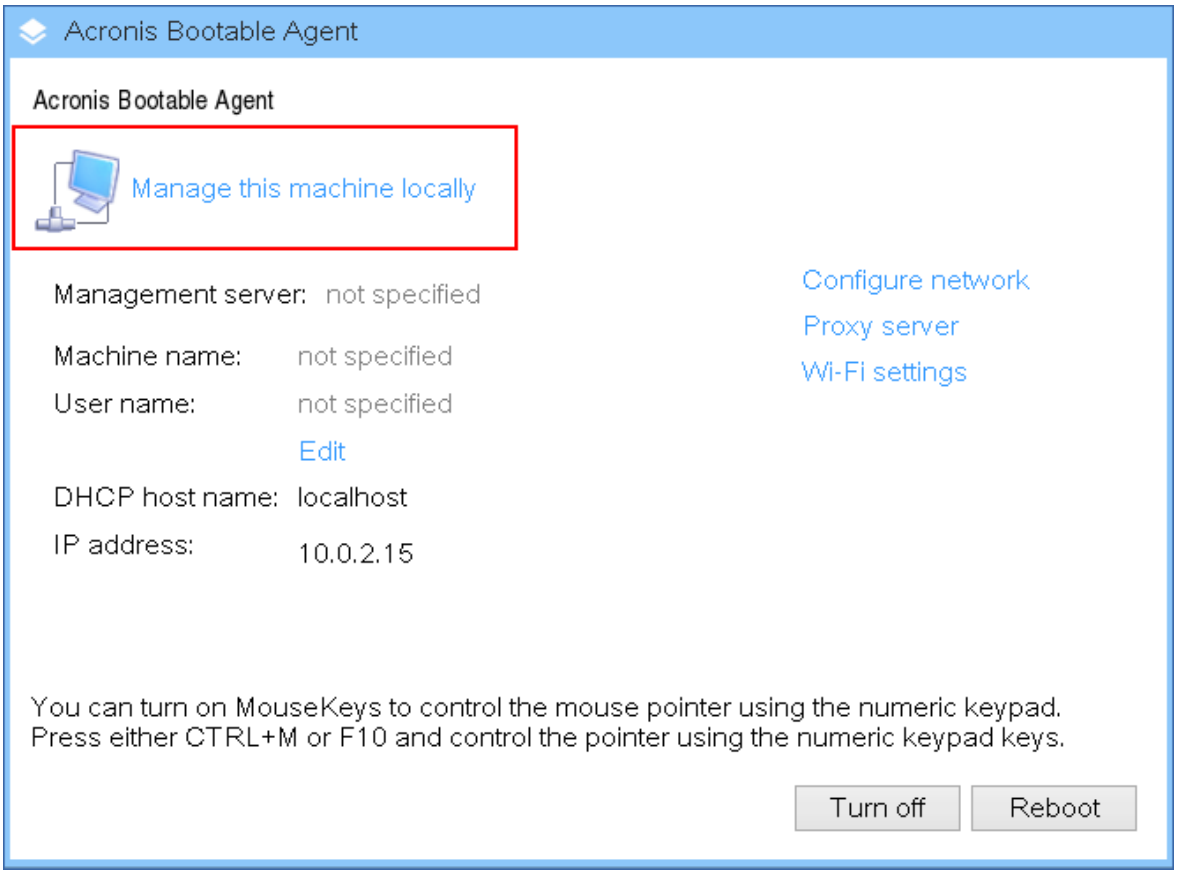
磁盘管理功能不可用于基于 Windows PE 4.0 和更高版本的可启动媒体。因此，磁盘管理支持 Windows 7 和更早的操作系统。如需在 Windows 8 和更高版本上执行磁盘管理操作，您需要安装 Acronis Disk Director。有关详细信息，请参阅此知识库文章：https://kb.acronis.com/content/47031。

执行磁盘管理操作

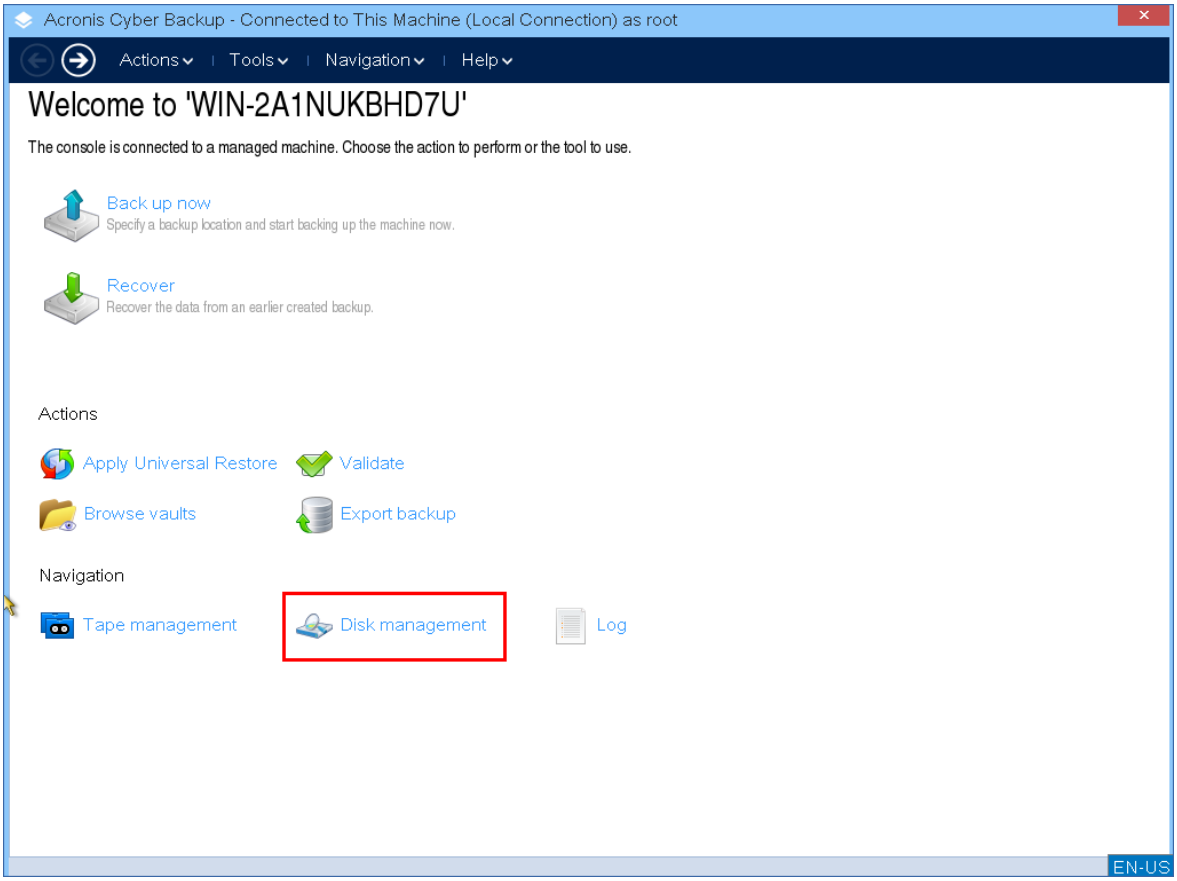
1. 从 Acronis 可启动应急媒体启动。



2. 如需在本地计算机上工作，单击**本地管理此计算机**。有关远程连接的更多信息，请参考在管理服务器上注册媒体。



3. 单击**磁盘管理**。



注意
如果存储空间在计算机上进行配置，可启动媒体下的磁盘管理操作可能无法正确工作。

支持的文件系统

可启动媒体支持以下文件系统的磁盘管理：

- FAT 16/32
- NTFS

如果需要在不同文件系统的卷上执行操作，请使用 Acronis Disk Director。该版本为管理带以下文件系统的磁盘和卷提供了更多的工具和实用程序：

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS
- JFS
- Linux SWAP

基本预防措施

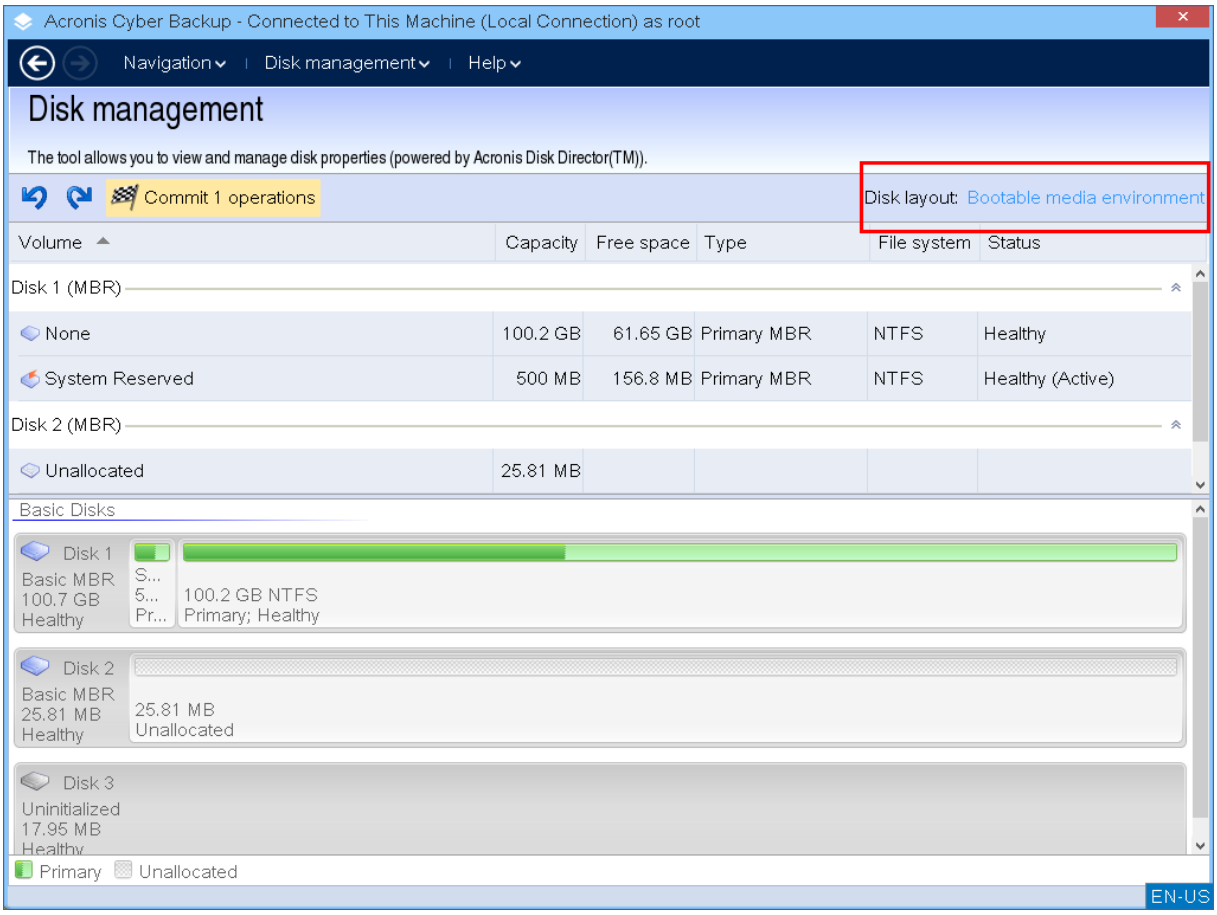
若要避免可能的磁盘和卷结构损坏或数据丢失，请采取所有必要的预防措施并遵循下列规则：

1. 备份要在其上创建或管理卷的磁盘。将您最重要的数据备份至另一个硬盘、网络共享或可移动媒体，这可让您安心地处理磁盘卷，因为您的数据非常安全。
2. 测试您的磁盘，确保其功能完好并且没有损坏的扇区或文件系统错误。
3. 当运行其它具有低级别磁盘访问的软件时，请勿执行行任何磁盘/卷操作。

为磁盘管理选择操作系统

在拥有两个或多个操作系统的计算机上，磁盘和卷的显示取决于当前所运行的操作系统。同一个卷在不同的操作系统下可能具有不同的代号。

当您需要在此计算机上执行磁盘管理操作时，必须指定将显示磁盘布局的操作系统。要执行此操作，请单击**磁盘布局**标签旁边的操作系统名称，然后在打开的窗口中选择所需的操作系统。



磁盘操作

使用可启动媒体，您可以执行以下操作。

- 磁盘初始化 - 初始化添加到系统的新硬件
- 基本磁盘克隆 - 从源基本 MBR 磁盘将完整的数据传输到目标磁盘
- 磁盘转换：MBR 至 GPT - 将 MBR 分区表转换为 GPT
- 磁盘转换：GPT 至 MBR - 将 GPT 分区表转换为 MBR
- 磁盘转换：基本至动态 - 将基本磁盘转换为动态磁盘
- 磁盘转换：动态至基本 - 将动态磁盘转换为基本磁盘

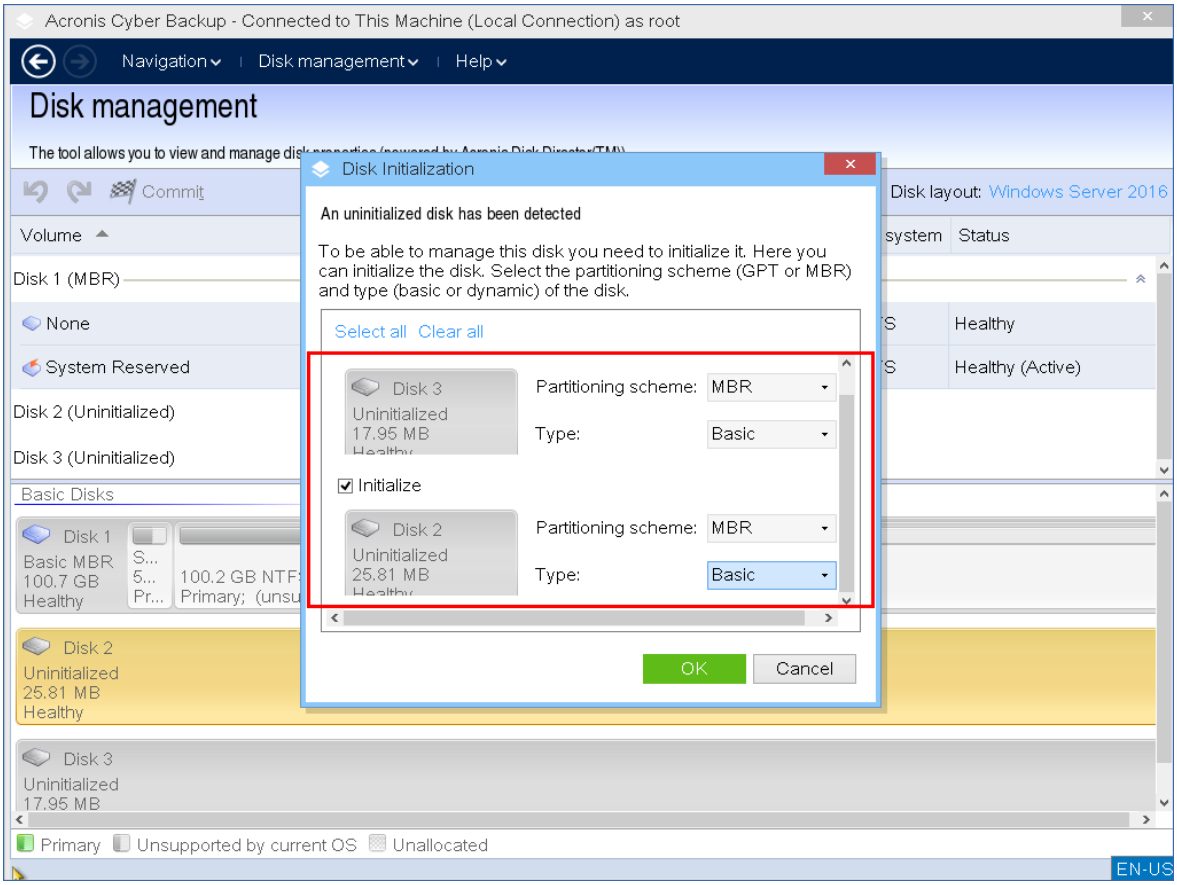
磁盘初始化

可启动媒体会将未初始化的磁盘显示为一个带有灰色图标的灰色块，由此表示系统无法使用该磁盘。

初始化磁盘

1. 右键单击所需的磁盘，然后单击**初始化**。
2. 在**磁盘初始化**窗口中，设置磁盘分区方案（MBR 或 GPT）和磁盘类型（基本或动态）。
3. 单击 **确定**，您可添加磁盘初始化的待处理操作。
4. 要完成添加的操作，请执行。未执行操作而退出程序将会取消该操作。

5. 初始化之后，所有的磁盘空间仍然未分配。若要能够进行使用，您需要在其上创建一个卷。



基本磁盘克隆

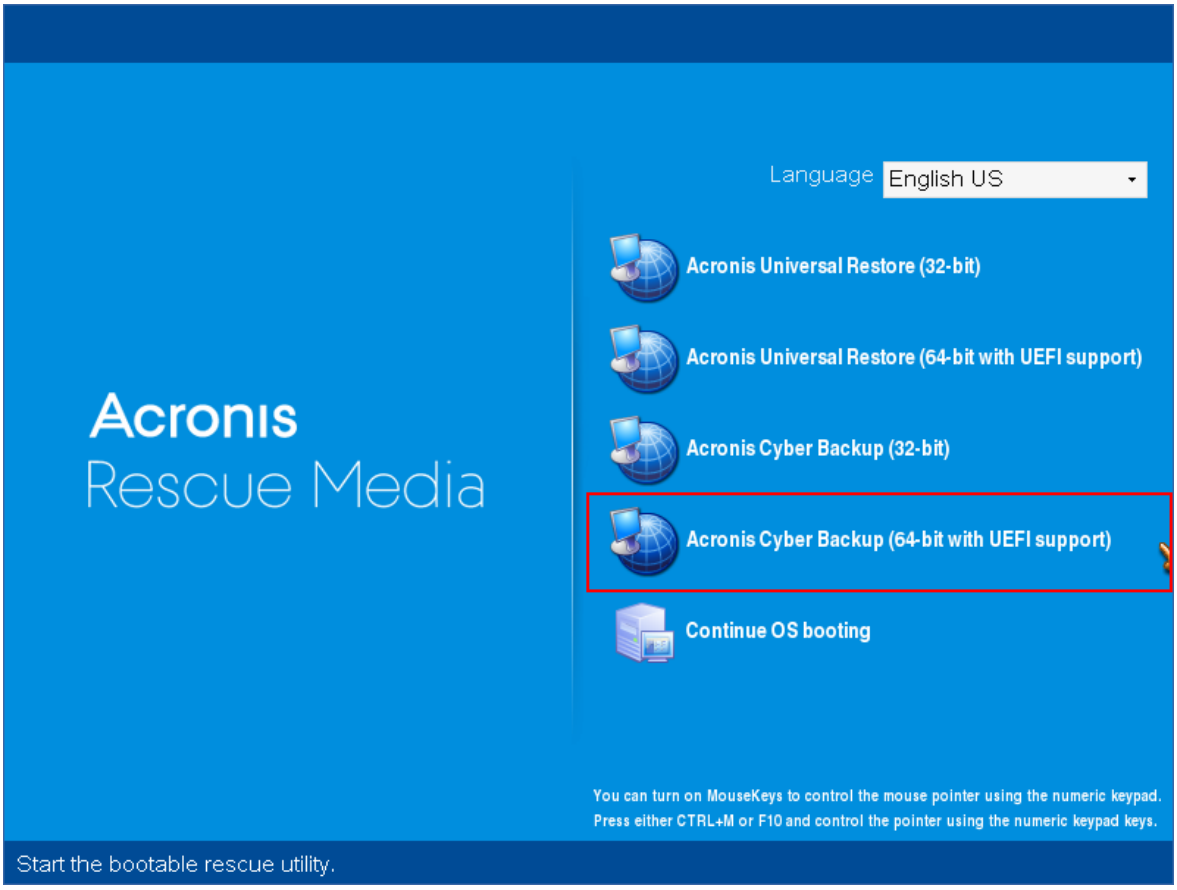
您可以用全功能基于 Linux 的可启动媒体，克隆基本 MBR 磁盘。磁盘克隆在您可以下载的现成可用可启动媒体中或在没有许可号的可启动媒体中不可用。

注意

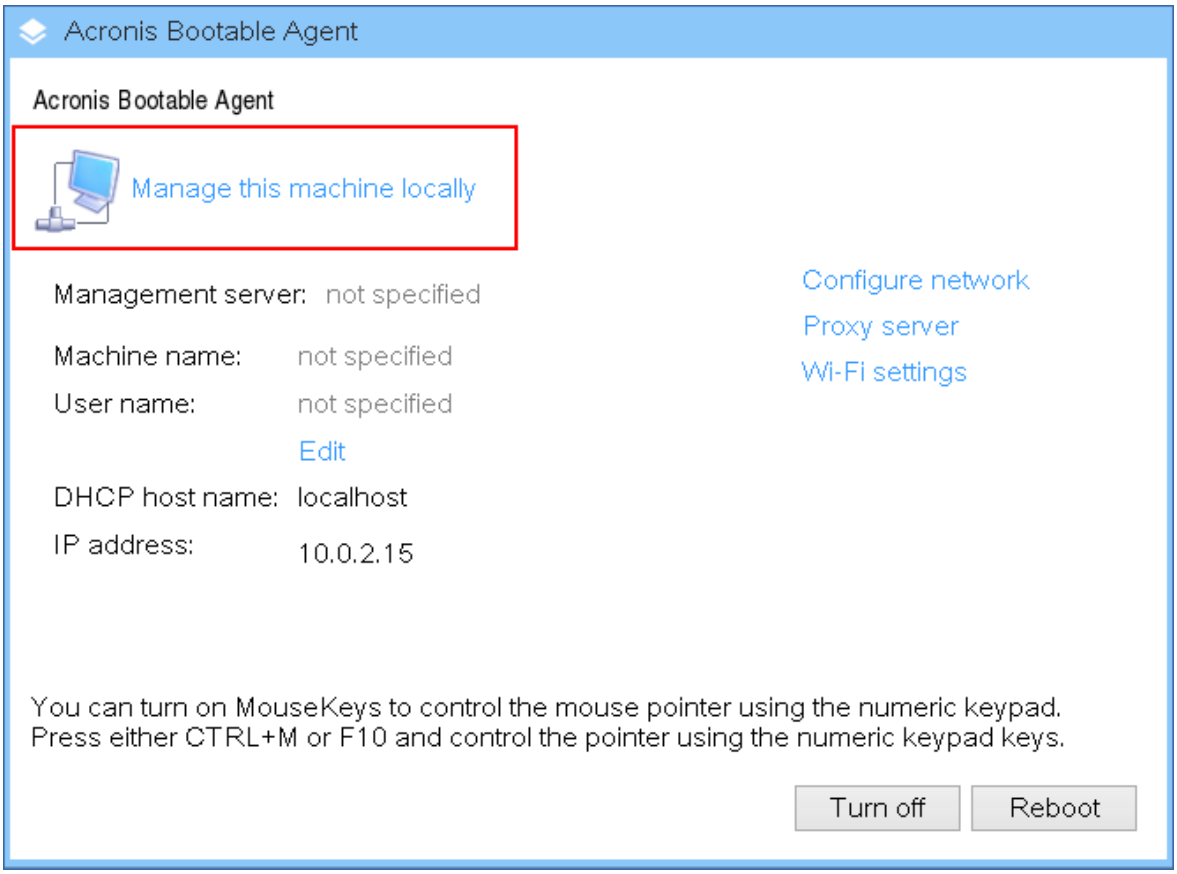
还可以使用 Acronis 安克诺斯数据保护软件 命令行实用程序克隆磁盘。

在可启动媒体下工作克隆基本磁盘

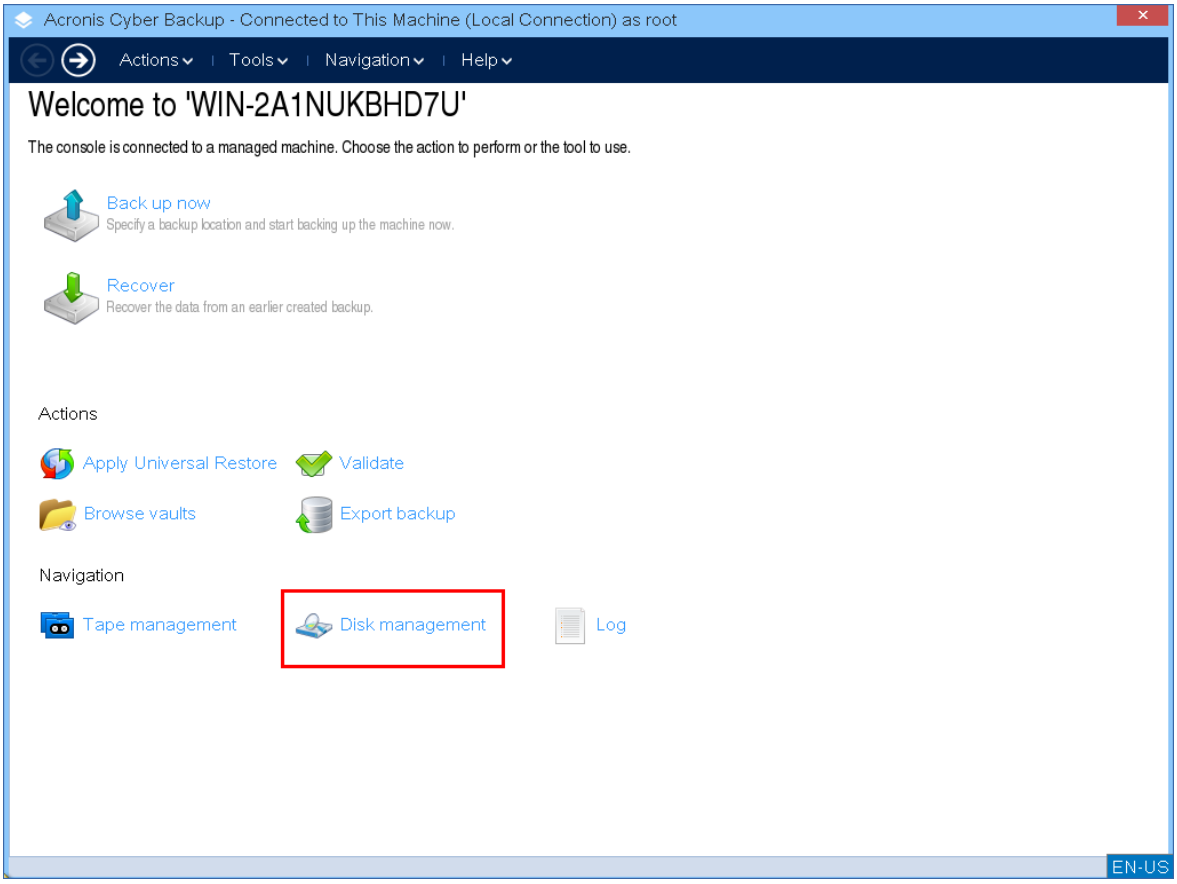
1. 从 Acronis 可启动应急媒体启动。



2. 要克隆本地计算机的磁盘，请单击**本地管理此计算机**。有关远程连接，请参阅管理服务器上注册媒体。

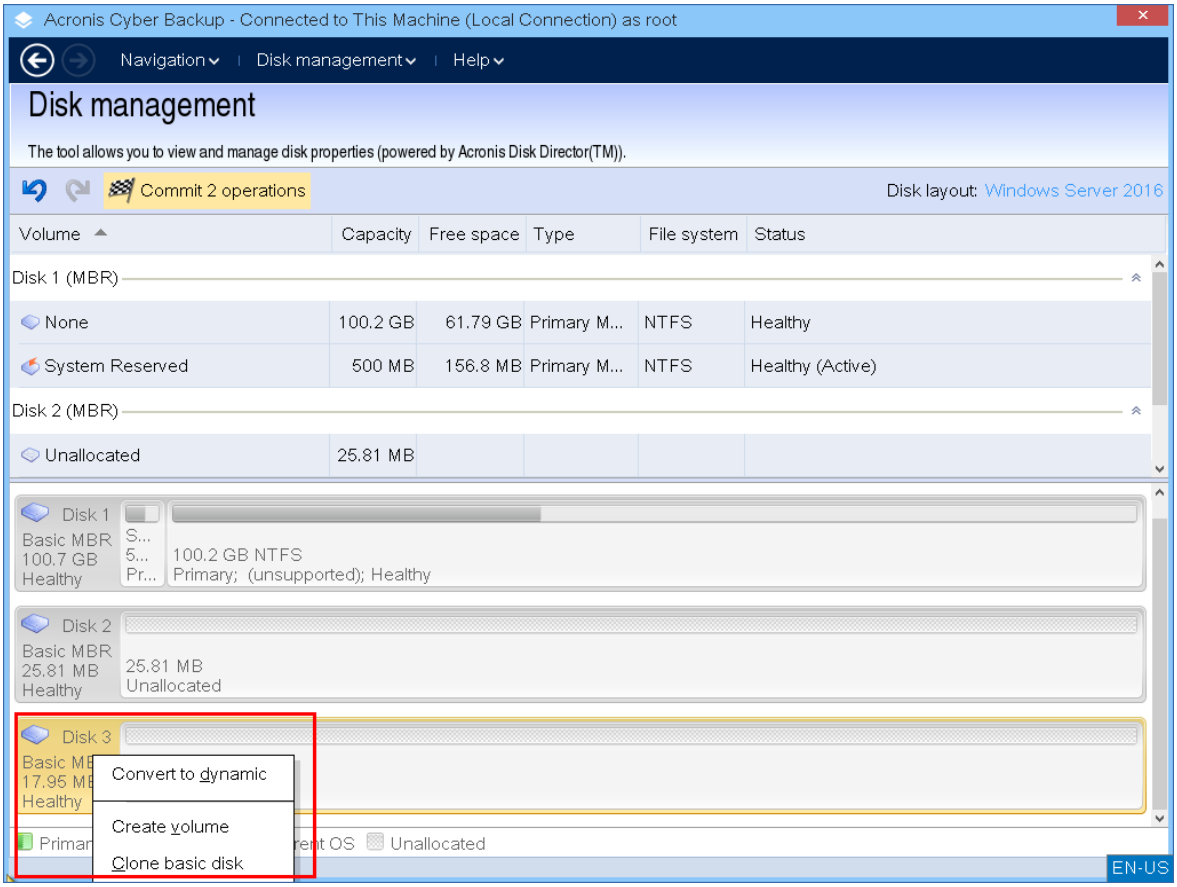


3. 单击**磁盘管理**。

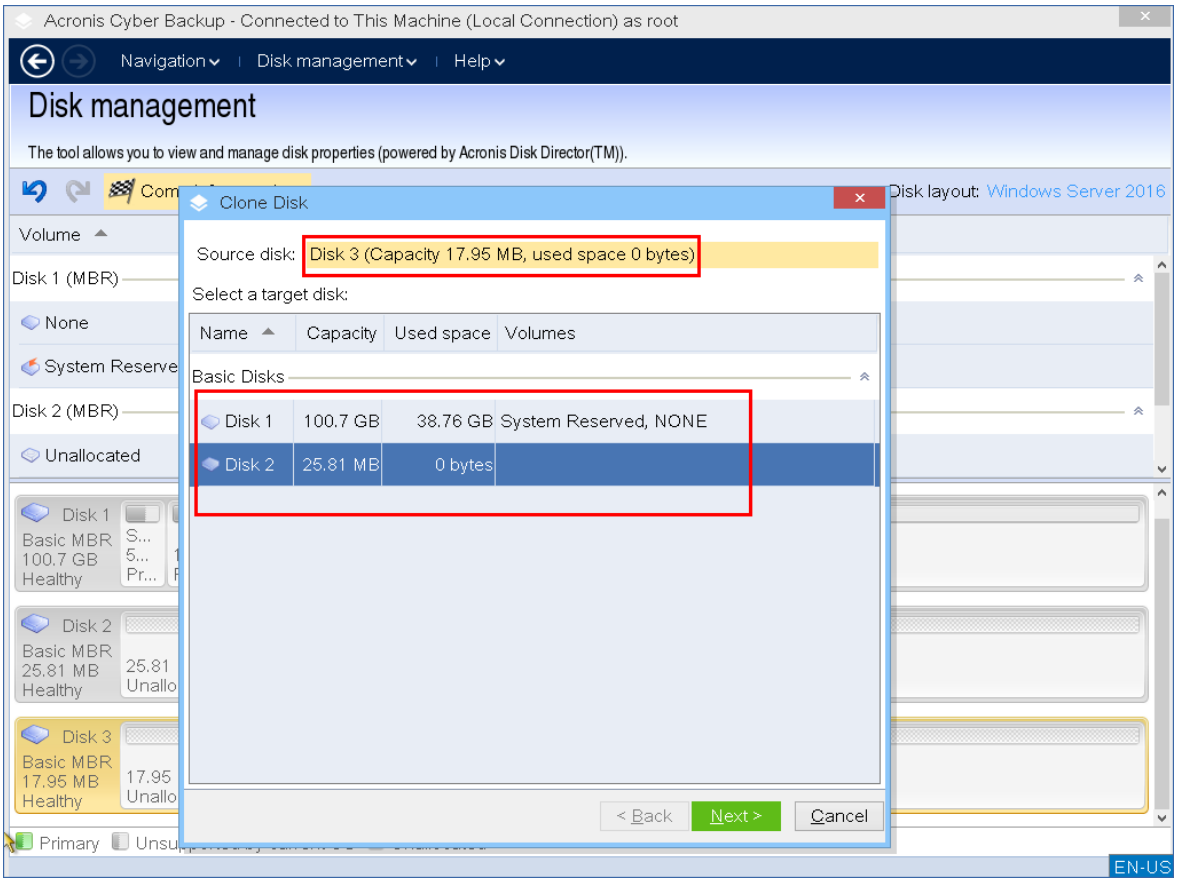


4. 将显示可用磁盘。右键单击要克隆的磁盘，然后单击**克隆基本磁盘**。

注意
只能克隆整个磁盘。分区克隆不可用。



5. 将显示可能的目标磁盘列表。程序允许您选择一个目标磁盘，如果它足够大，可以保存来自源磁盘的所有数据而不会丢失。选择目标磁盘，然后单击**下一步**。

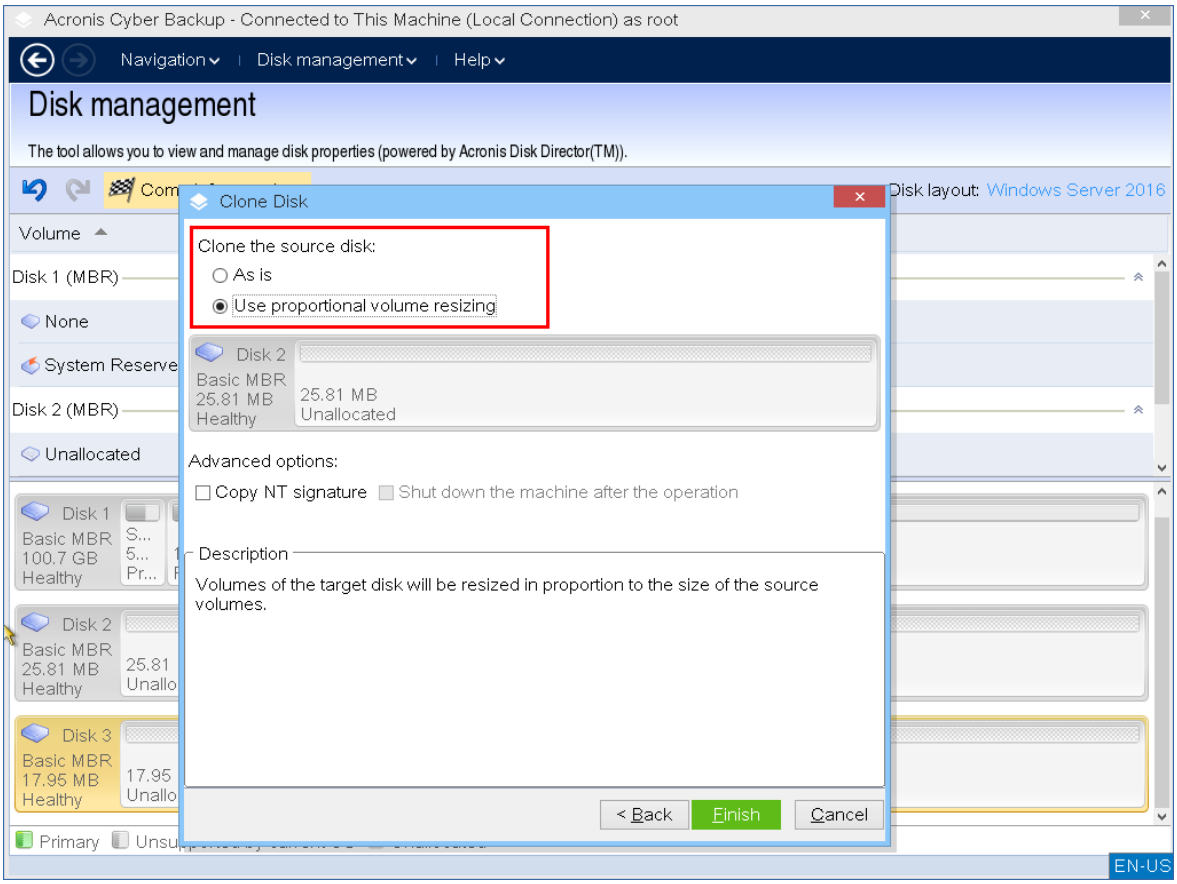


如果目标磁盘更大，则建议通过按原样克隆磁盘或按比例调整源磁盘卷的大小(默认选项)以避免在目标磁盘上留下未分配的空间。

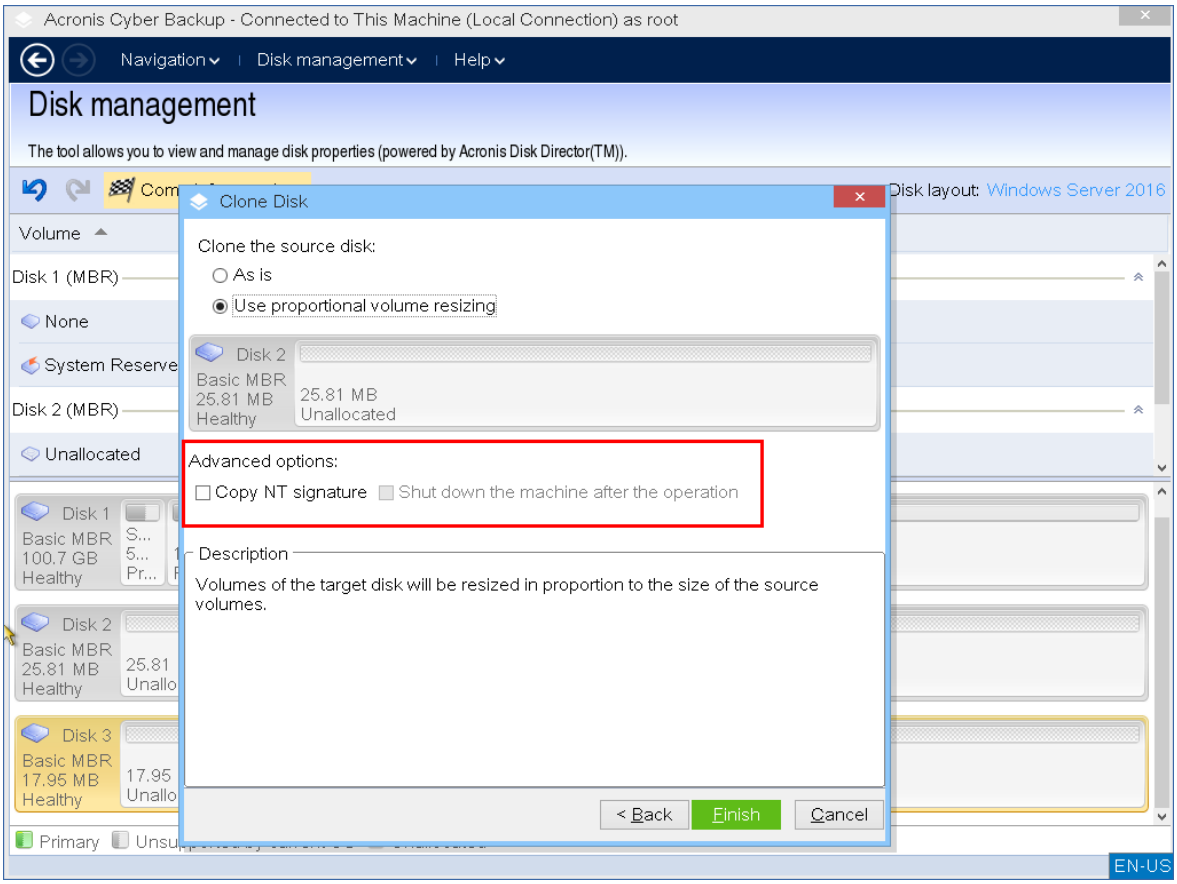
如果目标磁盘更小，则只能按比例调整大小。如果即使按比例调整大小也不可能安全克隆，则您将无法继续操作。

重要事项

如果目标磁盘上有数据，您会看到以下警告：*"所选的目标磁盘不为空。其卷上的数据将被覆盖。"*如果继续，目标磁盘上当前的所有数据都将不可撤销地丢失。



6. 选择是否复制 NT 签名。



当克隆含有系统卷的磁盘时，需要在目标磁盘卷上确保操作系统可启动。这表示操作系统必须具备与磁盘 NT 签名相符的系统卷信息(如卷代号)，此类信息在 MBR 磁盘记录中保存。但 NT 签名相同的两个磁盘是无法在同一个操作系统内正常运作的。

如果计算机上有两个磁盘拥有相同的 NT 签名，并包含一个系统卷，操作系统通过第一个磁盘启动运行，然后发现第二个磁盘上的相同签名后，会自动新生成一个唯一的 NT 签名，并分配给第二个磁盘。因此，第二个磁盘上的所有卷都将丢失代号，所有磁盘路径都将失效，而且程序将无法查找到上面的文件。磁盘上的操作系统就将无法启动。

若要保留目标磁盘卷上的系统可启动属性，可选择执行以下步骤之一：

a. **复制 NT 签名** - 为目标磁盘提供与注册表项相符的源磁盘 NT 签名，并将其复制在目标磁盘上。

   选择**复制 NT 签名**复选框。

   您会看到警告：*"如果硬盘上有操作系统，再次启动计算机前，从计算机上卸载源硬盘驱动器或者目标硬盘驱动器。否则，操作系统将从两个磁盘中的第一个磁盘启动，而第二个磁盘上的操作系统将无法启动。"*

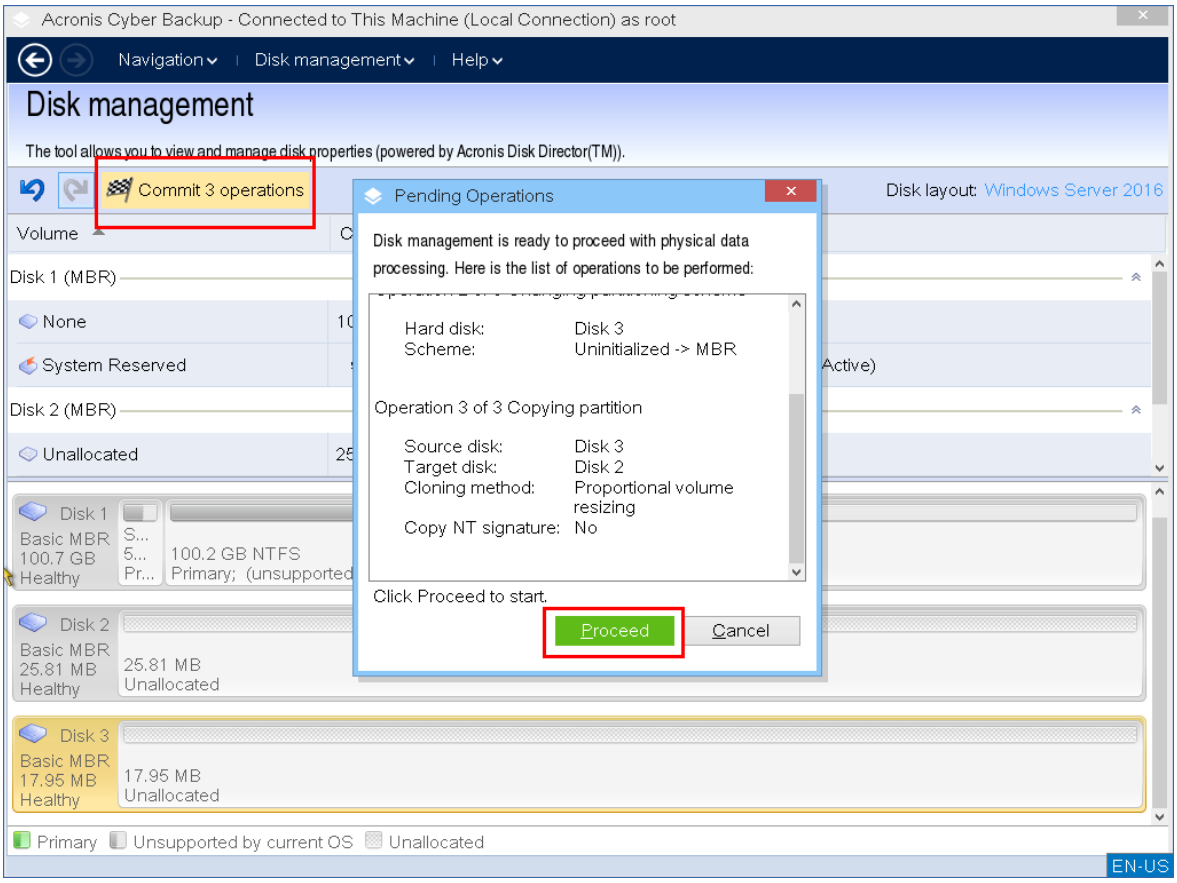
   将自动选择并禁用克隆**操作后关闭计算机**复选框。

b. **保留 NT 签名** - 保留旧目标磁盘签名并根据签名更新操作系统。

   必要时，单击以不选择**复制 NT 签名**复选框。

   操作后关闭计算机复选框将自动清除。

7. 单击**完成**以添加磁盘克隆操作。
8. 单击**执行**，然后在**待处理操作**窗口中单击**继续**。未执行操作而退出程序将会取消该操作。



9. 如果选择复制 NT 签名，请等待操作完成并关闭计算机，然后断开源或目标硬盘与计算机的连接。

磁盘转换：MBR 至 GPT

在下列情况下，您可能希望将 MBR 基本磁盘转换为 GPT 基本磁盘：

- 如果您需要一个磁盘上装有 4 个以上的主卷。
- 如果您需要更高的磁盘可靠性，以防止任何可能的数据损坏。

重要事项
包含当前运行操作系统的启动卷的基本 MBR 磁盘无法转换为 GPT。

将基本 MBR 磁盘转换为基本 GPT 磁盘

1. 右键单击要克隆的磁盘，然后单击**转换为 GPT**。
2. 通过单击 **确定** ，您将添加 MBR 转换至 GPT 磁盘的待处理操作。
3. 要完成添加的操作，请执行。未执行操作而退出程序将会取消该操作。

注意
GPT 分区磁盘会分区区域的末尾保留一定的空间用作备份区域，这用来存储 GPT 标题和分区表的副本。如果磁盘已满，卷大小不能自动减少，从 MBR 磁盘转换至 GPT 磁盘的操作将无法进行。
该操作是不可逆的。如果您有一个主卷并且属于 MBR 磁盘，首先将磁盘转换为 GPT 磁盘，然后再转换回 MBR 磁盘，则该卷将成为逻辑卷并将不能再作为系统卷使用。

动态磁盘转换:MBR 至 GPT

可启动媒体不支持动态磁盘 MBR 至 GPT 的直接转换。但是,为了达到目的,您可执行下列转换以达成此目标:

1. MBR 磁盘转换:动态至基本 使用 **转换为基本** 操作。
2. 基本磁盘转换:MBR 至 GPT 使用 **转换为 GPT** 操作。
3. GPT 磁盘转换:基本至动态 使用 **转换为动态** 操作。

磁盘转换:GPT 至 MBR

如果您计划安装不支持 GPT 磁盘的操作系统,则可以将 GPT 磁盘转换为 MBR。

重要事项
包含当前运行操作系统的启动卷的基本 GPT 磁盘无法转换为 MBR。

将 GPT 磁盘转换为 MBR 磁盘

1. 右键单击要克隆的磁盘,然后单击**转换为 MBR**。
2. 通过单击 **确定** ,您将添加 GPT 转换至 MBR 磁盘的待处理操作。
3. 要完成添加的操作,请执行。未执行操作而退出程序将会取消该操作。

注意
在执行该操作后,此磁盘上的卷将变为逻辑卷。此操作不可逆。

基本到动态磁盘的转换

以下情况下将基本磁盘转换为动态磁盘:

- 如果您计划将磁盘用作动态磁盘组的一部分。
- 如果您需要为数据存储提高磁盘可靠性。

将基本磁盘转换成动态磁盘

1. 右键单击要转换的磁盘,然后单击**转换为动态磁盘**。
2. 单击**确定**。

转换将立即执行,如有必要,您的计算机将重新启动。

注意
动态磁盘将占用物理磁盘的最后空间来存储数据库,包括各动态卷的四个级别的描述(卷-组件-分区-磁盘)。如果在转换为动态磁盘过程中,发现基本磁盘已满并且其卷大小不能自动减少,基本磁盘转换至动态磁盘的操作将失败。
将含有系统卷的基本磁盘转换为动态磁盘需要花费一定的时间,在这一过程中,断电、无意关闭计算机或意外按下"重启"按钮可能导致磁盘无法启动。

与"Windows 磁盘管理器"相反,该程序可确保执行操作后磁盘上的**离线操作系统**可启动。

动态到基本磁盘的转换

您可能希望将动态磁盘转换回基本磁盘，例如，如果您要在计算机上开始使用不支持动态磁盘的操作系统。

将动态磁盘转换为基本磁盘：

1. 右键单击要转换的磁盘，然后单击**转换为基本磁盘**。
2. 单击**确定**。

转换将立即执行，如有必要，您的计算机将重新启动。

注意
该操作不适用于包含跨区卷、条带卷或 RAID-5 卷的动态磁盘。

转换完成后，磁盘空间的最后 8Mb 将被保留，供今后从基本磁盘至动态磁盘的转换使用。在某些情况下，可能的未分配空间与建议的最大卷大小可能有所不同(例如，当一个镜像的大小建立另一个镜像的大小时，或磁盘空间的最后 8Mb 为今后从基本至动态磁盘的转换而保留)。

注意
转换含有系统卷的磁盘需要花费一定时间，在此过程中，断电、无意关闭计算机或意外按下“重启”按钮都可能导致无法启动。

与“Windows 磁盘管理器”相反，该程序可确保：

- 磁盘包含的卷带有简单或镜像卷的**数据**时，可将动态磁盘安全转换为基本磁盘
- 在多启动系统中，操作过程中**脱机**的系统也可以启动

卷操作

使用可启动媒体，可以对卷执行以下操作：

- 创建卷 - 创建新卷。
- 删除卷 - 删除所选卷。
- 设为活动 - 将所选卷设为'活动'，以便计算机能够使用安装在该卷上的操作系统启动。
- 更改代号 - 更改所选卷的代号。
- 更改标签 - 更改所选卷的标签。
- 格式化卷 - 格式化卷，为其提供必要的文件系统。

动态卷的类型

简单卷

用一个物理磁盘上的可用空间创建的卷。它可包括磁盘的一个区域或几个区域，实际上由逻辑磁盘管理器 (LDM) 联合在一起。这在可靠性、速度和容量方面没有任何提升。

跨区卷

在可用磁盘空间上建立的磁盘区，这些磁盘空间是将几个物理磁盘通过 LDM 以虚拟方式连接在一起形成的。最多可将 32 个磁盘包括在一个卷中，从而克服了硬件大小的限制。但如果只有一个磁盘发生故障，所有的数据都将丢失并且如果不破坏整个卷，则无法删除跨区卷的任何部分。因此，跨区卷不具有更高的可靠性，也不能提供更好的 I/O 传输速率。

带区卷

有时被称为 RAID 0 的卷，包含同等大小的数据条带，写入卷中的各磁盘。这意味着若要创建一个带区卷，您将需要两多个动态磁盘。带区卷中的磁盘不必完全相同，但是在您要包括进卷中的各个磁盘上必须有未使用的空间。并且卷大小将取决于最小空间的大小通常，访问带区卷上的数据要比访问单个物理磁盘上的相同数据更快，因为 I/O 分散在多个磁盘上。

创建带区卷可改善性能，但没有提高可靠性 - 它们不包含冗余信息。

镜像卷

一个磁盘上的所有信息被复制在另一个磁盘上，以提供数据冗余。一个磁盘上的所有信息被复制在另一个磁盘上，以提供数据冗余。几乎任何卷都可以生成镜像，包括系统和启动卷，如果其中一个磁盘发生故障，仍可从剩余的磁盘访问数据。遗憾的是，使用镜像卷受到硬件大小和性能的限制更高。

镜像带区卷

一种具有容错能力的卷，有时也称为 RAID 1+0，结合了带区卷布局的高速 I/O 传输速度和镜像卷类型冗余的优势。但仍具有镜像体系结构固有的明显缺点 - 磁盘对卷大小比率较低。

RAID-5

一种具有容错能力的卷，其数据以等量方式存储于由三个或更多磁盘组成的阵列中。其磁盘不必完全相同，但是卷中各磁盘上的可用未分配空间的块区必须大小相同。奇偶校验信息(发生故障后可用于重建数据的计算值)同样也以等量方式存储于磁盘阵列中，并且它始终存储在与数据本身不同的磁盘上。若物理 磁盘发生故障，位于该磁盘上的 RAID-5 信息可通过余下的数据及 奇偶校验信息来重新创建。RAID-5 具有更高的可靠性，并凭借高于镜像卷的磁盘对卷大小比率，能够克服物理磁盘的大小限制。

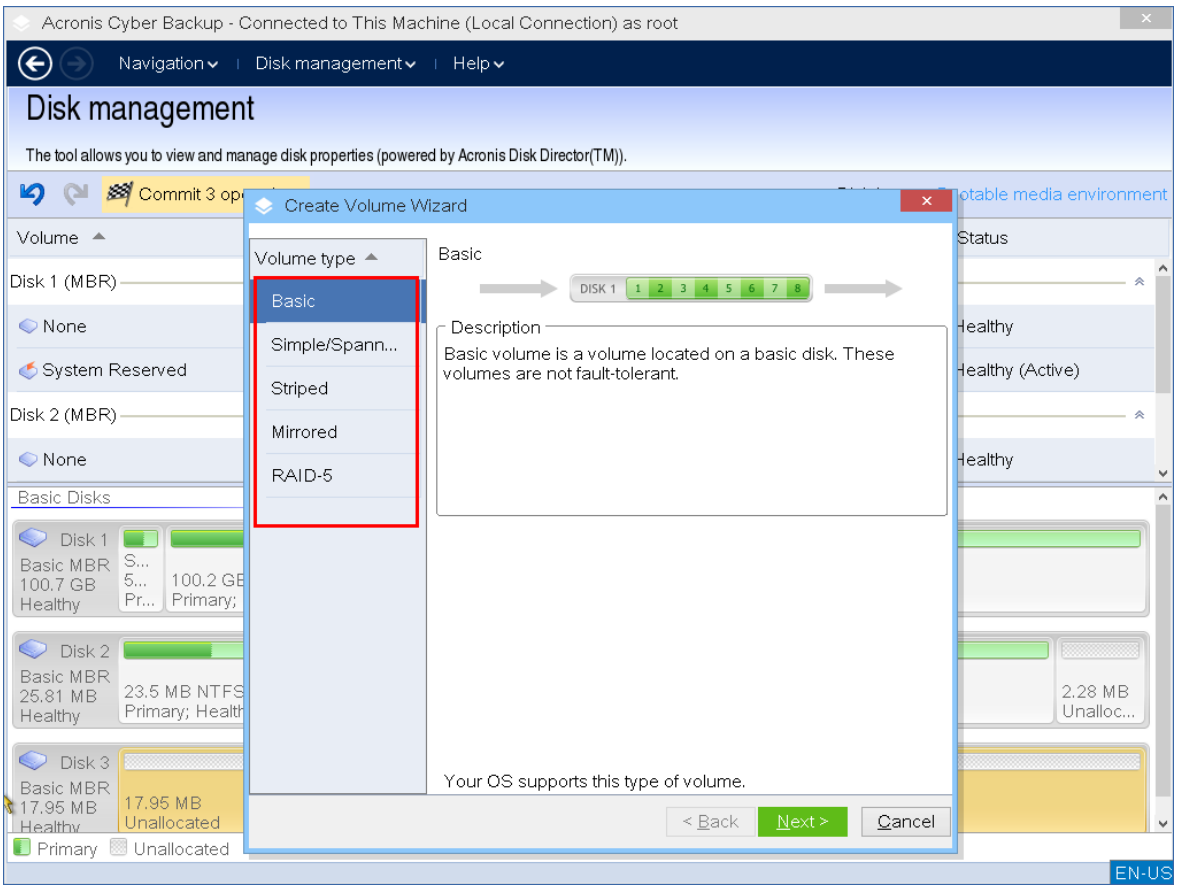
创建卷。

您可能需要一个新卷来：

- 以“完全按原样”配置恢复先前保存的备份副本
- 分开保存类似文件的集合 — 例如，在单独的卷上保存 MP3 集合或视频文件；
- 在特殊卷上保存其他卷/磁盘上的备份(映像)
- 在新卷上安装新的操作系统(或交换文件)
- 将新硬件添加至计算机

创建卷

1. 右键单击磁盘中任何未分配的空间，然后单击**创建卷**。**创建卷**向导打开



2. 选择卷类型。可使用以下选项：
   - 基本
   - 简单卷/跨区卷
   - ⬚⬚带卷
   - 镜像
   - RAID-5

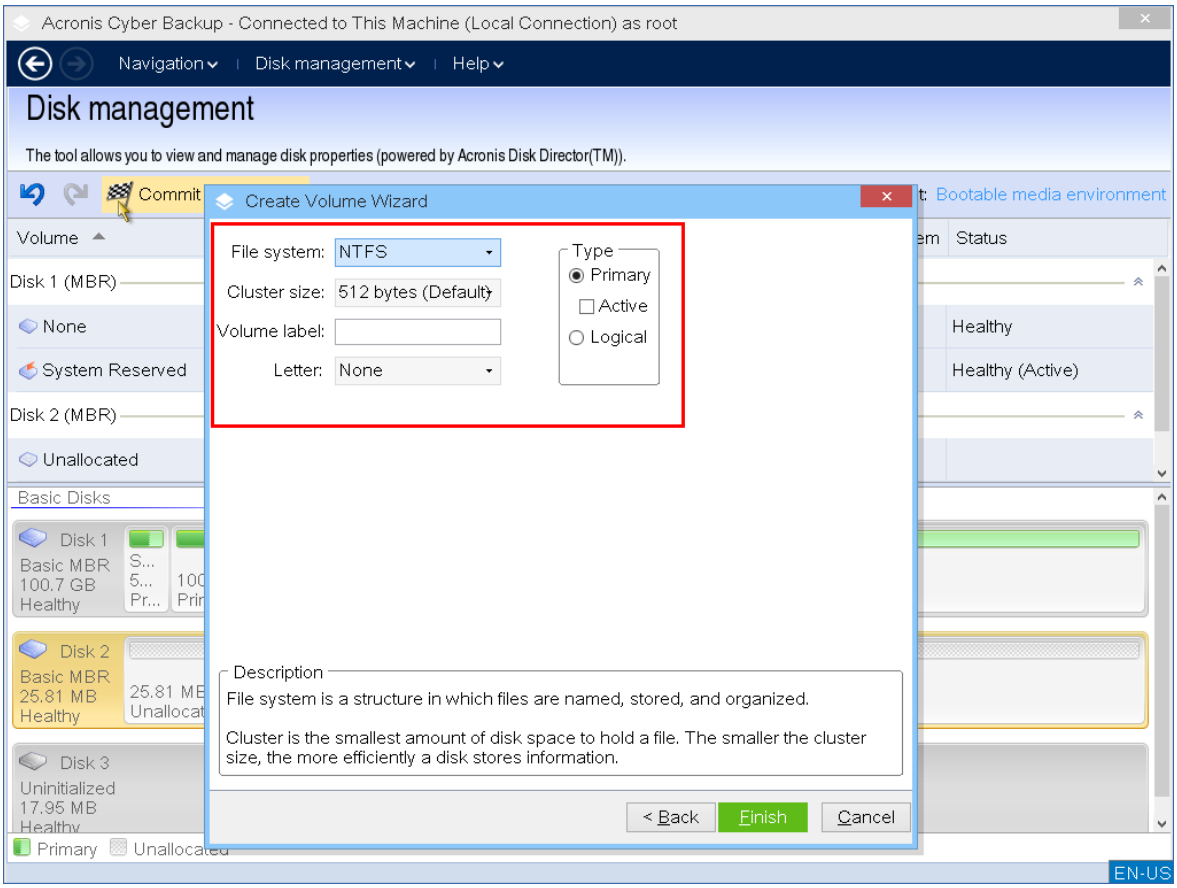
   如果目前安装在此计算机上的操作系统不支持所选的卷类型，您将收到一条警告，并且**下一步**按钮将被禁用。您必须选择另一卷类型以继续新卷创建。
3. 指定未分配的空间或选择目标磁盘。
   - 对于基本卷，请指定所选磁盘上未分配的空间。
   - 对于简单/跨区卷，请选择一个或多个目标磁盘。
   - 对于镜像卷，请选择两个目标磁盘。
   - 对于带区卷，请选择两个或多个目标磁盘。
   - 对于 RAID-5 卷，请选择三个目标磁盘。

   如果计划创建**动态**卷并选择一个或几个**基本**磁盘作为其目标磁盘，您将看到一个警告，通知您所选磁盘将自动转换为动态磁盘。
4. 设置卷大小。

最大值通常包括最大可能的未分配空间。在某些情况下，可能的未分配空间与建议的最大卷大小可能有所不同(例如，当一个镜像的大小建立另一个镜像的大小时，或磁盘空间的最后 8Mb 为今后从基本至动态磁盘的转换而保留)。

如果磁盘上的未分配空间大于该卷，则可以选择该磁盘上新基本卷的位置。

5. 设置卷选项。



您可在向导下一页上指定卷 **代号**（默认 - 字母表的第一个可用字母），还可选择指定 **标签**（默认 – 无）。也可在此处指定 **文件系统** 和 **群集大小** 。

可能的文件系统选项包括：

- FAT16（如果卷大小被设为超过 2 GB，则禁用）
- FAT32（如果卷大小被设为超过 32 GB，则禁用）
- NTFS
- 保留不格式化此卷。

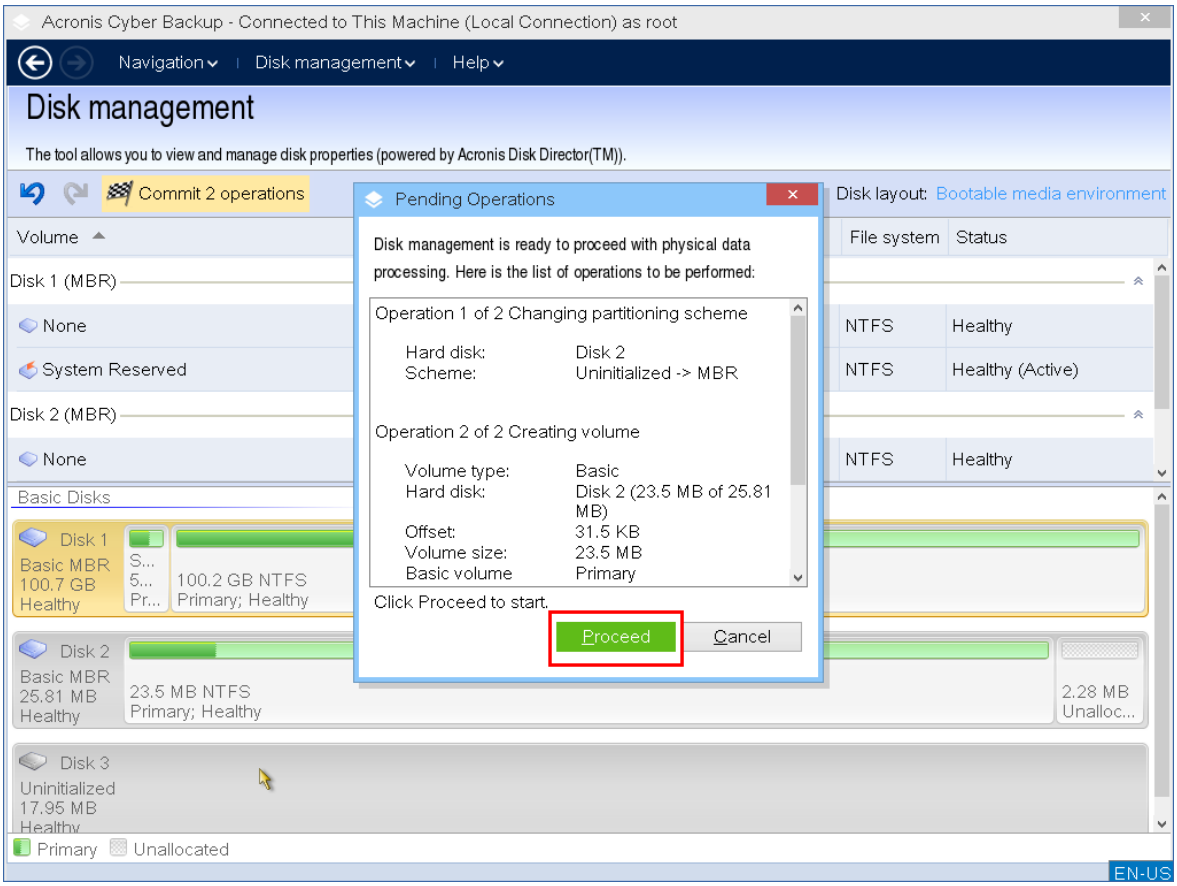
设置群集大小时，您可在每个文件系统预设的容量范围内选择任何数字。群集大小最好适合卷的所选文件系统。如果您为 FAT16/FAT32 设置 64K 的群集大小或为 NTSF 设置 8KB-64KB 的群集大小，Windows 可加载该卷，但某些程序（如安装程序）可能会错误地计算其磁盘空间。

如果您正在创建一个可以成为系统卷的基本卷，此页面将有所不同，会让您有机会选择卷 类型 — **主**（**活动主**）或 **逻辑** 。通常，选择 **主** 是为了在该卷上安装操作系统。如果您要在这个卷上安装在启动计算机时启动的操作系统，则选择**活动**（默认）值。如果没有选择**主**按钮，**活动**选项将处于未激活状态。如果该卷用于数据存储，选择**逻辑**。

注意

一个基本磁盘可包含最多四个主卷。如果它们已经存在，磁盘将必须转换为动态，否则 **活动** 和 **主** 选项将被禁用，您将只能选择 **逻辑** 卷类型。

6. 单击**执行**，然后在**待处理操作**窗口中单击**继续**。未执行操作而退出程序将会取消该操作。



删除卷

删除卷

1. 右键单击要删除的卷。
2. 单击**删除卷**。

注意

该卷上的所有信息将不可避免地丢失。

3. 单击 **确定**，您可添加卷删除的待处理操作。
4. 要完成添加的操作，请执行。未执行操作而退出程序将会取消该操作。

删除卷后，其空间将被添加到未分配空间中。这可用于创建新卷或更改另一卷的类型。

设置活动卷

如果您有几个主卷，必须指定一个作为启动卷。为此，您可将一个卷设为活动卷。一个磁盘上只能有一个活动卷。

如果您需要设置一个活动卷：

1. 右键单击基本 MBR 上所需的主卷，然后单击**标记为活动**。
   如果系统中没有其他活动卷，将添加设置活动卷的待处理操作。如果系统中有另一个活动卷，您将看到警告，即必须首先将先前的活动卷设置为非活动。

   注意
   由于设置新的活动卷，先前活动卷号可能会被更改，并且某些已安装的程序可能会停止运行。

2. 通过单击**确定**，将添加设置活动卷的待处理操作。

   注意
   即使将操作系统置于新的活动卷上，在某些情况下，计算机也将无法通过该卷启动。您必须确认将新卷设为活动卷。

3. 要完成添加的操作，请执行。未执行操作而退出程序将会取消该操作。

更改卷代号

启动时，Windows 操作系统将指定硬盘卷的代号（C:、D:等）。应用程序和操作系统使用这些代号来查找卷上的文件和文件夹。连接另一个磁盘以及在现有磁盘上创建或删除卷，可能更改您的系统配置。因此，某些应用程序可能停止正常工作，或者可能无法自动找到并打开用户文件。为了避免这种情况，您可手动更改由操作系统自动指定的卷代号。

更改由操作系统指定的卷代号：

1. 右键单击所需卷，然后单击 **更改代号** 。
2. 在 **更改代号** 窗口选择一个新代号。
3. 单击 **确定** ，您可添加卷代号分配的待处理操作。
4. 要完成添加的操作，请执行。未执行操作而退出程序将会取消该操作。

更改卷标签

卷标签是一个可选属性。这是为了便于识别而指定给卷的名称。

更改卷标

1. 右键单击所选卷，然后单击**更改标签**。
2. 在**更改标签** 窗口的文本字段中输入新的标签。
3. 单击**确定**，将添加更改卷标的待处理操作。
4. 要完成添加的操作，请执行。未执行操作而退出程序将会取消该操作。

格式化卷

如果希望更改卷的文件系统，则可能需要格式化卷：

- 以节约更多的空间，这些空间由于使用 FAT16 或 FAT32 文件系统的群集大小而失去
- 作为一种快速而又较为可靠的销毁此卷上数据的方式

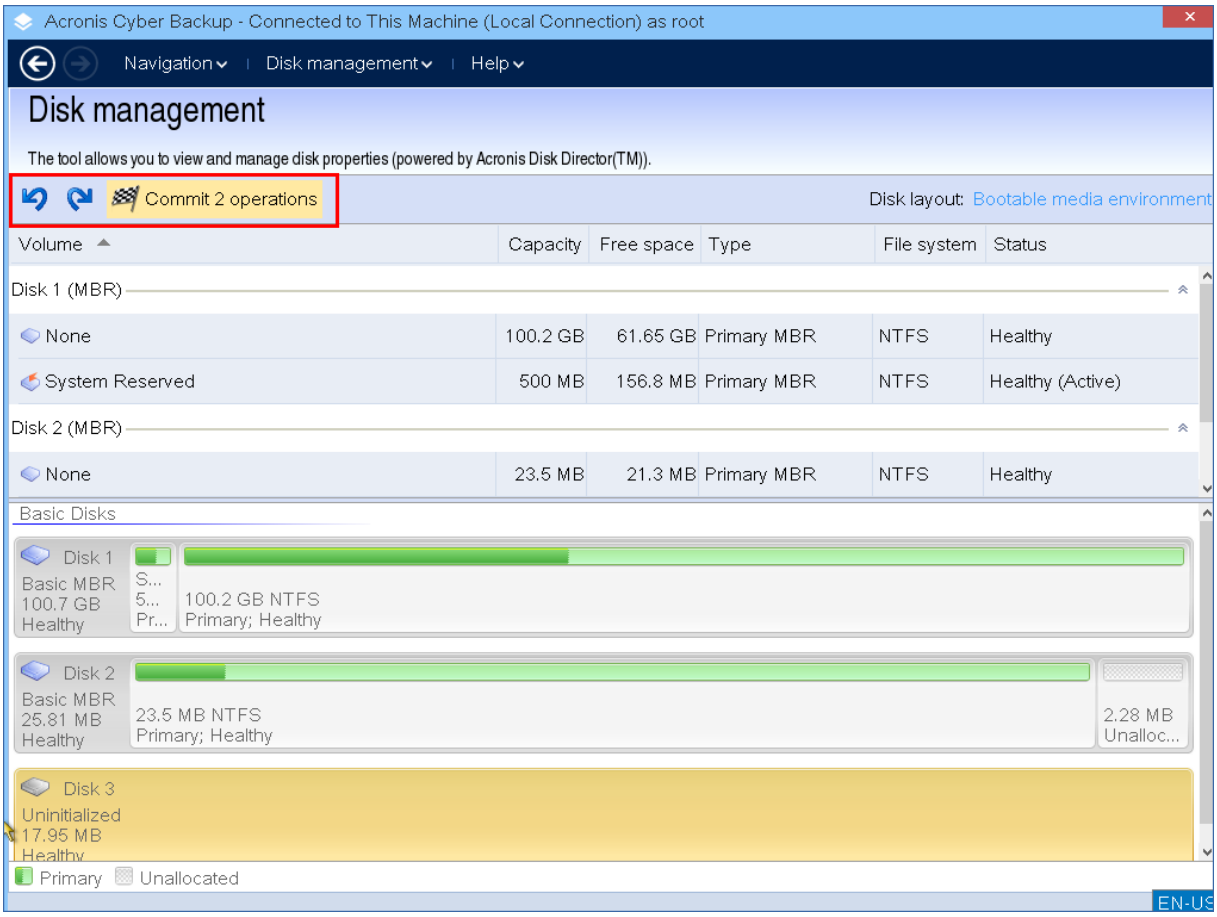
格式化卷：

1. 右键单击所需卷，然后单击**格式**。
2. 选择群集大小和文件系统。可能的文件系统选项包括：
   - FAT16（如果卷大小被设为超过 2 GB，则禁用）
   - FAT32（如果卷大小被设为超过 32 GB，则禁用）
   - NTFS
3. 单击 **确定** ，您可添加格式化卷的待处理操作。
4. 要完成添加的操作，请执行。未执行操作而退出程序将会取消该操作。

待处理操作

在发出并确认**执行**命令之前，所有操作都被视为挂起。这种方法可让您控制所有计划的操作、复核计划的更改，以及必要时在执行之前取消操作。

磁盘管理 视图中的工具栏上含有启动 **撤销** 、**重做** 和 **执行** 操作的图标，这些操作用于待处理操作。这些操作也可从中控台的 **磁盘管理** 菜单来启动。



所有计划的操作将被添加至待处理操作列表。

撤销操作可让您撤销列表中最近的操作。当列表不为空时，该操作可用：

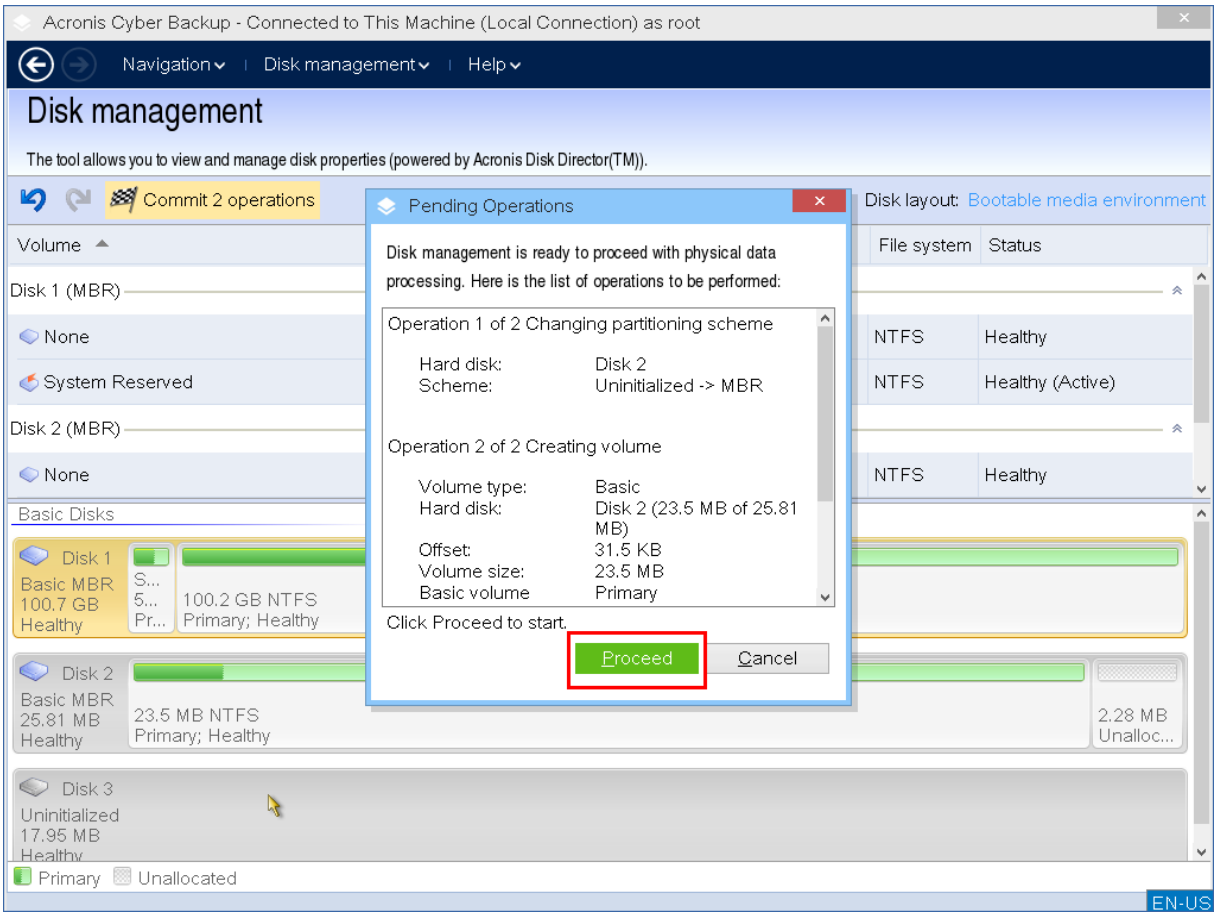
重做操作可让您恢复被撤销的最后待处理操作。

执行操作可将您转至**待处理**操作窗口，您可在此查看待处理操作列表。

要启动执行，请单击**继续**。

注意
选择**继续**操作后，将无法撤销任何行动或操作！

如果不想继续执行，请单击**取消**。将不会对待处理操作列表作出任何更改。未执行待处理操作而退出程序将会取消该操作。



通过可启动媒体进行的远程操作

要在 安克诺斯数据保护软件 中控台中查看可启动媒体，首先需要注册它，如 "在管理服务器上注册媒体"(第 331 页) 中所述。

在 安克诺斯数据保护软件 中控台中完成注册媒体后，它会显示在**设备** > **可启动媒体**中。

通过使用 Web 界面，可以远程管理媒体。例如，可以恢复数据、重新启动或关闭使用媒体启动的计算机，也可以查看有关媒体的信息、活动和警报。

使用可启动媒体远程恢复文件或文件夹

1. 在 安克诺斯数据保护软件 中控台中，转到**设备** > **可启动媒体**。
1. 选择要用于数据恢复的媒体。
2. 单击**恢复**。
3. 选择位置，然后选择所需的备份。请注意，备份是按位置过滤的。
4. 选择恢复点，然后单击**恢复文件/文件夹**。
5. 浏览到所需文件夹，或使用搜索栏获取所需文件和文件夹的列表。
   可以使用一个或多个通配符(* 和 ?)。有关使用通配符的更多详细信息，请参阅 "文件过滤器" (第 240 页)。
6. 单击以选择要恢复的文件，然后单击**恢复**。
7. 在**路径**中，选择恢复目标位置。

8. [可选] 对于高级恢复配置，请单击**恢复选项**。有关详细信息，请参阅 "恢复选项"(第 286 页)。
9. 单击**开始恢复**。
10. 选择文件覆盖选项之一：
    - **覆盖现有文件**
    - **覆盖现有文件(如果较旧)**
    - **不覆盖现有文件**

    选择是否自动重新启动计算机。
11. 单击**继续**以开始恢复。恢复进度显示在**活动**选项卡上。

使用可启动媒体远程恢复磁盘、卷或整台计算机

1. 在**设备**选项卡上，转到**可启动媒体**组，然后选择要用于数据恢复的媒体。
2. 单击**恢复**。
3. 选择位置，然后选择所需的备份。请注意，备份是按位置过滤的。
4. 选择恢复点，然后依次单击**恢复** > **整台计算机**。

   如有必要，按照 "恢复物理机"(第 271 页) 中所述配置目标计算机和卷映射。
5. 对于高级恢复配置，请单击**恢复选项**。有关详细信息，请参阅 "恢复选项"(第 286 页)。
6. 单击**开始恢复**。
7. 确认要将磁盘覆盖为其备份版本。选择是否自动重新启动计算机。
8. 恢复进度显示在**活动**选项卡上。

远程重新启动已启动的计算机

1. 在**设备**选项卡上，转到**可启动媒体**组，然后选择要用于数据恢复的媒体。
2. 单击**重启**。
3. 确认要重新启动使用媒体启动的计算机。

远程关闭已启动的计算机

1. 在**设备**选项卡上，转到**可启动媒体**组，然后选择要用于数据恢复的媒体。
2. 单击**关机**。
3. 确认要关闭使用媒体启动的计算机。

查看有关可启动媒体的信息

1. 在**设备**选项卡上，转到**可启动媒体**组，然后选择要用于数据恢复的媒体。
2. 单击**详细信息**、**活动**或**警告**以查看相应的信息。

远程删除可启动媒体

1. 在**设备**选项卡上，转到**可启动媒体**组，然后选择要用于数据恢复的媒体。
2. 单击**删除**，以从 安克诺斯数据保护软件 中控台中删除可启动媒体。
3. 确认要删除可启动媒体。

配置 iSCSI 设备

本节介绍如何在可启动媒体下工作时配置 Internet 小型计算机系统接口 (iSCSI) 设备。执行以下步骤后，您将能够轻松使用这些设备，就像已在本地将其连接到使用可启动媒体启动的计算机上一样。

iSCSI 目标服务器（或**目标门户**）是托管 iSCSI 设备的服务器。**iSCSI 目标**是目标服务器上的一个组件；此组件会共享设备并列出允许访问设备的 iSCSI 发起程序。**iSCSI 发起程序**是计算机上的一个组件；此组件提供计算机与 iSCSI 目标之间的交互。在使用可启动媒体启动的计算机上配置对 iSCSI 设备的访问时，需要指定设备的 iSCSI 目标门户以及目标中列出的其中一个 iSCSI 发起程序。如果目标共享多台设备，您将能够访问所有这些设备。

在基于 Linux 的可启动媒体中添加 iSCSI 设备

1. 单击**工具** > **配置 iSCSI/NDAS 设备**。
2. 单击**添加主机**。
3. 指定 iSCSI 目标门户的 IP 地址和端口，以及允许访问设备的任何 iSCSI 发起程序的名称。
4. 如果主机要求进行验证，请为其指定用户名和密码。
5. 单击**确定**。
6. 从列表中选择 iSCSI 目标，然后单击**连接**。
7. 如果在 iSCSI 目标设置中启用了 CHAP 身份验证，则系统会提示您提供凭据才能访问 iSCSI 目标。指定与 iSCSI 目标设置中相同的用户名和目标密码。单击**确定**。
8. 单击**关闭**以关闭窗口。

在基于 PE 的可启动媒体中添加 iSCSI 设备

1. 单击**工具** > **运行 iSCSI 设置**。
2. 单击**发现**选项卡。
3. 在**目标门户**下，单击**添加**，然后指定 iSCSI 目标门户的 IP 地址和端口。单击**确定**。
4. 单击**常规**选项卡，单击**更改**，然后指定允许访问设备的任何 iSCSI 发起程序的名称。
5. 单击**目标**选项卡，单击**刷新**，从列表中选择 iSCSI 目标，然后单击**连接**。单击**确定**以连接到 iSCSI 目标。
6. 如果在 iSCSI 目标设置中启用了 CHAP 身份验证，则您会看到**身份验证失败**错误。在此情况下，单击**连接**，单击**高级**，选中**启用 CHAP 登录**复选框，然后指定与 iSCSI 目标设置中相同的用户名和目标密码。单击**确定**关闭窗口，然后单击**确定**以连接到 iSCSI 目标。
7. 单击**确定**关闭窗口。

启动恢复管理器

启动恢复管理器 是驻留在硬盘驱动器上的可启动组件。通过 启动恢复管理器，可以启动可启动应急实用程序，而无需使用单独的可启动媒体。

启动恢复管理器 对移动用户尤其有用。如果出现故障，请重新启动计算机、等待出现提示**按 F11 运行 Acronis 启动恢复管理器...**，然后按 F11 键。程序将启动，您便可以执行恢复。在装有 GRUB 启动加载程序的计算机上，从启动菜单中选择 启动恢复管理器，而不是在重新启动期间按 F11 键。

在外出时，也可以使用 启动恢复管理器 进行备份。

要使用 启动恢复管理器，必须激活它。因此，启用启动时提示**按 F11 运行 Acronis 启动恢复管理器**（或者，如果使用 GRUB 启动加载程序，则将**启动恢复管理器**项目添加到 GRUB 菜单）。

注意

要在有未加密系统卷的计算机上激活 启动恢复管理器，该计算机必须有至少 100 MB 的可用空间。需要重新启动计算机的恢复操作需要额外的 100 MB。

如果有 BitLocker 加密卷的计算机至少有一个其他未加密卷，则可以在该计算机上激活 启动恢复管理器。未加密卷必须有至少 500 MB 的可用空间。对于需要重新启动计算机的恢复操作，计算机必须有额外 500 MB 可用空间。

重要事项

如果 启动恢复管理器 无法激活，则创建一键恢复备份的备份操作会失败。

激活 启动恢复管理器 将使用自身的启动代码覆盖主启动记录 (MBR)，除非使用 GRUB 启动加载程序且该加载程序已安装在 MBR 中。因此，您可能需要重新激活第三方启动加载程序（如果此类启动加载程序已安装）。

在 Linux 环境下，使用启动加载程序（如 LILO）替代 GRUB 时，请考虑在激活 启动恢复管理器 前将其安装在 Linux 根（或启动）分区启动记录，不要安装在 MBR 上。否则，在激活后重新手动配置启动加载程序。

激活 启动恢复管理器

在运行适用于 Windows 的代理程序或适用于 Linux 的代理程序的计算机上，可以在 安克诺斯数据保护软件 Web 中控台中激活 启动恢复管理器。

在 安克诺斯数据保护软件 Web 中控台中激活 启动恢复管理器

1. 选择要激活 启动恢复管理器 的计算机。
2. 单击**详细信息**。
3. 启用 **启动恢复管理器** 开关。
4. 等待软件激活 启动恢复管理器。

在没有安装代理程序的计算机上激活 启动恢复管理器

1. 从可启动媒体启动计算机。
2. 依次单击**工具** > **激活 启动恢复管理器**。
3. 等待软件激活 启动恢复管理器。

取消激活 启动恢复管理器

要停用 启动恢复管理器，请重复激活过程并选择相应的相反操作。停用操作会禁用启动时提示**按 F11 运行 Acronis 启动恢复管理器**（或 GRUB 中的菜单项目）。

如果 启动恢复管理器 没有激活，则在启动失败时需要执行以下操作之一来恢复系统：

- 从单独的可启动媒体启动计算机
- 从 PXE 服务器或 Microsoft 远程安装服务 (RIS) 使用网络启动

Acronis PXE 服务器

Acronis PXE 服务器允许通过网络启动计算机到 Acronis 可启动组件。

网络启动：

- 消除了需要技术支持人员在现场向必须启动的系统中安装可启动媒体的麻烦
- 在组操作期间，相比使用物理可启动媒体，减少了启动多台计算机所需的时间。

使用 Acronis 可启动媒体生成器将可启动组件上载到 Acronis PXE 服务器。若要上载可启动组件，请启动可启动媒体生成器，然后按照"基于 Linux 的可启动媒体"中的分步说明执行操作。

如果网络上有动态主机控制协议 (DHCP) 服务器，则可从 Acronis PXE 服务器启动多台计算机。然后，已启动的计算机的网络接口将自动获取 IP 地址。

限制：

Acronis PXE 服务器不支持 UEFI 启动加载程序。

安装 Acronis PXE 服务器

安装 Acronis PXE 服务器

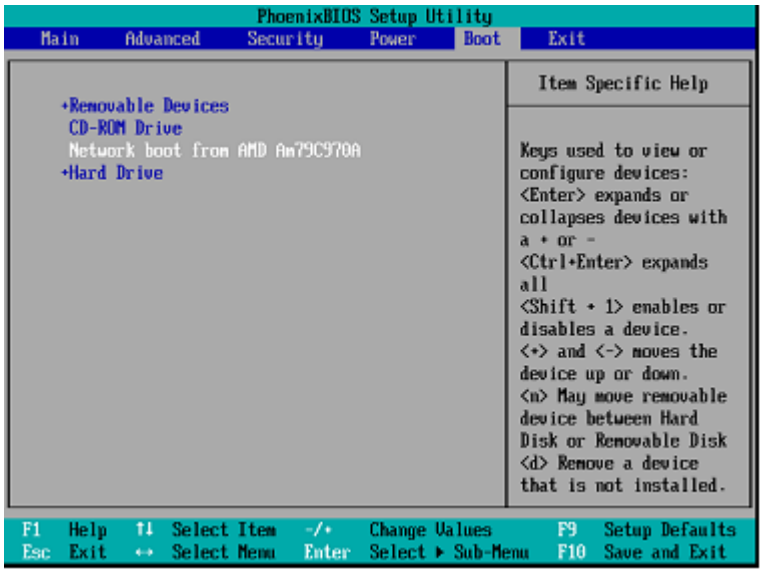
1. 以管理员身份登录，然后启动 Acronis 安克诺斯数据保护软件 安装程序。
2. [可选] 要更改安装程序的语言，请单击**设置语言**。
3. 接受许可协议和隐私声明的条款，然后单击**继续**。
4. 单击**自定义安装设置**。
5. 单击**安装内容**旁边的**更改**。
6. 勾选 **PXE 服务器**复选框。如果您不希望在此计算机上安装其他组件，请清除相应的复选框。单击**完成**以继续。
7. [可选] 更改其他安装设置。
8. 单击**安装**以继续安装过程。
9. 安装完成后，单击**关闭**。

安装之后，Acronis PXE 服务器立即作为服务运行。以后每次系统重新启动时，它将自动启动。可以采用与其他 Windows 服务相同的方式停止和启动 Acronis PXE 服务器。

设置计算机从 PXE 启动

对于裸机，只要 BIOS 支持网络启动即可。

对于硬盘上已有操作系统的计算机，必须配置 BIOS，以便网络接口卡为其第一启动设备，或至少在硬盘前启动。下面是一个合理配置 BIOS 的示例：如果未插入可启动媒体，计算机将从网络启动。



在一些版本的 BIOS 中，需要在启用网络界面卡后保存更改至 BIOS，以便在启动设备列表中显示网络界面卡。

如果硬件有多个网络界面卡，请确保将 BIOS 支持的卡插入网络电缆。

跨子网工作

要启用 Acronis PXE 服务器以便在另一子网中工作（跨交换机），请配置交换机以转送 PXE 流量。PXE 服务器 IP 地址按与 DHCP 服务器地址相同的方式，使用 IP 帮助程序逐个界面配置。有关详细信息，请参阅：https://docs.microsoft.com/en-us/troubleshoot/mem/configmgr/boot-from-pxe-server。

保护移动设备

该备份应用程序允许您将移动数据备份到云存储，然后在发生丢失或损坏时恢复备份的移动数据。请注意，备份到云存储需要帐户和云订购许可。

受支持的移动设备

可以在运行以下操作系统之一的移动设备上安装备份应用程序：

- iOS 10.3 及更高版本（iPhone、iPod 和 iPad）
- Android 5.0 及更高版本

备份内容

- 联系人
- 照片
- 视频
- 日历
- 提醒（仅限 iOS 设备）

需要知道的内容

- 您仅可以将数据备份至云存储。
- 无论何时打开应用程序，您都会看到数据更改汇总，并且可以手动启动备份。
- 默认情况下，**持续备份**功能已启用。如果该设置打开：
  - 对于 Android 7.0 或更高版本，备份应用程序会自动即时检测新数据，并将它上传到云。
  - 对于 Android 5 和 6，它会每隔三小时检查所做的更改。可以在应用程序设置中关闭持续备份。
- 在应用程序设置中，**仅使用 Wi-Fi** 选项默认处于启用状态。如果该设置打开，则备份应用程序仅在 Wi-Fi 连接可用时才会备份数据。如果 Wi-Fi 连接丢失，则备份过程不会开始。对于也要使用蜂窝连接的应用程序，请关闭此选项。
- 有两种节能方法：
  - 默认禁用的**充电时备份**功能。如果该设置打开，则备份应用程序仅在您的设备连接到电源时才会备份数据。如果在持续备份过程中断开设备与电源的连接，则备份会暂停。
  - 默认启用的**省电模式**。如果该设置打开，则备份应用程序仅在设备电池电量较高时才会备份数据。设备电池电量变低时，持续备份会暂停。该选项适用于 Android 8 或更高版本。
- 您可以从在您的帐户下注册的任意移动设备访问备份的数据。这有助于将数据从旧的移动设备传输到新的移动设备。Android 设备上的联系人和照片可以恢复到 iOS 设备上，反之亦然。还可以使用 安克诺斯数据保护软件 Web 中控台将照片、视频或联系人下载到任何设备。
- 从在您的帐户下注册的移动设备中备份的数据仅在此帐户下可用。其他任何人都无法查看或恢复您的数据。

- 在备份应用程序中，只可以恢复最新的数据版本。如果需要从特定备份版本恢复，请在平板电脑或计算机上使用 安克诺斯数据保护软件 Web 中控台。
- [仅适用于 Android 设备] 如果在备份期间存在 SD 卡，则存储在该卡上的数据也会备份。如果在恢复期间存在 SD 卡，则数据将恢复到 SD 卡上**由备份恢复**的目标文件夹，否则应用程序会请求指定要将数据恢复到的其他位置。

从哪里获取备份应用程序

1. 在移动设备上，打开浏览器并转到 https://backup.acronis.com/。
2. 使用您的帐户登录。
3. 依次单击**所有设备** > **添加**。
4. 在**移动设备**下，选择设备类型。
   您将重定向到应用程序商店或 Google Play 商店，具体取决于设备类型。
5. [仅限 iOS 设备] 单击**获取**。
6. 单击**安装**以安装备份应用程序。

如何开始备份数据

1. 打开该应用程序。
2. 使用您的帐户登录。

点击**设置**创建您的第一个备份。

1. 选择要备份的数据分类。默认情况下，选定所有分类。
2. [可选设置] 启用**加密备份**以通过加密方式保护您的备份。在此情况下，您还将需要：
   a. 输入加密密码两次。

      注意
      确保记住该密码，因为无法恢复或更改遗忘的密码。

   b. 点击**加密**。
3. 点击**备份**。
4. 允许应用程序访问个人数据。如果您拒绝访问某些数据分类，将不会备份这些数据分类。

开始备份。

如何将数据恢复到移动设备

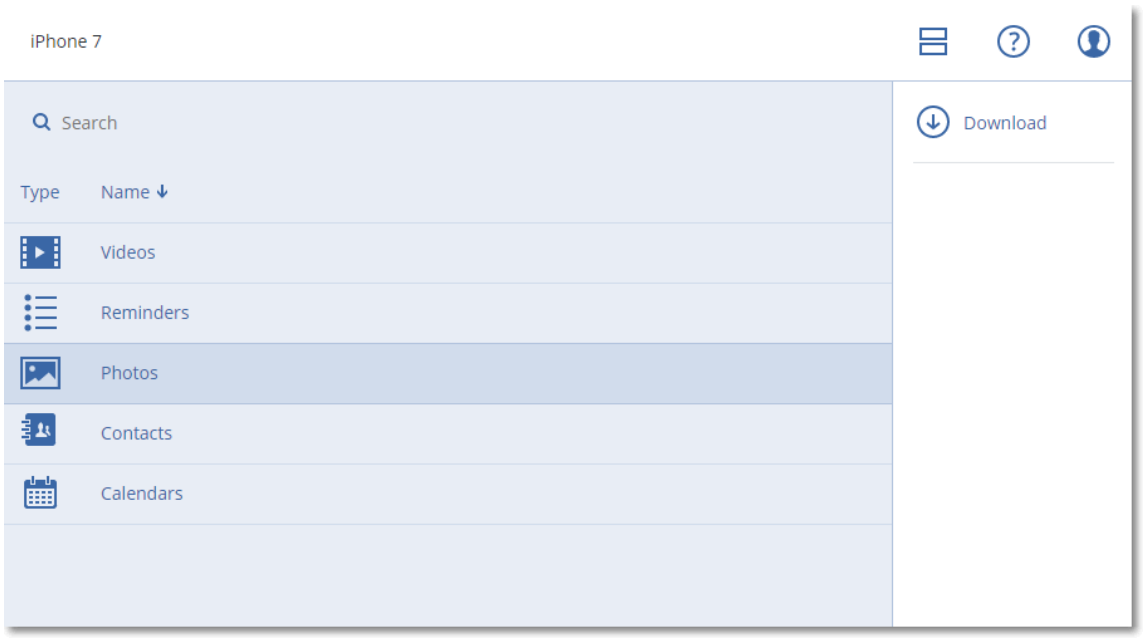
1. 打开备份应用程序。
2. 点击**浏览**。
3. 点击设备名称。
4. 请执行以下任一操作：

- 若要恢复所有备份的数据，请点击**全部恢复**。无需执行更多操作。
- 若要恢复一个或多个数据分类，请点击**选择**，然后点击所需数据分类的复选框。点击**恢复**。无需执行更多操作。
- 若要恢复属于同一数据分类的一个或多个数据项目，请点击数据分类。继续执行后续步骤。

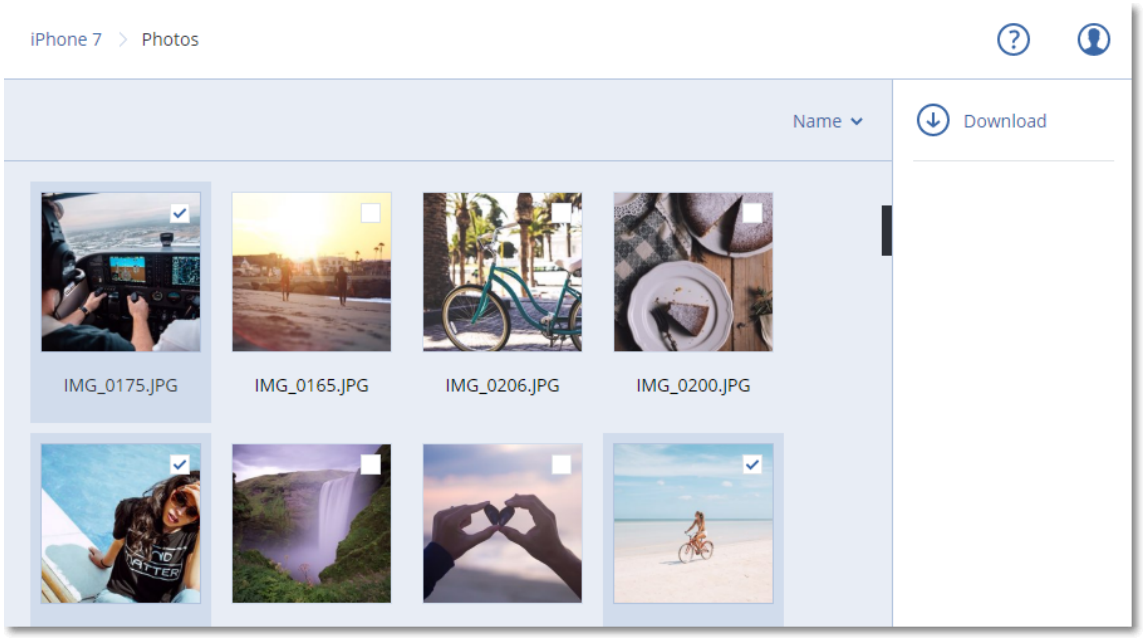
5. 请执行以下任一操作：
   - 若要恢复单个数据项目，请点击该项目。
   - 若要恢复多个数据项目，请点击**选择**，然后点击所需数据项目的复选框。
6. 点击**恢复**。

如何通过 安克诺斯数据保护软件 Web 中控台查看数据

1. 在计算机上，打开浏览器并键入 安克诺斯数据保护软件 Web 中控台 URL。
2. 使用您的帐户登录。
3. 在**所有设备**中，单击您移动设备名称下的**恢复**。
4. 请执行以下任一操作：
   - 要下载所有照片、视频、联系人、日历或提醒，请选择相应的数据分类。单击**下载**。



   - 要下载单独的照片、视频、联系人、日历或提醒，请单击相应的数据分类名称，然后选中所需数据项目的复选框。单击**下载**。



- 要预览照片或联系人，请单击相应的数据分类名称，然后单击所需的数据项目。

保护 Microsoft 应用程序

重要事项
本部分中所述的一些功能仅适用于本地部署。

保护 Microsoft SQL Server 和 Microsoft Exchange Server

有两种保护这些应用程序的方法：

- **数据库备份**
  这是与其相关联的数据库和元数据的文件级备份。数据库可以恢复到活动应用程序或恢复为文件。
- **应用程序感知备份**
  这是同样收集应用程序元数据的磁盘级备份。此元数据允许浏览和恢复应用程序数据，而无需恢复整个磁盘或卷。磁盘或卷也可作为整体进行恢复。这意味着单个解决方案和单个保护计划可用于灾难恢复和数据保护目的。

对于 Microsoft Exchange Server，您可以选择**邮箱备份**。这是通过 Exchange Web 服务协议执行的单个邮箱备份。邮箱或邮箱项目可以恢复至活动 Exchange Server 或 Microsoft 365。Microsoft Exchange Server 2010 Service Pack 1 (SP1) 和更高版本支持邮箱备份。

保护 Microsoft SharePoint

Microsoft SharePoint 服务器场由运行 SharePoint 服务的前端服务器、运行 Microsoft SQL Server 的数据库服务器和从前端服务器卸载某些 SharePoint 服务的应用程序服务器(可选)组成。某些前端和应用程序服务器可能彼此完全相同。

若要保护整个 SharePoint 服务器场，请执行以下操作：

- 使用应用程序感知备份来备份所有数据库服务器。
- 使用常用的磁盘级备份来备份所有独有前端服务器和应用程序服务器。

所有服务器的备份都应按同一个预定完成。

若要仅保护内容，可以单独备份内容数据库。

保护域控制器

运行 Active Directory 域服务的计算机可以受应用程序感知备份保护。如果域包含多个域控制器，并且您恢复其中一个域控制器，将执行非权威还原，并且在恢复后不会发生 USN 回滚。

恢复应用程序

下表总结了可用的应用程序恢复方法。

	从数据库备份	从应用程序感知备份	从磁盘备份
Microsoft SQL Server	将数据库恢复至活动 SQL Server 实例 将数据库恢复为文件	整台计算机 将数据库恢复至活动 SQL Server 实例 将数据库恢复为文件	整台计算机
Microsoft Exchange Server	将数据库恢复至活动 Exchange 将数据库恢复为文件 粒度恢复至活动 Exchange 或 Microsoft 365*	整台计算机 将数据库恢复至活动 Exchange 将数据库恢复为文件 粒度恢复至活动 Exchange 或 Microsoft 365*	整台计算机
Microsoft SharePoint 数据库服务器	将数据库恢复至活动 SQL Server 实例 将数据库恢复为文件 使用 SharePoint Explorer 进行粒度恢复	整台计算机 将数据库恢复至活动 SQL Server 实例 将数据库恢复为文件 使用 SharePoint Explorer 进行粒度恢复	整台计算机
Microsoft SharePoint 前端 Web 服务器	-	-	整台计算机
Active Directory 域服务	-	整台计算机	-

*从邮箱备份恢复也提供粒度恢复。

先决条件

在配置应用程序备份前，请确保满足下列要求。

要检查 VSS Writer 状态，请使用 `vssadmin list writers` 命令。

命令要求

对于 Microsoft SQL Server，请确保：

- 至少启动一个 Microsoft SQL Server 实例。
- 用于 VSS 的 SQL 编写器已打开。

对于 Microsoft Exchange Server，请确保：

- Microsoft Exchange 信息存储服务已启动。
- Windows PowerShell 已安装。对于 Exchange 2010 或更高版本，Windows PowerShell 版本必须至少为 2.0。
- Microsoft .NET Framework 已安装。

  对于 Exchange 2007，Microsoft .NET Framework 版本必须至少为 2.0。

  对于 Exchange 2010 或更高版本，Microsoft .NET Framework 版本必须至少为 3.5。
- 用于 VSS 的 Exchange 编写器已打开。

注意

适用于 Exchange 的代理程序需要一个临时存储空间才能运行。默认情况下，临时文件位于 `%ProgramData%\Acronis\Temp` 中。请确保 `%ProgramData%` 文件夹所在卷上的可用空间至少是 Exchange 数据库大小的 15%。或者，可以先更改临时文件的位置，然后再创建 Exchange 备份，如 https://kb.acronis.com/content/40040 中所述。

在域控制器上，请确保：

- 用于 VSS 的 Active Directory 编写器已打开。

在创建保护计划时，请确保：

- 对于物理机，卷影复制服务 (VSS) 备份选项已启用。
- 对于虚拟机，适用于虚拟机的卷影复制服务 (VSS) 备份选项已启用。

应用程序感知备份的其他要求

在创建保护计划时，请确保选择**整台计算机**进行备份。必须在保护计划中禁用**逐扇区**备份选项，否则将无法从此类备份执行应用程序数据的恢复。如果由于自动切换到**逐扇区**模式而在此模式下执行计划，那么也将无法恢复应用程序数据。

ESXi 虚拟机的要求

如果应用程序在由适用于 VMware 的代理程序备份的虚拟机上运行，请确保：

- 要备份的虚拟机满足以下 VMware 文档的文章"Windows 备份实施"中列出的应用程序一致的备份和恢复的要求：https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html
- VMware 工具已安装在计算机上，并且处于最新状态。
- 用户帐户控制 (UAC) 已在计算机上禁用。如果您不希望禁用 UAC，则必须在启用应用程序备份时提供内置域管理员 (DOMAIN\Administrator) 的凭据。

Hyper-V 虚拟机的要求

如果应用程序在由适用于 Hyper-V 的代理程序备份的虚拟机上运行，请确保：

- 来宾操作系统为 Windows Server 2008 或更改版本。
- 对于 Hyper-V 2008 R2：来宾操作系统为 Windows Server 2008/2008 R2/2012。
- 虚拟机没有动态磁盘。

- Hyper-V 主机和来宾操作系统之间存在网络连接。这需要在虚拟机内执行远程 WMI 查询。
- 用户帐户控制 (UAC) 已在计算机上禁用。如果您不希望禁用 UAC，则必须在启用应用程序备份时提供内置域管理员 (DOMAIN\Administrator) 的凭据。
- 虚拟机配置匹配以下条件：
  - Hyper-V 集成服务已安装在计算机上，并且处于最新状态。重要更新为 https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - 在虚拟机设置中，**管理** > **集成服务** > **备份(卷检查点)** 选项已启用。
  - 对于 Hyper-V 2012 及更高版本：虚拟机没有检查点。
  - 对于 Hyper-V 2012 R2 及更高版本：虚拟机具有 SCSI 控制器（检查**设置** > **硬件**）。

数据库备份

在备份数据库前，请确保满足"先决条件"中列出的要求。

按如下所述选择数据库，然后相应地指定保护计划的其他设置。

选择 SQL 数据库

SQL 数据库的备份包含数据库文件 (.mdf, .ndf)、日志文件 (.ldf) 和其他关联文件。这些文件在 SQL Writer 服务的帮助下备份。当卷影复制服务 (VSS) 请求备份或恢复时，该服务必须正在运行。

SQL 事务日志会在每次成功的备份后截断。可以在保护计划选项中禁用 SQL 日志截断。

选择 SQL 数据库

1. 单击**设备** > **Microsoft SQL**。

   软件会显示 SQL Server Always On 可用性组 (AAG)、运行 Microsoft SQL Server 的计算机、SQL Server 实例和数据库的树图。
2. 浏览到要备份的数据。

   展开树节点，或双击树图右侧列表中的项目。
3. 选择要备份的数据。您可以选择 AAG、运行 SQL Server 的计算机、SQL Server 实例或个别数据库。
   - 如果您选择 AAG，则将备份选定 AAG 中包含的所有数据库。有关备份 AAG 或单个 AAG 数据库的更多信息，请参阅"保护 Always On 可用性组 (AAG)"。
   - 如果您选择运行 SQL Server 的计算机，则将备份连接至选定计算机上运行的所有 SQL Server 实例的所有数据库。
   - 如果您选择 SQL Server 实例，则将备份连接至选定实例的所有数据库。
   - 如果您直接选择数据库，将仅备份选定的数据库。
4. 单击**保护**。如果出现提示，请提供访问 SQL Server 数据的凭据。

   如果使用 Windows 身份验证，则该帐户必须是计算机上的**备份操作员**或**管理员**组的成员和要备份的每个实例上的 **sysadmin** 角色的成员。

   如果使用 SQL Server 身份验证，则该帐户必须是要备份的每个实例上的 **sysadmin** 角色的成员。

选择 Exchange Server 数据

下表总结了可选择进行备份的 Microsoft Exchange Server 数据和备份该数据所需的最低用户权限。

Exchange 版本	数据项目	用户权限
2007	存储组	**Exchange 组织管理员**角色组的成员资格
2010/2013/2016/2019	数据库、数据库可用性组 (DAG)	**服务器管理**角色组的成员资格。

完整备份包含所有选定的 Exchange Server 数据。

增量备份包含已更改的数据库文件块、检查点文件和少量较新的日志文件(相比于相应的数据库检查点)。由于对数据库文件的更改包含在备份中,因此无需备份自上一次备份以来的所有事务日志记录。仅比检查点更新的日志需要在恢复后重演。这可使恢复更快,并确保成功的数据库备份,即使在启用了循环日志记录时也是如此。

事务日志文件会在每次成功的备份后截断。

选择 Exchange Server 数据

1. 单击**设备** > **Microsoft Exchange**。

   软件会显示 Exchange Server 数据库可用性组 (DAG)、运行 Microsoft Exchange Server 的计算机和 Exchange Server 数据库的树图。如果已按照"邮箱备份"中所述的步骤配置了用于 Exchange 的代理程序,则邮箱也会显示在此树图中。
2. 浏览到要备份的数据。

   展开树节点,或双击树图右侧列表中的项目。
3. 选择要备份的数据。
   - 如果选择 DAG,将备份每个群集数据库的一个副本。有关备份 DAG 的更多信息,请参阅"保护数据库可用性组 (DAG)"。
   - 如果您选择运行 Microsoft Exchange Server 的计算机,则将备份加载到选定计算机上运行的 Exchange Server 的所有数据库。
   - 如果您直接选择数据库,将仅备份选定的数据库。
   - 如果已按照"邮箱备份"中所述的步骤配置了用于 Exchange 的代理程序,则可以选择用于备份的邮箱。
4. 如果出现提示,请提供访问该数据的凭据。
5. 单击**保护**。

保护 Always On 可用性组 (AAG)

SQL Server 高可用性解决方案概述

Windows Server 故障转移群集 (WSFC) 功能允许您通过实例级别(故障转移群集实例，FCI) 或数据库级别(AlwaysOn 可用性组，AAG) 的冗余来配置高可用的 SQL Server。您还可以组合这两种方法。

在故障转移群集实例中，SQL 数据库位于共享存储上。只能从活动群集节点访问此存储。如果活动节点失败，则会发生故障转移，并且其他节点将成为活动节点。

在可用性组中，每个数据库副本都依赖于不同的节点。如果主副本变得不可用，则会为位于其他节点的辅助副本分配主要角色。

因此，群集本身已相当于灾难恢复解决方案。然而，可能会出现群集无法提供数据保护的情况：例如，数据库逻辑损坏，或整个群集出现故障。同时，群集解决方案无法防止有害内容更改，因为这些更改经常立即复制到所有群集节点。

受支持的群集配置

此备份软件仅支持 SQL Server 2012 或更高版本的 Always On 可用性组 (AAG)。不支持其他群集配置(如故障转移群集实例、数据库镜像和日志传送) 。

群集数据的备份和恢复需要多少代理程序?

为了成功地执行群集数据的备份和恢复，需要在 WSFC 群集的每个节点上安装适用于 SQL 的代理程序。

备份 AAG 中包含的数据库

1. 在 WSFC 群集的每个节点上安装适用于 SQL 的代理程序。

   注意
   在其中一个节点上安装该代理程序后，软件将在**设备** > **Microsoft SQL** > **数据库**下显示 AAG 及其节点。若要在剩余节点上安装适用于 SQL 的代理程序，请选择 AAG，单击**详细信息**，然后单击每个节点旁边的**安装代理程序**。

2. 如"选择 SQL 数据库或数据库集"所述，选择要备份的 AAG。
   您必须选择 AAG 本身来备份 AAG 的所有数据库。要备份一组数据库，请在 AAG 的所有节点中定义这组数据库。

   警告!
   所有节点中的数据库集必须完全相同。如果即使有一个集不同，或者没有在所有节点上定义，群集备份将无法正常工作。

3. 配置"群集备份模式"备份选项。

恢复 AAG 中包含的数据库

1. 选择要恢复的数据库，然后选择要从其恢复数据库的恢复点。

   在**设备** > **Microsoft SQL** > **数据库**下选择群集数据库，然后单击**恢复**后，软件仅显示与备份数据库选定副本的时间相对应的恢复点。

   查看群集数据库的所有恢复点的最简单方法是在"备份存储"选项卡上选择整个 AAG 的备份。AAG 备份的名称基于以下模板：<AAG 名称> - <保护计划名称>，且有一个特殊图标。
2. 若要配置恢复，请遵循"恢复 SQL 数据库"中描述的步骤，从第 5 步开始。

   软件将自动定义数据将恢复到的群集节点。节点名称将显示在**恢复至**字段中。您可以手动更改目标节点。

重要事项

在恢复过程中，不能覆盖 Always On 可用性组中包含的数据库，因为 Microsoft SQL Server 禁止这样做。在恢复之前，您需要从 AAG 中排除目标数据库。或者，只需将数据库恢复为新的非 AAG 数据库。恢复完成后，您可以重新构建原始 AAG 配置。

保护数据库可用性组 (DAG)

Exchange Server 群集概述

Exchange 群集主要为高可用性数据库提供快速的故障转移并确保无数据丢失。通常，通过拥有群集成员（群集节点）上的数据库或存储组的一份或多份副本来实现。如果托管活动数据库副本的群集节点或活动数据库副本本身出现故障，则托管被动副本的其他节点将自动接替故障节点的操作，并在最短的停机时间内提供对 Exchange 服务的访问。因此，群集本身已相当于灾难恢复解决方案。

然而，可能会出现故障转移群集解决方案无法提供数据保护的情况：例如，数据库逻辑损坏、群集中的特定数据库无副本或整个群集出现故障。同时，群集解决方案无法防止有害内容更改，因为这些更改经常立即复制到所有群集节点。

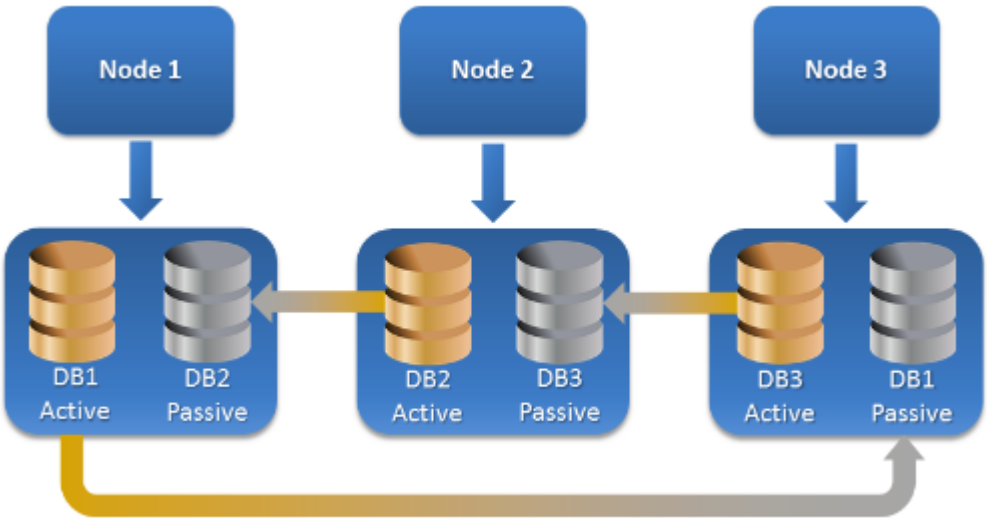
群集感知备份

使用群集感知备份时，只可以备份群集数据的一个副本。如果数据在群集中的位置发生更改（由于切换或故障转移），软件会跟踪此数据的所有重定位位置，并安全地备份。

受支持的群集配置

仅对 Exchange Server 2010 或更高版本中的数据库可用性组 (DAG) 支持群集感知备份。不支持其他群集配置，如适用于 Exchange 2007 的单一副本群集 (SCC) 和群集连续复制 (CCR)。

DAG 是一个最多可包括 16 台 Exchange 邮箱服务器的组。任何节点都可托管其他任何节点的一个邮箱数据库副本。每个节点都可托管被动和主动数据库副本。每个数据库最多可创建 16 个副本。



群集感知备份和恢复需要多少个代理程序?

为了成功备份和恢复群集数据库，需要在 Exchange 群集的每个节点上安装适用于 Exchange 的代理程序。

注意

在其中一个节点上安装该代理程序后，安克诺斯数据保护软件 Web 中控台将在**设备** > **Microsoft Exchange** > **数据库**下显示 DAG 及其节点。若要在剩余节点上安装适用于 Exchange 的代理程序，请选择 DAG，单击**详细信息**，然后单击每个节点旁边的**安装代理程序**。

备份 Exchange 群集数据

1. 创建保护计划时，按"选择 Exchange Server 数据"中所述选择 DAG。
2. 配置"群集备份模式"备份选项。
3. 请相应地指定保护计划的其他设置。

重要事项

对于群集感知备份，请确保选择 DAG 本身。如果选择 DAG 内的个别节点或数据库，将仅备份选定项目，会忽略**群集备份模式**选项。

恢复 Exchange 群集数据

1. 为要恢复的数据库选择恢复点。无法为恢复选择整个簇。

   在**设备** > **Microsoft Exchange** > **数据库** > <簇名称> > <节点名称> 下选择群集数据库的副本并单击**恢复**时，软件仅显示与备份此副本的时间相对应的恢复点。

   查看群集数据库的所有恢复点的最简单方法是在"备份存储"选项卡上选择其备份。
2. 遵循"恢复 Exchange 数据库"中所述的步骤，从第 5 步开始操作。

   软件将自动定义数据将恢复到的群集节点。节点名称将显示在**恢复至**字段中。您可以手动更改目标节点。

应用程序感知备份

应用程序感知磁盘级别备份适用于物理机、ESXi 虚拟机和 Hyper-V 虚拟机。

备份运行 Microsoft SQL Server、Microsoft Exchange Server 或 Active Directory 域服务的计算机时，请启用**应用程序备份**以对这些应用程序的数据提供额外保护。

为什么使用应用程序感知备份？

通过使用应用程序感知备份，您确保：

1. 应用程序在一致状态下备份，因此将在恢复计算机后立即可用。
2. 您可以恢复 SQL 和 Exchange 数据库、邮箱和邮箱项目，而不恢复整台计算机。
3. SQL 事务日志会在每次成功的备份后截断。可以在保护计划选项中禁用 SQL 日志截断。Exchange 事务日志仅在虚拟机上截断。如果您要在物理机上截断 Exchange 事务日志，可以启用 VSS 完整备份选项。
4. 如果域包含多个域控制器，并且您恢复其中一个域控制器，将执行非权威还原，并且在恢复后不会发生 USN 回滚。

使用应用程序感知备份需要哪些内容？

在物理机上，除了适用于 Windows 的代理程序，还必须安装适用于 SQL 的代理程序和适用于 Exchange 的代理程序。

在虚拟机上，不需要安装任何代理程序；假定该计算机由适用于 VMware 的代理程序 (Windows) 或适用于 Hyper-V 的代理程序备份。

注意

对于正在运行 Windows Server 2022 的 Hyper-V 虚拟机，在无代理程序模式下不支持应用程序感知备份 - 即，当备份由适用于 Hyper-V 的代理程序执行时。要保护这些计算机上的 Microsoft 应用程序，请在来宾操作系统中安装适用于 Windows 的代理程序。

适用于 VMware(虚拟设备) 的代理程序和适用于 VMware (Linux) 的代理程序可以创建应用程序感知备份，但无法基于这些备份恢复应用程序数据。若要从这些代理程序创建的备份中恢复应用程序数据，您需要在有权访问存储备份的位置的计算机上安装适用于 VMware (Windows) 的代理程序、适用于 SQL 的代理程序或适用于 Exchange 的代理程序。在配置应用程序数据的恢复时，请在**备份存储**选项卡上选择相应恢复点，然后在**要从中浏览的计算机**中选择此计算机。

"先决条件"(第 381 页) 和 "应用程序感知备份所需的用户权限"(第 389 页) 中列出了其他要求。

应用程序感知备份所需的用户权限

应用程序感知备份包含磁盘上存在的 VSS 感知应用程序的元数据。若要访问此元数据，代理程序需要具有下列相应权限的帐户。启用应用程序备份时，系统会提示您指定此帐户。

- 对于 SQL Server：

  如果使用 Windows 身份验证，则该帐户必须是计算机上的**备份操作员**或**管理员**组的成员和要备份的每个实例上的 **sysadmin** 角色的成员。如果使用 SQL Server 身份验证，则该帐户必须是要备份的每个实例上的 **sysadmin** 角色的成员。
- 对于 Exchange Server：

  Exchange 2007：该帐户必须是计算机上**管理员**组的成员和 **Exchange 组织管理员**角色组的成员。

  Exchange 2010 和更高版本：该帐户必须是计算机上**管理员**组的成员和**组织管理**角色组的成员。
- 对于 Active Directory：

  帐户必须是域管理员。

虚拟机的其他要求

如果应用程序在由适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序备份的虚拟机上运行，请确保用户帐户控制 (UAC) 已在计算机上禁用。如果您不希望禁用 UAC，则必须在启用应用程序备份时提供内置域管理员 (DOMAIN\Administrator) 的凭据。

对运行 Windows 的计算机的其他要求

对于所有 Windows 版本，必须禁用用户帐户控制 (UAC) 策略以允许应用程序感知备份。如果您不希望禁用 UAC 策略，则必须在启用应用程序备份时提供内置域管理员 (DOMAIN\Administrator) 的凭据。

在 Windows 中禁用 UAC 策略

1. 在注册表编辑器中，找到以下注册表项：
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. 将 **EnableLUA** 值更改为 **0**。
3. 重新启动计算机。

邮箱备份

Microsoft Exchange Server 2010 Service Pack 1 (SP1) 和更高版本支持邮箱备份。

如果在管理服务器上注册至少一个适用于 Exchange 的代理程序，则会提供邮箱备份。代理程序必须安装在与 Microsoft Exchange Server 属于相同 Active Directory 林的计算机上。

在备份邮箱之前，您必须将适用于 Exchange 的代理程序连接至运行 Microsoft Exchange Server 的**客户端访问**服务器角色 (CAS) 的计算机。在 Exchange 2016 及更高版本中，CAS 角色不可用作单独的安装选项。它作为邮箱服务器角色的一部分自动安装。如此，即可将代理程序连接到运行**邮箱角色**的任何服务器。

将适用于 Exchange 的代理程序连接至 CAS

1. 单击**设备** > **添加**。
2. 单击 **Microsoft Exchange Server**。
3. 单击 **Exchange 邮箱**。

   如果未在管理服务器上注册适用于 Exchange 的代理程序，则软件会建议您安装该代理程序。安装完成后，从步骤 1 开始重复执行此过程。
4. [可选] 如果在管理服务器上已注册多个适用于 Exchange 的代理程序，则单击**代理程序**，然后更改将执行备份的代理程序。
5. 在**客户端访问服务器**中，指定启用了 Microsoft Exchange Server 的**客户端访问**角色的计算机的完全限定域名 (FQDN)。

   在 Exchange 2016 及更高版本中，客户端访问服务作为邮箱服务器角色的一部分自动安装。如此，即可指定运行**邮箱角色**的任何服务器。我们在本节下文中将此服务器称为 CAS。
6. 在**身份验证类型**中，选择 CAS 使用的身份验证类型。可以选择 **Kerberos**(默认) 或**基本**。
7. [仅适用于基本身份验证] 选择要使用的协议。可以选择 **HTTPS**(默认) 或 **HTTP**。
8. [仅适用于采用 HTTPS 协议的基本身份验证] 如果 CAS 使用已从证书颁发机构获得的 SSL 证书，并且您希望软件在连接至 CAS 时检查该证书，请选中**检查 SSL 证书**复选框。否则，请跳过此步骤。
9. 提供将用于访问 CAS 的帐户的凭据。此帐户的要求在"所需用户权限"中列出。
10. 单击**添加**。

结果，邮箱会显示在**设备** > **Microsoft Exchange** > **邮箱**下方。

选择 Exchange Server 邮箱

按如下所述选择邮箱，然后相应地指定保护计划的其他设置。

选择 Exchange 邮箱

1. 单击**设备** > **Microsoft Exchange**。

   软件会显示 Exchange 数据库和邮箱的树图。
2. 单击**邮箱**，然后选择要备份的邮箱。
3. 单击**备份**。

所需用户权限

要访问邮箱，用于 Exchange 的代理程序需要具有相应权限的帐户。配置邮箱的各种操作时，系统会提示您指定此帐户。

拥有**组织管理**角色组中的帐户成员资格即可访问任何邮箱，包括将在以后创建的邮箱。

所需最低用户权限如下：

- 该帐户必须是**服务器管理**和**收件人管理**角色组的成员。
- 该帐户必须为代理程序将访问其邮箱的所有用户或用户组启用 **ApplicationImpersonation** 管理角色。

有关配置 **ApplicationImpersonation** 管理角色的信息，请参阅以下 Microsoft 知识库文章：https://msdn.microsoft.com/en-us/library/office/dn722376.aspx。

恢复 SQL 数据库

本部分介绍如何从数据库备份和应用程序感知备份恢复。

可以将 SQL 数据库恢复到 SQL Server 实例，前提是运行该实例的计算机上安装了适用于 SQL 的代理程序。

如果使用 Windows 身份验证，需要提供计算机上的**备份操作员**或**管理员**组和目标实例上的 **sysadmin** 角色的成员帐户的凭据。如果使用 SQL Server 身份验证，需要提供目标实例上的 **sysadmin** 角色的成员帐户的凭据。

此外，您可以将数据库恢复为文件。如果您需要提取数据以供第三方工具进行数据挖掘、审核或进一步处理，这一点非常有用。您可以将 SQL 数据库文件附加到 SQL Server 实例，如"附加 SQL Server 数据库"中所述。

如果您仅使用适用于 VMware (Windows) 的代理程序，则将数据库恢复为文件是唯一可用的恢复方法。无法使用适用于 VMware(虚拟设备) 的代理程序恢复数据库。

系统数据库的恢复方式与用户数据库基本相同。"恢复系统数据库"中介绍了系统数据库恢复的特性。

将 SQL 数据库恢复至 SQL Server 实例

1. 请执行以下任一操作：
   - 从应用程序感知备份恢复时，在**设备**下，选择原先包含要恢复的数据的计算机。
   - 从数据库备份恢复时，单击**设备** > **Microsoft SQL**，然后选择要恢复的数据库。
2. 单击**恢复**。
3. 选择恢复点。请注意，恢复点按位置过滤。

   如果计算机处于脱机状态，将不显示恢复点。请执行以下任一操作：
   - [仅从应用程序感知备份恢复时]如果备份位置是云或共享存储(即其他代理程序可以访问它)，单击**选择计算机**，选择具有适用于 SQL 的代理程序并处于联机状态的计算机，然后选择恢复点。
   - 在备份存储选项卡上选择一个恢复点。

   上述任一操作中的浏览所选择的计算机将变为 SQL 数据库恢复的目标计算机。
4. 请执行以下任一操作：
   - 从应用程序感知备份恢复时，单击**恢复** > **SQL 数据库**，选择要恢复的数据库，然后单击**恢复**。
   - 从数据库备份恢复时，单击**恢复** > **将数据库恢复至实例**。
5. 默认情况下，数据库将恢复至原始数据库。如果原始数据库不存在，将重新创建它。您可以选择另一个 SQL Server 实例(在同一台计算机上运行) 来将数据库恢复至该实例。

   若要将数据库作为不同的数据库恢复到同一个实例：

   a. 单击数据库名称。

   b. 在**恢复至**中，选择**新数据库**。

c. 指定新数据库名称。

d. 指定新数据库路径和日志路径。您指定的文件夹不得包含原始数据库和日志文件。

6. [可选] [不适用于作为新数据库恢复到其原始实例的数据库] 要在恢复后更改数据库状态，请单击数据库名称，然后选择以下状态之一：

   - **可以使用 (RESTORE WITH RECOVERY)**(默认)

     恢复完成后，将可以使用数据库。用户将具有对数据库的完全访问权限。软件将回滚事务日志中存储的已恢复数据库的所有未提交事务。您将无法从本机 Microsoft SQL 备份中恢复其他事务日志。

   - **非运行 (RESTORE WITH NORECOVERY)**

     恢复完成后，数据库将处于非运行状态。用户不具有对数据库的访问权限。软件将保留已恢复数据库的所有未提交事务。您将无法从本机 Microsoft SQL 备份中恢复其他事务日志，需要访问必要的恢复点。

   - **只读 (RESTORE WITH STANDBY)**

     恢复完成后，用户将具有对数据库的只读权限。软件将撤消任何未提交事务。但是，它将撤消操作保存在临时备用文件中，以便可以还原恢复效果。

     此值主要用于在出现 SQL Server 错误时检测时间点。

7. 单击**开始恢复**。

恢复进度显示在**活动**选项卡上。

将 SQL 数据库恢复为文件

1. 请执行以下任一操作：
   - 从应用程序感知备份恢复时，在**设备**下，选择原先包含要恢复的数据的计算机。
   - 从数据库备份恢复时，单击**设备** > **Microsoft SQL**，然后选择要恢复的数据库。
2. 单击**恢复**。
3. 选择恢复点。请注意，恢复点按位置过滤。

   如果计算机处于脱机状态，将不显示恢复点。请执行以下任一操作：
   - [仅从应用程序感知备份恢复时] 如果备份位置是云或共享存储(即其他代理程序可以访问它)，单击**选择计算机**，选择具有适用于 SQL 的代理程序或适用于 VMware 的代理程序并处于联机状态的计算机，然后选择恢复点。
   - 在备份存储选项卡上选择一个恢复点。

   上述任一操作中的浏览所选择的计算机将变为 SQL 数据库恢复的目标计算机。
4. 请执行以下任一操作：
   - 从应用程序感知备份恢复时，单击**恢复** > **SQL 数据库**，选择要恢复的数据库，然后单击**恢复为文件**。
   - 从数据库备份恢复时，单击**恢复** > **将数据库恢复为文件**。
5. 单击**浏览**，然后选择要将文件保存到的本地或网络文件夹。
6. 单击**开始恢复**。

恢复进度显示在**活动**选项卡上。

恢复系统数据库

实例的所有系统数据库都同时恢复。当恢复系统数据库时，软件将在单用户模式中自动重新启动目标实例。在恢复完成后，软件将重新启动实例并恢复其他数据库(如有)。

恢复系统数据库时应注意的其他事项：

- 系统数据库只能恢复至与原始实例版本相同的实例。
- 系统数据库始终在"可以使用"状态下进行恢复。

恢复 master 数据库

系统数据库包括**主**数据库。**主**数据库会记录有关实例的所有数据库的信息。因此，备份中的**主**数据库包含有关备份时实例中存在的数据库的信息。在恢复**主**数据库后，可能需要执行以下操作：

- 在成备份后显示在实例中的数据库对于该实例不可见。若要将这些数据库转回生产，请通过使用 SQL Server Management Studio 将它们手动附加到实例。
- 在完成备份后删除的数据库将在实例中显示为离线。可使用 SQL Server Management Studio 删除这些数据库。

连接 SQL Server 数据库

本部分介绍如何使用 SQL Server Management Studio 连接 SQL Server 中的数据库。一次只能连接一个数据库。

连接数据库需要任何以下权限：**创建数据库**、**创建任何数据库**或**修改任何数据库**。通常，这些权限已授予给实例的 **sysadmin** 角色。

连接数据库

1. 运行 Microsoft SQL Server Management Studio。
2. 连接至所需的 SQL Server 实例，然后展开该实例。
3. 右键单击**数据库**，然后单击**附加**。
4. 单击**添加**。
5. 在**定位数据库文件**对话框中，查找并选择数据库的 .mdf 文件。
6. 在**数据库详细信息**部分，确保找到了其余数据库文件(.ndf 和 .ldf 文件)。

   详细信息。对于以下情况，可能无法自动找到 SQL Server 数据库文件：
   - 它们不在默认位置，或者它们与主数据库文件 (.mdf) 不在同一文件夹下。解决方案：在**当前文件路径**列中，手动指定所需文件的路径。
   - 您恢复了构成数据库的部分文件。解决方案：从备份中恢复缺少的 SQL Server 数据库文件。
7. 找到所有文件后，单击**确定**。

恢复 Exchange 数据库

本部分介绍如何从数据库备份和应用程序感知备份恢复。

您可以将 Exchange Server 数据恢复至活动 Exchange Server。这可以是原始 Exchange Server 或在具有相同完全限定域名 (FQDN) 的计算机上所运行相同版本的 Exchange Server。适用于 Exchange 的代理程序必须安装在目标计算机上。

下表总结了可选择进行恢复的 Exchange Server 数据和恢复该数据所需的最低用户权限。

Exchange 版本	数据项目	用户权限
2007	存储组	**Exchange 组织管理员**角色组的成员资格。
2010/2013/2016/2019	数据库	**服务器管理**角色组的成员资格。

此外，您可以将数据库（存储组）恢复为文件。数据库文件以及事务日志文件将从备份提取到您指定的文件夹。如果您需要提取数据以进行审核或使用第三方工具进一步处理，或当恢复因某种原因失败并且您要寻找工作区来手动加载数据库时，这非常有用。

如果您仅使用适用于 VMware (Windows) 的代理程序，则将数据库恢复为文件是唯一可用的恢复方法。无法使用适用于 VMware（虚拟设备）的代理程序恢复数据库。

在下面的过程中，我们将数据库和存储组均称为“数据库”。

将 Exchange 数据库恢复至活动 Exchange Server

1. 请执行以下任一操作：
   - 从应用程序感知备份恢复时，在**设备**下，选择原先包含要恢复的数据的计算机。
   - 从数据库备份恢复时，单击**设备** > **Microsoft Exchange** > **数据库**，然后选择要恢复的数据库。
2. 单击**恢复**。
3. 选择恢复点。请注意，恢复点按位置过滤。

   如果计算机处于脱机状态，将不显示恢复点。请执行以下任一操作：
   - [仅从应用程序感知备份恢复时]如果备份位置是云或共享存储（即其他代理程序可以访问它），单击**选择计算机**，选择具有适用于 Exchange 的代理程序并处于联机状态的计算机，然后选择恢复点。
   - 在备份存储选项卡上选择一个恢复点。

   在上述任一操作中选择进行浏览的计算机变为 Exchange 数据恢复的目标计算机。
4. 请执行以下任一操作：
   - 从应用程序感知备份恢复时，单击**恢复** > **Exchange 数据库**，选择要恢复的数据库，然后单击**恢复**。
   - 从数据库备份恢复时，单击**恢复** > **将数据库恢复至 Exchange Server**。
5. 默认情况下，数据库将恢复至原始数据库。如果原始数据库不存在，将重新创建它。

   若要将数据库恢复为不同的数据库，请执行以下操作：
   a. 单击数据库名称。
   b. 在**恢复至**中，选择**新数据库**。
   c. 指定新数据库名称。

d. 指定新数据库路径和日志路径。您指定的文件夹不得包含原始数据库和日志文件。

6. 单击**开始恢复**。

恢复进度显示在**活动**选项卡上。

将 Exchange 数据库恢复为文件

1. 请执行以下任一操作：
   - 从应用程序感知备份恢复时，在**设备**下，选择原先包含要恢复的数据的计算机。
   - 从数据库备份恢复时，单击**设备** > **Microsoft Exchange** > **数据库**，然后选择要恢复的数据库。
2. 单击**恢复**。
3. 选择恢复点。请注意，恢复点按位置过滤。

   如果计算机处于脱机状态，将不显示恢复点。请执行以下任一操作：
   - [仅在从应用程序感知备份恢复时] 如果备份位置是云或共享存储（即其他代理程序可以访问它），单击**选择计算机**，选择具有适用于 Exchange 的代理程序或适用于 VMware 的代理程序并处于联机状态的计算机，然后选择恢复点。
   - 在备份存储选项卡上选择一个恢复点。

   在上述任一操作中选择进行浏览的计算机变为 Exchange 数据恢复的目标计算机。
4. 请执行以下任一操作：
   - 从应用程序感知备份恢复时，单击**恢复** > **Exchange 数据库**，选择要恢复的数据库，然后单击**恢复为文件**。
   - 从数据库备份恢复时，单击**恢复** > **将数据库恢复为文件**。
5. 单击**浏览**，然后选择要将文件保存到的本地或网络文件夹。
6. 单击**开始恢复**。

恢复进度显示在**活动**选项卡上。

加载 Exchange Server 数据库

在恢复数据库文件之后，您可以通过加载数据库使它们联机。可使用 Exchange Management 控制台、Exchange 系统管理器或 Exchange 管理外壳执行加载。

所恢复的数据库将处于“异常关闭”状态。如果已将处于“异常关闭”状态的数据库恢复至其原始位置（即 Active Directory 中存在有关原始数据库的信息），系统可以加载它。当将某个数据库恢复至备用位置（如新数据库或作为恢复数据库）时，直到使用 `Eseutil /r <Enn>` 命令使该数据库处于“干净关闭”状态时才能加载它。`<Enn>` 将为需要在其中应用事务日志文件的数据库（或包含该数据库的存储组）指定日志文件前缀。

必须已给用于连接数据库的帐户委派 Exchange Server 管理员角色或目标服务器的本地管理员组。

有关如何加载数据库的详细信息，请参阅以下文章：

- Exchange 2010 或更高版本：http://technet.microsoft.com/zh-cn/library/aa998871.aspx
- Exchange 2007：http://technet.microsoft.com/zh-cn/library/aa998871(v=EXCHG.80).aspx

恢复 Exchange 邮箱和邮箱项目

本部分介绍如何从数据库备份、应用程序感知备份和邮箱备份恢复 Exchange 邮箱和邮箱项目。邮箱或邮箱项目可以恢复至活动 Exchange Server 或 Microsoft 365。

可以恢复以下项目：

- 邮箱(存档邮箱除外)
- 公用文件夹

> **注意**
> 仅可在数据库备份中使用。请参阅 "选择 Exchange Server 数据"(第 384 页)

- 公用文件夹项目
- 电子邮件文件夹
- 电子邮件
- 日历事件
- 任务
- 联系人
- 日记条目
- 便笺

可以使用搜索功能查找项目。

恢复至 Exchange Server

可以向 Microsoft Exchange Server 2010 Service Pack 1 (SP1) 和更高版本执行粒度恢复。源备份可能包含任何受支持 Exchange 版本的数据库或邮箱。

粒度恢复可以由适用于 Exchange 的代理程序或适用于 VMware 的代理程序 (Windows) 执行。目标 Exchange Server 和运行代理程序的计算机必须属于相同的 Active Directory 林。

当邮箱恢复为现有邮箱时，将覆盖带有匹配 ID 的现有项目。

恢复邮箱项目不会覆盖任何内容。而是会在目标文件夹中重新创建邮箱项目的完整路径。

用户帐户的要求

要从备份恢复的邮箱必须在 Active Directory 中具有关联的用户帐户。

用户邮箱及其内容仅在*已启用*其相关联的用户帐户时才能恢复。共享、房间和设备邮箱仅在*已禁用*其相关联的用户帐户时才能恢复。

在恢复期间，将跳过不满足上述条件的邮箱。

如果跳过某些邮箱，恢复将会成功但出现警告。如果跳过所有邮箱，恢复将会失败。

恢复至 Microsoft 365

可以从 Microsoft Exchange Server 2010 及更高版本的备份执行恢复。

当邮箱恢复为现有 Microsoft 365 邮箱时，现有项目保持不变，并且恢复的项目会置于它们旁边。

当恢复单个邮箱时，需要选择目标 Microsoft 365 邮箱。通过一个恢复操作恢复多个邮箱时，软件会尝试将每个邮箱都恢复为具有相同名称的用户的邮箱。如果找不到该用户，会跳过该邮箱。如果跳过某些邮箱，恢复会成功但出现警告。如果跳过所有邮箱，恢复将会失败。

有关恢复至 Microsoft 365 的详细信息，请参阅 "保护 Microsoft 365 邮箱"(第 402 页)。

恢复邮箱

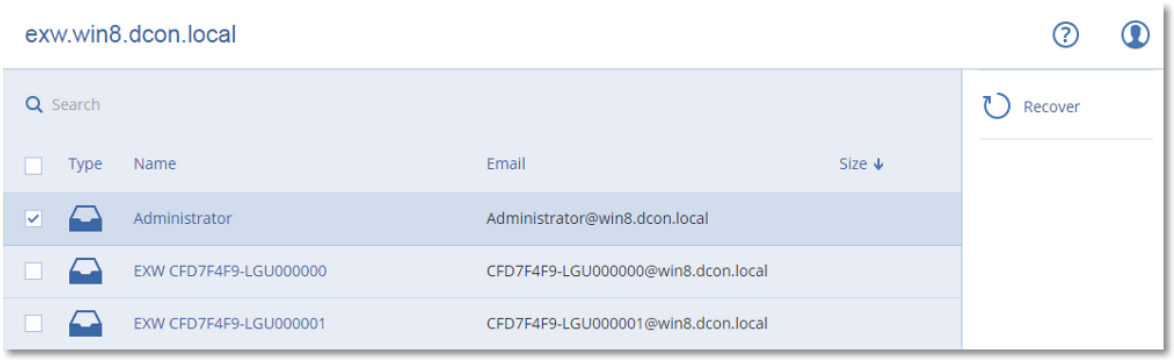
从应用程序感知备份或数据库备份恢复邮箱

1. [仅当从数据库备份恢复至 Microsoft 365 时] 如果适用于 Office 365 的代理程序未安装在运行 Exchange Server 且已备份的计算机上，请执行以下任一操作：
   - 如果贵组织中没有适用于 Office 365 的代理程序，请在已备份的计算机(或安装相同版本 Microsoft Exchange Server 的其他计算机)上安装适用于 Office 365 的代理程序。
   - 如果贵组织中已有适用于 Office 365 的代理程序，请将库从已备份的计算机(或从安装相同版本 Microsoft Exchange Server 的其他计算机)复制到安装有适用于 Office 365 的代理程序的计算机，如“复制 Microsoft Exchange 库”中所述。
2. 请执行以下任一操作：
   - 从应用程序感知备份恢复时：在**设备**下，选择原先包含要恢复的数据的计算机。
   - 从数据库备份恢复时，依次单击**设备** > **Microsoft Exchange** > **数据库**，然后选择原先包含要恢复的数据的数据库。
3. 单击**恢复**。
4. 选择恢复点。请注意，恢复点按位置过滤。

   如果计算机处于脱机状态，将不显示恢复点。使用其他方法恢复：
   - [仅在从应用程序感知备份恢复时] 如果备份位置是云或共享存储(即其他代理程序可以访问它)，单击**选择计算机**，选择具有适用于 Exchange 的代理程序或适用于 VMware 的代理程序并处于联机状态的计算机，然后选择恢复点。
   - 在备份存储选项卡上选择一个恢复点。

   在上述一项操作中选择用于浏览的计算机(而非处于脱机状态的初始计算机)将执行恢复。
5. 依次单击**恢复** > **Exchange 邮箱**。
6. 选择要恢复的邮箱。

   您可以按名称搜索邮箱。不支持通配符。



7. 单击**恢复**。
8. [仅在恢复至 Microsoft 365 时]:
   a. 在**恢复至**中，选择 **Microsoft Office 365**。
   b. [如果在步骤 6 中仅选择了一个邮箱] 在**目标邮箱**中，指定目标邮箱。
   c. 单击**开始恢复**。

   无需再执行此过程的其他步骤。
9. 单击**带有 Microsoft Exchange Server 的目标计算机**以选择或更改目标计算机。此步骤允许恢复至不运行适用于 Exchange 的代理程序的计算机。

   指定已启用**客户端访问**角色(在 Microsoft Exchange Server 2010/2013 中)或**邮箱角色**(在 Microsoft Exchange Server 2016 或更高版本中)的计算机的完全限定域名 (FQDN)。该计算机必须与执行恢复的计算机属于相同的 Active Directory 林。

   如果出现提示，请提供将用于访问计算机的帐户的凭据。此帐户的要求在 "所需用户权限"(第 390 页) 中列出。
10. [可选] 单击**用于重新创建任何缺少的邮箱的数据库**来更改自动选择的数据库。
11. 单击**开始恢复**。

恢复进度显示在**活动**选项卡上。

从邮箱备份恢复邮箱

1. 单击**设备** > **Microsoft Exchange** > **邮箱**。
2. 选择要恢复的邮箱，然后单击**恢复**。

   您可以按名称搜索邮箱。不支持通配符。

   如果邮箱已删除，请在备份存储选项卡上将它选中，然后单击**显示备份**。
3. 选择恢复点。请注意，恢复点按位置过滤。
4. 依次单击**恢复** > **邮箱**。
5. 执行上述过程中的步骤 8 至 11。

恢复邮箱项目

从应用程序感知备份或数据库备份恢复邮箱项目

1. [仅当从数据库备份恢复至 Microsoft 365 时] 如果适用于 Office 365 的代理程序未安装在运行 Exchange Server 且已备份的计算机上，请执行以下任一操作：
   - 如果贵组织中没有适用于 Office 365 的代理程序，请在已备份的计算机(或安装相同版本 Microsoft Exchange Server 的其他计算机)上安装适用于 Office 365 的代理程序。

- 如果贵组织中已有适用于 Office 365 的代理程序，请将库从已备份的计算机（或从安装相同版本 Microsoft Exchange Server 的其他计算机）复制到安装有适用于 Office 365 的代理程序的计算机，如“复制 Microsoft Exchange 库”中所述。

2. 请执行以下任一操作：
   - 从应用程序感知备份恢复时：在**设备**下，选择原先包含要恢复的数据的计算机。
   - 从数据库备份恢复时，依次单击**设备** > **Microsoft Exchange** > **数据库**，然后选择原先包含要恢复的数据的数据库。
3. 单击**恢复**。
4. 选择恢复点。请注意，恢复点按位置过滤。

   如果计算机处于脱机状态，将不显示恢复点。使用其他方法恢复：
   - [仅在从应用程序感知备份恢复时] 如果备份位置是云或共享存储（即其他代理程序可以访问它），单击**选择计算机**，选择具有适用于 Exchange 的代理程序或适用于 VMware 的代理程序并处于联机状态的计算机，然后选择恢复点。
   - 在备份存储选项卡上选择一个恢复点。

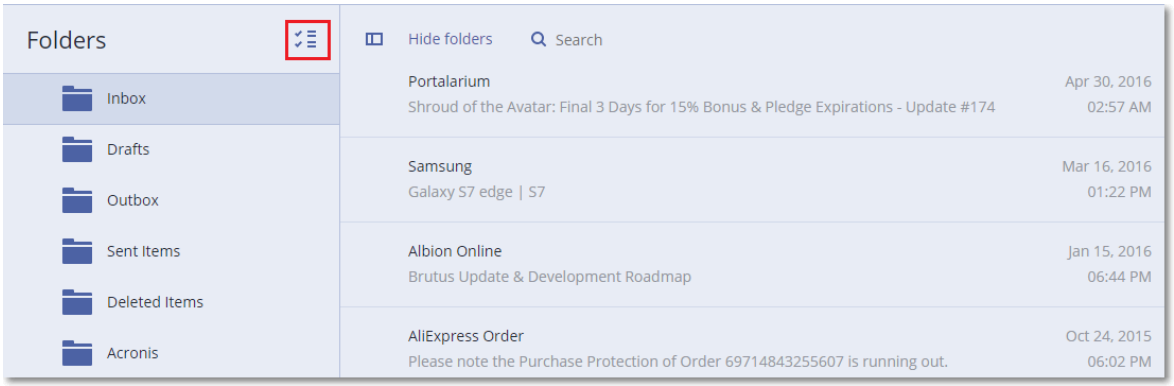
   在上述一项操作中选择用于浏览的计算机（而非处于脱机状态的初始计算机）将执行恢复。
5. 依次单击**恢复** > **Exchange 邮箱**。
6. 单击原先包含要恢复的项目的邮箱。
7. 选择要恢复的项目。

   提供以下搜索选项。不支持通配符。
   - 对于电子邮件：按主题、发件人、收件人和日期搜索。
   - 对于事件：按标题和日期搜索。
   - 对于任务：按主题和日期搜索。
   - 对于联系人：按名称、电子邮件地址和电话号码搜索。

   当选择电子邮件时，您可以单击**显示内容**来查看其内容，包括附件。

   注意
   单击附加的文件的名称可下载它。

   若要能够选择文件夹，请单击恢复文件夹图标。



8. 单击**恢复**。
9. 要恢复至 Microsoft 365，请在**恢复至**中，选择 **Microsoft Office 365**。

   若要恢复至 Exchange Server，请保留**恢复至**中的默认 **Microsoft Exchange** 值。

10. [仅在恢复至 Exchange Server 时] 单击**带有 Microsoft Exchange Server 的目标计算机**以选择或更改目标计算机。此步骤允许恢复至不运行适用于 Exchange 的代理程序的计算机。

    指定已启用**客户端访问**角色(在 Microsoft Exchange Server 2010/2013 中)或**邮箱角色**(在 Microsoft Exchange Server 2016 或更高版本中)的计算机的完全限定域名 (FQDN)。该计算机必须与执行恢复的计算机属于相同的 Active Directory 林。

    如果出现提示,请提供将用于访问计算机的帐户的凭据。此帐户的要求在 "所需用户权限"(第 390 页)中列出。
11. 在**目标邮箱**中,查看、更改或指定目标邮箱。

    默认情况下,选择原始邮箱。如果此邮箱不存在或者选择了非原始目标计算机,必须指定目标邮箱。
12. [仅在恢复电子邮件时] 在**目标文件夹**中,查看或更改目标邮箱中的目标文件夹。默认情况下,**恢复项目**文件夹处于选中状态。由于 Microsoft Exchange 的限制,活动、任务、便笺和联系人都会恢复到其原始位置,而不论是否指定任何不同的**目标文件夹**。
13. 单击**开始恢复**。

恢复进度显示在**活动**选项卡上。

从邮箱备份恢复邮箱项目

1. 单击**设备** > **Microsoft Exchange** > **邮箱**。
2. 选择原先包含要恢复的项目的邮箱,然后单击**恢复**。

    您可以按名称搜索邮箱。不支持通配符。

    如果邮箱已删除,请在备份存储选项卡上将它选中,然后单击**显示备份**。
3. 选择恢复点。请注意,恢复点按位置过滤。
4. 依次单击**恢复** > **电子邮件**。
5. 选择要恢复的项目。

    提供以下搜索选项。不支持通配符。

    - 对于电子邮件:按主题、发件人、收件人和日期搜索。
    - 对于事件:按标题和日期搜索。
    - 对于任务:按主题和日期搜索。
    - 对于联系人:按名称、电子邮件地址和电话号码搜索。

    当选择电子邮件时,您可以单击**显示内容**来查看其内容,包括附件。

    注意
    单击附加的文件的名称可下载它。

    当选择电子邮件时,您可以单击**作为电子邮件发送**来将邮件发送到电子邮件地址。从管理员帐户的电子邮件地址发送邮件。

    为了能够选择文件夹,请单击"恢复文件夹"图标: 
6. 单击**恢复**。
7. 执行上述过程中的步骤 9 至 13。

复制 Microsoft Exchange Server 库

当将 Exchange 邮箱或邮箱项目恢复至 Microsoft 365 时，可能需要将以下库从已备份的计算机(或从装有相同 Microsoft Exchange Server 版本的其他计算机)复制到装有适用于 Office 365 的代理程序的计算机。

根据已备份的 Microsoft Exchange Server 版本，复制以下文件。

Microsoft Exchange Server 版本	库	默认位置
Microsoft Exchange Server 2010	ese.dll esebcli2.dll store.exe	%ProgramFiles%\Microsoft\Exchange Server\V14\bin
Microsoft Exchange Server 2013	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll	%WINDIR%\system32
Microsoft Exchange Server 2016, 2019	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll msvcp110.dll	%WINDIR%\system32

库应放置于 **%ProgramData%\Acronis\ese** 文件夹中。如果此文件夹不存在，请手动创建它。

更改 SQL Server 或 Exchange Server 访问凭据

您可以更改 SQL Server 或 Exchange Server 的访问凭据，而无需重新安装代理程序。

更改 SQL Server 或 Exchange Server 访问凭据

1. 单击**设备**，然后单击 **Microsoft SQL** 或 **Microsoft Exchange**。
2. 选择要更改访问凭据的 AlwaysOn 可用性组、数据库可用性组、SQL Server 实例或 Exchange Server。
3. 单击**指定凭据**。
4. 指定新的访问凭据，然后单击**确定**。

更改用于邮箱备份的 Exchange Server 访问凭据

1. 依次单击**设备** > **Microsoft Exchange**，然后展开**邮箱**。
2. 选择要更改其访问凭据的 Exchange Server。
3. 单击**设置**。
4. 在 **Exchange 管理员帐户**下，指定新的访问凭据，然后单击**保存**。

保护 Microsoft 365 邮箱

重要事项

本部分适用于 Acronis 安克诺斯数据保护软件 的本地部署。如果使用的是云部署，请参阅 https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-microsoft-365-data.html。

有关许可选项的详细信息，请参阅 Acronis Cyber Backup for Microsoft 365 许可。

为什么要备份 Microsoft 365 邮箱？

即使 Microsoft 365 是云服务，常规备份也会提供额外一层保护，以免出现用户错误和有意的恶意操作。即使在 Microsoft 365 保留期到期后，也可以从备份中恢复已删除的项目。此外，还可以应法规遵从性要求保留 Microsoft 365 邮箱的本地副本。

恢复

可从邮箱备份中恢复以下项目：

- 邮箱
- 电子邮件文件夹
- 电子邮件
- 日历事件
- 任务
- 联系人
- 日记条目
- 便笺

可以使用搜索功能查找项目。

可以对 Microsoft 365 或活动的 Exchange Server 执行恢复。

当邮箱恢复为现有 Microsoft 365 邮箱时，将覆盖 ID 匹配的现有项。当邮箱恢复为现有 Exchange Server 邮箱时，现有项目将保持不变。恢复项目将置于它们的旁边。

恢复邮箱项目不会覆盖任何内容。而是会在目标文件夹中重新创建邮箱项目的完整路径。

限制

- 将保护计划应用到 500 多个邮箱可能导致备份性能下降。若要保护大量邮箱，请创建多个保护计划，并将它们预定在不同的时间运行。
- 存档邮箱(**就位存档**)无法备份。
- 邮箱备份仅包括对用户可见的文件夹。邮箱备份中不包括**可恢复项目**文件夹及其子文件夹(**删除**、**版本**、**清除**、**审核**、**发现保留**、**日历日志记录**)。

- 无法恢复到新的 Microsoft 365 邮箱。必须先手动创建新的 Microsoft 365 用户，然后才能将各项恢复到此用户的邮箱。
- 不支持恢复到其他 Microsoft 365 组织。
- Microsoft 365 支持的一些项目类型或属性可能不受 Exchange Server 支持。在恢复到 Exchange Server 期间将跳过它们。

添加 Microsoft 365 组织

要添加 Microsoft 组织，您需要知道应用程序 ID、应用程序密码和 Microsoft 365 租户 ID。有关如何查找这些文件的详细信息，请参阅获取应用程序 ID 和应用程序秘钥。

添加 Microsoft 365 组织

1. 在连接到 Internet 的 Windows 计算机上安装适用于 Office 365 的代理程序。组织中必须仅有一个适用于 Office 365 的代理程序。
2. 在 安克诺斯数据保护软件 Web 中控台中，单击 **Microsoft Office 365**。
3. 在打开的窗口中，输入应用程序 ID、应用程序秘钥和 Microsoft 365 租户 ID。
4. 单击**登录**。

结果，贵组织的数据项目会显示在 安克诺斯数据保护软件 Web 中控台中的 **Microsoft Office 365** 选项卡上。

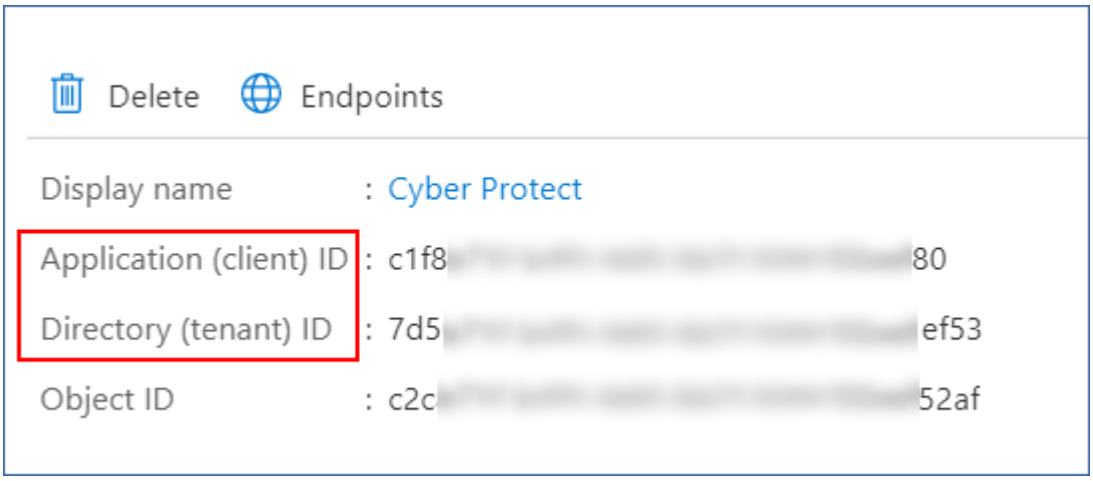
获取应用程序 ID 和应用程序秘钥

要使用 Microsoft 365 的新式身份验证，您需要在 Azure Active Directory 中创建自定义应用程序并授予其特定的 API 权限。因此，您将获得在 Web 中控台中输入所需的**应用程序 ID**、**应用程序密钥**和**目录(租户)ID**。

在 Azure Active Directory 中创建应用程序

1. 以管理员身份登录到 Azure 门户。
2. 导航到o **Azure Active Directory** > **应用程序注册**，然后单击**新注册**。
3. 指定自定义应用程序的名称，例如 安克诺斯数据保护软件。
4. 在**支持的帐户类型**中，选择**仅此组织目录中的帐户**。
5. 单击**注册**。

您的应用程序现已创建。在 Azure 门户中，导航到应用程序的**概述**页面并检查应用程序(客户端)ID 和目录(租户 ID)。



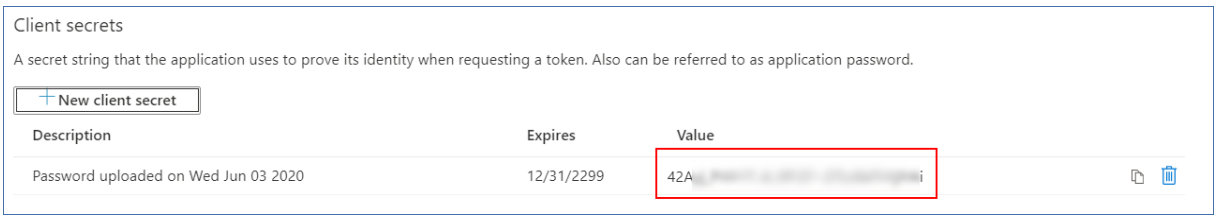
有关如何在 Azure 门户中创建应用程序的详细信息，请参阅 Microsoft 文档。

向应用程序授予必要的 API 权限。

1. 在 Azure 门户中，导航到应用程序的 **API 权限**，然后单击**添加权限**。
2. 选择**我的组织使用的 API** 选项卡，然后搜索 **Office 365 Exchange Online**。
3. 单击 **Office 365 Exchange Online**，然后单击**应用程序权限**。
4. 选中 **full_access_as_app** 复选框，然后单击**添加权限**。
5. 在 **API 权限**中，单击**添加权限**。
6. 选择**Microsoft Graph**。
7. 选择**应用程序权限**。
8. 展开**目录**选项卡，然后选择 **Directory.Read.All** c复选框。单击**添加权限**。
9. 勾选所有权限，然后单击**为<your application's name>授予管理员许可**。
10. 单击**是**来确认选择。

创建应用程序密钥

1. 在 Azure 门户中，导航到应用程序的**证书和秘钥 > 新客户端秘钥**。
2. 在打开的对话框中，选择到期日期：**从不**，然后单击**添加**。
3. 查看**值**字段中的应用程序秘钥，并牢记。



有关应用程序秘钥的详细信息，请参阅 Microsoft 文档。

更改 Microsoft 365 访问凭据

可以更改 Microsoft 365 的访问凭据，而无需重新安装代理程序。

更改 Microsoft 365 访问凭据

1. 在安克诺斯数据保护软件 Web 中控台中，转到**设备** > **Microsoft Office 365**。
2. 选择 Microsoft 365 组织。
3. 单击**指定凭据**。
4. 输入应用程序 ID、应用程序密钥和 Microsoft 365 租户 ID。有关如何查找这些文件的详细信息，请参阅获取应用程序 ID 和应用程序秘钥。
5. 单击**登录**。

选择邮箱

按如下所述选择邮箱，然后相应地指定保护计划的其他设置。

选择邮箱

1. 在安克诺斯数据保护软件 Web 中控台中，转到**设备** > **Microsoft Office 365**。
2. 选择要备份的邮箱。
3. 单击**备份**。

恢复邮箱和邮箱项目

恢复邮箱

1. [仅在恢复至 Exchange Server 时] 确保存在一位 Exchange 用户，其登录名与将要恢复的邮箱的用户的用户名相同。如果不存在，请创建该用户。请参阅 "用户帐户的要求"(第 396 页) 中该用户的完整要求列表。
2. 在安克诺斯数据保护软件 Web 中控台中，转到**设备** > **Microsoft Office 365**。
3. 选择要恢复的邮箱，然后单击**恢复**。
   您可以按名称搜索邮箱。不支持通配符。
   如果邮箱已删除，请在备份存储选项卡上将它选中，然后单击**显示备份**。
4. 选择恢复点。请注意，恢复点按位置过滤。
5. 依次单击**恢复** > **邮箱**。
6. 要恢复至 Exchange Server，请在**恢复至**中，选择 **Microsoft Exchange**。继续恢复，如 "恢复邮箱"(第 397 页) 中所述，从第 9 步开始。无需再执行此过程的其他步骤。
   要恢复至 Microsoft 365，请在**恢复至**中，保留默认的 **Microsoft Office 365** 值。
7. 在**目标邮箱**中，查看、更改或指定目标邮箱。
   默认情况下，选择原始邮箱。如果此邮箱不存在，必须指定目标邮箱。
8. 单击**开始恢复**。

恢复邮箱项目

1. [仅在恢复至 Exchange Server 时] 确保存在一位 Exchange 用户，其登录名与将要恢复的邮箱的用户的用户名相同。如果不存在，请创建该用户。请参阅 "用户帐户的要求"(第 396 页) 中该用户的完整要求列表。
2. 在安克诺斯数据保护软件 Web 中控台中，转到**设备** > **Microsoft Office 365**。

3. 选择原先包含要恢复的项目的邮箱，然后单击**恢复**。
   您可以按名称搜索邮箱。不支持通配符。
   如果邮箱已删除，请在备份存储选项卡上将它选中，然后单击**显示备份**。
4. 选择恢复点。请注意，恢复点按位置过滤。
5. 依次单击**恢复** > **电子邮件**。
6. 选择要恢复的项目。
   提供以下搜索选项。不支持通配符。
   - 对于电子邮件：按主题、发件人、收件人和日期搜索。
   - 对于事件：按标题和日期搜索。
   - 对于任务：按主题和日期搜索。
   - 对于联系人：按名称、电子邮件地址和电话号码搜索。

   当选择电子邮件时，您可以单击**显示内容**来查看其内容，包括附件。

   注意
   单击附加的文件的名称可下载它。

   当选择电子邮件时，您可以单击**作为电子邮件发送**来将邮件发送到电子邮件地址。从管理员帐户的电子邮件地址发送邮件。

   为了能够选择文件夹，请单击“恢复文件夹”图标： 
7. 单击**恢复**。
8. 要恢复至 Exchange Server，请在**恢复至**中，选择 **Microsoft Exchange**。
   要恢复至 Microsoft 365，请在**恢复至**中，保留默认的 **Microsoft Office 365** 值。
9. [仅当恢复至 Exchange Server 时] 要选择或更改目标计算机，请单击**装有 Microsoft Exchange Server 的目标计算机**。此步骤允许恢复至不运行适用于 Exchange 的代理程序的计算机。
   指定启用了 Microsoft Exchange Server 的**客户端访问**角色的计算机的完全限定域名 (FQDN)。该计算机必须与执行恢复的计算机属于相同的 Active Directory 林。
   如果出现提示，请提供将用于访问计算机的帐户的凭据。此帐户的要求在 "所需用户权限"(第 390 页) 中列出。
10. 在**目标邮箱**中，查看、更改或指定目标邮箱。
    默认情况下，选择原始邮箱。如果此邮箱不存在，必须指定目标邮箱。
11. [仅在恢复电子邮件时] 在**目标文件夹**中，查看或更改目标邮箱中的目标文件夹。默认情况下，**恢复项目**文件夹处于选中状态。
12. 单击**开始恢复**。

保护 Google Workspace 数据

此功能仅适用于 Acronis 安克诺斯数据保护软件 的云部署。有关此功能的详细说明，请参阅 https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-google-workspace-data.html。

保护 Oracle 数据库

在以下位置处提供的单独文档中介绍了“保护 Oracle 数据库”：https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_OracleBackup_whitepaper.pdf。

与虚拟机有关的特殊操作

从备份运行虚拟机(即时恢复)

您可以从包含操作系统的磁盘级别备份中运行虚拟机。此操作(也称为即时恢复)让您可以在几秒内快速启动虚拟服务器。直接从备份仿真虚拟磁盘,因此不会消耗数据存储(存储)上的空间。只需要用于保留对虚拟磁盘的更改的存储空间。

我们建议运行此临时虚拟机最多三天。然后,您可以在不停机的情况下完全删除它或将其转换为常规虚拟机(完成)。

只要临时虚拟机存在,保留规则就无法应用到由该计算机使用的备份。原始计算机的备份可以继续运行。

用法示例

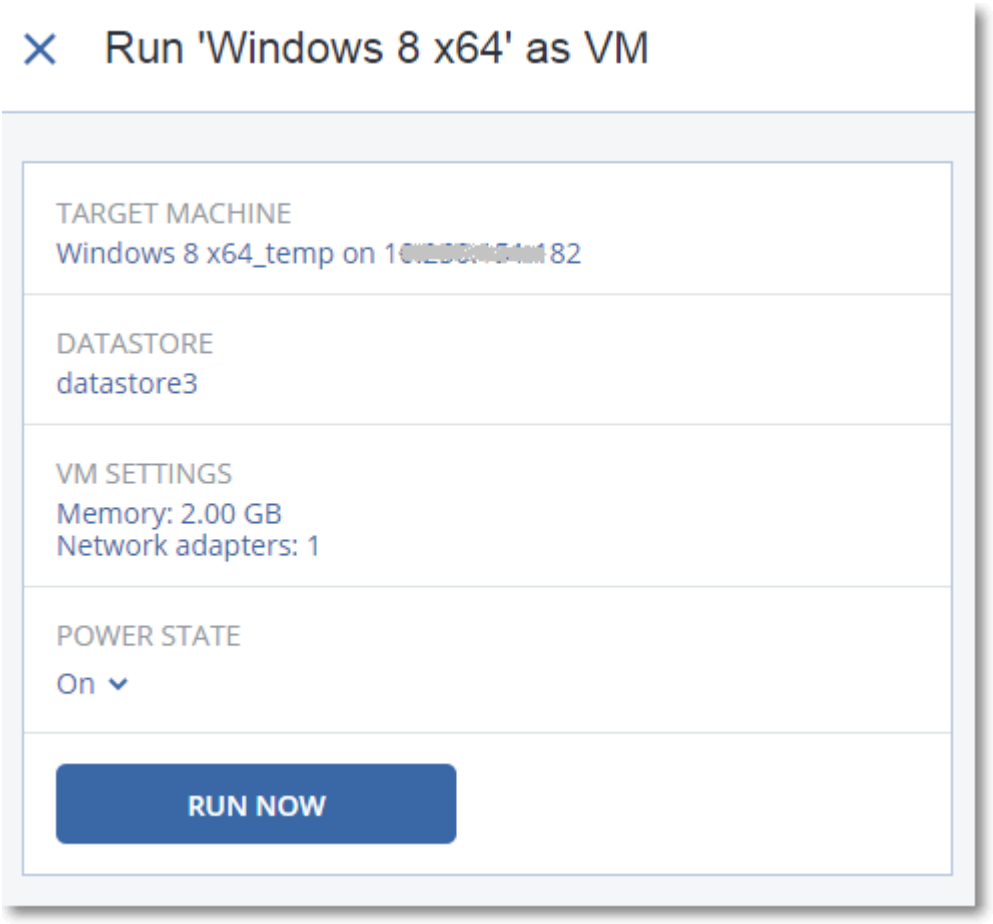
- **灾难恢复**
  使失败计算机的副本立即联机。
- **测试备份**
  从备份运行计算机,并确保来宾操作系统和应用程序正常运作。
- **访问应用程序数据**
  当计算机正在运行时,请使用应用程序的本机管理工具访问和提取所需的数据。

先决条件

- 必须在网络安全保护服务中注册至少一个适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序。
- 备份可存储在网络文件夹中、存储节点上或安装了适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序的计算机的本地文件夹中。如果您选择某个网络文件夹,该文件夹必须可从该计算机访问。还可以从存储在云存储中的备份运行虚拟机,但运行速度缓慢,因为此操作需要从备份进行大量随机存取读取。无法从存储在 SFTP 服务器、磁带设备或安全区中的备份运行虚拟机。
- 备份必须包含整台计算机或操作系统启动所需的所有卷。
- 物理机和虚拟机的备份均可使用。无法使用 Virtuozzo 容器的备份。
- 包含 Linux 逻辑卷 (LVM) 的备份必须由适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序创建。虚拟机的类型必须与原始计算机(ESXi 或 Hyper-V) 的类型相同。

运行计算机

1. 请执行以下任一操作:
   - 选择备份计算机,单击**恢复**,然后选择恢复点。
   - 在备份存储选项卡上选择一个恢复点。
2. 单击**作为 VM 运行**。
   软件自动选择主机和其他所需参数。



3. [可选] 单击**目标计算机**，然后更改虚拟机类型（ESXi 或 Hyper-V）、主机或虚拟机名称。
4. [可选] 为 ESXi 单击**数据存储**或为 Hyper-V 单击**路径**，然后为虚拟机选择数据存储。
   对虚拟机的更改会在计算机运行时累积。确保所选数据存储具有足够的可用空间。如果您计划通过永久保留虚拟机来保留这些更改，请选择适合在生产中运行计算机的数据存储。
5. [可选] 单击 **VM 设置**以更改虚拟机的内存大小和网络连接。
6. [可选] 选择 VM 电源状态（**开**/**关**）。
7. 单击**立即运行**。

结果，计算机将出现在 Web 界面中，并带有以下图标之一：  或 

。无法选择此类虚拟机进行备份。

删除计算机

我们不建议直接在 vSphere/Hyper-V 中删除临时虚拟机。这可能会在 Web 界面中导致人工产物。此外，从中运行计算机的备份可能会保持一段时间的锁定状态（它无法由保留规则删除）。

删除从备份运行的虚拟机

1. 在**所有设备**选项卡上，选择从备份运行的计算机。
2. 单击**删除**。

该计算机将从 Web 界面中删除。还将从 vSphere 或 Hyper-V 清单和数据存储(存储)中删除该计算机。在计算机运行期间数据所发生的所有更改都将丢失。

定型计算机

当从备份运行虚拟机时,将直接从该备份获取虚拟磁盘的内容。因此,如果丢失与备份位置或保护代理程序的连接,计算机将变得不可访问,甚至损坏。

您可以选择使此计算机成为永久计算机,即,将其所有虚拟机以及在计算机运行期间发生的更改恢复至存储这些更改的数据存储中。此过程名为定型。

将在不停机的情况下执行定型。虚拟机在最终确定期间不会关机。

最终虚拟磁盘的位置在**作为 VM 运行**操作参数(ESXi 的**数据存储**或 Hyper-V 的**路径**)中进行定义。在开始最终确定之前,请确保此数据存储的可用空间、共享功能和性能适合在生产中运行计算机。

注意
在 Windows Server 2008/2008 R2 和 Microsoft Hyper-V Server 2008/2008 R2 中运行的 Hyper-V 不支持最终确定,因为这些 Hyper-V 版本中缺少必要的 API。

定型从备份中运行的计算机

1. 在**所有设备**选项卡上,选择从备份运行的计算机。
2. 单击**定型**。
3. [可选]指定计算机的新名称。
4. [可选]更改磁盘配置模式。默认设置为**精简**。
5. 单击**定型**。

计算机名称会立即更改。恢复进度显示在**活动**选项卡上。完成恢复后,计算机图标会更改为常规虚拟机的图标。

您需要知道有关最终确定的内容

最终确定与常规恢复

由于以下原因,最终确定进程比常规恢复慢:

- 最终确定期间,代理程序会执行对备份不同部分的随机访问。正在对整台计算机进行恢复时,代理程序会按顺序从备份中读取数据。
- 如果最终确定期间虚拟机正在运行,则代理程序会更频繁地从备份中读取数据,以同时维持这两个进程。在常规恢复期间,虚拟机会停止。

基于云备份运行的计算机的最终确定

由于对备份数据的访问十分密集,因此最终确定速度高度取决于备份位置与代理程序之间的连接带宽。相较于本地备份,位于云中的备份的最终确定将更慢。如果 Internet 连接速度较慢或不稳定,则基于云备份运行的计算机的最终确定可能会失败。如果您计划执行最终确定并拥有此选项,我们建议您从本地备份运行虚拟机。

在 VMware vSphere 中工作

此部分介绍特定于 VMware vSphere 环境的操作。

虚拟机的复制

复制仅适用于 VMware ESXi 虚拟机。

复制是创建虚拟机的完全副本(副本),然后使该副本与原始计算机保持同步的过程。通过复制关键虚拟机,您将使此计算机的副本始终处于可以启动的状态。

可以手动或按您指定的预定启动复制。第一个复制是完整复制(复制整台计算机)。所有后续复制均为增量复制,并且使用块更改跟踪执行,除非禁用此选项。

复制与备份

和预定备份不同,副本仅保留虚拟机的最新状态。副本会消耗数据存储空间,而备份可以保留在更便宜的存储上。

但是,打开副本的速度比恢复快很多,并且比从备份运行虚拟机更快。开机时,副本性能比从备份运行的 VM 更快,并且不会加载适用于 VMware 的代理程序。

用法示例

- **将虚拟机复制到远程站点。**
  复制可使您通过将虚拟机从主站点克隆到次要站点承来受部分或完全的数据中心故障。次要站点通常位于不太可能受环境、基础架构或其他可能导致主站点故障的因素影响的远程设施中。
- **在单个站点内复制虚拟机(从一个主机/数据存储复制到另一个)。**
  站点内复制可用于高可用性和灾难恢复方案。

可对副本执行的操作

- **测试副本**
  副本将开启以供测试。使用 vSphere Client 或其他工具检查副本是否正确工作。当测试正在进行时会暂停复制。
- **故障转移到副本**
  故障转移是将工作负载从原始虚拟机转移到其副本的操作。当故障转移正在进行时会暂停复制。
- **备份副本**
  备份和复制都需要访问虚拟磁盘,从而影响虚拟机运行所在主机的性能。如果您希望同时具有虚拟机的副本和备份,但不希望在生产主机上放置额外负载,可将该计算机复制到不同的主机,并设置该副本的备份。

限制条件

无法复制以下类型的虚拟机:

- 在 ESXi 5.5 和更低版本上运行的容错计算机。
- 从备份运行的计算机。
- 虚拟机的副本。

创建复制计划

必须为每台计算机单独创建复制计划。无法将现有计划应用到其他计算机。

创建复制计划

1. 选择要复制的虚拟机。
2. 单击**复制**。
   软件显示新的复制计划模板。
3. [可选] 若要修改复制计划名称，请单击默认名称。
4. 单击**目标计算机**，然后执行以下操作：
   a. 选择要创建新副本还是使用原始计算机的现有副本。
   b. 选择 ESXi 主机并指定新副本名称，或选择现有副本。
      新副本的默认名称为 **[Original Machine Name]_replica**。
   c. 单击**确定**。
5. [仅当复制到新计算机时] 单击**数据存储**，然后为虚拟机选择数据存储。
6. [可选] 单击**预定**可更改复制预定。
   默认情况下，从周一到周五每天执行复制。您可以选择要运行复制的时间。
   如果您要更改复制频率，请移动滑块，然后指定预定。
   还可以执行以下操作：
   - 为预定何时有效设定日期范围。选中**在日期范围内运行计划**复选框，然后指定日期范围。
   - 禁用预定。在此情况下，将手动启动复制。
7. [可选] 单击齿轮图标可修改复制选项。
8. 单击**应用**。
9. [可选] 要手动运行计划，请单击计划面板上的**立即运行**。

在运行复制计划后，虚拟机副本将出现在**所有设备**列表中，并带有以下图标： 

测试副本

为测试准备副本

1. 选择要测试的副本。
2. 单击**测试副本**。
3. 单击**开始测试**。
4. 选择是否将开机副本连接到网络。默认情况下，副本不会连接到网络。
5. [可选] 如果选择将副本连接到网络，则选中**停止原始虚拟机**复选框，以在基于副本启动前停止原始计算机。
6. 单击**开始**。

停止测试副本

1. 选择正在进行测试的副本
2. 单击**测试副本**。
3. 单击**停止测试**。
4. 确认您的决定。

故障转移至副本

故障转移至副本

1. 选择要作为故障转移目标的副本。
2. 单击**副本操作**。
3. 单击**故障转移**。
4. 选择是否将开机副本连接到网络。默认情况下，副本将与原始计算机连接到同一个网络。
5. [可选] 如果选择将副本连接到网络，请清除**停止原始虚拟机**复选框以使原始计算机保持联机状态。
6. 单击**开始**。

当副本处于故障转移状态时，您可以选择以下操作之一：

- **停止故障转移**
  如果原始计算机已修复，则停止故障转移。副本将关机。将恢复复制。
- **执行到副本的永久故障转移**
  此即时操作会从虚拟机中删除“副本”标志，因此无法再复制该虚拟机。如果您希望恢复复制，请编辑复制计划以选择此计算机作为源。
- **故障恢复**
  如果您已故障转移至并非用于连续操作的站点，则执行故障恢复。副本将恢复至原始或新虚拟机。到原始计算机的恢复完成后，它将开机并且复制将继续。如果您选择恢复至新计算机，请编辑复制计划以选择此计算机作为源。

停止故障转移

停止故障转移

1. 选择处于故障转移状态的副本。
2. 单击**副本操作**。
3. 单击**停止故障转移**。
4. 确认您的决定。

执行永久故障转移

执行永久故障转移

1. 选择处于故障转移状态的副本。
2. 单击**副本操作**。
3. 单击**永久故障转移**。

4. [可选] 更改虚拟机的名称。
5. [可选] 选中**停止原始虚拟机**复选框。
6. 单击**开始**。

故障恢复

从副本故障恢复

1. 选择处于故障转移状态的副本。
2. 单击**副本操作**。
3. 单击**从副本故障恢复**。
   软件自动选择原始计算机作为目标计算机。
4. [可选] 单击**目标计算机**，然后执行以下操作：
   a. 选择故障恢复到新计算机还是现有计算机。
   b. 选择 ESXi 主机并指定新计算机名称，或选择现有计算机。
   c. 单击**确定**。
5. [可选] 当故障恢复至新计算机时，您还可以执行以下操作：
   - 单击**数据存储**以为虚拟机选择数据存储。
   - 单击 **VM 设置**以更改内存大小、处理器数量以及虚拟机的网络连接。
6. [可选] 单击**恢复选项**以修改故障恢复选项。
7. 单击**开始恢复**。
8. 确认您的决定。

复制选项

若要修改复制选项，请单击复制计划名称旁边的齿轮图标，然后单击**复制选项**。

块更改跟踪 (CBT)

此选项类似于备份选项“块更改跟踪 (CBT)”。

磁盘调配

此选项定义副本的磁盘调配设置。

预设为：**精简配置**。

以下值可用：**精简配置**、**完整配置**、**保留原始设置**。

错误处理

此选项类似于备份选项“错误处理”。

预/后命令

此选项类似于备份选项“预/后命令”。

适用于虚拟机的卷影复制服务 VSS

此选项类似于备份选项“适用于虚拟机的卷影复制服务 VSS”。

故障恢复选项

要修改故障恢复选项，请在配置故障恢复时单击**恢复选项**。

错误处理

此选项类似于恢复选项“错误处理”。

性能

此选项类似于恢复选项“性能”。

预/后命令

此选项类似于恢复选项“预/后命令”。

VM 电源管理

此选项类似于恢复选项“VM 电源管理”。

植入初始副本

要加快到远程位置的复制速度并节省网络带宽，您可以执行副本种子。

重要事项
要执行副本植入，必须在目标 ESXi 上运行适用于 VMware 的代理程序(虚拟设备)。

植入初始副本

1. 请执行以下任一操作：
   - 如果可以关闭原始虚拟机，请关闭它，然后跳到步骤 4。
   - 如果不可以关闭原始虚拟机，请继续执行下一步。
2. 创建复制计划。
   在创建该计划时，请在**目标计算机**中选择**新副本**以及托管原始计算机的 ESXi。
3. 运行一次该计划。
   将在原始 ESXi 上创建一个副本。
4. 将虚拟机(或该副本)文件导出到外部硬盘驱动器。
   a. 将外部硬盘驱动器连接到运行 vSphere Client 的计算机。
   b. 将 vSphere Client 连接到原始 vCenter\ESXi。
   c. 选择库存中新创建的副本。
   d. 依次单击**文件** > **导出** > **导出 OVF 模板**。

e. 在**目录**中，指定外部硬盘驱动器上的文件夹。
f. 单击**确定**。
5. 将硬盘驱动器转移到远程位置。
6. 将副本导入到目标 ESXi。
   a. 将外部硬盘驱动器连接到运行 vSphere Client 的计算机。
   b. 将 vSphere Client 连接到目标 vCenter\ESXi。
   c. 依次单击**文件 > 部署 OVF 模板**。
   d. 在**从文件或 URL 部署**中，指定在步骤 4 中导出的模板。
   e. 完成导入过程。
7. 编辑在步骤 2 中创建的复制计划。在**目标计算机**中，选择**现有副本**，然后选择导入的副本。

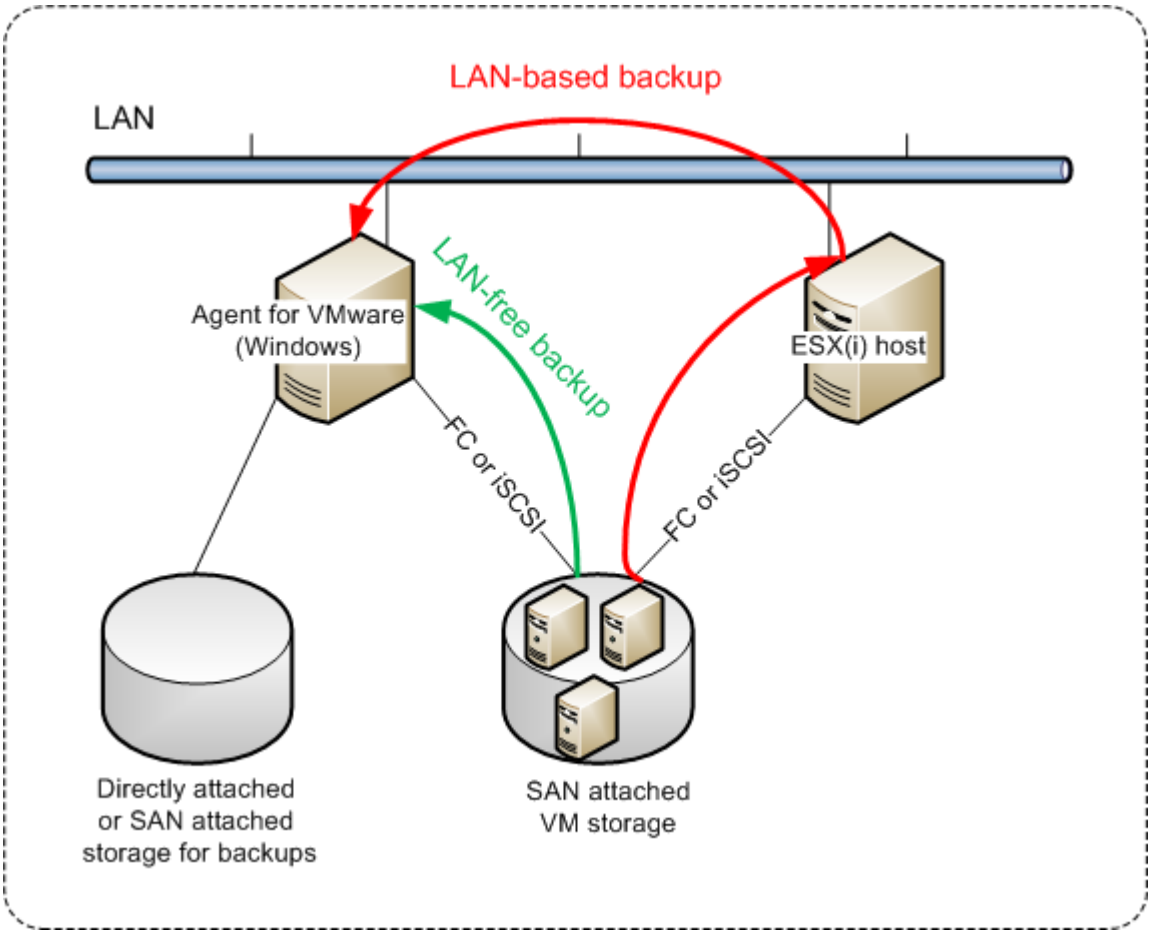
这样，软件将继续更新副本。将以增量方式执行所有复制。

无需 LAN 的备份

如果您的生产 ESXi 主机负载过重，以致于虚拟设备的运行不符合需要，可考虑在 ESXi 基础设施以外的物理计算机上安装适用于 VMware 的代理程序 (Windows)。

如果 ESXi 使用 SAN 连接存储，则在连接至相同 SAN 的计算机上安装代理程序。代理程序将直接从存储备份虚拟机，而不是通过 ESXi 主机和 LAN。此功能称为无需 LAN 的备份。

下图说明了基于 LAN 和无需 LAN 的备份。如果您具有光纤通道 (FC) 或 iSCSI 存储局域网，无需 LAN 即可访问虚拟机。要完全消除通过 LAN 传输已备份数据，可将备份存储在代理程序计算机的本地磁盘或 SAN 连接存储上。



启用代理程序来直接访问数据存储

1. 在对 vCenter 服务器具有网络访问权限的 Windows 计算机上安装适用于 VMware 的代理程序。
2. 将托管数据存储的逻辑单元号 (LUN) 连接到计算机。考虑以下事项：
   - 使用用于将数据存储连接到 ESXi 的同一协议（即 iSCSI 或 FC）。
   - LUN *不得*初始化，在**磁盘管理**中必须显示为“脱机”磁盘。如果 Windows 初始化 LUN，它可能损坏，并且不支持 VMware vSphere 读取。

     为了避免 LUN 初始化，在安装适用于 VMware 的代理程序 (Windows) 期间，系统会自动将 **SAN 策略**设置为**全部脱机**。

因此，代理程序将使用 SAN 传输模式访问虚拟磁盘，即她将通过 iSCSI/FC 读取原始 LUN 扇区，无需识别 VMFS 文件系统（Windows 无法感知）。

限制

- 在 vSphere 6.0 和更高版本中，如果某些 VM 磁盘位于 VMware 虚拟卷 (VVol) 上，而某些磁盘不在，则代理程序无法使用 SAN 传输模式。无法备份此类虚拟机。
- 加密的虚拟机（已在 VMware vSphere 6.5 中引入）将通过 LAN 备份，即使您配置代理程序的 SAN 传输模式也是如此。该代理程序将回退在 NBD 传输上，因为 VMware 不支持用于备份加密虚拟磁盘的 SAN 传输。

示例

如果您使用的是 iSCSI SAN，在运行 Windows 且已安装适用于 VMware 的代理程序的计算机上配置 iSCSI 启动程序。

配置 SAN 策略

1. 以管理员身份登录，打开命令提示符，键入 `diskpart`，然后按 **Enter** 键。
2. 键入 `san`，然后按 **Enter** 键。确保 **SAN 策略：全部脱机**已显示。
3. 如果为“SAN 策略”设置其他值，则执行以下操作：
   a. 键入 `san policy=offlineall`。
   b. 按 **Enter**。
   c. 若要检查设置是否已正确应用，请执行第 2 步。
   d. 重新启动计算机。

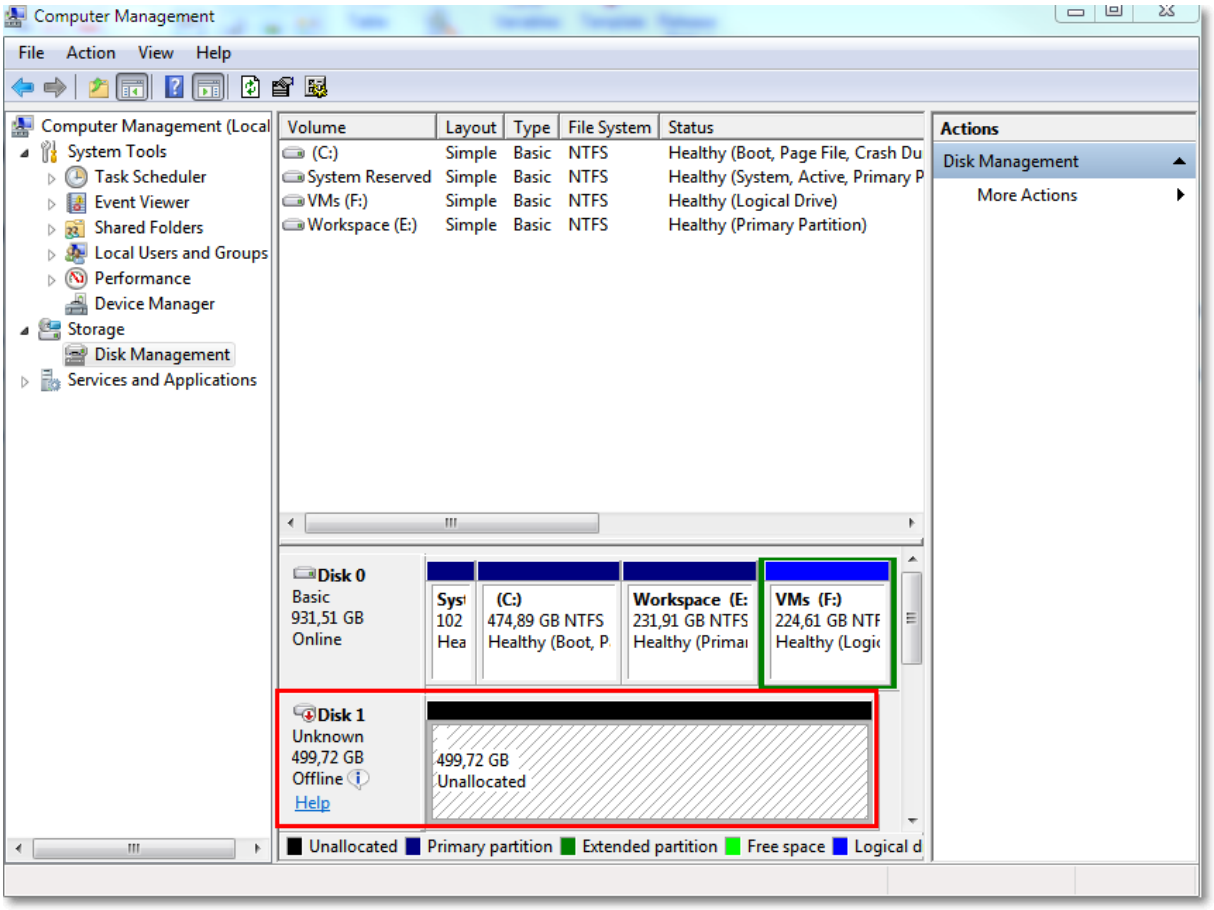
配置 iSCSI 启动程序

1. 转到**控制面板** > **管理工具** > **iSCSI 启动程序**。

   注意
   若要查找**管理工具**，可能需要将**控制面板**视图更改为**主页**或**分类**以外的内容或者使用搜索。

2. 如果这是首次启动 Microsoft iSCSI 启动程序，请确认您要启动 Microsoft iSCSI 启动程序服务。
3. 在**目标**选项卡上，键入目标 SAN 设备的完全限定的域名 (FQDN) 名称或 IP 地址，然后单击**快速连接**。
4. 选择托管数据存储的 LUN，然后单击**连接**。
   如果不显示 LUN，请确保在 iSCSI 目标上进行分区可以启用运行代理程序的计算机，以便访问 LUN。该计算机必须添加到此目标上允许的 iSCSI 启动程序列表。
5. 单击**确定**。

准备就绪的 SAN LUN 应显示在**磁盘管理**中，如下面的屏幕截图所示。



使用 SAN 硬件快照

如果 VMware vSphere 使用存储区域网络 (SAN) 存储系统作为数据存储，则您可以启用适用于 VMware 的代理程序 (Windows)，以便在执行备份时使用 SAN 硬件快照。

重要事项
仅支持 NetApp SAN 存储。

为什么使用 SAN 硬件快照？

适用于 VMware 的代理程序需要虚拟机快照来创建一致的备份。因为该代理程序从快照读取虚拟磁盘内容，所以在整个备份期间必须保留快照。

默认情况下，代理程序使用 ESXi 主机所创建的原生 VMware 快照。此快照保留期间，虚拟磁盘文件处于只读状态，并且主机会将所有更改写入磁盘以区分 delta 文件。备份过程完成后，主机会删除此快照，即：将 delta 文件与虚拟磁盘文件合并。

保留和删除快照都会影响虚拟机性能。对于大虚拟磁盘和快速数据更改，这些操作需要很长时间，在此期间性能可能降低。在极端情况下，几台计算机同时备份，不断增加的 delta 文件可能几乎填满数据存储，导致所有虚拟机关闭。

您可以通过将快照卸载到 SAN 来降低监控程序资源利用率。在这种情况下，操作顺序如下：

1. ESXi 会在备份过程开始时拍摄一个 VMware 快照，以使虚拟磁盘保持一致状态。
2. SAN 会创建一个卷或 LUN 的硬件快照，包含虚拟机及其 VMware 快照。此操作通常需要几秒钟。
3. ESXi 会删除 VMware 快照。适用于 VMware 的代理程序从 SAN 硬件快照读取虚拟磁盘内容。

因为 VMware 快照只保留几秒钟，可最大限度地减少虚拟机性能下降。

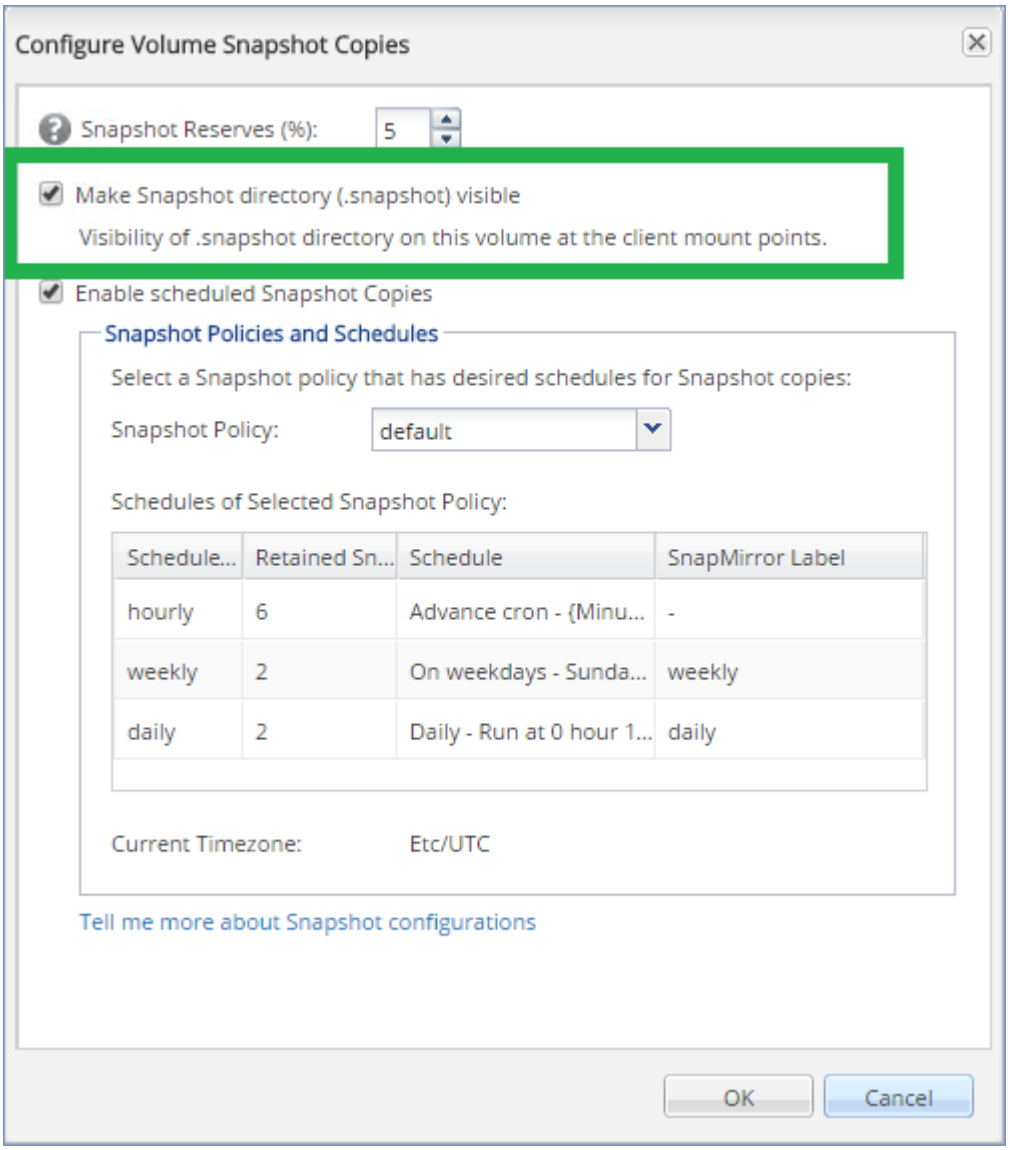
使用 SAN 硬件快照需要哪些内容？

如果要在备份虚拟机时使用 SAN 硬件快照，请确保符合以下所有条件：

- NetApp SAN 存储满足“NetApp SAN 存储要求”中所述的要求。
- 如“配置运行适用于 VMware 的代理程序的计算机”中所述，配置运行适用于 VMware 的代理程序的计算机。
- SAN 存储在管理服务器上注册。
- [如果有适用于 VMware 的代理程序未参与上述注册] 将位于 SAN 存储上的虚拟机分配到支持 SAN 的代理程序，如“虚拟机绑定”中所述。
- 在保护计划选项中启用了“SAN 硬件快照”备份选项。

NetApp SAN 存储要求

- SAN 存储必须用作 NFS 或 iSCSI 数据存储。
- SAN 必须在 **Clustered Data ONTAP (cDOT)** 模式下运行 Data ONTAP 8.1 或更高版本。不支持 **7-mode** 模式。
- 在 NetApp OnCommand System Manager 中，必须为数据存储所在卷勾选**快照副本** > **配置** > **使快照目录 (.snapshot) 可见**复选框。

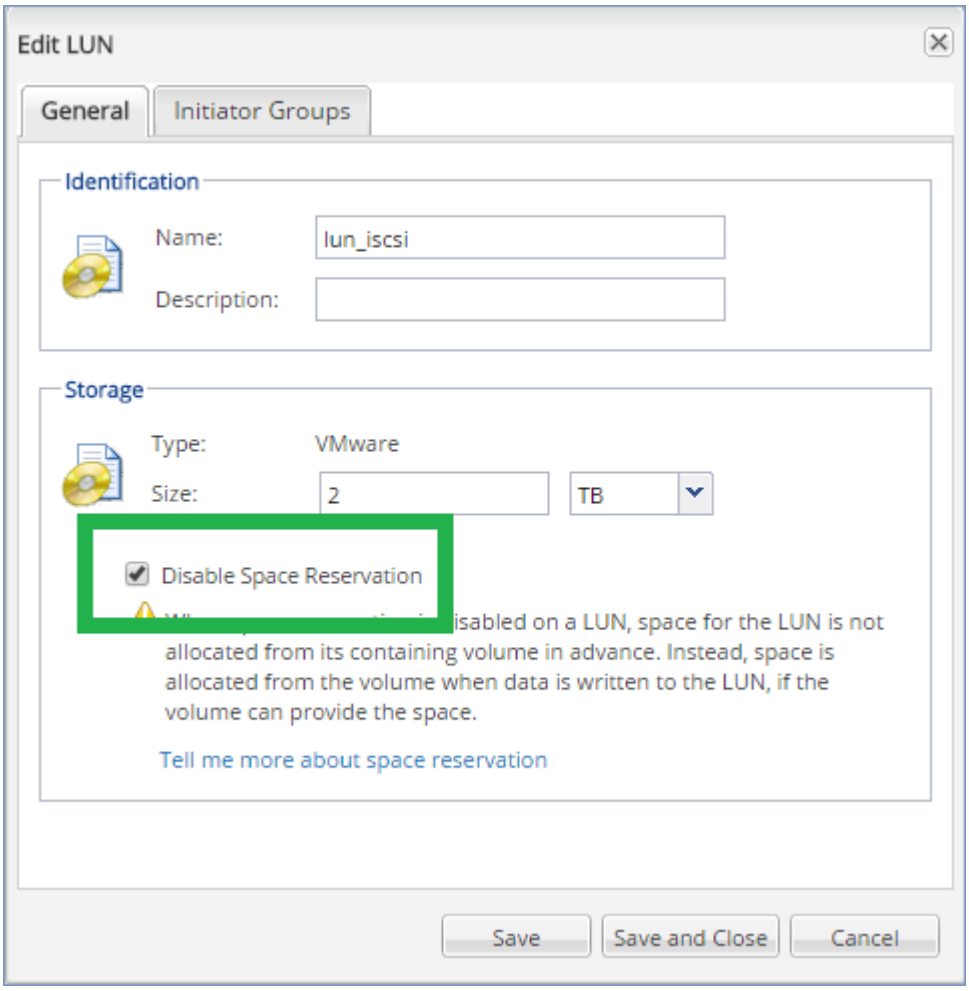


- [适用于 NFS 数据存储] 必须在创建数据存储时指定的存储虚拟机 (SVM) 上启用从 Windows NFSv3 客户端访问 NFS 共享。可以通过以下命令启用访问权限：

```
vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
```

  有关详细信息，请参阅 NetApp 最佳实践文档：https://kb.netapp.com/support/s/article/ka21A0000000k89QAA/top-windows-nfsv3-0-issues-workarounds-and-best-practices

- [适用于 iSCSI 数据存储] 在 NetApp OnCommand System Manager 中，必须为数据存储所在 iSCSI LUN 勾选**禁用空间预留**复选框。



配置运行适用于 VMware 的代理程序的计算机

根据 SAN 存储是用于 NFS 还是 iSCSI 数据存储，参阅下文对应的部分。

配置 iSCSI 发起程序

确保符合以下所有条件：

- 已安装 Microsoft iSCSI 发起程序。
- Microsoft iSCSI 发起程序服务启动类型设置为**自动**或**手动**。此操作可以在**服务**管理单元中完成。
- iSCSI 发起程序的配置如"无需 LAN 的备份"的示例部分中所述。

配置 NFS 客户端

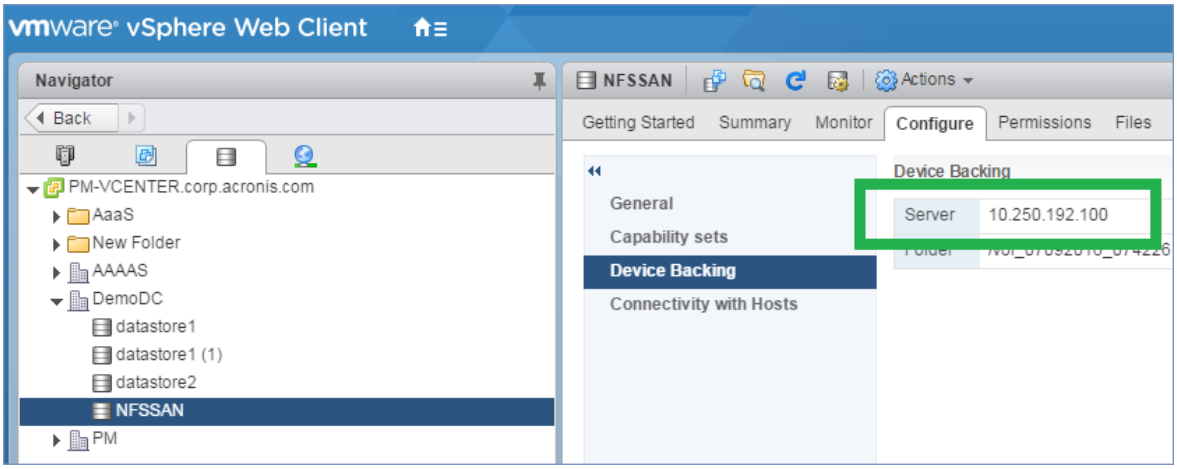
确保符合以下所有条件：

- 已安装适用于 NFS 的 Microsoft **Services**（在 Windows Server 2008 中）或**适用于 NFS 的客户端**（在 Windows Server 2012 及更高版本中）。
- NFS 客户端配置用于匿名访问。可按以下方式执行此操作：

a. 打开注册表编辑器。
b. 找到以下注册表项：**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default**
c. 在此注册表项中，创建新的 **DWORD** 值 **AnonymousUID** 并将其值数据设置为 0。
d. 同时在此注册表项中，创建新的 **DWORD** 值 **AnonymousGID** 并将其值数据设置为 0。
e. 重新启动计算机。

在管理服务器上注册 SAN 存储

1. 单击**设置** > **SAN 存储**。
2. 单击**添加存储**。
3. [可选] 在**名称**中，更改存储名称。
   此名称将显示在 **SAN 存储**选项卡上。
4. 在**主机名或 IP 地址**中，指定创建数据存储时指定的 NetApp 存储虚拟机（SVM，也称为文件管理器）。
   若要在 VMware vSphere Web 客户端中查找所需信息，请选择该数据存储，然后单击**配置** > **设备支持**。主机名或 IP 地址显示在**服务器**字段中。



5. 在**用户名**和**密码**中，指定 SVM 管理员凭据。

重要事项
指定的帐户必须是 SVM 上的本地管理员，而不是整个 NetApp 系统管理管理员。

可以指定一个现有用户或创建一个新用户。若要创建新用户，请在 NetApp OnCommand System Manager 中，导航到**配置** > **安全** > **用户**，然后创建一个新用户。

6. 选择一个或多个适用于 VMware 的代理程序 (Windows)，将向此类代理程序授予该 SAN 设备的读取权限。
7. 单击**添加**。

使用本地连接存储器

您可以将其它磁盘连接到适用于 VMware 的代理程序（虚拟设备），这样代理程序便可以备份到此本地连接存储器。此方法可减少代理程序和备份位置之间的网络流量。

运行在带有备份虚拟机的相同主机或群集上的虚拟设备可直接访问计算机所驻留的数据存储。这意味着该设备通过使用 HotAdd 传输可附加备份磁盘，从而备份流量将从一个本地磁盘流向另一个。如果数据存储以**磁盘/LUN** 方式连接，而不是 **NFS**，则备份完全无需 LAN。如果采用 NFS 数据存储，数据存储和主机之间会有网络流量。

如果代理程序始终备份相同虚拟机，应使用本地连接存储器。如果 vSphere 中运行多个代理程序，其中一个或几个使用本地连接存储器，您需要将各个代理程序手动绑定到需要备份的所有虚拟机。否则，如果管理服务器在代理程序中重新分配虚拟机，虚拟机的备份会分散到多个存储器。

您可在已经工作的代理程序中添加存储器，或在从 OVF 模板部署代理程序时添加。

将存储器连接至已经工作的代理程序

1. 在 VMware vSphere 库存记录中，右键单击适用于 VMware 的代理程序（虚拟设备）。
2. 通过编辑虚拟机设置来添加磁盘。磁盘大小必须至少为 10 GB。

   警告！
   添加现有磁盘时请小心谨慎。一旦创建存储器，该磁盘上先前包含的所有数据将会丢失。

3. 转至虚拟设备中控台。屏幕底部提供了**创建存储器**链接。如果没有提供，请单击**刷新**。
4. 单击**创建存储器**链接，选择磁盘并为其指定标签。由于文件系统限制，标签长度限制为 16 个字符。

若要选择本地连接存储器作为备份目标

创建保护计划时，在**备份位置**中，选择**本地文件夹**，然后键入本地连接存储器相应的盘符，例如 **D:**。

虚拟机绑定

本节概述了管理服务器如何在 VMware vCenter 中组织多个代理程序的操作。

安装在 Windows 中的虚拟设备和代理程序使用以下分配算法。

分配算法

虚拟机会在适用于 VMware 的代理程序之间自动均匀分配。所说的均匀是指各个代理程序管理相同数量的计算机。虚拟机所占存储空间不计算在内。

但是，在为计算机选择代理程序时，软件会尝试优化整个系统的性能。软件尤其会考虑代理程序和虚拟机的位置。托管在同一主机上的代理程序为首选。如果没有位于同一主机上的代理程序，则来自同一群集的代理程序为首选。

虚拟机指定给代理程序后，此计算机的所有备份都将委托给此代理程序。

重新分配

每当既定的平衡被打破时，或者更确切地说，当代理程序中的负载不平衡达到 20% 时，都会发生再分配。这可能发生在添加或删除计算机或代理程序时，或计算机迁移至不同的主机或群集，或将计算机手动绑定至代理程序时。如果发生再分配，管理服务器会使用同一算法重新分配计算机。

例如，您想到需要更多的代理程序帮助处理吞吐量以及将额外的虚拟设备部署至群集。管理服务器会将最适合的计算机指定至新代理程序。将会减少旧代理程序的负载。

当从管理服务器删除代理程序时，计算机被指定给分布在剩余代理程序中的代理程序。但是，如果代理程序被破坏或从 vSphere 手动删除代理程序，则不会发生此情况。仅当从 Web 界面删除此类代理程序时才会开始重新分配。

查看分配结果

您可以在以下位置查看自动分配结果：

- 在**所有设备**部分的每个虚拟机的**代理程序**列中
- 在**设置** > **代理程序**部分中选择代理程序时在**详细信息**面板的**已指派虚拟机**部分中

手动绑定

适用于 VMware 的代理程序绑定通过指定必须始终备份该计算机的代理程序，允许您从该分配流程中排除虚拟机。将维持整体平衡，但只有移除原始代理程序，才能将此特定计算机传递到其他代理程序。

将计算机与代理程序绑定

1. 选择计算机。
2. 单击**详细信息**。
   在**已指派代理程序**部分中，软件会显示当前管理选定计算机的代理程序。
3. 单击**更改**。
4. 选择**手动**。
5. 选择要将计算机绑定到的代理程序。
6. 单击**保存**。

解除计算机与代理程序的绑定

1. 选择计算机。
2. 单击**详细信息**。
   在**已指派代理程序**部分中，软件会显示当前管理选定计算机的代理程序。
3. 单击**更改**。
4. 选择**自动**。
5. 单击**保存**。

禁用代理程序的自动指派

您可以禁用适用于 VMware 的代理程序的自动指派，通过指定此代理程序必须备份的计算机列表，将自动指派从分配流程中排除。将维持其他代理程序之间的整体平衡。

如果没有其他注册的代理程序，或者所有其他代理程序都已禁用自动指派，则无法禁用代理程序的自动指派。

禁用代理程序的自动指派

1. 依次单击**设置** > **代理程序**。
2. 选择要禁用自动指派的适用于 VMware 的代理程序。
3. 单击**详细信息**。
4. 禁用**自动指派**开关。

用法示例

- 如果您想通过光纤通道使用适用于 VMware 的代理程序 (Windows) 备份特定(大型)计算机，而使用虚拟设备备份其他计算机，手动绑定就非常方便。
- 如果您正在使用 SAN 硬件快照，则需要手动绑定。将已为其配置 SAN 硬件快照的适用于 VMware 的代理程序 (Windows) 与位于 SAN 数据存储的计算机绑定。
- 如果代理程序具有一个本地连接存储器，则需要将 VM 与该代理程序绑定。
- 禁用自动指派可让您确保特定计算机可预见地按照您指定的时间表备份。仅备份一个 VM 的代理程序在预定时间到来时不能忙着备份其他 VM。
- 如果您有多个在地理位置上分开的 ESXi 主机，则禁用自动指派会很有用。如果您禁用自动指派，然后将每个主机上的 VM 与同一主机上运行的代理程序绑定，则可以确保代理程序永远不会备份远程 ESXi 主机上运行的计算机，从而节省网络流量。

VM 迁移支持

本节介绍虚拟机在 vSphere 环境中迁移时有望实现的功能，包括属于 vSphere 群集一部分的 ESXi 主机之间的迁移。

vMotion

vMotion 将虚拟机的状态和配置移至另一主机，而计算机磁盘保留在共享存储上的相同位置。

- 不支持且禁用适用于 VMware 的代理程序(虚拟设备)的 vMotion。
- 在备份期间禁用虚拟机的 vMotion。备份将在迁移完成后继续运行。

Storage vMotion

Storage vMotion 可将虚拟机磁盘从一个数据存储移至另一个数据存储。

- 不支持且禁用适用于 VMware 的代理程序(虚拟设备)的 Storage vMotion。
- 在备份期间禁用虚拟机的 Storage vMotion。备份将在迁移后继续运行。

管理虚拟化环境

您可以在其本机演示中查看 vSphere、Hyper-V 和 Virtuozzo 环境。安装并注册相应代理程序后，**VMware**、**Hyper-V** 或 **Virtuozzo** 选项卡会显示在**设备**下。

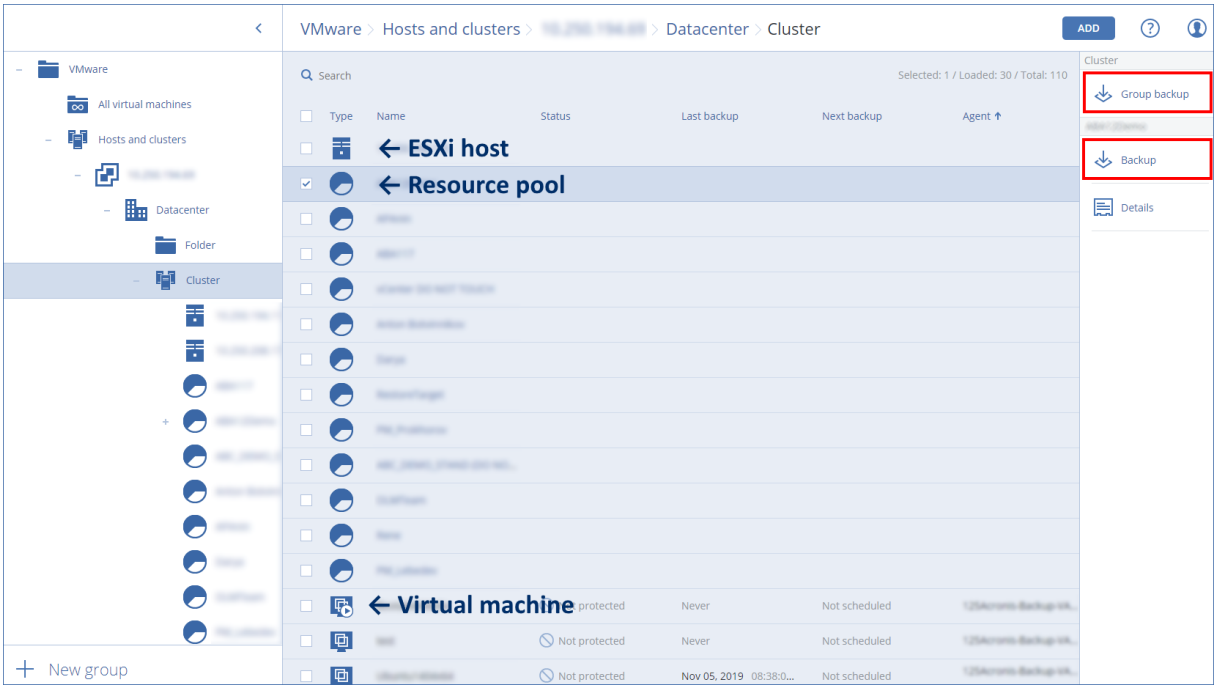
在 **VMware** 选项卡中，可以备份以下 vSphere 基础架构对象：

- 数据中心
- 文件夹:
- 群集

- ESXi 主机
- 资源集区

这些基础架构对象中的每一个都充当虚拟机的组对象。将保护计划应用于这些组对象中的任何一个时，系统将备份其中包含的所有虚拟机。可以通过单击**备份**来备份选定的组计算机，也可以通过单击**组备份**来备份包括选定组的父组计算机。

例如，您已选择相应群集，然后选择其中的资源集区。如果单击**备份**，则系统将备份选定资源集区中包括的所有虚拟机。如果单击**组备份**，则系统将备份相应群集中包括的所有虚拟机。



您可以更改 vCenter 服务器或独立 ESXi 主机的访问凭据，而无需重新安装代理程序。

更改 vCenter 服务器或 ESXi 主机访问凭据

1. 在**设备**下，单击 **VMware**。
2. 单击**主机和群集**。
3. 在**主机和群集**列表(在**主机和群集**树的右侧)中，选择在安装适用于 VMware 的代理程序期间指定的 vCenter 服务器或独立 ESXi 主机。
4. 单击**详细信息**。
5. 在**凭据**下，单击用户名。
6. 指定新的访问凭据，然后单击**确定**。

在 vSphere Client 中查看备份状态

可以在 vSphere Client 中查看虚拟机的备份状态和上次备份时间。

该信息显示在虚拟机摘要(**摘要** > **自定义属性/注释/注意**，具体取决于客户端类型和 vSphere 版本)中。还可以在**虚拟机**选项卡上为任何主机、数据中心、文件夹、资源集区或整个 vCenter 服务器启用**上次备份**和**备份状态**列。

要提供这些属性，除了“适用于 VMware 的代理程序 - 必要权限”中所述的权限之外，适用于 VMware 的代理程序还必须具有以下权限：

- **全局 > 管理自定义属性**
- **全局 > 设置自定义属性**

适用于 VMware 的代理程序 - 必要权限

本节介绍操作 ESXi 虚拟机以及额外进行虚拟设备部署所需的权限。

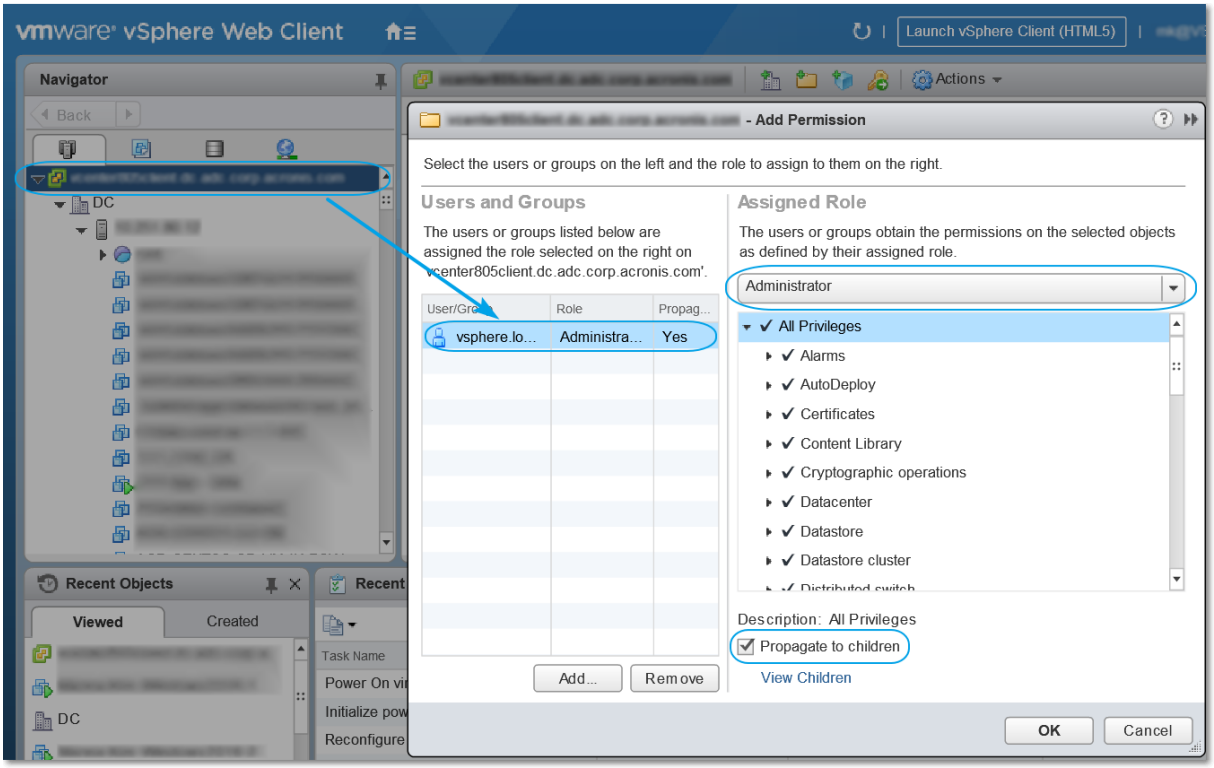
注意
必须在 ESXi 主机上安装 vStorage API，才能启用虚拟机备份。请参阅 https://kb.acronis.com/content/14931。

要对 vCenter 对象（例如，虚拟机、ESXi 主机、群集、vCenter 等）执行任何操作，则适用于 VMware 的代理程序会使用用户提供的 vSphere 凭据在 vCenter 或 ESXi 主机上进行身份验证。从 vCenter 级别开始，vSphere 帐户（用于由适用于 VMware 的代理程序连接到 vSphere）必须在所有级别的 vSphere 基础架构上具有所需的权限。

在适用于 VMware 的代理程序安装或配置期间，指定具有必要权限的 vSphere 帐户。如果需要在以后更改帐户，请参考“管理虚拟化环境”部分。

要将权限指派给 vCenter 级别上的 vSphere 用户，请执行以下操作：

1. 登录到 vSphere Web 客户端。
2. 右键单击 vCenter，然后单击**添加权限**。
3. 选择或添加具有所需角色的新用户（该角色必须包含下表中的所有必需权限）。
4. 选择**传播给子项**选项。



对象	权限	操作				
		备份 VM	恢复到新 VM	恢复到现有 VM	在备份中运行 VM	VA 部署
密码操作 (从 vSphere 6.5 开始)	添加磁盘	+*				
	直接访问	+*				
数据存储	分配空间		+	+	+	+
	浏览数据存储				+	+
	配置数据存储	+	+	+	+	+
	低级别文件操作				+	+
全球	许可证	+	+	+	+	
	禁用方法	+	+	+		
	启用方法	+	+	+		
	管理自定义属性	+	+	+		
	设置自定义属性	+	+	+		
主机 > 配置	VM 自动启动配置					+

	存储分区配置				+	
主机 > 清查	修改群集					+
主机 > 本地操作	创建 VM				+	+
	删除 VM				+	+
	重新配置 VM				+	+
网络	分配网络		+	+	+	+
资源	将 VM 分配到资源集区		+	+	+	+
	导入					+
虚拟机 > 配置	添加现有磁盘	+	+		+	
	添加新磁盘		+	+	+	+
	添加或删除设备		+		+	+
	高级	+	+	+		+
	更改 CPU 计数		+			
	磁盘更改跟踪	+		+		
	磁盘租赁	+		+		
	内存		+			
	删除磁盘	+	+	+	+	
	重命名		+			
	设置批注				+	
	设置		+	+	+	
虚拟机 > 来宾操作	来宾操作程序执行	+**				+
	来宾操作查询	+**				+
	来宾操作修改	+**				
虚拟机 > 互动	获取来宾控制票证(在 vSphere 4.1 和 5.0 中)				+	+
	配置 CD 媒体		+	+		
	中控台互动					+

	通过 VIX API 管理的来宾操作系统(在 vSphere 5.1 和更高版本中)				+	+
	关闭电源			+	+	+
	接通电源		+	+	+	+
虚拟机 > 清查	**从现有基础上创建**		+	+	+	
	新建		+	+	+	+
	移动					+
	注册				+	
	移除		+	+	+	+
	注销				+	
虚拟机 > 调配	**允许磁盘访问**		+	+	+	
	允许只读磁盘访问权限	+		+		
	允许下载虚拟机	+	+	+	+	
虚拟机 > 状态 **虚拟机 > 快照管理** (vSphere 6.5 及更高版本)	**创建快照**	+		+	+	+
	删除快照	+		+	+	+
vApp	**添加虚拟机**				+	

* 仅在备份加密计算机时需要此权限。

** 仅应用程序感知备份需要此权限。

备份群集 Hyper-V 计算机

在 Hyper-V 群集中，虚拟机可以在群集节点之间迁移。遵循以下建议可以设置正确的群集 Hyper-V 计算机备份：

1. 无论计算机迁移到什么节点，都必须可用于备份。要确保适用于 Hyper-V 的代理程序可以访问任意节点上的计算机，代理程序服务必须使用对每个群集节点具有管理权限的域用户帐户运行。

建议在 Agent for Hyper-V 安装过程中，为代理程序服务指定这样一个帐户。

2. 在群集每个节点上安装用于 Hyper-V 的代理程序。
3. 在管理服务器上注册所有代理程序。

恢复的计算机的高可用性

在将备份的磁盘恢复至*现有* Hyper-V 虚拟机时，该计算机的"高可用性"属性会保持原样。

如果将备份的磁盘恢复为*新的* Hyper-V 虚拟机，或者在保护计划之内执行 Hyper-V 虚拟机转换，则生成的计算机不会具备高可用性。该计算机会被视为备用计算机，通常处于关闭状态。如果需要在生产环境中使该计算机，可以在**故障转移群集管理**管理单元中配置该计算机的高可用性属性。

限制同时备份虚拟机的总数

预定备份选项定义在执行给定保护计划时代理程序可以同时备份的虚拟机数量。

如果多个保护计划在时间上重叠，则会将其备份选项中指定的数量相加。即使最终的总数在程序上限制为 10，但重叠的计划会影响备份性能，同时使主机和虚拟机存储过载。

可以进一步减少适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序可以同时备份的虚拟机的总数。

若要限制适用于 VMware 的代理程序 (Windows) 或适用于 Hyper-V 的代理程序可以备份的虚拟机的总数

1. 在运行代理程序的计算机上，创建新的文本文档并使用文本编辑器(如记事本)打开它。
2. 将以下行复制并粘贴到文件中：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. 将 `00000001` 替换为要设置的限制的十六进制值。例如，`00000001` 表示 1，`0000000A` 表示 10。
4. 将该文档另存为 **limit.reg**。
5. 以管理员身份运行该文件。
6. 确认要编辑 Windows 注册表。
7. 执行以下操作来重新启动代理程序：
   a. 在**开始**菜单中，单击**运行**，然后键入：**cmd**
   b. 单击**确定**。
   c. 运行以下命令：

```
net stop mms
net start mms
```

若要限制适用于 VMware 的代理程序(虚拟设备)或适用于 VMware 的代理程序 (Linux) 可以备份的虚拟机的总数

1. 在运行代理程序的计算机上，启动命令外壳：
   - **适用于 VMware 的代理程序（虚拟设备）：**按 CTRL+SHIFT+F2（处于虚拟设备 UI 中）。
   - **适用于 VMware 的代理程序 (Linux)：**以根用户身份登录到运行 Acronis 安克诺斯数据保护软件 设备的计算机。密码与 安克诺斯数据保护软件 Web 中控台所用的相同。
2. 使用文本编辑器（例如，**vi**）打开文件 **/etc/Acronis/MMS.config**。
3. 找到以下部分：

   ```
   <key name="SimultaneousBackupsLimits">
       <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
   </key>
   ```

4. 将 `10` 替换为要设置的限制的十进制值。
5. 保存文件。
6. 重新启动代理程序：
   - **适用于 VMware 的代理程序（虚拟设备）：**执行 `reboot` 命令。
   - **适用于 VMware 的代理程序 (Linux)：**执行以下命令：

     ```
     sudo service acronis_mms restart
     ```

计算机迁移

您可以通过将其备份恢复至非原始计算机来执行计算机迁移。

下表总结了可用的迁移选项。

备份计算机类型	可用恢复目标							
	物理机	ESXi 虚拟机	Hyper-V 虚拟机	Virtuozzo 虚拟机*	Virtuozzo 容器*	Virtuozzo Hybrid Infrastructure 虚拟机*	Scale Computing HC3 虚拟机	RHV/oVirt 虚拟机*
物理机	+	+	+	-	-	+	+	+
VMware ESXi 虚拟机	+	+	+	-	-	+	+	+
Hyper-V 虚拟机	+	+	+	-	-	+	+	+
Virtuozzo 虚拟机*	+	+	+	+	-	+	+	+
Virtuozzo 容器*	-	-	-	-	+	-	-	-
Virtuozzo	+	+	+	-	-	+	+	+

Hybrid Infrastructure 虚拟机*								
Scale Computing HC3 虚拟机	+	+	+	-	-	+	+	+
Red Hat Virtualization /oVirt 虚拟机*	+	+	+	-	-	+	+	+

* 仅可用于云部署。

有关如何执行迁移的说明，请参考以下部分：

- 物理到虚拟 (P2V) - "将物理机恢复到虚拟机"(第 273 页)
- 虚拟到虚拟 (V2V) - "恢复虚拟机"(第 274 页)
- 虚拟到物理 (V2P) - "恢复虚拟机"(第 274 页) 或 "使用可启动媒体恢复磁盘和卷"(第 277 页)

尽管可以在 Web 界面中执行 V2P 迁移，但是我们建议在特定情况下使用可启动媒体。有时，您可能希望使用媒体迁移到 ESXi 或 Hyper-V。

媒体允许您执行以下操作：

- 执行包含逻辑卷 (LVM) 的 Linux 计算机的 P2V 迁移和 V2P 迁移。使用适用于 Linux 的代理程序或可启动媒体来创建要恢复的备份和可启动媒体。
- 为对系统可启动性至关重要的特定硬件提供驱动程序。

Windows Azure 和 Amazon EC2 虚拟机

要备份 Windows Azure 或 Amazon EC2 虚拟机，请在计算机上安装保护代理程序。备份和恢复操作与物理机相同。但是，当在云部署中设置计算机数量的配额时，将计算机视为虚拟。

与物理机的不同点在于，Windows Azure 和 Amazon EC2 虚拟机无法从可启动媒体中启动。如果需要恢复到新的 Windows Azure 或 Amazon EC2 虚拟机，请遵循以下步骤。

将计算机作为 Windows Azure 或 Amazon EC2 虚拟机进行恢复

1. 在 Windows Azure 或 Amazon EC2 中根据映像/模板创建新虚拟机。新计算机必须具有与想要恢复的计算机相同的磁盘配置。
2. 在新计算机上安装适用于 Windows 的代理程序或适用于 Linux 的代理程序。
3. 恢复备份计算机，如“物理机”中所述。在配置恢复时，选择新计算机作为目标计算机。

网络要求

备份计算机上安装的代理程序必须能够通过网络与管理服务器进行通信。

本地部署

- 当代理程序和管理服务器同时安装在 Azure/EC2 云中时，意味着所有计算机都已位于同一网络中。无需执行其他操作。
- 当管理服务器不在 Azure/EC2 云中时，云中的计算机将无法通过网络访问安装管理服务器的本地网络。若要使此类计算机中安装的代理程序能够与管理服务器进行通信，必须在本地和云 (Azure/EC2) 网络之间创建虚拟专用网络 (VPN) 连接。有关如何创建 VPN 连接的说明，请参阅以下文章：

  Amazon EC2：http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-create-cgw

  Windows Azure：https://docs.microsoft.com/zh-cn/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

云部署

在云部署中，管理服务器位于其中一个 Acronis 数据中心中，从而使代理程序能够访问它。无需执行其他操作。

保护 SAP HANA

在以下位置处提供的单独文档中介绍了“保护 SAP HANA”：https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_SAP_HANA_whitepaper_en-US.pdf。

反恶意软件和 Web 保护

安克诺斯数据保护软件 中的反恶意软件保护会为您提供以下好处:

- 面向所有阶段的顶级保护:前瞻性、主动和被动。
- 内部的四种不同反恶意软件技术为您提供同类产品中最佳的多层保护。
- 管理 Microsoft Security Essentials 和 Windows Defender Antivirus。

防病毒和反恶意软件保护

防病毒和反恶意软件保护模块让您可以保护 Windows 和 macOS 计算机免受所有最新恶意软件威胁的影响。请注意,属于反恶意软件保护一部分的 Active Protection 功能在 macOS 计算机上不受支持。查看支持的反恶意软件功能的完整列表:操作系统支持的功能。

Acronis 安克诺斯数据保护软件 在 Windows Security Center 中受支持并进行注册。

如果在将防病毒和反恶意软件保护模块应用于计算机时,您的计算机已经使用第三方防病毒解决方案进行保护,则系统将生成一条警报并会停止实时保护,以便防止出现潜在的兼容性和性能问题。您将需要禁用或卸载第三方防病毒解决方案,以启用完整功能的 Acronis 安克诺斯数据保护软件 防病毒和反恶意软件防护。

以下反恶意软件功能会提供给您使用:

- 在实时保护和手动模式下检测文件中的恶意软件(适用于 Windows、macOS)
- 检测过程中的恶意行为(适用于 Windows)
- 阻止访问恶意 URL(适用于 Windows)
- 将危险文件放入隔离区。
- 将受信任的公司应用程序添加到白名单

防病毒和反恶意软件保护模块会为您提供两种类型的扫描:

- 实时保护扫描
- 手动恶意软件扫描

实时保护扫描

“实时保护”会检查计算机上正在执行或打开的所有文件,以防止恶意软件威胁。

可以选择以下扫描类型之一:

- “访问时检测”是指反恶意软件程序在后台运行,并在系统开机的整个过程中主动地不断扫描计算机系统来查找病毒和其他恶意威胁。在执行某个文件,以及对该文件进行各种操作(比如打开以进行读取/编辑)的情况下,都可以检测到恶意软件。
- “执行时检测”是指只会在可执行文件运行时进行扫描,以确保文件未受感染且不会对您的计算机或数据造成任何损坏。被感染文件的副本不会被发现。

手动恶意软件扫描

根据时间表执行反恶意软件扫描。

可以在**仪表板** > **概述** > 最近受影响小组件中，监控反恶意软件扫描的结果。

防病毒和反恶意软件保护设置

要了解如何创建具有防病毒和反恶意软件保护模块的保护计划，请参阅“创建保护计划”。

可以为防病毒和反恶意软件保护模块指定以下设置。

Active Protection

Active Protection 可保护系统免受勒索软件和加密货币挖掘恶意软件的侵害。勒索软件会加密文件并要求支付赎金才提供加密密钥。加密货币挖矿恶意软件在后台执行数学计算，以便盗取处理能力和网络流量。

在 Cyber Backup 版本的 Acronis 安克诺斯数据保护软件 中，Active Protection 是保护计划中的一个单独模块。因此，可以单独对它进行配置并将其应用于不同的设备或设备组。在 Protect 版本的 Acronis 安克诺斯数据保护软件 中，Active Protection 是防病毒和防恶意软件保护模块的一部分。

Active Protection 适用于运行以下操作系统的计算机：

- 桌面操作系统：Windows 7 Service Pack 1 及更高版本
  在运行 Windows 7 的计算机上，请确保已安装 Windows 7 更新 (KB2533623)。
- 服务器操作系统：Windows Server 2008 R2 及更高版本。

该计算机上必须安装适用于 Windows 的代理程序。

工作方式

Active Protection 可以监控在受保护计算机上运行的进程。当第三方进程尝试加密文件或挖掘加密货币时，Active Protection 会生成警告，并且如果配置中指定了其他操作，它还会执行这些操作。

此外，Active Protection 可以防止未经授权更改备份软件的自身进程、注册表记录、可执行文件与配置文件，以及位于本地文件夹中的备份。

为了识别恶意进程，Active Protection 使用行为启发分析。Active Protection 将某进程执行的操作链与恶意行为模式数据库中记录的事件链进行比较。这种方式使 Active Protection 能通过恶意软件的典型行为检测新的恶意软件。

默认设置：**已启用**。

Active Protection 设置

在**对检测的操作**中，选择软件在检测到勒索软件活动时将执行的操作，然后单击**完成**。

可选择以下其中一个选项：

- **仅通知**
  软件将生成有关进程的警告。
- **停止进程**
  软件将生成警告并停止进程。

- **使用缓存还原**

  软件将生成警告，停止进程，并会使用服务缓存还原被更改的文件。

  默认设置：**使用缓存还原**

网络文件夹保护

保护映射为本地驱动器的网络文件夹选项定义防病毒和反恶意软件保护是否保护映射为本地驱动器的网络文件夹免受本地恶意进程的攻击。

此选项适用于通过 SMB 或 NFS 协议共享的文件夹。

如果文件最初位于映射驱动器上，则通过**使用缓存还原**操作从缓存提取时，无法将其保存到原始位置。而是将其保存到此选项的设置中指定的文件夹中。默认文件夹为 **C:\ProgramData\Acronis\Restored Network Files**。如果此文件夹不存在，将对其进行创建。如果要更改此路径，请指定一个本地文件夹。不支持网络文件夹（包括映射驱动器上的文件夹）。

默认设置：**已启用**。

服务器端保护

此选项定义防病毒和反恶意软件保护是否保护网络文件夹，此类文件夹由您从网络中其他服务器的外部输入连接共享，这些服务器可能带来威胁。

默认设置：**已禁用**。

设置受信任和阻止的连接

在**受信任**选项卡上，可以指定允许用于修改任何数据的连接。必须定义用户名和 IP 地址。

在**已阻止**选项卡上，可以指定将不允许用于修改任何数据的连接。必须定义用户名和 IP 地址。

自我保护

自我保护可以防止未经授权更改软件的自身进程、注册表记录、可执行文件与配置文件、安全区 以及位于本地文件夹中的备份。我们建议不要禁用此功能。

默认设置：**已启用**。

允许进程修改备份

在启用**自我保护**时，**允许特定进程修改备份**选项可用。

它适用于位于本地文件夹中扩展名为 .tibx、.tib、.tia 的文件。

通过此选项，您可以指定可以修改备份文件的进程，即使这些文件通过自我保护进行保护。例如，如果删除备份文件或使用脚本将它们移动到其他位置，则这非常有用。

如果禁用此选项，则仅可由备份软件供应商签名的进程修改备份文件。如此一来，软件可以应用保留规则，并在用户通过 Web 界面发出请求时删除备份。其他进程（无论是否可疑）都无法修改备份。

如果启用此选项，可以允许其他进程修改备份。指定进程可执行文件的完整路径，以驱动器号开头。

默认设置：**已禁用**。

Cryptomining 进程检测

此选项定义防病毒和反恶意软件保护是否检测潜在加密货币挖矿恶意软件。

加密货币挖矿恶意软件会降低有用应用程序的性能、增加电费帐单、可能引起系统崩溃，甚至可能因为滥用导致硬件损坏。建议您将加密货币挖矿恶意软件添加到**有害**进程列表，以阻止它运行。

默认设置：**已启用**。

Cryptomining 进程检测设置

选择软件在检测到 Cryptomining 活动时将执行的操作，然后单击**完成**。可选择以下其中一个选项：

- **仅通知**
  软件会生成有关加密货币挖矿活动的可疑进程的警告。
- **停止进程**
  软件会生成警告并停止加密货币挖矿活动的可疑进程。

默认设置：**停止进程**。

隔离

隔离区是一个文件夹，用于将可疑（可能已感染）或潜在危险的文件保留在隔离的位置。

在以下时间过后删除隔离文件 - 定义几天后将删除隔离文件。

默认设置：**30 天**。

行为检测

Acronis 安克诺斯数据保护软件 通过使用行为启发分析来识别恶意进程以保护您的系统：将某进程执行的操作链与恶意行为模式数据库中记录的操作链进行比较。因此，新恶意软件会通过其典型行为检测到。

默认设置：**已启用**。

行为检测设置

在"**对检测的操作**"中，选择软件在检测到恶意软件活动时将执行的操作，然后单击**完成**。

可选择以下其中一个选项：

- **仅通知**
  软件将生成有关恶意软件活动的可疑进程的警告。
- **停止进程**
  软件将生成警告并停止恶意软件活动的可疑进程。

- **隔离**
  软件将生成警告、停止过程，然后将可执行文件移动到隔离文件夹。

默认设置：**隔离**。

实时保护

实时保护会在系统开机的整个过程中不断检查计算机系统以查找病毒和其他恶意威胁。

默认设置：**已启用**。

配置对检测的操作，以进行实时保护

在**对检测的操作**中，选择软件在检测到病毒或其他恶意威胁时将执行的操作，然后单击**完成**。

可选择以下其中一个选项：

- **阻止并通知**
  软件会阻止进程并生成有关恶意软件活动的可疑进程的警告。
- **隔离**
  软件会生成警告、停止过程，然后将可执行文件移动到隔离文件夹。

默认设置：**隔离**。

配置扫描模式，以进行实时保护

在**扫描模式**中，选择软件在检测到病毒或其他恶意威胁时将执行的操作，然后单击 **完成**。

可选择以下其中一个选项：

- **访问时智能** - 在访问文件进行读取或写入或者启动程序时，它会监控所有系统活动并自动扫描文件。
- **执行时** - 仅在可执行文件启动时自动扫描此类文件，以确保文件未受感染且不会对您的计算机或数据造成任何损坏。

默认设置：**访问时智能**。

预定扫描

可以通过启用**预定扫描**设置，来定义将检查计算机以查找恶意软件所依据的预定。

对检测的操作：

- **隔离**
  软件会生成警告，然后将可执行文件移动到隔离文件夹。
- **仅通知**
  软件会生成有关恶意软件活动的可疑进程的警告。

默认设置：**隔离**。

扫描类型：

- **完整**
  与“快速扫描”相比，“完整扫描”所需时间要长得多，因为将检查每个文件。
- **快速**
  “快速扫描”仅扫描计算机上通常驻留恶意软件的常规区域
- **自定义**
  “自定义扫描”会检查管理员为“保护计划”选择的文件/文件夹。

可以在一个保护计划中预定所有三种扫描：**快速**、**完整**和**自定义**扫描。

默认设置：

- **快速** 且 **完整** 扫描已排程。
- **自定义**扫描默认处于禁用状态。

使用以下事件预定任务运行：

- **按时间预定** - 根据指定时间运行任务。
- **用户登录系统时** - 默认情况下，任何用户登录都会启动任务。可以修改此设置，以便只有特定用户帐户才能触发该任务。
- **用户注销系统时** - 默认情况下，任何用户注销都会启动任务。可以修改此设置，以便只有特定用户帐户才能触发该任务。

  注意
  系统关机时任务将不会运行。关闭和注销在日程安排配置中是不同的事件。

- **系统启动时** - 操作系统启动时运行任务。
- **系统关闭时** - 操作系统关闭时运行任务。

默认设置：**按时间预定**。

预定类型：

- **月** – 选择运行任务的月份和月份中的特定周或特定天。
- **天** – 选择运行任务的特定天。
- **小时** – 选择运行任务的特定天、重复次数和任务运行的时间间隔。

默认设置：**每天**。

开始时间 – 选择任务运行的确切时间。

在日期范围内运行 – 设置配置的计划有效的日期范围。

开始条件 – 定义为了运行任务而应同时满足的所有条件。

用于反恶意软件扫描的开始条件类似于 "开始条件"(第 212 页) 中所描述的备份模块的开始条件。可以定义以下其他开始条件：

- **在时间窗口内分配任务开始时间** - 此选项允许您设置任务的时间范围，以避免出现网络瓶颈。可以以小时或分钟为单位指定延迟。例如，如果默认开始时间为上午 10 点，延迟时间为 60 分钟，则任务将在上午 10 点到上午 11 点之间开始。

- **如果计算机关闭，则在计算机启动时运行遗漏的任务**
- **在任务运行期间防止进入睡眠或休眠模式**- 此选项仅对运行 Windows 的计算机有效。
- **如果开始条件不满足，请务必在以下时间过后运行任务** - 指定任务一定会在其过后启动的时间段，而不考虑其他开始条件。

仅扫描新的和修改的文件 - 仅扫描新创建和修改的文件。

默认设置：**已启用**。

如果计划**完整扫描**，有两个附加选项：

- **扫描存档文件**

  默认设置：**已启用**。

  - **最大递归深度**

    可以扫描嵌入式存档的层数。例如，MIME 文档 > ZIP 存档> Office 存档 > 文档内容。

    默认设置：**16**。
  - **最大大小**

    要扫描的存档文件的最大大小。

    默认设置：**无限制**。
- **扫描可移动驱动器**

  默认设置：**已禁用**。

  - **映射的（远程）网络驱动器**
  - **USB 存储设备**（如闪存驱动器和外部硬盘驱动器）
  - **CD/DVD**

排除

为了尽可能减少启发分析所使用的资源，以及消除所谓的误报（即将受信任的程序报告为勒索软件），可以定义以下设置：

在**受信任**选项卡上，可以指定：

- 永远不会被视为恶意软件的进程。始终信任由 Microsoft 签名的进程。
- 不会监控其中文件更改的文件夹。
- 不会执行预定扫描的文件和文件夹。

在**已阻止**选项卡上，可以指定：

- 始终被阻止的进程。只要在计算机上启用 Active Protection，这些进程就无法启动。
- 将阻止其中任何进程的文件夹。

指定进程可执行文件的完整路径，以驱动器号开头。例如：`C:\Windows\Temp\er76s7sdkh.exe`。

要指定文件夹，您可以使用通配符 * 和 ?。星号 (*) 可替代 0 个或更多字符。问号 (?)只替代刚好一个字符。诸如 `%AppData%` 之类的环境变量无法使用。

默认设置：默认情况下，不会定义任何例外。

URL 过滤

有关详细说明，请参阅 URL 过滤。

Active Protection

在 Cyber Backup 版本的 Acronis 安克诺斯数据保护软件 中，Active Protection 是保护计划中的一个单独模块。该模块有以下设置：

- 对检测的操作
- 自我保护
- 网络文件夹保护
- 服务器端保护
- Cryptomining 进程检测
- 排除

在 Protect 版本的 Acronis 安克诺斯数据保护软件 中，Active Protection 是防病毒和防恶意软件保护模块的一部分。

Active Protection 适用于运行以下操作系统的计算机：

- 桌面操作系统：Windows 7 Service Pack 1 及更高版本
  在运行 Windows 7 的计算机上，请确保已安装 Windows 7 更新 (KB2533623)。
- 服务器操作系统：Windows Server 2008 R2 及更高版本。

该计算机上必须安装适用于 Windows 的代理程序。

要详细了解 Active Protection 及其设置，请参阅 "防病毒和反恶意软件保护设置"(第 439 页)。

Windows Defender防病毒

Windows Defender Antivirus 是 Microsoft Windows 的一个内置反恶意软件组件，从 Windows 8 开始提供。

Windows Defender Antivirus 模块让您可以配置 Windows Defender Antivirus 安全策略，并通过 安克诺斯数据保护软件 Web 中控台跟踪其状态。

该模块适用于安装有 Windows Defender Antivirus 的计算机。

预定扫描

指定预定扫描的时间表。

扫描模式：

- **完整** - 除了在“快速扫描”下扫描的项目外，还会对所有文件和文件夹进行全面检查。与“快速扫描”相比，它执行所需的计算机资源较多。
- **快速** - 快速检查内存中进程和通常会发现恶意软件的文件夹。它执行所需的计算机资源较少。

定义将执行扫描的时间和周几。

每日快速扫描 - 定义每日快速扫描的时间。

可以设置以下选项，具体取决于您的需求：

在计算机打开但不在使用时，启动预定扫描

运行预定扫描之前，请检查最新的病毒和间谍软件定义

将扫描期间的 CPU 使用率限制为

有关 Windows Defender Antivirus 预定/时间表设置的更多详细信息，请参阅 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings

默认操作

针对检测到的不同严重级别的威胁，定义要执行的默认操作：

- **清除** - 清除计算机上检测到的恶意软件。
- **隔离** - 将检测到的恶意软件放入隔离区文件夹中，但不删除它。
- **删除** - 从计算机中删除检测到的恶意软件。
- **允许** - 不删除或隔离检测到的恶意软件。
- **用户自定义** - 系统将提示用户指定要对检测到的恶意软件执行的操作。
- **无操作** - 将不执行任何操作。
- **阻止** - 阻止检测到的恶意软。

有关 Windows Defender Antivirus 默认操作设置的更多详细信息，请参阅 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings

实时保护

启用**实时保护**以检测并停止恶意软件在计算机上安装或运行。

扫描所有下载 - 如果选中该选项，将对下载的所有文件和附件执行扫描。

启用行为监控 - 如果选中该选项，将启用行为监控。

扫描网络文件 - 如果选中该选项，将扫描网络文件。

允许对映射的网络驱动器进行完整扫描 - 如果选中该选项，将完整扫描映射的网络驱动器。

允许电子邮件扫描 - 如果启用该选项，引擎将根据其特定格式解析邮箱和邮件文件，以分析邮件正文和附件。

有关 Windows Defender Antivirus 实时保护设置的更多详细信息，请参阅 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings

高级

指定高级扫描设置：

- **扫描存档文件** - 将存档文件（例如 .zip 或 .rar 文件）包含到扫描中。
- **扫描可移动驱动器** - 在完整扫描期间扫描可移动驱动器。
- **创建系统还原点** - 在某些情况下，重要的文件或注册表项可能会因“误报”而遭删除，因此您将能够从还原点进行恢复。
- **在以下时间过后删除隔离文件** - 定义将删除隔离文件的时限。
- **需要进一步分析时会自动发送文件样本：**
  - **始终提示** - 发送文件之前，系统会要求您确认。
  - **自动发送安全样本** - 除了可能包含个人信息的文件外，将自动发送大多数样本。此类文件将需要进一步确认。
  - **自动发送所有样本** - 将自动发送所有样本。
- **禁用 Windows Defender Antivirus GUI** - 如果选中该选项，则 Windows Defender Antivirus 用户界面将不会提供给用户使用。可以通过 安克诺斯数据保护软件 Web 中控台管理 Windows Defender Antivirus 策略。
- **MAPS (Microsoft Active Protection 服务)** - 帮助您选择如何应对潜在威胁的在线社区。
  - **我不想加入 MAPS** - 不会将有关检测到的软件的信息发送给 Microsoft。
  - **基本成员资格** - 将有关检测到的软件的基本信息发送给 Microsoft。
  - **高级成员资格** - 将有关检测到的软件的更详细信息发送给 Microsoft。

  有关更多详细信息，请参阅 https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise

有关 Windows Defender Antivirus 高级设置的更多详细信息，请参阅 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings

排除

可以定义以下要排除扫描的文件和文件夹：

- **进程** - 将排除扫描定义的进程读取或写入的任何文件。您需要定义指向进程的可执行文件的完整路径。
- **文件和文件夹** - 将排除扫描指定的文件和文件夹。您需要定义指向文件夹或文件的完整路径，或定义文件扩展名。

有关 Windows Defender Antivirus 排除设置的更多详细信息，请参阅 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings

Microsoft Security Essentials

Microsoft Security Essentials 是 Microsoft Windows 的一个内置反恶意软件组件，随 Windows 8 以前的版本一起提供。

Microsoft Security Essentials 模块让您可以配置 Microsoft Security Essentials 安全策略，并通过 安克诺斯数据保护软件 Web 中控台跟踪其状态。

该模块适用于安装有 Microsoft Security Essentials 的计算机。

Microsoft Security Essentials 的设置与 Microsoft Windows Defender Antivirus 几乎相同，不同之处在于前者缺少“实时保护”设置并且无法通过 安克诺斯数据保护软件 Web 中控台定义排除。

URL 过滤

恶意软件通常由恶意站点或受感染站点进行分发，并使用所谓的“驱动下载”方法进行感染。“URL 过滤”功能让您可以保护计算机免受来自 Internet 的恶意软件和网络钓鱼之类的威胁的影响。可以阻止用户访问可能含有恶意内容的网站。

URL 过滤让您还可以控制 Web 使用，以遵守外部法规和公司内部策略。您可以为 40 多个网站类别配置不同的访问策略。

当前，Windows 计算机上的 HTTP/HTTPS 连接将由保护代理程序进行检查。

URL 过滤功能需要连接 Internet，才能起作用。

注意
如果将 URL 过滤与也使用 URL 过滤功能的第三方防病毒解决方案并行使用，则可能会发生冲突。可以通过 Windows Security Center 确定其他已安装的防病毒解决方案的状态。
如果出现兼容性或性能问题，请卸载第三方解决方案或在保护计划中禁用 URL 过滤模块

工作方式

用户在浏览器的地址栏中跟踪链接或输入 URL。拦截器获取链接，并将它发送到保护代理程序。保护代理解析 URL，检查数据库，然后向拦截器返回一个结论。如果 URL 被禁止，拦截器将阻止对它的访问，并通知用户不允许它查看此内容。

配置 SAN 过滤

1. 创建保护计划(具有已启用的 URL 过滤模块)。
2. 指定 URL 过滤设置(见下文)。
3. 将保护计划指派给计算机。

要检查哪些 URL 已被阻止,请转到**仪表板** > **警告**。

URL 过滤设置

可以为 URL 过滤模块指定以下设置。

恶意网站访问

指定用户打开恶意网站时将执行的操作:

- **阻止** – 将阻止对恶意网站的访问并生成警报。
- **始终询问用户** – 将要求用户选择是继续访问网站还是返回。

要过滤的类别

有 44 个可以配置访问策略的网站类别:默认情况下,允许从所有类别访问网站。

	网站类别	说明
1	**广告**	此类别包含其主要目的是服务于广告的领域。
2	**消息板**	此类别包含论坛、讨论板和问答类型的网站。此类别不包括公司网站上客户提问的特定部分。
3	**个人网站**	此类别包含个人网站,以及所有类型的博客:个人、群组,甚至公司博客。博客是在万维网上发布的期刊。它由条目("帖子")组成,通常以相反的时间顺序显示,因此最新的帖子优先显示。
4	**公司/企业网站**	这是一个广泛的类别,包含通常不属于任何其他类别的公司网站。
5	**计算机软件**	此类别包含提供计算机软件的网站,这些软件通常是开源软件、免费软件或共享软件。它也可能包含一些在线软件商店。
6	**医药**	此类别包含与医药/酒精/烟草相关的网站,它包含有关(合法)医药或医用物品、酒精或烟草产品的使用或销售的讨论。 请注意,"麻醉品"类别包括非法药物。
7	**教育**	此类别包含属于官方教育机构的网站,包括那些 .edu 域之外的网站。它还包括教育网站,例如百科全书。
8	**娱乐**	此类别包含提供与艺术活动和博物馆相关信息的网站,以及评论或评级内容(比如电影、音乐或艺术)的网站。

9	**文件共享**	此类别包含文件共享网站，用户可以在其中上传文件并与他人共享文件。它还包含种子共享网站和种子追踪程序。
10	**财务**	此类别包含属于提供在线访问的全球所有银行的网站。还包含某些信用合作社和其他金融机构。但是，一些本地银行可能会被发现。
11	**赌博**	此类别包含赌博网站。这些是“网上赌博”或“网上彩票”类型的网站，通常需要先付款，然后用户才能在网上轮盘赌、扑克、二十一点或类似游戏中进行赌博。其中有些是合法的，这意味着有赢的机会；有些是欺诈性的，这意味着没有机会获胜。它还检测“打假秘籍”网站，这些网站介绍在赌博网站和网上彩票网站上赚钱的方法。
12	**游戏**	此类别包含提供在线游戏的网站，通常基于 Adobe Flash 或 Java 小程序。检测游戏是免费还是需要订购许可无关紧要，但是，赌场风格的网站会在“赌博”类别中进行检测。 此类别不包含： • 开发视频游戏的公司的官方网站（除非他们制作在线游戏） • 讨论游戏的讨论网站 • 可以下载非联机游戏的网站（其中一些属于“非法”类别） • 需要用户下载并运行可执行文件的游戏，例如 《魔兽世界》；这些游戏可以通过不同的方法来阻止运行，例如防火墙
13	**政府**	此类别包含政府网站，包括政府机构、大使馆以及办事处网站。
14	**黑客**	此类别包含为黑客提供黑客工具、文章和讨论平台的网站。它还包含提供常见平台漏洞利用的网站，这些漏洞让 Facebook 或 Gmail 帐户易遭黑客入侵。
15	**非法活动**	此类别是与仇恨、暴力和种族歧视相关的广泛类别，旨在阻止以下类别的网站： • 属于恐怖组织的网站 • 具有种族主义或仇外内容的网站 • 讨论攻击性运动和/或煽动暴力的网站
16	**健康和健身**	此类别包含与医疗机构关联的网站；与疾病预防和治疗相关的网站；提供与减肥、饮食、类固醇、合成代谢或 HGH 产品有关的产品的网站以及提供整形外科信息的网站。。
17	**爱好**	此类别包含的网站展示与通常在个人空闲时间进行的活动相关的资源，比如收藏、艺术和美术以及自行车运动。
18	**Web 托管**	此类别包含免费和商业网站托管服务，允许私人用户和组织创建和发布网站。
19	**非法下载**	此类别包含与软件盗版相关的网站，包括： • 点对点（BitTorrent、emule、DC ++）跟踪器网站，众所周知，它们在未经版权所有者同意的情况下有助于分发受版权保护的内容 • 破解软件（盗版商业软件）网站和讨论区 • 为用户提供破解密钥、密钥生成器和序列号以方便非法使用软件的网站 其中一些网站也可能会被检测为色情或酒精/雪茄网站，因为它们经常使用色情或酒精广告来赚钱。

20	**即时消息**	此类别包含即时消息和聊天网站，使用户可以实时聊天。它还将检测 yahoo.com 和 gmail.com，因为它们都包含嵌入式即时通讯服务。
21	**工作/职业**	此类别包含的网站展示工作公告板、与工作相关类别的广告和职业机会，以及此类服务的内容聚合器。它不包含招聘机构或常规公司网站上的“职位”页面。
22	**成人内容**	此类别包含由网站创建者标记为要求成人受众的内容。它包含各种各样的网站，从印度爱经和性教育网站到铁杆色情制品。
23	**麻醉剂**	此类别包含分享有关娱乐和非法毒品信息的网站。此类别还包含涉及开发或扩散毒品的网站。
24	**新闻**	此类别包含提供文本和视频新闻的新闻网站。它致力于包含全球和本地新闻网站；但是，某些小型本地新闻网站可能未包含在内。
25	**网上约会**	此类别包含网上约会网站（付费和免费），其中用户可以使用一些条件来搜索其他人。他们还可以发布自己的个人资料，以使其他人可以搜索他们。此类别包括免费和付费网上约会网站。 因为大多数流行的社交网络都可以用作网上约会网站，所以 Facebook 等一些流行网站也会在此类别中检测到。建议将此类别与“社交网络”类别一起使用。
26	**在线支付**	此类别包含提供在线支付或转帐的网站。它将检测流行的付款网站，例如 PayPal 或 Moneybookers。它还将启发式地检测要求输入信用卡信息的常规网站上的网页，从而可以检测到隐藏的、未知的或非法的在线商店。
27	**照片共享**	此类别包含照片共享网站，其主要目的是让用户上传和共享照片。
28	**网上商店**	此类别包含已知的在线商店。如果网站在线销售商品或服务，则该网站被视为网上商店。
29	**淫秽作品**	此类别包含的网站含有性爱内容与色情。它包括付费和免费网站。它包含提供图片、故事和视频的网站，还将检测混合内容网站上的色情内容。
30	**门户**	此类别包含的网站汇聚了来自多个来源和不同领域的信息，通常提供诸如搜索引擎、电子邮件、新闻和娱乐信息等特性。
31	**收音机**	此类别包含的网站可提供 Internet 音乐流服务，从在线广播电台到按需（免费或付费）提供音频内容的网站。
32	**宗教**	此类别包含宣扬宗教或派别的网站。它还包含与一种或多种宗教有关的讨论区。
33	**搜索引擎**	此类别包含搜索引擎网站，比如 Google、Yahoo 和 Bing。
34	**社交网络**	此类别包含社交网络网站。这包括 MySpace.com、Facebook.com、Bebo.com 等。但是，专门的社交网络（如 YouTube.com）将列在“视频/照片”类别中。
35	**运动**	此类别包含提供运动信息、新闻和教程的网站。
36	**自杀**	此类别包含宣扬、提供或鼓吹自杀的网站。它不包含预防自杀的诊所。
37	**通俗小**	此类别主要包含与软色情和名人八卦相关的网站。许多小报风格的新闻网站可能在此

	报	处列出了子类别。此类别的检测也基于启发式方法。
38	**浪费时间**	此类别包含个人往往花费大量时间访问的网站。这可能包括其他类别的网站，例如社交网络或娱乐。
39	**旅行**	此类别包含展示旅行服务、旅行装备以及旅行目的地评论和评级的网站。
40	**视频**	此类别包含托管由用户上传或由各内容提供商提供的各种视频或照片的网站。这包括诸如 YouTube、Metacafe、Google Video 之类的网站，以及诸如 Picasa 或 Flickr 之类的照片网站。它还将检测嵌入在其他网站或博客中的视频。
41	**暴力动画片**	此类别包含讨论、共享和提供暴力动画片或日本漫画的网站，由于暴力、露骨的语言或性内容，可能对未成年人不合适。 此类别不包含提供“猫和老鼠”等主流动画片的网站。
42	**武器**	此类别包含的网站提供用于销售或交换的武器、其制造或使用方法。它还包含狩猎资源以及气枪和 BB 枪以及近战武器的使用。
43	**电子邮件**	此类别包含的网站提供电子邮件功能作为 Web 应用程序。
44	**Web 代理**	此类别包含的网站提供 Web 代理服务器服务。当用户打开网页、在表单中输入所请求的 URL 并单击“提交”时，这是一个“浏览器内部的浏览器”类型的网站。Web 代理站点将下载实际页面，并将其显示在用户浏览器中。 这些是检测到此类型的以下原因(可能需要阻止)： • 针对匿名浏览。由于对目标 Web 服务器的请求是从代理 Web 服务器发出的，因此只有其 IP 地址可见，并且如果服务器管理员跟踪用户，则跟踪将在 Web 代理上结束 - 可能会也可能不会保留查找原始用户所需的日志。 • 针对位置欺骗。用户 IP 地址通常用于按源位置对服务进行性能分析(某些国家政府网站可能只能从本地 IP 地址访问)，使用这些服务可能会帮助用户欺骗其真实位置。 • 针对访问禁止内容。如果使用简单的 URL 过滤器，它将仅看到 Web 代理 URL，而看不到用户访问的实际服务器。 • 针对避免公司监控。业务策略可能需要监控员工的 Internet 访问情况。通过 Web 代理访问所有内容，用户可能会逃避不会提供正确信息的监控。 由于 SDK 不仅会分析 HTML 页面(如果提供)，而且还会分析 URL，因此对于某些类别，SDK 仍将能够检测到内容。但是，仅使用 SDK 不能避免其他原因。

如果启用**按类别显示阻止的 URL 的所有通知**复选框，则按类别列出的阻止URL 的通知将显示在托盘中。如果一个网站有几个子域，也会为它们生成通知，因此它们的数量可能很大。

排除

可以将已知安全的 URL 添加到受信任的 URL 列表中。可以将构成威胁的 URL 添加到已阻止 URL 的列表中。

添加 URL 到列表

1. 在保护计划的 URL 筛选模块中，单击**排除**。
2. 选择所需列表：**受信任**或**已阻止**
3. 单击**添加**。
4. 指定 URL 或 IP 地址，然后单击复选标记。

URL 排除示例：

- 如果将 xyz.com 添加为受信任/不受信任，则 xyz.com 域中的所有地址都将视为受信任/不受信任，具体取决于要将其添加到的位置。
- 如果要添加特定子域，可以将 **mail.xyz.com** 添加为受信任/不受信任，这不会导致所有 **xyz.com** 地址都是受信任或不受信任。
- 如果要将 IPv4 添加为受信任/不受信任，则必须使用以下格式才能有效：**20.53.203.50**。
- 如果要同时添加多个 URL 排除项，请确保在新行中添加每个条目：

  acronis.com

  mail.xyz.com

  20.53.203.50

隔离

隔离区是计算机硬盘上的特殊隔离文件夹，用于放置防病毒和反恶意软件保护检测到的可疑文件，以防止威胁进一步传播。

“隔离区”让您可以查看所有计算机上的可疑文件和潜在危险文件，并决定是删除还是还原它们。如果从系统中删除计算机，则隔离的文件将自动删除。

文件如何进入隔离文件夹?

1. 您配置保护计划并定义针对被感染文件的默认操作（即放入“隔离区”）。
2. 系统在“预定扫描”或“访问时扫描”过程中会检测恶意文件，然后将它们放入安全文件夹（即“隔离区”）中。
3. 系统会更新计算机上的隔离列表。
4. 经过在保护计划的**在以下时间过后删除隔离文件**设置中定义的时限后，文件会自动从隔离文件夹中清除。

管理隔离的文件

要管理隔离的文件，请转到**反恶意软件保护** > **隔离区**。您将看到一个列表，其中包含来自所有计算机的隔离文件。

名称	说明
文件	文件名。

隔离日期	文件放入隔离区的日期和时间。
设备	在其上找到被感染文件的设备。
威胁名称	威胁名称。
保护计划	将可疑文件放入隔离区所依据的保护计划。

可以对隔离的文件采取两种操作：

- **删除** - 从所有计算机中永久删除隔离的文件。
- **还原** - 将隔离的文件无任何修改地还原到原始位置。当前，如果原始位置中有一个名称相同的文件，则该文件将被还原的文件覆盖。

计算机上的隔离区位置

隔离的文件的默认位置如下所示：

在 Windows 计算机上：`%ProgramData%\%product_name%\Quarantine`

在 Mac/Linux 计算机上：`/usr/local/share/%product_name%/quarantine`

公司白名单

重要事项
企业白名单要求在管理服务器上安装扫描服务。

防病毒解决方案可能会将公司合法的特定应用程序识别为可疑应用程序。为了防止这些误报检测，将受信任的应用程序手动添加到白名单中，这非常耗时。

安克诺斯数据保护软件 可以自动执行该过程：防病毒和反恶意软件保护模块会扫描备份并分析扫描数据，以便将此类应用程序移至白名单，从而防止出现误报检测。此外，公司范围白名单还会进一步提高扫描性能。

可以启用和禁用白名单。如果禁用白名单，则添加到其中的文件将暂时处于隐藏状态。

自动添加到白名单

1. 对至少两台计算机上的备份运行云扫描。可以使用 "备份扫描计划"(第 301 页) 执行此操作。
2. 在白名单设置中，启用**自动生成白名单**开关。

手动添加到白名单

即使**自动生成白名单**开关已禁用，也可以手动将文件添加到白名单。

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**反恶意软件保护** > **白名单**。
2. 单击**添加文件**。
3. 指定指向相应文件的路径，然后单击**添加**。

将隔离的文件添加到白名单

可以将已隔离的文件添加到白名单。

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**反恶意软件保护** > **隔离**。
2. 选择已隔离的文件，然后单击**添加到白名单**。

白名单设置

如果启用**自动生成白名单**开关，则必须指定以下启发式保护级别之一：

- **低**

  仅在进行长时间检查后，才会将公司应用程序添加到白名单中。此类应用程序更受信任。不过，此种方法会提高误报检测的可能性。将文件视为干净且受信任的标准很高。
- **默认**

  公司应用程序将根据建议的保护级别添加到白名单中，以减少可能的误报检测。将文件视为干净且受信任的标准适中。
- **高**

  企业应用程序将更快地添加到白名单中，以减少可能的误报检测。不过，这并不能保证软件是干净的，并且以后可能会将它识别为可疑软件或恶意软件。将文件视为干净且受信任的标准较低。

查看白名单中项目的相关详细信息

可以单击白名单中的项目，以查看有关该项目的详细信息并进行在线分析。

如果不确定已添加的项目，可以在 VirtusTotal 分析器中对该项目进行检查。单击**在 VirusTotal 上检查**时，该站点会分析可疑文件和 URL，以使用已添加项目的文件哈希来检测恶意软件的类型。可以查看**文件哈希 (MD5)** 字符串中的哈希。

计算机值表示在备份扫描期间找到此类哈希的计算机数量。仅当项目来自备份扫描或隔离区时才会填充此值。如果文件已手动添加到白名单，则此字段保持为空。

备份的反恶意软件扫描

为防止从备份中还原被感染的文件，您可以扫描备份中的恶意软件。“备份扫描”功能仅支持用于 Windows 操作系统。仅当在 安克诺斯数据保护软件 管理服务器上安装扫描服务时，它才可用。

若要扫描备份中的恶意软件，请创建备份扫描计划。

注意
出于安全和性能原因，建议您使用指定的计算机进行扫描。此计算机将可以访问扫描的所有备份。

您可以在仪表板上的“备份扫描详细信息”小组件中查看扫描结果。另外，您还可以在**备份存储** > **位置** > **<备份名称>**中查看备份状态。如果备份扫描不在执行，则备份处于**未扫描**状态。执行备份扫描后，备份的更新状态为：

- **无恶意软件**
- **检测到恶意软件**

限制

- 只能扫描**整台计算机**或**磁盘/卷**类型的备份中是否存在恶意软件。
- 将仅扫描文件系统为 NTFS 且具有 GPT 和 MBR 分区的卷。
- 受支持的备份位置:**云存储**、**本地文件夹**、**网络文件夹**
- 可以选择扫描具有连续数据保护恢复点的备份,但仅扫描常规恢复点(不包括 CDP 恢复点)。仅扫描常规恢复点。
- 当选择 CDP 备份用于整台计算机的安全恢复时,将在不使用 CDP 恢复点中数据的情况下安全恢复计算机。要恢复 CDP 数据,请运行**文件/文件夹**恢复。

协作和通信应用程序的保护

Zoom、Cisco Webex Meetings 和 Microsoft Teams 现已广泛用于视频/网络会议和通信。安克诺斯数据保护软件 让您可以保护协作工具。

Zoom、Cisco Webex Meetings 和 Microsoft Teams 的保护配置非常类似。在下面的示例中，我们将了解 Zoom 的配置。

如需设置 Zoom 保护

1. 在安装协作应用程序的计算机上安装保护代理程序。
2. 登录到 安克诺斯数据保护软件 Web 中控台，然后应用保护计划(具有已启用的以下模块之一)：
   - **防病毒和反恶意软件保护**（已启用 **Self-Protection** 和 **Active Protection** 设置）- 如果您拥有其中一个 安克诺斯数据保护软件 版本。
   - **Active Protection**（已启用 **Self-Protection** 设置）- 如果您拥有其中一个 Cyber Backup 版本。
3. [可选] 对于自动更新安装，请在保护计划中配置**修补程序管理**模块。

这样，您的 Zoom 应用程序的以下活动将受到保护：

- 自动安装 Zoom 客户端更新
- 保护 Zoom 进程免受代码注入
- 由 Zoom 进程阻止可疑操作
- 保护“主机”文件以免添加与 Zoom 有关的域

漏洞评估和修补程序管理

漏洞评估 (VA) 是一个过程，对系统中发现的漏洞进行识别、量化并确定优先级。通过在保护计划中使用漏洞评估模块，可以扫描计算机以查找漏洞，以及检查操作系统和已安装的应用程序是否是最新版本并且可以正常运行。

运行以下操作系统的计算机支持漏洞评估扫描：

- Windows。有关详细信息，请参阅 "支持的 Microsoft 和第三方产品"(第 459 页)。
- Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure) 计算机。有关详细信息，请参阅 "支持的 Linux 产品"(第 460 页)。

修补程序管理 (PM) 功能可用于管理计算机上已安装的应用程序和操作系统的修补程序/更新，并使系统始终保持最新。在修补程序管理模块中，可以自动或手动批准计算机上的更新安装。

运行 Windows 操作系统的计算机支持修补程序管理。有关详细信息，请参阅 "支持的 Microsoft 和第三方产品"(第 459 页)。

漏洞评估

漏洞评估过程包括以下步骤：

1. 创建保护计划 (具有已启用的漏洞评估模块)、指定 漏洞评估设置，然后将计划指派给计算机。
2. 系统(按预定或手动) 会将用于运行漏洞评估扫描的命令发送到保护代理程序。
3. 代理程序获取命令、开始扫描计算机以查找漏洞，然后生成扫描活动。
4. 在漏洞评估扫描完成后，代理程序会生成结果并将它们发送给监视服务。
5. 监视服务处理来自代理程序的数据，并在 漏洞评估小部件 中显示结果和发现的漏洞列表。
6. 通过使用此信息，您可以确定必须修复哪些找到的漏洞。

可以在**仪表板** > **概述** > **漏洞/现有漏洞**小部件中监控漏洞评估扫描的结果。

支持的 Microsoft 和第三方产品

支持以下适用于 Windows 操作系统的 Microsoft 产品和第三方产品进行漏洞评估。

支持的 Microsoft 产品

桌面操作系统

- Windows 7(Enterprise、Professional、Ultimate)
- Windows 8
- Windows 8.1
- Windows 10

服务器操作系统

- Windows Server 2019
- Windows Server 2016

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office 和相关组件

- Microsoft Office 2019(x64，x86)
- Microsoft Office 2016(x64，x86)
- Microsoft Office 2013(x64，x86)
- Microsoft Office 2010(x64，x86)

Windows 相关组件

- Internet Explorer
- Microsoft Edge
- Windows Media Player
- .NET Framework
- Visual Studio 和应用程序
- 操作系统的组件

服务器应用程序

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Sharepoint Server 2016
- Microsoft Sharepoint Server 2016

Windows 支持的第三方产品

安克诺斯数据保护软件 支持漏洞评估和修补各种第三方应用程序，包括协作工具和 VPN 客户端，这些应用程序在远程工作场景中至关重要。

有关 Windows 支持的第三方产品的完整列表，请参阅 https://kb.acronis.com/content/62853。

支持的 Linux 产品

支持以下 Linux 发行版和版本进行漏洞评估：

- Virtuozzo 7.0.11
- Virtuozzo 7.0.10 (320)
- Virtuozzo 7.0.9 (539)
- Virtuozzo 7.0.8 (524)

- CentOS 7.x
- Acronis Cyber Infrastructure 3.x
- Acronis Storage 2.4.0
- Acronis Storage 2.2.0

漏洞评估设置

要了解如何创建具有漏洞评估模块的保护计划，请参阅 "创建保护计划"(第 180 页)。可以按预定或手动(即在保护计划中使用 **立即运行** 操作)执行漏洞评估扫描。

可以在漏洞评估模块中指定以下设置。

扫描内容

定义要扫描哪些软件产品以查找漏洞：

- Windows 计算机：
  - **Microsoft 产品**
  - **Windows 第三方产品**
    (有关 Windows 操作系统支持的第三方产品的更多信息，请参阅 https://kb.acronis.com/content/62853)
- Linux 计算机：
  - **扫描 Linux 程序包**

预定

根据将在选定计算机上执行的漏洞评估扫描来定义预定：

使用以下事件预定任务运行：

- **按时间预定** - 根据指定时间运行任务。
- **用户登录系统时** - 默认情况下，任何用户登录都会启动任务。可以修改此设置，以便只有特定用户帐户才能触发该任务。
- **用户注销系统时** - 默认情况下，任何用户注销都会启动任务。可以修改此设置，以便只有特定用户帐户才能触发该任务。

  注意
  系统关机时任务将不会运行。关闭和注销在日程安排配置中是不同的事件。

- **系统启动时** - 操作系统启动时运行任务。
- **系统关闭时** - 操作系统关闭时运行任务。

默认设置：**按时间预定**。

预定类型：

- **月** – 选择运行任务的月份和月份中的特定周或特定天。
- **天** – 选择运行任务的特定天。

- **小时** – 选择运行任务的特定天、重复次数和任务运行的时间间隔。

默认设置：**每天**。

开始时间 – 选择任务运行的确切时间。

在日期范围内运行 – 设置配置的计划有效的日期范围。

开始条件 – 定义为了运行任务而应同时满足的所有条件。

用于反恶意软件扫描的开始条件类似于 "开始条件"(第 212 页) 中所描述的备份模块的开始条件。可以定义以下其他开始条件：

- **在时间窗口内分配任务开始时间** - 此选项允许您设置任务的时间范围，以避免出现网络瓶颈。可以以小时或分钟为单位指定延迟。例如，如果默认开始时间为上午 10 点，延迟时间为 60 分钟，则任务将在上午 10 点到上午 11 点之间开始。
- **如果计算机关闭，则在计算机启动时运行遗漏的任务**
- **在任务运行期间防止进入睡眠或休眠模式**- 此选项仅对运行 Windows 的计算机有效。
- **如果开始条件不满足，请务必在以下时间过后运行任务** - 指定任务一定会在其过后启动的时间段，而不考虑其他开始条件。

注意
在 Linux 上不支持开始条件。

Windows 计算机的漏洞评估

可以扫描 Windows 计算机和适用于 Windows 的第三方产品以查找漏洞。

1. 在 安克诺斯数据保护软件 Web 中控台中，请创建保护计划，并启用**漏洞评估**模块。
2. 指定漏洞评估设置：
   - **扫描内容** – 选择 **Microsoft 产品**、**Windows 第三方产品**或两者。
   - **时间表** - 定义执行漏洞评估的时间表。
     有关 **时间表** 选项的详细信息，请参阅 "漏洞评估设置"(第 461 页)。
3. 将计划指派给 Windows 计算机。

在漏洞评估扫描过后，即可查看已发现漏洞的列表。可以处理该信息，并确定必须修复哪些已发现的漏洞。

要监控漏洞评估的结果，请查看 **仪表板** > **概述** > **漏洞/现有漏洞** 小组件。

Linux 计算机的漏洞评估

可以扫描 Linux计算机以查找是否存在应用程序级和内核级漏洞。

配置 Linux 计算机的漏洞评估

1. 在 安克诺斯数据保护软件 Web 中控台中，请创建保护计划，并启用**漏洞评估**模块。
2. 指定漏洞评估设置：

- **扫描内容** - 选择**扫描 Linux 程序包**。
- **时间表** - 定义执行漏洞评估的时间表。

  有关 **时间表** 选项的详细信息，请参阅 "漏洞评估设置"(第 461 页) 。

3. 将计划指派给 Linux 计算机。

在漏洞评估扫描过后，即可查看已发现漏洞的列表。可以处理该信息，并确定必须修复哪些已发现的漏洞。

要监控漏洞评估的结果，请查看 **仪表板** > **概述** > **漏洞/现有漏洞** 小组件。

管理发现的漏洞

如果漏洞评估执行至少一次并发现了一些漏洞，则可以在**软件管理** > **漏洞**中看到它们。漏洞列表会同时显示有可用修补程序的漏洞和没有建议修补程序的漏洞。可以使用过滤器来仅显示带有可用修补程序的漏洞。

名称	说明
名称	漏洞的名称。
受影响的产品	发现漏洞的软件产品。
计算机	受影响的计算机数量。
严重性	发现的漏洞严重性。根据通用漏洞评分系统 (CVSS)，可以指派以下级别： • **严重**：9 - 10 CVSS • **高**：7 - 9 CVSS • **中**：3 - 7 CVSS • **低**：0 - 3 CVSS • **无**
修补程序	合适修补程序的数量。
已发布	漏洞在“常见漏洞和披露”(CVE) 中发布的日期和时间。
检测到	检测到计算机的现有漏洞的第一个日期。

可以在列表中单击发现的漏洞的名称来查找它的描述。

开始漏洞修复过程

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**软件管理** > **漏洞**。
2. 在列表中选择相应漏洞，然后单击 **安装修补程序**。漏洞修复向导将打开。
3. 选择要安装的修补程序。单击**下一步**。
4. 选择要安装修补程序的计算机。
5. 选择安装修补程序后是否重新启动计算机：
   - **否** - 在安装修补程序之后，永远不会启动重新启动。
   - **如果需要** - 仅当应用更新需要，才会进行重新启动。

- **是** - 安装修补程序之后，始终启动重新启动。但是，您可指定延迟启动。

  备份完成之前，请勿重新启动 - 如果备份进程正在运行，则计算机重新启动将延迟到备份完成为止。

6. 单击**安装修补程序**。

结果是，所选修补程序会安装在选定计算机上。

修补程序管理

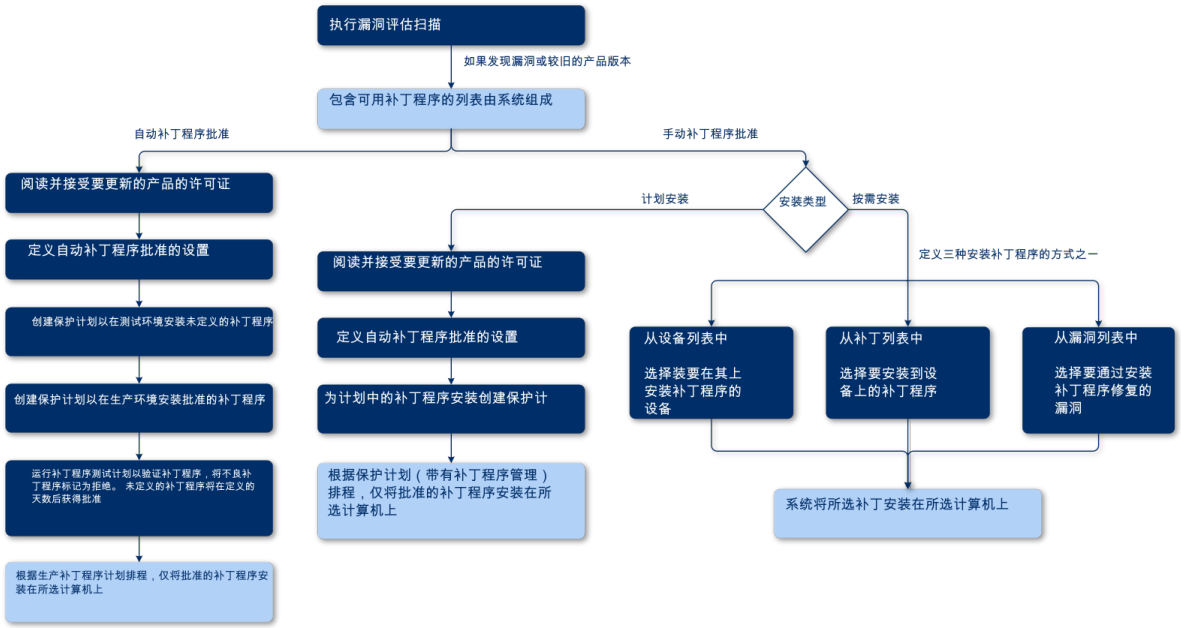
修补程序管理功能可用于：

- 安装操作系统级别和应用程序级别的更新
- 手动或自动批准修补程序
- 手动并按预定安装修补程序
- 根据不同的标准精确定义要应用的修补程序：严重性、类别和批准状态
- 执行更新前备份以防止可能的失败更新
- 定义安装修补程序后要应用的重新启动选项

安克诺斯数据保护软件 引入对等技术，以最大程度地减少网络带宽流量。可以选择一个或多个将从 Internet 下载更新的专用代理程序，然后将它们在网络中的其他代理程序之间分发。所有代理程序也将作为对等代理程序彼此共享更新。

工作方式

可以配置自动或手动修补程序批准。在以下方案中，可以同时看到自动和手动修补程序批准工作流程。



1. 首先，您需要使用具有已启用的**漏洞评估**模块的保护计划，至少执行一次漏洞评估扫描。在执行扫描后，系统会将发现的漏洞列表和可用修补程序进行组合。
2. 然后，可以配置自动修补程序批准或使用手动修补程序批准方法。
3. 定义如何安装修补程序 - 根据预定或手动。根据您的喜好，可以通过三种方式进行手动修补程序安装：
   - 转到修补程序列表（**软件管理** > **修补程序**），然后安装必要修补程序。
   - 转到漏洞列表（**软件管理** > **漏洞**），然后开始修复过程（其中还包括修补程序安装）。
   - 转到设备列表（**设备** > **所有设备**）、选择要更新的特定计算机，然后在这些计算机上安装修补程序。

可以在**仪表板** > **概述** > **修补程序安装历史记录**小部件中监控修补程序安装的结果。

修补程序管理设置

要了解如何创建具有修补程序管理模块的保护计划，请参阅“创建保护计划”。通过使用保护计划，可以指定要在定义的计算机上自动安装针对 Microsoft 产品和其他适用于 Windows 操作系统的第三方产品的更新。

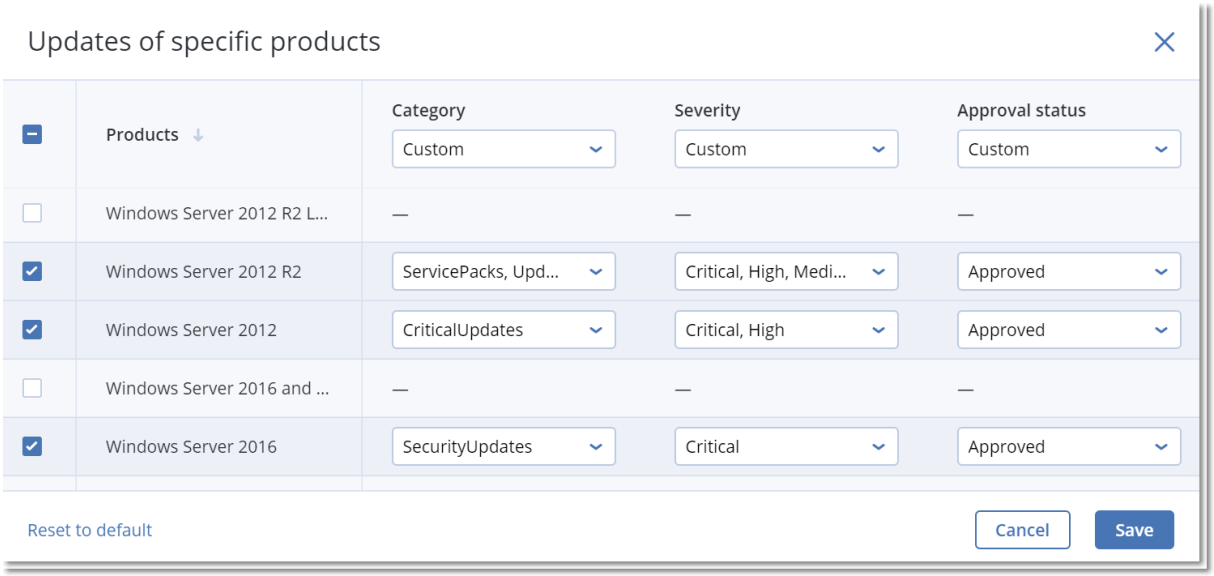
可以为修补程序管理模块指定以下设置。

Microsoft 产品

要在选定计算机上安装 Microsoft 更新，请启用**更新 Microsoft 产品**选项。

选择要安装的更新：

- **所有更新**
- **仅安全和重要更新**
- **指定产品的更新**：可以为不同产品定义自定义设置。如果要更新特定产品，可以按类别、严重性或批准状态为每个产品定义要安装的更新。

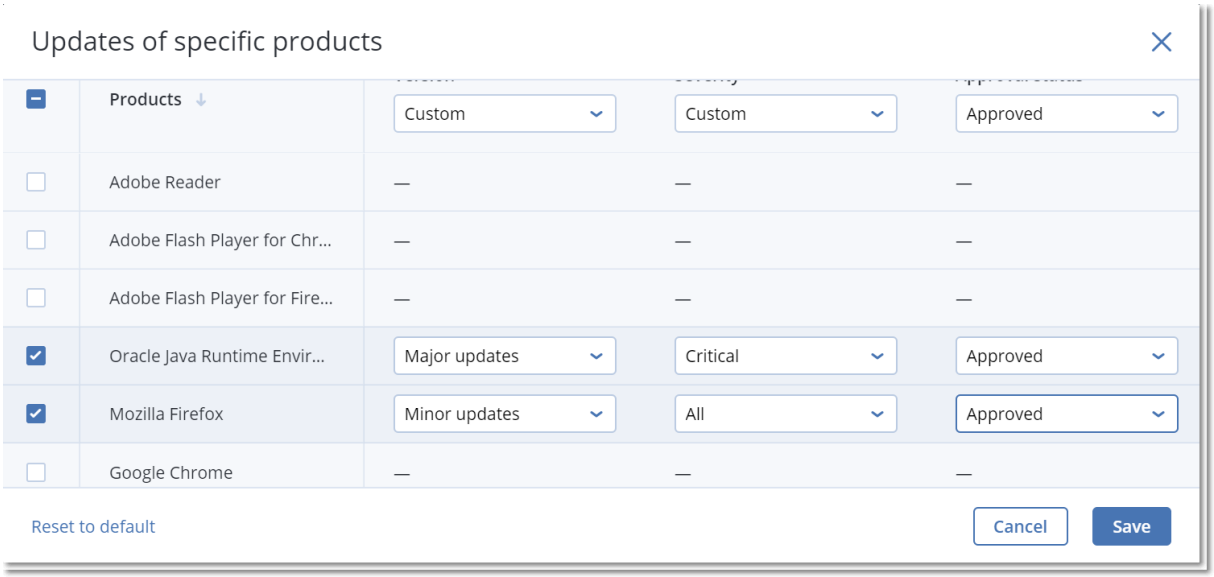


Windows 第三方产品

要在选定计算机上安装适用于 Windows 操作系统的第三方更新，请启用 **Windows 第三方产品**选项。

选择要安装的更新：

- **仅最新主要更新**让您可以安装最新可用版本的更新。
- **仅最新次要更新**让您可以安装次要版本的更新。
- **指定产品的更新**：可以为不同产品定义自定义设置。如果要更新特定产品，可以按类别、严重性或批准状态为每个产品定义要安装的更新。



预定

定义在选定计算机上安装更新所依据的预定。

使用以下事件预定任务运行：

- **按时间预定** - 根据指定时间运行任务。
- **用户登录系统时** - 默认情况下，任何用户登录都会启动任务。可以修改此设置，以便只有特定用户帐户才能触发该任务。
- **用户注销系统时** - 默认情况下，任何用户注销都会启动任务。可以修改此设置，以便只有特定用户帐户才能触发该任务。

  注意
  系统关机时任务将不会运行。关闭和注销在日程安排配置中是不同的事件。

- **系统启动时** - 操作系统启动时运行任务。
- **系统关闭时** - 操作系统关闭时运行任务。

默认设置：**按时间预定**。

预定类型：

- **月** – 选择运行任务的月份和月份中的特定周或特定天。
- **天** – 选择运行任务的特定天。
- **小时** – 选择运行任务的特定天、重复次数和任务运行的时间间隔。

默认设置:**每天**。

开始时间 – 选择任务运行的确切时间。

在日期范围内运行 – 设置配置的计划有效的日期范围。

开始条件 – 定义为了运行任务而应同时满足的所有条件。

用于反恶意软件扫描的开始条件类似于 "开始条件"(第 212 页) 中所描述的备份模块的开始条件。可以定义以下其他开始条件:

- **在时间窗口内分配任务开始时间** - 此选项允许您设置任务的时间范围,以避免出现网络瓶颈。可以以小时或分钟为单位指定延迟。例如,如果默认开始时间为上午 10 点,延迟时间为 60 分钟,则任务将在上午 10 点到上午 11 点之间开始。
- **如果计算机关闭,则在计算机启动时运行遗漏的任务**
- **在任务运行期间防止进入睡眠或休眠模式**- 此选项仅对运行 Windows 的计算机有效。
- **如果开始条件不满足,请务必在以下时间过后运行任务** - 指定任务一定会在其过后启动的时间段,而不考虑其他开始条件。

更新前备份

在安装软件更新之前运行备份 - 在计算机上安装任何更新之前,系统会创建该计算机的增量备份。如果之前没有创建备份,则将创建完整的计算机备份。如果修补程序安装失败,这将让您可以回滚到原始配置。为了使**更新前备份**选项起作用,相应计算机必须在保护计划中同时启用修补程序管理和备份模块,以及具有要备份的项目(整台计算机或启动+系统卷) 。如果您选择不合适的项目进行备份,则系统不会不允许您启用**更新前备份**选项。

管理修补程序的列表

漏洞评估完成后,您将在**软件管理** > **修补程序**中找到可用的修补程序。

名称	说明
名称	修补程序的名称
严重性	修补程序的严重性: • **严重** • **高** • **中** • **低** • **无**
供应商	修补程序的供应商
产品	修补程序适用的产品

已安装的版本	已安装的产品版本
版本	修补程序的版本
类别	修补程序所属的类别: • **重要更新** - 针对特定问题广泛发布的修复程序，用于解决与安全性无关的重要错误。 • **安全更新** - 针对特定产品广泛发布的修复程序，用于解决安全问题。 • **定义更新** - 病毒或其他定义文件的更新。 • **更新汇总** - 修补程序、安全更新、重要更新以及打包在一起以方便部署的更新的累积集合。汇总通常针对特定领域(例如安全性)或特定组件(例如 Internet 信息服务 (IIS))。 • **服务包** - 所有修补程序、安全更新、重要更新以及自产品发布以来创建的更新的累积集合。服务包中也可能包含有限数量的客户要求的设计更改或功能。 • **工具** - 辅助完成一项或任务集的实用程序或功能。 • **功能包** - 新功能发布，通常在下次发布时引入到产品中。 • **更新** - 针对特定问题广泛发布的修复程序，用于解决与安全性无关的不重要错误。 • **应用程序**– 应用程序的修补程序。
Microsoft 知识库	如果是 Microsoft 产品的修补程序，则提供知识库文章 ID
发布日期	修补程序的发布日期
计算机	受影响的计算机数量
批准状态	批准状态主要是自动批准方案所需要的，并且能够在保护计划中定义要按状态安装的更新。 可以为修补程序定义以下状态之一: • **已批准** - 修补程序安装在至少一台计算机上，并且经验证可以正常运行 • **已拒绝** - 修补程序不安全，可能会损坏计算机系统 • **未定义** - 修补程序状态不清楚，并且应该进行验证
许可协议	• 阅读并接受 • 不同意。如果您不同意许可协议，则修补程序状态将变为**已拒绝**，并且不会安装它
漏洞	漏洞的数量。如果单击它，系统会将您重定向到漏洞的列表。
大小	修补程序的平均大小

语言	修补程序支持的语言
供应商站点	供应商的官方站点

自动修补程序批准

自动修补程序批准让您可以更轻松地在计算机上安装更新。我们考虑该示例的工作方式。

工作方式

您应该有两个环境:测试和生产。测试环境用于测试修补程序安装,并确保它们不会造成任何损害。在测试环境中测试了修补程序安装后,即可在生产环境中自动安装这些安全修补程序。

配置自动修补程序批准

配置自动修补程序批准

1. 对于计划更新其产品的每个供应商,您必须阅读并接受许可协议。否则,将无法进行自动修补程序安装。
2. 配置自动批准的设置。
3. 准备保护计划(例如,“测试修补”,其中具有已启用的**修补程序管理**模块),然后将它应用于测试环境中的计算机。指定修补程序安装的以下条件:修补程序批准状态必须为**未定义**。需要执行此步骤来验证修补程序,并在安装修补程序后检查计算机是否正常运行。
4. 准备保护计划(例如,“生产修补”,其中具有已启用的**修补程序管理**模块),然后将它应用于生产环境中的计算机。指定修补程序安装的以下条件:修补程序状态必须为**已批准**。
5. 运行“测试修补”计划并检查结果。没有问题的计算机的批准状态可以保留为**未定义**,而不能正常工作的计算机的状态必须设置为**已拒绝**。
6. 根据**自动批准**选项中设置的天数,状态为**未定义**的修补程序将变为**已批准**。
7. 启动“生产修补”计划后,仅会将状态为**已批准**的修补程序安装在生产计算机上。

手动步骤如下所列。

第 1 步.阅读并接受要更新的产品的许可协议

1. 在 安克诺斯数据保护软件 Web 中控台中,转到**软件管理** > **修补程序**。
2. 选择相应修补程序,然后阅读并接受许可协议。

第 2 步.配置自动批准的设置

1. 在 安克诺斯数据保护软件 Web 中控台中,转到**软件管理** > **修补程序**。
2. 单击**设置**。
3. 启用**自动批准**选项,并指定天数。这意味着自首次尝试安装修补程序起经过指定的天数后,状态为**未定义**的修补程序将自动变为**已批准**。

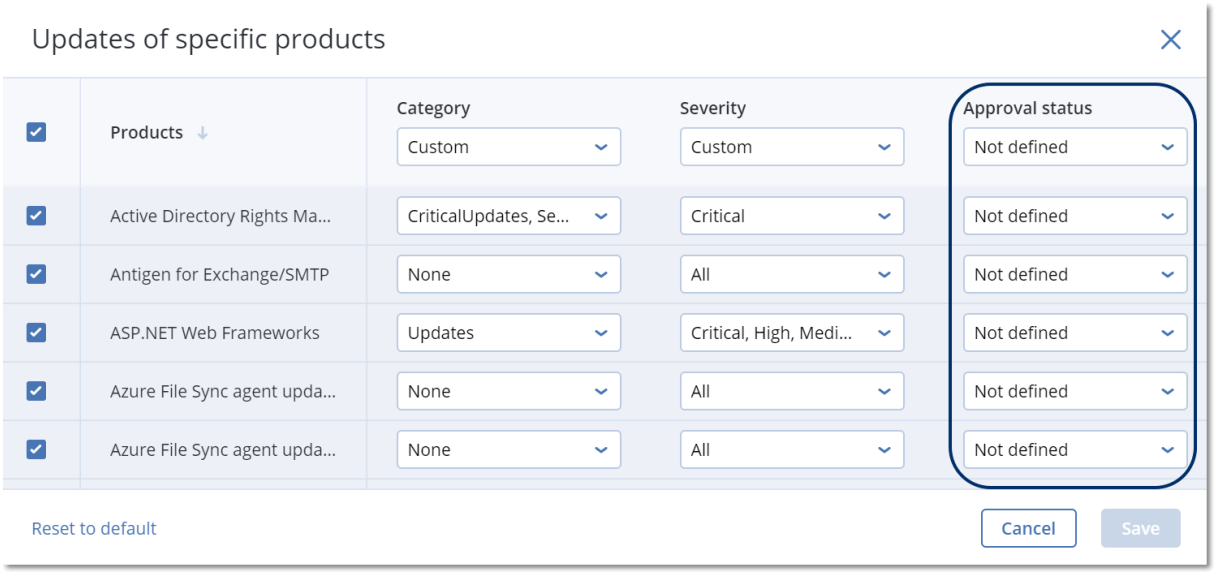
   例如,指定 10 天。针对测试计算机和安装的修补程序执行“测试修补”计划。那些损坏计算机的补丁,您标记为**拒绝**,而其余修补程序则保持为**未定义**。经过 10 天后,状态为**未定义**的修补程序将自动切换为**已批准**。

4. 启用**自动接受许可协议**选项。在修补程序安装过程中，这是自动接受许可所必需的，无需用户确认。

第 3 步.准备“测试修补”保护计划

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**计划** > **保护**。
2. 单击**创建计划**。
3. 启用**修补程序管理**模块。
4. 定义要为 Microsoft 和第三方产品安装哪些更新、预定并预更新备份。有关这些设置的更多详细信息，请参考“修补程序管理设置”。

重要事项
对于要更新的所有产品，将**批准状态**定义为**未定义**。当更新时间到来时，代理程序将在测试环境中的选定计算机上仅安装**未定义**修补程序。

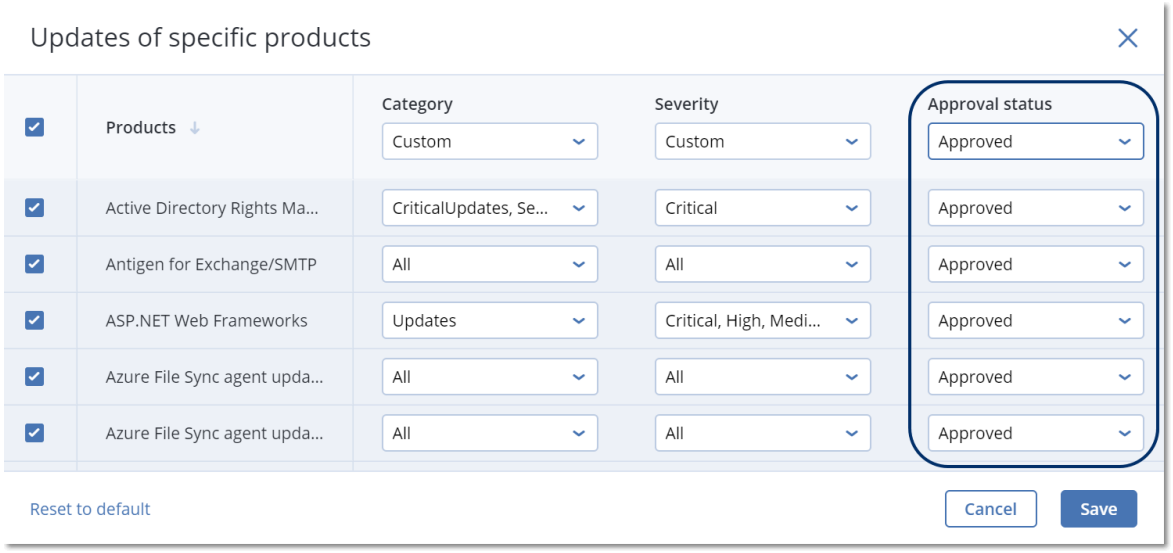


第 4 步.准备产品修补保护计划

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**计划** > **保护**。
2. 单击**创建计划**。
3. 启用**修补程序管理**模块。
4. 定义要为 Microsoft 和第三方产品安装哪些更新、预定并预更新备份。有关这些设置的更多详细信息，请参考“修补程序管理设置”。

重要事项
对于要更新的所有产品，将**批准状态**定义为**批准**。当更新时间到来时，代理程序将在产品环境中的选定计算机上仅安装**已批准**的修补程序。

注意



步骤 5.运行测试修补保护计划并检查结果

1. 运行测试修补保护计划(按预定或手动)
2. 此后,检查哪些已安装的修补程序是安全的,哪些是不安全的。
3. 转至**软件管理** > **修补程序**,并将那些不安全的修补程序的**批准状态**定义为**已拒绝**。

手动修补批准

手动修补批准过程如下:

1. 在 安克诺斯数据保护软件 Web 中控台中,转到**软件管理** > **修补程序**。
2. 选择想要安装的修补程序,然后阅读并接受许可协议。
3. 对于批准进行安装的修补程序,将**批准状态**设置为**已批准**。
4. 创建具有已启用的修补程序管理的保护计划模块。可以配置预定或通过单击修补程序管理模块设置中的**立即运行**手动启动计划。

这样,仅批准的修补程序将安装在选定的计算机上。

按需要安装修补程序

根据您的喜好,可以通过三种方式进行手动修补程序安装:

- 转到修补程序列表(**软件管理** > **修补程序**),然后安装必要修补程序。
- 转到漏洞列表(**软件管理** > **漏洞**),然后开始修复过程(其中还包括修补程序安装)。
- 转到设备列表(**设备** > **所有设备**)、选择要更新的特定计算机,然后在这些计算机上安装修补程序。

我们可以从修补程序清单中选择需要安装的修补程序:

1. 在安克诺斯数据保护软件 Web 中控台中，转到**软件管理 > 修补程序**。
2. 接受想要安装的修补程序的许可协议。
3. 选择您要安装的修补程序并单击**安装**。
4. 选择必须要安装修补程序的计算机。
5. 定义在安装修补程序程序后是否进行重新启动。
   - **从不** - 在修补之后，从不会启动重新启动。
   - **如果需要** – 仅在应用修补程序需要重新启动时才重新启动。
   - **始终** – 在修补之后始终进行重新启动。始终可以指定重新启动延迟。

   备份完成之前，请勿重新启动 - 如果备份进程正在运行，则计算机重新启动将延迟到备份完成为止。
6. 单击**安装修补程序**。

选定的修补程序将安装在选定的计算机上。

列表中的修补程序生命周期

要使修补程序列表保持最新，请转到**软件管理 > 修补程序 > 设置**，然后指定**列表中的生命周期**选项。

生命周期列表选项定义检测到的可用修补程序将保持在修补程序列表中多久。通常，如果修补程序已成功安装在检测到缺少修补程序的所有计算机上或者定义的时间已过去，修补程序将从列表中删除。

- **永久** – 修补程序始终保留在列表中。
- **7 天** – 在其首次安装 7 天之后，删除修补程序。

  例如，您有两台必须安装修补程序的计算机。其中一台是联机的，另一台是脱机的。修补程序已安装在第一台计算机上。7 天之后，修补程序将从修补程序列表中删除，即使它没有安装在第二台计算机上，因为它已脱机。
- **30 天** – 在其首次安装 30 天之后，删除修补程序。

智能保护

威胁源

Acronis Cyber Protection Operations Center (CPOC) 会生成仅发送到相关地理区域的安全警告。这些安全警告提供信息涉及恶意软件、漏洞、自然灾害、公共健康和其他类型的可能影响数据保护的全球事件。威胁信息通知您有关所有潜在威胁的信息并允许您阻止它们。

安全警告可以通过由安全专家提供的大量特定操作进行解决。有一些警告只是用于通知您即将到来的威胁的信息，但不提供建议操作。

工作方式

Acronis Cyber Protection Operations Center 会监控外部威胁并生成有关恶意软件、漏洞、自然灾害和公共健康威胁的警报。将可以在 安克诺斯数据保护软件 Web 中控台的**威胁源**部分中查看所有这些警报。您可以根据警报类型执行相应的建议操作。

下图说明了威胁源的主要工作流程。

要对从 Acronis Cyber Protection Operations Center 收到的警报运行建议的操作，请执行以下操作：

1.在 安克诺斯数据保护软件 Web 中控台中，转到**仪表板** > **威胁源**，以查看是否存在任何现有的安全警报。

2.在列表中选择一个警报，然后查看提供的详细信息。

3。单击**开始**以启动向导。

4.启用要执行的操作以及必须将这些操作应用到的目标计算机。建议进行以下操作：

- **漏洞评估** - 扫描选定计算机以查找漏洞
- **修补程序管理** – 在选定的计算机上安装修补程序。
- **反恶意软件保护** – 对选定的计算机运行全面的扫描
- **受保护或不受保护计算机的备份** – 备份受保护/不受保护的计算机

5.单击**开始**。

6.在**活动**页面上，验证活动是否已成功执行。

删除所有警告

在以下时间段后威胁源警告将自动清除：

- 自然灾害 – 1 周
- 漏洞 – 1 个月
- 恶意软件 – 1 个月
- 公共健康 - 1 周

数据保护地图

数据保护地图功能允许您：

- 获取有关计算机上已存储数据(分类、位置、保护状态和其他信息)的信息。
- 检测数据是否受保护。如果数据通过备份得到保护(启用了备份模块的保护计划)，则数据视为受到保护。
- 执行数据保护操作。

工作方式

1. 首先，通过启用数据保护地图模块创建保护计划。
2. 然后，在执行了该计划并且已发现和分析数据后，将在数据保护地图小部件上得到直观的数据保护表示。
3. 还可以转至**设备** > **数据保护地图**，并查找每台设备的不受保护文件的信息。
4. 还可以采取操作来保护在设备上检测到的不受保护的文件。

管理检测到的不受保护文件

要保护检测为不受保护的重要文件，请执行以下操作：

1. 在安克诺斯数据保护软件 Web 中控台中，转到**设备** > **数据保护地图**。
   在设备列表中，可以找到有关不受保护文件的数量、每台设备上此类文件的大小以及上次数据发现的一般信息。
   要保护特定计算机上的文件，请单击省略号图标 (...)，然后单击**保护所有文件**。您将重定向到计划列表，其中可以通过启用备份模块来创建保护计划。
   要从列表中删除具有不受保护文件的特定设备，请单击**隐藏直到下一次数据发现**。
2. 要查看特定设备上不受保护文件的更详细信息，请单击设备名称。
   您将看到每个文件扩展名和每个位置上不受保护文件的列表。您可以按文件扩展名筛选此列表。
3. 要保护所有不受保护文件，请单击**保护所有文件**。您将重定向到计划列表，其中可以通过启用备份模块来创建保护计划。

要以报告形式获取有关不受保护文件的信息，请单击**下载 CSV 格式的详细报告**。

数据保护地图设置

要了解如何创建具有数据保护地图模块的保护计划，请参阅“创建保护计划”。

可以为数据保护地图模块指定以下设置。

预定

可以根据将为数据保护地图执行的任务，定义不同的设置来创建预定。

使用以下事件预定任务运行：

- **按时间预定** - 根据指定时间运行任务。
- **用户登录系统时** - 默认情况下，任何用户登录都会启动任务。可以修改此设置，以便只有特定用户帐户才能触发该任务。
- **用户注销系统时** - 默认情况下，任何用户注销都会启动任务。可以修改此设置，以便只有特定用户帐户才能触发该任务。

  注意
  系统关机时任务将不会运行。关闭和注销在日程安排配置中是不同的事件。

- **系统启动时** - 操作系统启动时运行任务。
- **系统关闭时** - 操作系统关闭时运行任务。

默认设置：**按时间预定**。

预定类型：

- **月** – 选择运行任务的月份和月份中的特定周或特定天。
- **天** – 选择运行任务的特定天。
- **小时** – 选择运行任务的特定天、重复次数和任务运行的时间间隔。

默认设置：**每天**。

开始时间 – 选择任务运行的确切时间。

在日期范围内运行 – 设置配置的计划有效的日期范围。

开始条件 – 定义为了运行任务而应同时满足的所有条件。

用于反恶意软件扫描的开始条件类似于 "开始条件"(第 212 页) 中所描述的备份模块的开始条件。可以定义以下其他开始条件:

- **在时间窗口内分配任务开始时间** - 此选项允许您设置任务的时间范围, 以避免出现网络瓶颈。可以以小时或分钟为单位指定延迟。例如, 如果默认开始时间为上午 10 点, 延迟时间为 60 分钟, 则任务将在上午 10 点到上午 11 点之间开始。
- **如果计算机关闭, 则在计算机启动时运行遗漏的任务**
- **在任务运行期间防止进入睡眠或休眠模式**- 此选项仅对运行 Windows 的计算机有效。
- **如果开始条件不满足, 请务必在以下时间过后运行任务** - 指定任务一定会在其过后启动的时间段, 而不考虑其他开始条件。

扩展名和例外规则

在**扩展名**选项卡上, 可以定义在数据发现期间将视为重要的文件扩展名列表, 并检查它们是否受保护。使用以下格式定义扩展名:

```
.html, .7z, .docx, .zip, .pptx, .xml
```

在**例外规则**选项卡上, 可以定义在数据发现期间不检查其保护状态的文件和文件夹。

- **隐藏文件和文件夹** – 如果选中, 则在数据检查期间将跳过隐藏的文件和文件夹。
- **系统文件和文件夹** – 如果选中, 则在数据检查期间将跳过隐藏的文件和文件夹。

远程桌面访问

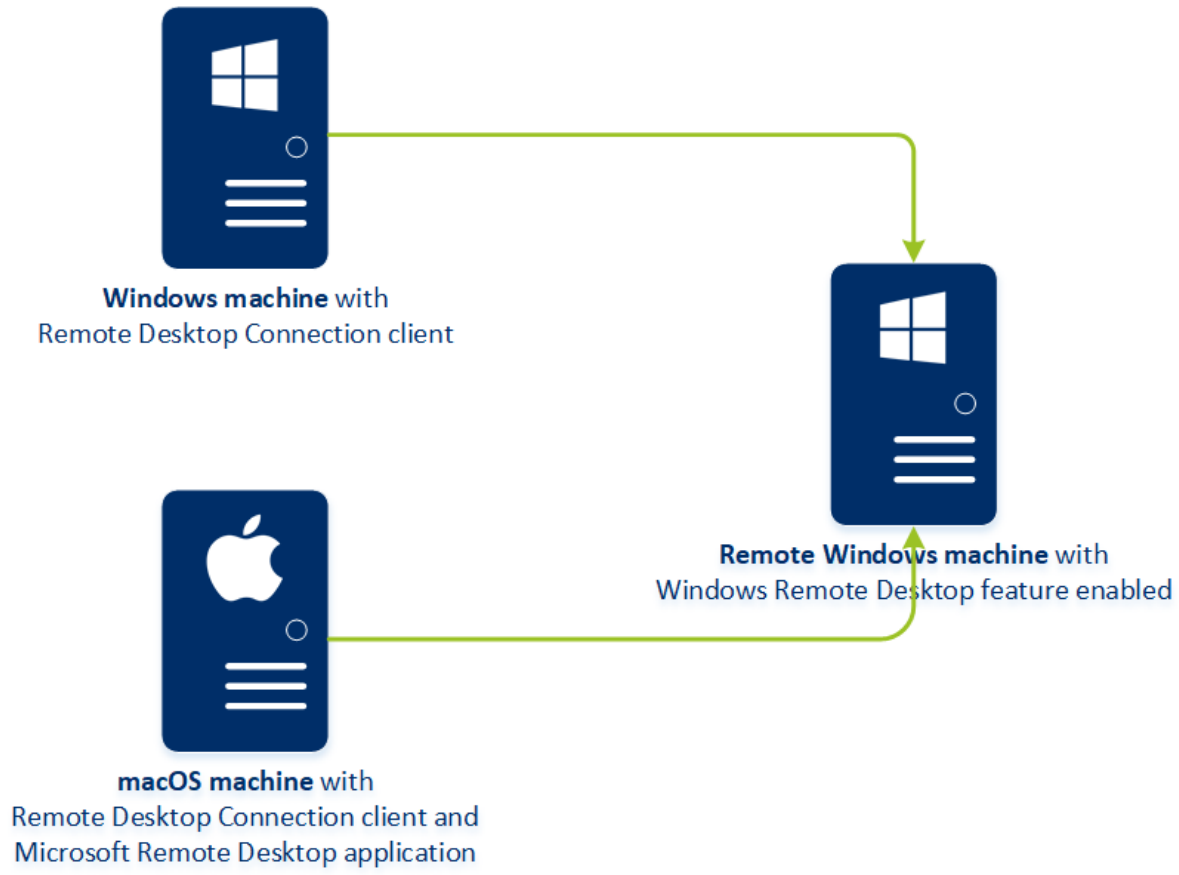
远程服务(RDP 和 HTML5 客户端)

安克诺斯数据保护软件 会为您提供远程访问功能。您可以直接从 Web 中控台远程连接并管理用户计算机。这可使您轻松帮助用户解决其计算机上的问题。

先决条件:

- 保护代理程序已安装在远程计算机上,并已在管理服务器上注册。
- 计算机已获指派适用的 安克诺斯数据保护软件 许可证。
- 启动连接的计算机已安装远程桌面连接客户端。
- 启动 RDP 连接的计算机必须能够通过其主机名访问管理服务器。必须正确配置 DNS 设置,或者必须将管理服务器主机名设置到主机文件中。

可在安装 Windows 和 macOS 的计算机上建立远程连接。



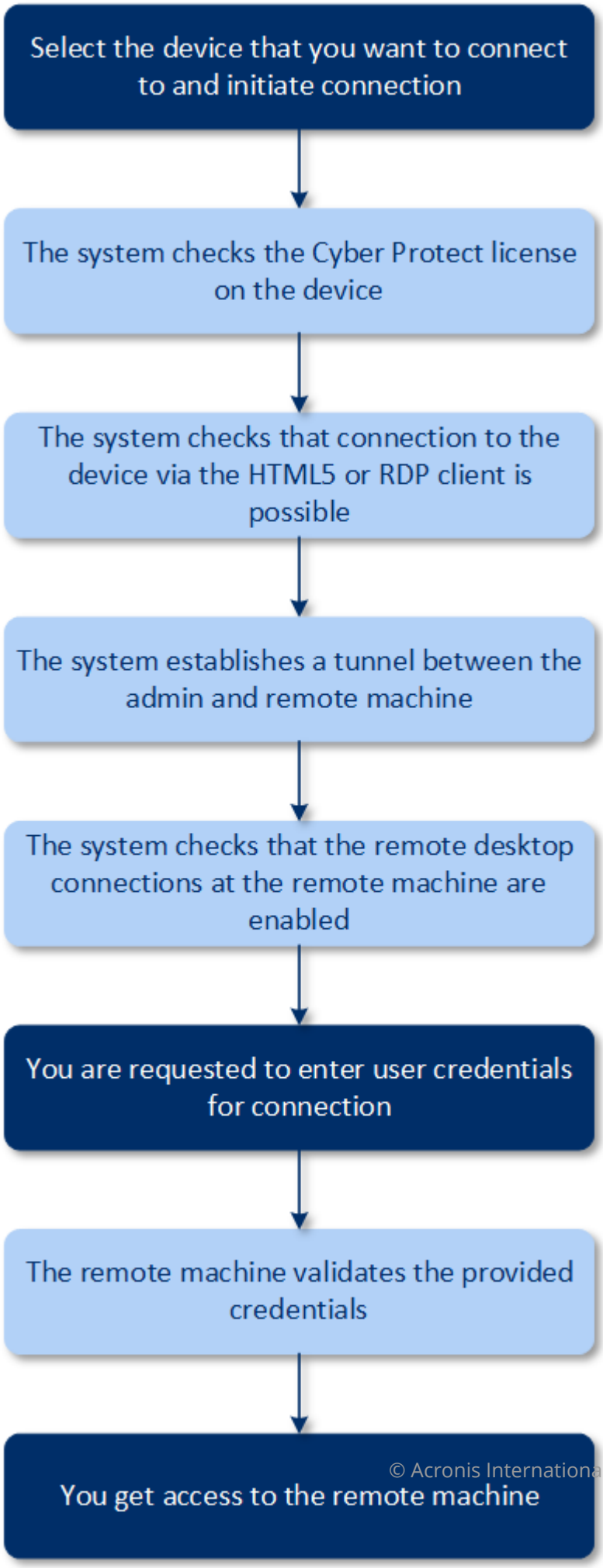
远程服务功能可用于通过可用的 Windows 远程桌面功能连接到 Windows 计算机。这就是为什么无法对 Windows 10 Home 或 macOS 系统进行远程访问。

要建立从 macOS 计算机到远程计算机的连接,请确保在 macOS 计算机上安装以下应用程序:

- 远程桌面连接客户端
- Microsoft 远程桌面连接应用程序

工作方式

如果尝试连接到远程计算机，系统将先检查此计算机是否具有 安克诺斯数据保护软件 许可证。随后，系统将检查是否可以通过 HTML5 或 RDP 客户端进行连接。您通过 RDP 或 HTML5 客户端发起连接。系统会建立到远程计算机的通道，并检查远程计算机是否已启用远程桌面连接。然后输入凭据，验证通过后即可以访问远程计算机。



如何连接到远程计算机

要连接到远程计算机，请执行以下操作：

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设备** > **所有设备**。
2. 单击想要远程连接的计算机，然后单击**网络安全保护桌面** > **通过 RDP 客户端连接**或**通过 HTML5 客户端连接**。

   注意
   仅当管理服务器安装在运行 Linux 的计算机上时，才可以通过 HTML5 客户端进行连接。

3. [可选，仅对于通过 RDP 客户端连接] 下载并安装远程桌面连接客户端。启动到远程计算机的连接。
4. 指定登录名和密码以访问远程计算机然后单击**连接**。

这样您就可以连接到远程计算机并且可以管理它。

共享远程连接

在家工作的员工可能需要访问其办公室的计算机，但贵组织可能未配置用于远程连接的 VPN 或其他工具。安克诺斯数据保护软件 让您可以将 RDP 链接与您的用户共享，从而使他们可以远程访问其计算机。

若要启用共享远程连接功能

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **保护** > **远程连接**。
2. 选择复选框**共享远程桌面连接**。

结果，当在 安克诺斯数据保护软件 Web 中控台中选择一台设备时，将显示**共享远程连接**新选项。

如何与您的用户共享远程连接

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设备** > **所有设备**。
2. 选择要提供远程连接的设备。
3. 请单击**共享远程连接**。
4. 单击**获取链接**。在打开的窗口中，复制生成的链接。该链接可与需要远程访问此设备的用户共享。该链接的有效时间为 10 小时。

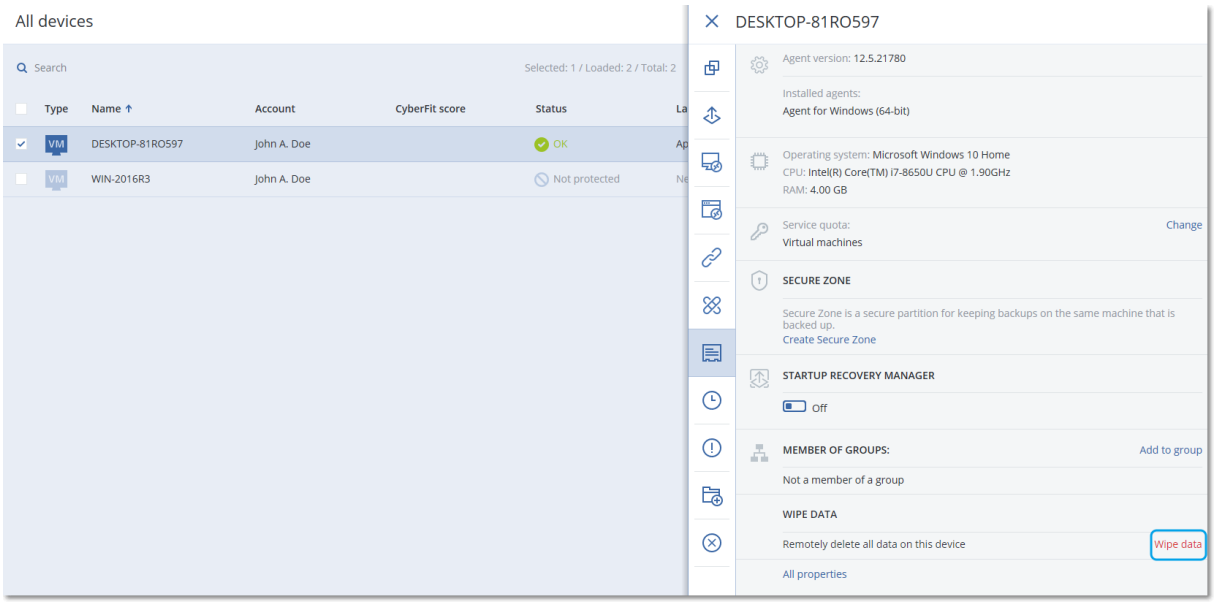
在获取此链接后，您可以通过电子邮件或其他方式与您的用户共享。与链接共享的用户必须单击该链接，然后选择连接类型：

- 通过 RDP 客户端连接。
  此连接将提示您下载并安装远程连接客户端。
- 通过 HTML5 客户端连接。
  此链接不需要在用户计算机上安装任何 RDP 客户端。用户将被重定向到登录屏幕，并且必须输入访问计算机的凭据。

远程擦除

远程擦除允许 安克诺斯数据保护软件 服务管理员和计算机所有者删除所管理计算机上的数据，例如在计算机遗失或被盗的情况下。这样可以阻止在未经授权的情况下访问任何敏感信息。

远程擦除仅适用于运行 Windows 10 的计算机。如需接收擦除指令，计算机必须开启并连接到互联网。



如需从计算机擦除数据

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设备** > **所有设备**。
2. 选择要擦除数据的计算机。

   注意
   一次只能擦除一台计算机的数据。

3. 单击**详细信息**，然后单击**擦除数据**。
   如果您选择的计算机处于脱机状态，则无法使用**擦拭数据**选项。
4. 确认选择。
5. 输入该计算机本地管理员的凭据，然后单击**擦除数据**。

   注意
   如需查看擦除流程的详细信息，以及擦除流程的发起人，可以访问**仪表板** > **活动**。

设备组

设备组主要用于方便地管理大量注册设备。

可以将保护计划应用于组。一旦组中出现新设备，该设备就会受到备份计划保护。如果设备从组中删除，则该设备将不再受到备份计划保护。应用于组的计划无法从组成员中吊销，只能从组本身中吊销。

只有相同类型的设备才能添加到一个组。例如，在 **Hyper-V** 下，可以创建一个 Hyper-V 虚拟机组。在**具有代理程序的计算机**下，可以创建一组安装有代理程序的计算机。在**所有设备**下，无法创建组。

单台设备可以是多个组的成员。

内建组

在注册一台设备后，该设备就会显示在**设备**选项卡上其中一个内建根组中。

*无法*编辑或删除根组。*无法*将备份计划应用于根组。

一些根组包含内建子根组。*无法*编辑或删除这些组。但是，*可以*将备份计划应用于内建子根组。

自定义组

因为每台计算机的角色不同，使用单个保护计划保护内建组中的所有设备可能无法满足需要。每个部门都有特定的备份数据，有些数据需要经常备份，另一些数据则是每年备份两次。因此，您可能需要创建适用于不同计算机组的各种保护计划。在这种情况下，可考虑创建自定义组。

自定义组可包含一个或多个嵌套组。任何自定义组均可编辑或删除。有以下类型的自定义组：

- **静态组**

  静态组包含手动添加的计算机。静态组的内容从不改变，除非您主动添加或删除计算机。

  示例：为财务部创建自定义组，并将会计人员的计算机手动添加到此组。在将保护计划应用于该组时，会计人员的计算机将受到保护。如果聘用了新的会计，您可手动向该组添加新的计算机。
- **动态组**

  动态组包含根据创建组时指定的搜索条件自动添加的计算机。动态组的内容自动改变。在满足指定条件时，计算机仍然留在该组中。

  示例 1：属于财务部的计算机的主机名称包含“财务”一词。将部分计算机名称指定为组成员条件，然后将保护计划应用于该组。如果聘用了新的会计，一旦注册新计算机，就会将该计算机添加到该组，从而实现自动保护。

  示例 2：财务部成立了一个独立的活动目录组织单位 (OU)。将财务组织单位指定为组成员条件，然后将保护计划应用于该组。如果聘用了新的会计，一旦注册新计算机并将其添加到组织单位（无需在意先后顺序），就会将该计算机添加到该组，从而实现自动保护。

创建静态组

1. 单击**设备**，然后选择包含要为其创建静态组的设备的内建组。
2. 单击要在其中创建组的组旁边的齿轮图标。
3. 单击**新建组**。
4. 指定组名称，然后单击**确定**。
   新创建的组将出现在组树中。

将设备添加至静态组

1. 单击**设备**，然后选择要添加到组的一个或多个设备。
2. 单击**添加至组**。
   软件显示一个可以向其中添加所选设备的组的树图。
3. 如果要创建新组，请执行以下操作。否则，请跳过此步骤。
   a. 选择要在其中创建组的组。
   b. 单击**新建组**。
   c. 指定组名称，然后单击**确定**。
4. 选择要向其中添加设备的组，然后单击**完成**。

将设备添加到静态组的另一种方法是选择组，然后单击**添加设备**。

创建动态组

1. 单击**设备**，然后选择包含要为其创建动态组的设备的组。
2. 使用搜索字段搜索设备。可以使用下面所述的多个属性和运算符。
3. 单击搜索字段旁边的**另存为**。

   注意
   某些属性不支持用于组创建。请参阅下面“搜索查询”部分中的表。

4. 指定组名称，然后单击**确定**。

搜索查询

下表汇总了可以在搜索查询中使用的可用属性。

属性	含义	搜索查询示例	支持用于组创建
name	• 物理机的主机名称 • 虚拟机的名称	`name = 'en-00'`	是

属性	含义	搜索查询示例	支持用于组创建
	• 数据库名称 • 邮箱的电子邮件地址		
parameters.MacAddress	MAC 地址。	parameters.MacAddress LIKE '00-22-4D-50-25-E5'	是
comment	设备的注释。它可以自动指定，也可以手动指定。 默认值： • 对于运行 Windows 的物理机，Windows 中的计算机描述会自动复制为注释。该值每 15 分钟同步一次。 • 为其他设备清空。 **注意** 如果在注释字段中手动添加文本，则自动同步 Windows 描述将处于禁用状态。要再次启用它，请清除已添加的注释。 要刷新设备自动同步的注释，请在 **Windows 服务**中重新启动 Managed Machine Service，或在命令提示符下运行以下命令： `net stop mms` `net start mms` 要查看注释，请在**设备**下选择设备，单击**详细信息**，然后查找**注释**部分。 要添加或更改注释，请单击**添加**或**编辑**。 对于已安装保护代理程序的设备，有两个单独的注释字段：	comment = 'important machine' comment = ''(无注释的所有计算机)	是

属性	含义	搜索查询示例	支持用于组创建
	• 代理程序注释 ◦ 对于运行 Windows 的物理机，Windows 中的计算机描述会自动复制为注释。该值每 15 分钟同步一次。 ◦ 为其他设备清空。 **注意** 如果在注释字段中手动添加文本，则自动同步 Windows 描述将处于禁用状态。要再次启用它，请清除已添加的注释。 • 设备注释 ◦ 如果代理程序注释是自动指定的，则它会复制为设备注释。手动添加的代理程序注释不会复制为设备注释。 ◦ 设备注释不会复制为代理程序注释。 设备可以指定一个或两个注释，也可以将它们都保留为空白。如果指定了两个注释，则设备注释优先。 要查看代理程序注释，请在**设置** > **代理程序**下选择具有代理程序的设备、单击**详细信息**，然后查找**注释**部分。 要查看设备注释，请在**设备**下选择相应设备、单击**详细信息**，然后查找**注释**部分。 要手动添加或更改注释，请单击**添加**或**编辑**。		

属性	含义	搜索查询示例	支持用于组创建
ip	IP 地址(仅适用于物理机)。	ip RANGE ('10.250.176.1','10.250.176.50')	是
cpuArch	CPU 架构。 可能的值: • 'x64' • 'x86'	cpuArch = 'x64'	是
memorySize	RAM 大小(以兆字节 MiB 为单位)。	memorySize < 1024	是
cpuName	CPU 名称。	cpuName LIKE '%XEON%'	是
insideVm	内部附带代理程序的虚拟机。 可能的值: • true • false	insideVm = true	是
tzOffset	计算机时区偏移值(以分钟计)。	tzOffset = 120	是
parameters.Architecture	操作系统架构。 可能的值: • 'x86' • 'x64'	parameters.Architecture = 'x86'	是
osName	操作系统名称。	osName LIKE '%Windows XP%'	是
osType	操作系统类型。 可能的值: • 'windows' • 'linux' • 'macosx'	osType IN ('linux', 'macosx')	是
osProductType	操作系统产品类型。 可能的值: • 'dc' 代表域控制器。 • 'server'	osProductType = 'server'	是

属性	含义	搜索查询示例	支持用于组创建
	• 'workstation'		
virtualType	虚拟机类型。 可能的值： • 'vmwesx' VMware 虚拟机。 • 'mshyperv' Hyper-V 虚拟机。 • 'pcs' Virtuozzo 虚拟机。 • 'hci' Virtuozzo Hybrid Infrastructure 虚拟机。 • 'scale' Scale Computing HC3 虚拟机。 • 'ovirt' oVirt 虚拟机	virtualType = 'vmwesx'	是
osSp	操作系统 service pack。	osSp = 1	是
osVersionMajor	操作系统的主版本。	osVersionMajor = 1	是
osVersionMinor	操作系统的次要版本。	osVersionMminor = 1	是
isOnline	计算机可用性。 可能的值： • true • false	isOnline = true	否
tenant	设备所属单元的名称。	tenant = 'Unit 1'	是
tenantId	设备所属单元的标识符。 若要获取单元 ID，在**设备**下，选择该设备，单击**详细信息** > **所有属性**。ID 会显示在 ownerId 字段中。	tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'	是
state	设备状态。 可能的值：	state = 'backup'	否

属性	含义	搜索查询示例	支持用于组创建
	• 'idle' • 'interactionRequired' • 'canceling' • 'backup' • 'recover' • 'install' • 'reboot' • 'failback' • 'testReplica' • 'run_from_image' • 'finalize' • 'failover' • 'replicate' • 'createAsz' • 'deleteAsz' • 'resizeAsz'		
status	资源状态。 可能的值： • 'notProtected' • 'ok' • 'warning' • 'error' • 'critical'	status = 'ok'	否
protectedByPlan	设备受具有给定 ID 的保护计划保护。 若要获取该计划 ID，请单击**计划** > **备份**，选择该计划，在**状态**列中单击图表，然后单击一个状态。系统将创建一个具有该计划 ID 的新搜索。	protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
okByPlan	设备受具有给定 ID 的保护计划保护，并且具有**确定**状态。	okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
errorByPlan	设备受具有给定 ID 的保护计划保护，并且具有**错误**	errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否

属性	含义	搜索查询示例	支持用于组创建
	状态。		
warningByPlan	设备受具有给定 ID 的保护计划保护，并且具有**警告**状态。	warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
runningByPlan	设备受具有给定 ID 的保护计划保护，并且具有**正在运行**状态。	runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
interactionByPlan	设备受具有给定 ID 的保护计划保护，并且具有**需要互动**状态。	interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
ou	属于指定活动目录组织单位的计算机。	ou IN ('RnD', 'Computers')	是
id	设备 ID。 若要获取该设备 ID，在**设备**下，选择该设备，单击**详细信息** > **所有属性**。ID 会显示在 id 字段中。	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	是
lastBackupTime	上次成功备份的日期和时间。 格式为“YYYY-MM-DD HH:MM”。	lastBackupTime > '2022-03-11' lastBackupTime <= '2022-03-11 00:15' lastBackupTime is null	否
lastBackupTryTime	上次备份尝试的时间。 格式为“YYYY-MM-DD HH:MM”。	lastBackupTryTime >= '2022-03-11'	否
nextBackupTime	下次备份的时间。 格式为“YYYY-MM-DD HH:MM”。	nextBackupTime >= '2022-08-11'	否
agentVersion	已安装的保护代理程序的版本。	agentVersion LIKE '12.0.*'	是
hostId	保护代理程序的内部 ID。 要获取保护代理程序 ID，请在**设备**下选择相应计算机，依次单击**详细信息** > **所**	hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	是

属性	含义	搜索查询示例	支持用于组创建
	有属性。使用 agent 属性的“id”值。		
resourceType	资源类型。 可能的值： • 'machine' • 'virtual_machine.vmwesx' • 'virtual_machine.mshyperv' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen'	resourceType = 'machine' resourceType in ('mssql_aag_database', 'mssql_database')	是
hasAsz	在带有 Acronis 安全区 的物理机上的保护代理程序。 可能的值： • true • false	hasAsz=true	是
chassis	计算机底座类型。 可能的值： • unknown • laptop • desktop • server • other	chassis='laptop'	是

注意

如果跳过小时和分钟值，则开始时间视为 YYYY-MM-DD 00:00，结束时间视为 YYYY-MM-DD 23:59:59。例如，lastBackupTime = 2020-02-20，表示搜索结果将包括间隔 lastBackupTime >= 2020-02-20 00:00 和 lastBackup time <= 2020-02-20 23:59:59 之间的所有备份

运算符

下表汇总了可用运算符。

运算符	含义	示例
AND	逻辑与运算符。	name like 'en-00' AND tenant = 'Unit 1'
OR	逻辑或运算符。	state = 'backup' OR state = 'interactionRequired'
IN (<value1>,... <valueN>)	此运算符用于测试一个表达式是否与值列表中的任何值匹配。	osType IN ('windows', 'linux')
NOT	逻辑非运算符。	NOT(osProductType = 'workstation')
NOT IN (<value1>,... <valueN>)	此运算符与 IN 运算符的作用相反。	NOT osType IN ('windows', 'linux')
LIKE 'wildcard pattern'	此运算符用于测试表达式是否与通配符模式相匹配。 可以使用以下通配符运算符: • * 或 % 星号和百分比符号代表零个、一个或多个字符 • _ 下划线代表单个字符	name LIKE 'en-00' name LIKE '*en-00' name LIKE '*en-00*' name LIKE 'en-00_'
RANGE(<starting_value>, <ending_value>)	此运算符用于测试一个表达式是否在一个值范围内(包含范围值)。	ip RANGE ('10.250.176.1','10.250.176.50')
= or ==	等于运算符。	osProductType = 'server'
!= 或 <>	不等于运算符。	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'
<	小于运算符。	memorySize < 1024
>	大于运算符。	diskSize > 300GB
<=	小于或等于运算符。	lastBackupTime <= '2022-05-11 00:15'
>=	大于或等于运算符。	nextBackupTime >= '2022-09-11'

将保护计划应用于组

1. 单击**设备**,然后选择包含要向其应用保护计划的组的内建组。
   软件将显示子组列表。
2. 选择要向其应用保护计划的组。
3. 单击**组备份**。
   软件将显示可应用于组的保护计划列表。
4. 请执行以下任一操作:

- 展开现有保护计划，然后单击**应用**。
- 单击**新建**，然后按照“备份”中所述的步骤创建新的保护计划。

监测和报告

概述 仪表板可让您监控受保护基础架构的当前状态。

报告部分可让您生成关于受保护基础架构的按需和预定报告。只有使用高级许可证才可使用报告部分。

概览仪表板

概览仪表板提供大量可自定义的小部件，这些小组件概述了受保护的基础架构。可以在 20 多个小组件中进行选择，它们显示为饼图、表、图形、条形图和列表。小部件具有可单击元素，可让您调查和解决问题。小部件信息每五分钟更新一次。

使用高级许可证，可以使用 .pdf 或/和 .xlsx 格式下载仪表板的当前状态或通过电子邮件发送它。若要通过电子邮件发送仪表板，请确保已配置**电子邮件服务器**设置。

可用的小组件取决于 安克诺斯数据保护软件 版本。默认小部件如下所示：

小部件	可用性	说明
网络安全保护	在网络备份版本中不可用	显示有关备份大小、被阻止的恶意软件、被阻止的 URL、已发现的漏洞和已安装的修补程序的总体信息。
保护状态	所有版本可用	显示所有计算机的当前保护状态。
活动	所有版本可用	显示在指定时间段内执行的活动的摘要。
活动警告摘要	所有版本可用	按警报类型和严重性显示活动警报的摘要。
修补程序安装状态	在网络备份版本中不可用	显示按修补程序安装状态分组的计算机数量。
按类别划分的缺少更新	在网络备份版本中不可用	显示计算机按类别划分的缺少更新数量。
磁盘运行状况状态	在网络备份版本中不可用	按状态显示磁盘数量。
设备	所有版本可用	显示环境中设备的相关详细信息。
活动警告详细信息	所有版本可用	显示活动警报的相关详细信息。
现有漏洞	所有版本可用	显示环境中操作系统和应用程序以及受影响的计算机的现有漏洞。
修补程序安装历史记录	在网络备份版本中不可用	显示已安装修补程序的相关详细信息。
最近受影响	所有版本可用	显示关于最近被感染计算机的详细信息
位置汇总	所有版本可用	显示关于备份位置的详细信息

添加小部件的步骤

单击**添加小部件**，然后执行以下任一操作：

- 单击要添加的小部件。将使用默认设置添加小部件。
- 要在添加小部件之前对其进行编辑，请在选中小部件时单击铅笔图标。在完成编辑小部件后，单击**完成**。

在仪表板上重新排列小部件的步骤

通过单击小部件名称即可对其进行拖放。

编辑小部件的步骤

单击小部件名称旁边的铅笔图标。编辑小部件可对其重命名、更改时间范围、设置过滤器以及对行分组。

删除小部件的步骤

单击小部件名称旁边的 X 符号。

Cyber Protection

该小部件显示有关备份大小、被阻止的恶意软件、被阻止的 URL、已发现的漏洞和已安装的修补程序的总体信息。

上排显示当前统计数据：

- **今天已备份** - 过去 24 小时内恢复点大小的总和
- **被阻止的恶意软件** - 有关被阻止的恶意软件的当前活动警告数量
- **被阻止的 URL** - 被阻止的 URL 的当前活动警告数量
- **现有漏洞** - 当前存在的漏洞数量
- **准备安装的修补程序** - 当前可安装的修补程序数量

下排显示总体统计数据：

- 所有备份的压缩大小
- 所有计算机上被阻止的恶意软件数量
- 所有计算机上被阻止的 URL 数量
- 所有计算机上发现的漏洞数量
- 所有计算机上已安装的更新/修补程序数量

保护状态

保护状态

该小部件显示所有计算机的当前保护状态。

计算机可以为下列状态之一：

- **受保护** - 计算机已应用保护计划。
- **不受保护** - 计算机未应用保护计划。这包括未应用保护计划的已发现计算机和受控计算机。

- **受控** - 计算机已安装保护代理程序。
- **已发现** - 计算机未安装保护代理程序。

如果单击相应计算机状态，系统会将您重定向到具有此状态的计算机列表，以获取更多详细信息。

发现的计算机

该小部件显示在指定时间范围内发现的计算机列表。

磁盘运行状况监视

磁盘运行状况监控提供有关当前磁盘状态及其预测的信息，这样您可以防止可能与磁盘故障相关的数据丢失。HDD 和 SSD 磁盘均受支持。

限制：

- 仅对于运行 Windows 的计算机支持磁盘运行状况预测。
- 只监控物理机的磁盘。虚拟机的磁盘无法进行监控并且不会显示在磁盘运行状况小部件中。
- 不支持 RAID 配置。
- 在 NVMe 驱动器上，仅对于通过 Windows API 传输 SMART 数据的驱动器支持磁盘运行状况监控。对于需要直接从驱动器读取 SMART 数据的 NVMe 驱动器，磁盘运行状况监控不受支持。

磁盘运行状况可以表示为以下状态之一：

- **正常**
  磁盘运行状况为 70% 和 100% 之间。
- **警告**
  磁盘运行状况为 30% 和 70% 之间。
- **严重**
  磁盘运行状况为 0% 和 30% 之间。
- **计算磁盘数据**
  正在计算当前磁盘状态和预测

工作方式

“磁盘运行状况预测服务”使用基于人工智能的预测模型。

1. 保护代理程序会收集磁盘的 SMART 参数，并将此数据传递给“磁盘运行状况预测服务”：
   - SMART 5 - 重新分配的扇区数。
   - SMART 9 - 开机时间。
   - SMART 187 - 报告的无法修正错误。
   - SMART 188 - 命令超时。
   - SMART 197 - 当前待处理的扇区数。
   - SMART 198 - 无法修正的脱机扇区数。
   - SMART 200 - 写入错误率。
2. “磁盘运行状况预测服务”会处理收到的 SMART 参数、进行预测并提供以下磁盘运行状况特征：

- 磁盘运行状况当前状态:正常、警告、严重。
- 磁盘运行状况预测:负面、稳定、正面。
- 磁盘运行状况预测概率(百分比形式)。

预测期始终为一个月。

3. 监视服务接收这些特征,然后在 安克诺斯数据保护软件 web 中控台的磁盘运行状况小组件中显示相关信息。

磁盘运行状况小部件

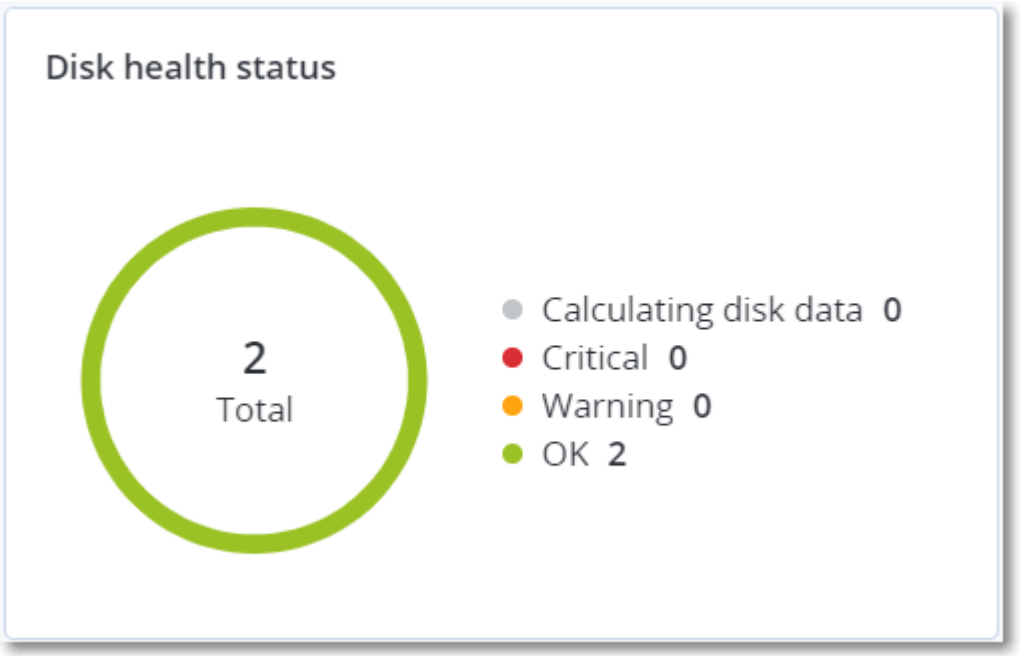
磁盘运行状况监控的结果显示在 安克诺斯数据保护软件 web 中控台中可用的以下小组件中:

- **磁盘运行状况概述**是一个树形图小部件,具有可以通过向下钻取来切换的两个级别的详细信息。
  - 计算机级别
    显示与选定组织单元的所有计算机有关的磁盘状态的概要信息。仅显示最严重的磁盘状态。将光标悬停在特定块上时,其他状态会显示在工具提示中。计算机块的大小取决于该计算机所有磁盘的总大小。计算机块的颜色取决于找到的最严重磁盘状态。

- 磁盘级别
  显示选定计算机的所有磁盘的当前磁盘运行状况状态。每个磁盘块显示以下任一磁盘运行状况预测及其可能性(百分比):
  - 将降级
  - 将保持稳定

- 将得到改进

- **磁盘运行状况状态**是一个饼图小部件，显示每个状态的磁盘数量。



磁盘运行状况状态警告

磁盘运行状况检查每 30 分钟运行一次，同时每天生成一次相应警告。当磁盘运行状况从 **警告** 更改为 **严重** 时，始终会生成警报。

警告名称	严重性	磁盘运行状况状态	说明
磁盘可能发生故障	警告	(30 – 70)	此计算机上的 <磁盘名称> 磁盘将来可能会发生故障。尽快运行该磁盘的完整映像备份、替换该磁盘，然后将映像恢复到新磁盘。
磁盘即将发生故障	重大	(0 – 30)	此计算机上的 <磁盘名称> 磁盘处于严重状态，很可能即将发生故障。目前不建议对该磁盘进行映像备份，因为增加的压力可能会导致磁盘发生故障。立即备份该磁盘上最重要的文件并替换该磁盘。

数据保护地图

数据保护地图功能允许您查找所有对您重要的数据，并在树形图可伸缩视图中获取有关所有重要文件的数量、大小、位置、保护状态的详细信息。

每个块的大小取决于属于组织单元/计算机的所有重要文件的总数/大小。

文件可以具有以下保护状态之一：

- **严重** - 有 51-100% 的不受保护文件（具有您指定的扩展名）未针对选定计算机/位置进行备份，并且将不会使用现有备份设置进行备份。
- **低** - 有 21-50% 的不受保护文件（具有您指定的扩展名）未针对选定计算机/位置进行备份，并且将不会使用现有备份设置进行备份。
- **中** - 有 1-20% 的不受保护文件（具有您指定的扩展名）未针对选定计算机/位置进行备份，并且将不会使用现有备份设置进行备份。
- **高** - 所有具有您指定扩展名的文件都已针对选定计算机/位置进行了保护（备份）。

数据保护检查的结果可以在“数据保护地图”小部件（一个树形图小部件，在计算机级别显示详细信息）的仪表板上找到：

将鼠标悬停在彩色块上可查看有关不受保护文件数量及其位置的信息。要保护它们，请单击**保护所有文件**。

漏洞评估小部件

易受攻击的计算机

该小部件按漏洞严重程度显示易受攻击的计算机。

根据通用漏洞评分系统 (CVSS) v3.0，发现的漏洞可能具有以下严重级别之一：

- 已保护：未发现任何漏洞
- 严重：9.0 - 10.0 CVSS
- 高：7.0 - 8.9 CVSS
- 中：4.0 - 6.9 CVSS
- 低：0.1 - 3.9 CVSS
- 无：0.0 CVSS

现有漏洞

该小部件显示计算机上当前存在的漏洞。在**现有漏洞**小组件中，有两列显示时间戳：

- **第一次检测** - 在计算机上最初检测到漏洞的日期和时间。
- **上次检测** - 在计算机上上次检测到漏洞的日期和时间。

修补程序安装小部件

具有四个与修补程序管理功能相关的小部件。

修补程序安装状态

该小部件显示按修补程序安装状态分组的计算机数量。

- **已安装** - 所有可用修补程序都已安装在计算机上
- **需要重新启动** - 安装修补程序后，计算机需要重新启动
- **失败** - 修补程序无法安装在计算机上

修补程序安装摘要

该小部件按修补程序安装状态显示计算机上修补程序的摘要。

修补程序安装历史记录

此小部件显示有关计算机上安装的修补程序的详细信息。

按类别划分的缺少更新

该小部件显示每个类别缺少的更新数量。显示以下类别：

- 安全更新
- 重要更新
- 其他

备份扫描详细信息

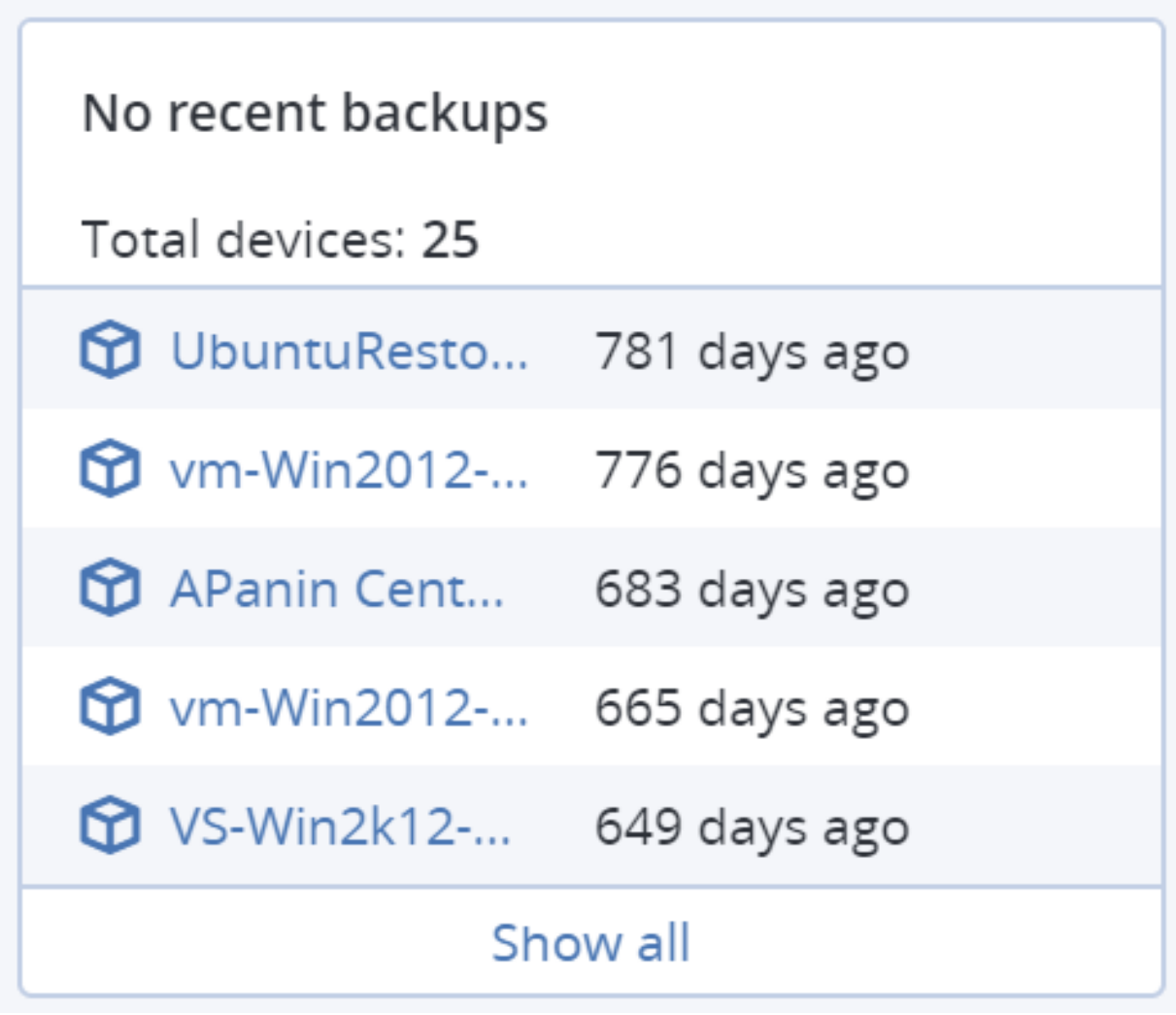
只有在管理服务器上安装了扫描服务时，此小组件才可用。该小部件显示有关在备份中检测到的威胁的详细信息。

最近受影响

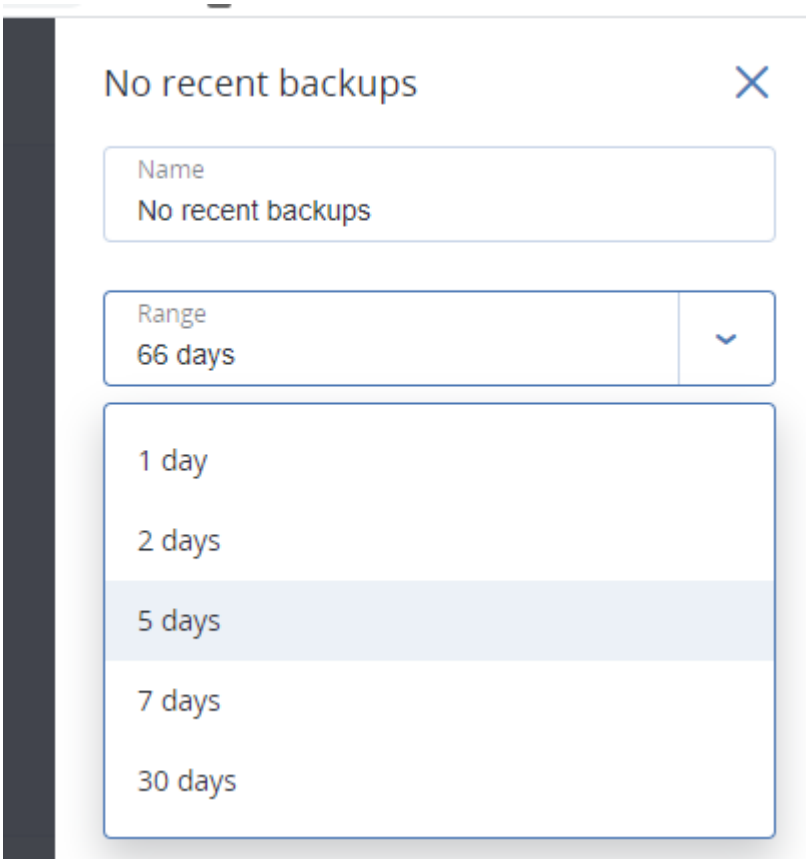
该小部件显示有关最近被感染计算机的详细信息。此处可以找到有关检测到的威胁以及被感染文件数量的信息。

无最近备份

此小组件将显示已应用保护计划的工作负载，其上次成功备份日期早于小组件设置中所指定的时间范围。



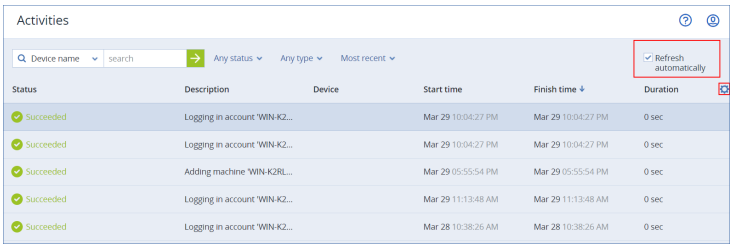
默认情况下，当添加此小组件时，它会显示过去 5 天的信息。可以使用下拉菜单选择另一个期间，也可以手动输入天数。可以输入的最大天数为 180。



“活动”选项卡

活动选项卡会提供过去 90 天内的活动概述。

要自定义**活动**选项卡的视图，请单击相应齿轮图标，然后选择要查看的列。要实时查看活动进度，请选中**自动刷新**复选框。请注意，频繁更新多个活动可能会降低管理服务器的性能。



可以按以下条件搜索列出的活动：

- **设备名称**
  这是在其上执行活动的计算机。
- **发起者**
  这是发起活动的帐户。

还可以按以下属性过滤活动：

- **状态**
  例如，成功、失败、正在进行、已取消。
- **类型**
  例如，应用计划、删除备份、安装软件更新。
- **时间**
  例如，最近的活动、过去 24 小时内的活动或默认保留期内特定时段内的活动。

要更改默认保留期，请编辑 task_manager.yaml 配置文件。

更改保留期

1. 在运行管理服务器的计算机上，在文本编辑器中打开以下配置文件：
   - 在 Windows 中：`%Program Files%\Acronis\TaskManager\task_manager.yaml`
   - 在 Linux 中：`/usr/lib/Acronis/TaskManager/task_manager.yaml`
2. 找到以下部分：

```
database:
  connection-string:""
  run-cleanup-at:"23:59"
  cleanup-batch-size:10
  max-cleanup-retries:10
  log-queries:false
  max-transaction-retries: 10
  shards:
   - connection-string: sqlite://task-manager.sqlite
     days-to-keep: 90
     space: "default"
     key: "00000000-0000-0000-0000-000000000000"
```

3. 根据需要编辑 `days-to-keep` 行。
   例如：

```
days-to-keep:30
```

   注意
   可以根据需要更改保留期。提高保留期会降低管理服务器的性能。

4. 重新启动 **Acronis Service Manager 服务**，如 "重新启动 Acronis Service Manager 服务"(第 175 页) 中所述。

报告

您可以使用预定义的报告或创建自定义报告。报告可以包括任何一组仪表板小组件。

您只能为您管理的单位配置报告。

可以通过电子邮件发送报告或按时间表下载报告。若要通过电子邮件发送报告，请确保已配置**电子邮件服务器**设置。如果要使用第三方软件处理报告，则预定以 .xlsx 格式将报告保存至特定文件夹。

可用报告取决于您的 安克诺斯数据保护软件 版本。默认报告如下所示：

报告名称	可用性	说明
警告	Cyber Backup Advanced 安克诺斯数据保护软件 Advanced	显示某一指定时间段内发生的警告。
备份扫描详细信息	安克诺斯数据保护软件 Advanced	显示有关备份中检测到威胁的详细信息。
备份	Cyber Backup Advanced 安克诺斯数据保护软件 Advanced	显示关于当前备份和恢复点的详细信息。
当前状态	Cyber Backup Advanced 安克诺斯数据保护软件 Advanced	显示环境的当前状态。
每日活动	Cyber Backup Advanced 安克诺斯数据保护软件 Advanced	显示某一指定时间段内已执行的磁带活动的摘要。
数据保护地图	安克诺斯数据保护软件 Advanced	显示有关计算机上所有重要文件的数量、大小、位置、保护状态的详细信息。
检测到威胁	Cyber Backup Advanced 安克诺斯数据保护软件 Advanced	按受阻止威胁的数量显示受影响计算机的详细信息，以及运行状况良好和易受攻击的计算机的详细信息。
发现的计算机	Cyber Backup Advanced 安克诺斯数据保护软件 Advanced	显示在组织网络中发现的所有计算机。
磁盘运行状况预测	安克诺斯数据保护软件 Advanced	显示 HDD/SSD 故障发生时间预测和当前磁盘状态。
现有漏洞	Cyber Backup	显示环境中操作系统和应用程序以及受影响的计算机的

	Advanced 安克诺斯数据保护软件 Advanced	现有漏洞。
许可证	Cyber Backup Advanced 安克诺斯数据保护软件 Advanced	显示可用许可证的摘要。
位置	Cyber Backup Advanced 安克诺斯数据保护软件 Advanced	显示某一指定时间段内备份位置的使用情况统计数据
修补程序管理摘要	安克诺斯数据保护软件 Advanced	显示缺少的修补程序、已安装的修补程序和适用的修补程序的数量。可以深入了解报告以获取缺少/已安装修补程序的信息以及所有系统的详细信息。
概要	Cyber Backup Advanced 安克诺斯数据保护软件 Advanced	显示有关某一指定时间段内受保护设备的概要信息。
磁带活动	Cyber Backup Advanced 安克诺斯数据保护软件 Advanced	显示在过去 24 小时内使用的磁带的列表。
每周活动	Cyber Backup Advanced 安克诺斯数据保护软件 Advanced	显示在指定时间段内执行的活动的摘要。

对报告的基本操作

- 要查看报告，请单击其名称。
- 要使用报告进行其他操作，请单击报告行上的省略号图标 (...)。
  可从报告中访问相同的操作。

若要添加报告

1. 单击**添加报告**。
2. 请执行以下任一操作：
   - 要添加预定义的报告，请单击其名称。
   - 若要添加自定义报表，请单击**自定义**。名称为**自定义**的新报告将添加到报告列表中。打开此报表并向其添加小组件。

3. [可选] 拖放小部件即可重新排列它们。
4. [可选] 按照下面的描述编辑报告。

若要编辑报告

1. 单击保护计划名称旁边的省略号图标 (...), 然后单击**编辑**。
2. 编辑报告。您可以:
   - 重命名报告
   - 为报告中包含的所有小部件更改时间范围
   - 预定通过电子邮件以 .pdf 或/和 .xlsx 格式发送报告
3. 单击**保存**。

若要安排报告

1. 选择一个报告, 然后单击**时间表**。
2. 启用**发送预定报告**开关。
3. 选择是通过电子邮件发送报告、将报告保存至文件夹, 还是两者均选。根据您的选择, 指定电子邮件地址、文件夹路径或两者均指定。
4. 选择报告格式:.pdf、.xlsx 或两者均选。
5. 选择报告期间:1 天、7 天或 30 天。
6. 选择发送或保存报告的日期和时间。
7. 单击**保存**。

导出和导入报告结构

可以将报告结构(一组小组件集和预定设置)导出和导入到一个 .json 文件。这在重新安装管理服务器或将报告结构复制到其他管理服务器的情况下可能有用。

若要导出报告结构, 请选择一个报告, 然后单击**导出**。

若要导入报告结构, 请单击**创建报告**, 然后单击**导入**。

转储报告数据

可以将报告数据转储保存至 .csv 文件中。转储包括自定义时间范围内的所有报告数据(未筛选)。

软件随时生成数据转储。如果您指定一长段时间, 则此操作可能需要很长时间。

转储报告数据

1. 选择一个报告, 然后单击**打开**。
2. 单击右上角的省略号图标 (...), 然后单击**转储数据**。
3. 在**位置**中, 为 .csv 文件指定文件夹路径。
4. 在**时间范围**中, 指定时间范围。
5. 单击**保存**。

配置警告严重性

警告是提醒实际或潜在问题的消息。您可以不同方式使用警告：

- 您可以通过**概述**选项卡的**警告**部分监控当前警告，快速识别和解决发现的问题。
- 在**设备**下，系统根据警告评估设备状态。**状态**列可让您过滤存在问题的设备。
- 当配置电子邮件通知时，可以选择将触发警告的通知。

警告可能具有以下某种严重性级别：

- **严重**
- **错误**
- **警告**

您可以按照下文所述，使用警告配置文件更改警告的严重性级别或彻底禁用警告。此操作需要重新启动管理服务器。

更改警告的严重性级别不会影响已经生成的警告。

警告配置文件

配置文件位于运行管理服务器的计算机上。

- 在 Windows 中：<安装路径>**\AlertManager\alert_manager.yaml**
  其中，<安装路径> 是管理服务器的安装路径。默认情况下，它是 **%ProgramFiles%\Acronis**。
- 在 Linux 中：**/usr/lib/Acronis/AlertManager/alert_manager.yaml**

此文件结构为 YAML 文件。每个警报都是 `alertTypes` 列表中的一个元素。

`name` 键标识警报。

`severity` 键定义警报严重性。它必须具有以下值之一：`critical`、`error` 或 `warning`。

可选的 `enabled` 键定义是启用还是禁用警报。其值必须是 `true` 或 `false`。默认条件下（无此键）启用所有警告。

更改警告严重性或禁用警告

1. 在安装了管理服务器的计算机上，在文本编辑器中打开 **alert_manager.yaml** 文件。
2. 找到想要更改或禁用的警告。
3. 请执行以下任一操作：
   - 要更改警报严重性，请更改 `severity` 键的值。
   - 要禁用警报，请添加 `enabled` 键，然后将其值设置为 `false`。
4. 保存文件。
5. 如下所述，重新启动管理服务器服务。

在 Windows 中重新启动管理服务器服务

1. 在**开始**菜单中，单击**运行**，然后键入：**cmd**
2. 单击**确定**。
3. 运行以下命令：

```
net stop acrmngsrv
net start acrmngsrv
```

在 Linux 中重新启动管理服务器服务

1. 打开**终端**。
2. 在任何目录中运行以下命令：

```
sudo service acronis_ams restart
```

高级存储选项

磁带设备

以下章节详细说明了如何使用磁带设备存储备份。

什么是磁带设备?

磁带设备泛指磁带库或独立磁带驱动器。

磁带库(自动库)是一个高容量的存储设备,其中包含:

- 一个或多个磁带驱动器
- 多个用来安装磁带的插槽(多达几千个)
- 一个或多个转换器(自动装置),用于在插槽和磁带驱动器之间移动磁带。

磁带库还可能包含其他组件,如条码阅读器或条码打印机。

自动磁带加载机是一个磁带库的特例。它包含一个驱动器、多个插槽、一个转换器和一个条码阅读器(可选)。

独立磁带驱动器(也称**流转化器**)包含一个插槽,一次只能安装一个磁带。

磁带支持概述

保护代理程序可以直接或借助存储节点将数据备份到磁带设备。两种方式都可以确保磁带设备全自动操作。连接到存储节点的磁带设备具有多个驱动器时,可以将多个代理程序同时备份到磁带。

与 RSM 和第三方软件的兼容性

与第三方软件的共存情况

不能在安装了专有磁带管理工具的第三方软件的计算机上使用磁带。若要在此类计算机上使用磁带,您需要卸载或停用第三方磁带管理软件。

与 Windows 可移动存储管理器 (RSM) 的交互

保护代理程序和存储节点不使用 RSM。检测磁带设备时,它们会禁用 RSM 的设备(除非其他软件正在使用)。如果希望使用磁带设备,请确保用户或第三方软件都不启用 RSM 中的设备。如果 RSM 中已启用磁带设备,则重复磁带设备检测操作。

支持的硬件

Acronis 安克诺斯数据保护软件 支持外部 SCSI 设备。这些设备连接至光纤通道或使用 SCSI、iSCSI、串行连接 SCSI (SAS) 接口。另外,Acronis 安克诺斯数据保护软件 还支持 USB 连接的磁带设备。

在 Windows 中，即使未安装设备转换器的驱动程序，Acronis 安克诺斯数据保护软件 也可以备份到磁带设备。这样的磁带设备在**设备管理器**中显示为**未知媒体转换器**。但是，必须安装设备驱动器的驱动程序。在 Linux 和可启动媒体下面，没有驱动程序时，无法备份到磁带设备。

不保证识别 IDE 或 SATA 连接的设备。这取决于操作系统中是否安装了适当的驱动程序。

要了解您的特定设备是否受支持，请使用 http://kb.acronis.com/content/57237 中所述的硬件兼容性工具。欢迎您向 发送有关测试结果的报告。硬件兼容性列表中列出了已确认支持的硬件：https://go.acronis.com/acronis-cyber-protect-advanced-tape-hcl。

磁带管理数据库

连接至计算机的所有磁带设备的信息存储在磁带管理数据库中。默认数据库路径如下所示：

- 在 Windows XP/Server 2003 中：`%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ARSM\Database`。
- 在 Windows 7 及更高版本的 Windows 中：`%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database`.
- 在 Linux 中：`/var/lib/Acronis/BackupAndRecovery/ARSM/Database`。

数据库大小取决于存储在磁带上的备份数量，每一百个备份约等于 10 MB。如果磁带库中含有数千个备份，则数据库可能会很大。在此情况下，您可能想要在不同的卷上存储磁带数据库。

在 Windows 中迁移数据库：

1. 停止 可移动存储管理服务。
2. 将所有文件从默认位置移至新位置。
3. 找到注册表项 `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings`。
4. 在注册表值 `ArsmDmlDbProtocol` 中指定新的位置路径。此字串最多可包含 32765 个字符。
5. 启动 可移动存储管理服务。

在 Linux 中迁移数据库：

1. 停止 `acronis_rsm` 服务。
2. 将所有文件从默认位置移至新位置。
3. 在文本编辑器中打开配置文件 `/etc/Acronis/ARSM.config`。
4. 找到行 `<value name="ArsmDmlDbProtocol" type="TString">`。
5. 更改此行下方的路径。
6. 保存文件。
7. 启动 `acronis_rsm` 服务。

TapeLocation 文件夹

`TapeLocation` 文件夹包含磁带上备份的所有卷的文件系统元数据的缓存。

默认 `TapeLocation` 文件夹路径为：

- 在 Windows XP/Server 2003 中：`%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation`

- 在 Windows 7 及更高版本中：`%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation`
- 在 Linux 中：`/var/lib/Acronis/BackupAndRecovery/TapeLocation`

`TapeLocation` 文件夹大小约为存储在磁带上的所有备份大小的 0.5-1%。对于启用了文件恢复选项的磁盘级别备份，`TapeLocation` 文件夹大小可能稍大一些，具体取决于备份文件的数量。

用于写入磁带的参数

磁带写入参数（块大小和缓存大小）允许您微调软件来实现最大性能。写入磁带需要这两个参数，但通常您只需要调整块大小。最佳值取决于磁带设备类型以及要备份的数据，例如文件数目及其大小。

注意
当软件从磁带读取数据时，它使用写入磁带时所使用的相同块大小。如果磁带设备不支持此块大小，读取将失败。

这些参数在附加磁带设备的每台计算机上进行设置。它可以是一台装有代理程序或存储节点的计算机。在运行 Windows 的计算机上，在注册表中执行此配置；在 Linux 计算机上，在配置文件 **/etc/Acronis/BackupAndRecovery.config** 中执行此配置。

在 Windows 中，创建相应的注册表项及其 DWORD 值。在 Linux 中，在配置文件末尾且紧挨在 `</registry>` 标记之前添加以下文本：

```
<key name="TapeLocation">
     <value name="WriteCacheSize" type="Dword">
          "value"
     </value>
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
</key>
```

DefaultBlockSize

这是写入磁带时所使用的块大小（以字节为单位）。

*可能的值：*0、32、64、128、256、512、1024、2048、4096、8192、16384、32768、65536、131072、262144、524288、1048576。

如果值为 0 或参数不存在，块大小将以如下方式确定：

- 在 Windows 中，值从磁带设备驱动程序中提取。
- 在 Linux 中，该值为 **64 KB**。

*注册表项（在运行 Windows 的计算机上）：***HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\DefaultBlockSize**

/etc/Acronis/BackupAndRecovery.config 中的行（在运行 Linux 的计算机上）：

```
<value name=DefaultBlockSize" type="Dword">
     "value"
</value>
```

如果磁带驱动器不接受指定值，软件会将其除以二，直到得到适用的值或值为 32 字节。如果未找到适用的值，软件会将指定值乘以二，直到得到适用的值或值为 1 MB。如果驱动器不接受任何值，则备份将失败。

WriteCacheSize

这是写入磁带时所使用的缓冲区大小(以字节为单位)。

*可能的值:*0、32、64、128、256、512、1024、2048、4096、8192、16384、32768、65536、131072、262144、524288、1048576，但不小于 **DefaultBlockSize** 参数值。

如果值为 0 或该参数不存在，则缓冲区大小为 **1 MB**。如果操作系统不支持此值，则软件会将其除以二，直到找到适用的值或达到 **DefaultBlockSize** 参数值。如果未找到操作系统支持的值，备份将失败。

注册表项(在运行 Windows 的计算机上)：
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\WriteCacheSize

/etc/Acronis/BackupAndRecovery.config 中的行(在运行 Linux 的计算机上)：

```
<value name="WriteCacheSize" type="Dword">
     "value"
</value>
```

如果您指定不受操作系统支持的非零值，备份将失败。

磁带相关备份选项

可以配置**磁带管理**备份选项来确定以下各项：

- 是否启用从存储在磁带上的磁盘级备份进行文件恢复。
- 保护计划完成后是否将磁带返回至插槽。
- 备份完成后是否弹出磁带。
- 是否使用可用磁带进行完整备份。
- 创建完整备份时是否覆盖磁带(仅限单机版磁带驱动器)。
- 是否使用磁带集来区分用于在一周的不同天所创建的备份或用于不同计算机类型的备份的磁带。

并行操作

Acronis 安克诺斯数据保护软件 可以使用磁带设备的各种组件同步执行操作。在使用驱动器的操作(备份、恢复、重新扫描或擦除)过程中，可以启动使用转换器的操作(移动磁带到其他插槽，或弹出

磁带)，反之亦然。如果磁带库具有多个驱动器，在使用其中一个驱动器的操作中，您还可以启动使用其他驱动器的操作。例如，使用相同磁带库的不同驱动器，可以同步备份或恢复多个计算机。

检测新磁带设备操作可以与任何其他操作同步进行。在清查过程中，不能进行任何其他操作，检测新磁带设备除外。

无法并行执行的操作排入队列。

限制

磁带设备的使用存在以下限制：

1. 计算机从基于 Linux 的 32 位可启动媒体启动时，不支持磁带设备。
2. 无法将以下数据类型备份到磁带：Microsoft 365 邮箱、Microsoft Exchange 邮箱。
3. 无法创建物理机和虚拟机的应用程序感知备份。
4. 在 macOS 中，仅支持文件级备份到基于磁带的受控位置。
5. 磁带上的备份不能进行合并。因此，备份到磁带时，**始终增量**备份方案不可用。
6. 磁带上的备份不能进行重复数据删除。
7. 如果磁带包含非删除备份，或者在其他磁带上具有从属备份，则软件不能自动覆盖该磁带。
   此规则的唯一例外是当启用了“创建完整备份时覆盖独立磁带驱动器中的磁带”时。
8. 如果恢复备份需要重启操作系统，则不能在该操作系统下恢复存储在磁带上的备份。使用可启动媒体进行此类恢复。
9. 您可以验证磁带上存储的任何备份，但您不能选择验证整个基于磁带的位置或磁带设备。
10. 基于磁带的受控位置不能进行加密保护。相反，可加密您的备份。
11. 软件不能将一个备份同时写入多个磁带，也不能将多个备份同时通过同一驱动器写入同一磁带。
12. 不支持使用网络数据管理协议 (NDMP) 的设备。
13. 不支持条码打印机。
14. 不支持线性磁带文件系统 (LTFS) 格式化的磁带。

由较早版本 Acronis 产品写入的磁带的可读性

下表汇总了由 Acronis True Image Echo、Acronis True Image 9.1、Acronis Backup & Recovery 10、Acronis Backup & Recovery 11 和 Acronis 安克诺斯数据保护软件 中的 Acronis Backup 11.5、11.7 和 12.5 产品系列写入的磁带的可读性。此表还说明了由 Acronis 安克诺斯数据保护软件 的各个组件写入的磁带的兼容性。

可以将增量备份和差异备份附加到由 Acronis Backup 11.5、11.7 和 12.5 创建的经重新扫描的备份。

	...在连接到装有以下产品的计算机的磁带设备上可读...			
	Acronis 安克诺斯数	Acronis 安克诺斯数据	Acronis 安克诺斯数	Acronis 安克诺斯数

			据保护软件 可启动媒体	保护软件 适用于 Windows 的代理程序	据保护软件 适用于 Linux 的代理程序	据保护软件 存储节点
由以下产品在本地连接的磁带设备(磁带驱动器或磁带库)上写入的磁带...	可启动媒体	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/Acronis Backup 11.5/11.7/12.5	+	+	+	-
	适用于 Windows 的代理程序	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/Acronis Backup 11.5/11.7/12.5	+	+	+	-
	适用于 Linux 的代理程序	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/Acronis Backup 11.5/11.7/12.5	+	+	+	-
通过以下产品在磁带设备上写入的磁带...	备份服务器	9.1	-	-	-	-
		Echo	-	-	-	-
	存储节点	ABR10	+	+	+	+
		ABR11/Acronis Backup 11.5/11.7/12.5	+	+	+	+

磁带设备入门指南

将计算机备份到本地连接的磁带设备

先决条件

- 磁带设备已根据制造商说明连接在计算机上。
- 代理程序已在此计算机上安装。

备份准备

1. 将磁带加载至磁带设备。
2. 登录 安克诺斯数据保护软件 Web 中控台。
3. 在**设置** > **磁带管理**中，展开计算机节点，然后单击**磁带设备**。
4. 确保显示所连接的磁带设备。否则，请单击**检测设备**。
5. 执行磁带清查：
   a. 单击磁带设备名称。
   b. 单击**清查**检测已加载的磁带。保持打开**完全清查**。请勿打开**将未识别或导入的磁带移至"可用磁带"集区**。单击**立即开始清查**。
   结果。加载的磁带已按照"清查"部分的说明移至正确的集区。

   注意
   对整个磁带设备执行完整清查可能需要很长时间。

   c. 如果加载的磁带已发送至**未识别的磁带**或**导入的磁带**集区，并且您想要将这些磁带用于备份，请手动将这些磁带移动到**可用磁带**集区。

   注意
   发送到**导入的磁带**池的磁带包含由 软件写入的备份。将此类磁带移动到**可用磁带**集区之前，请确保您不需要这些备份。

正在备份

按照"备份"部分中所述，创建保护计划。在指定备份位置时，请选择**磁带集区"Acronis"**。

结果

- 若要访问将要创建备份的位置，请单击**备份存储** > **磁带集区"Acronis"**。
- 带有备份的磁带将被移至 **Acronis** 集区。

备份至连接存储节点的磁带设备

先决条件

- 已在管理服务器上注册存储节点。
- 磁带设备已按照制造商的说明书连接在存储节点上。

备份准备

1. 将磁带加载至磁带设备。
2. 登录 安克诺斯数据保护软件 Web 中控台。
3. 单击**设置** > **磁带管理**，展开相应存储节点名称的节点，然后单击**磁带设备**。
4. 确保显示所连接的磁带设备。否则，请单击**检测设备**。
5. 执行磁带清查：
   a. 单击磁带设备名称。
   b. 单击**清查**检测已加载的磁带。保持打开**完全清查**。请勿打开**将未识别或导入的磁带移至"可用磁带"集区**。单击**立即开始清查**。
   结果。加载的磁带已按照"清查"部分的说明移至正确的集区。

   注意
   对整个磁带设备执行完整清查可能需要很长时间。

   c. 如果加载的磁带已发送至**未识别的磁带**或**导入的磁带**集区，并且您想要将这些磁带用于备份，请手动将这些磁带移动到**可用磁带**集区。

   注意
   发送到**导入的磁带**池的磁带包含由 软件写入的备份。将此类磁带移动到**可用磁带**集区之前，请确保您不需要这些备份。

   d. 确定您要备份到 **Acronis** 集区还是要创建新集区。
   详细信息。拥有多个集区有助于您为每个计算机或公司每个部门使用单独的磁带集。使用多个集区，可防止通过不同保护计划创建的备份混合在一个磁带上。
   e. 如果所选集区可以在需要时从**可用磁带**集区获取磁带，则跳过此步骤。
   否则，请将磁带从**可用磁带**集区移至所选集区。
   提示。要了解集区能否从**可用磁带**集区获取磁带，请单击相应集区，然后单击**信息**。

正在备份

按照"备份"部分中所述，创建保护计划。当指定备份位置时，请选择所创建的磁带集区。

结果

- 若要访问将要创建备份的位置，请单击**备份**，然后单击所创建磁带集区的名称。
- 带有备份的磁带将被移至所选集区。

磁带库详细使用提示

- 无需在每次加载新磁带时都执行完整清查操作。为节省时间，请按照“结合执行快速清查和完整清查”下的“清查”部分中所述的步骤进行操作。
- 您可以在同一磁带库中创建其他集区，然后选择任意一个集区作为备份目标位置。

在操作系统下从磁带设备进行恢复

在操作系统下从磁带设备进行恢复：

1. 登录 安克诺斯数据保护软件 Web 中控台。
2. 单击**设备**，然后选择已备份的计算机。
3. 单击**恢复**。
4. 选择恢复点。请注意，恢复点按位置过滤。
5. 软件将显示进行恢复所需的磁带列表。丢失的磁带显示为灰色。如果磁带设备的插槽为空，则将这些磁带加载到设备中。
6. 配置其他恢复设置。
7. 单击**开始恢复**开始恢复操作。
8. 若由于某种原因未加载任何需要的磁带，软件将显示所需磁带标识符的消息。请执行以下操作：
   a. 加载磁带。
   b. 执行快速清查。
   c. 单击**概述** > **活动**，然后单击具有**需要互动**状态的恢复活动。
   d. 单击**显示详细信息**，然后单击**重试**以继续恢复操作。

如果没有看到存储在磁带上的备份时怎么办？

这说明具有磁带内容的数据库由于某种原因丢失或损坏。

要恢复数据库，请执行以下操作：

1. 执行快速清查。

   警告！
   在清查期间，请勿打开**将未识别和导入的磁带移至“可用磁带”集区**。如果打开此开关，您可能会丢失所有备份。

2. 重新扫描**未识别的磁带**集区。该操作的结果是，您将获得加载磁带的内容。
3. 如果检测到的任何备份继续存在于尚未重新扫描的其他磁带上，则按提示加载然后重新扫描这些磁带。

在可启动媒体下从本地连接的磁带设备进行恢复

要在可启动媒体下从本地连接的磁带设备进行恢复：

1. 将进行恢复所需的磁带放入磁带设备中。
2. 从可启动媒体启动计算机。

3. 单击**本地管理此计算机**或单击**应急可启动媒体**两次，具体取决于您要使用的媒体类型。
4. 如果磁带设备连接使用 iSCSI 接口，请按"配置 iSCSI 和 NDAS 设备"所述配置该设备。
5. 单击**磁带管理**。
6. 单击**清查**。
7. 在**要清查的对象**中，选择磁带设备。
8. 单击**开始**开始清查。
9. 清查完成后，单击**关闭**。
10. 单击**操作 > 恢复**。
11. 单击**选择数据**，然后单击**浏览**。
12. 展开**磁带设备**，然后选择所需设备。系统将提示您确认重新扫描操作。单击**是**。
13. 选择**未识别的磁带**集区。
14. 选择要重新扫描的磁带。若要选择集区的所有磁带，请勾选**磁带名称**列标题旁边的复选框。
15. 如果磁带包含密码保护的备份，请选中相应的复选框，然后在**密码**框中指定该备份的密码。如果未指定密码或密码不正确，将不会检测到该备份。请记住这一点，以防在重新扫描之后看不到该备份。

    提示。如果磁带包含由各种密码保护的多个备份，您需要反复重新扫描几次，依次指定每个密码。
16. 单击**开始**开始重新扫描。该操作的结果是，您将获得加载磁带的内容。
17. 如果检测到的任何备份继续存在于尚未重新扫描的其他磁带上，则按提示加载然后重新扫描这些磁带。
18. 重新扫描完成后，单击**确定**。
19. 在**存档视图**中，选择要恢复数据所在的备份，然后选择要恢复的数据。单击**确定**后，**恢复数据**页面将显示进行恢复所需的磁带列表。丢失的磁带显示为灰色。如果磁带设备的插槽为空，则将这些磁带加载到设备中。
20. 配置其他恢复设置。
21. 单击**确定**来启动恢复。
22. 若由于某种原因未加载任何需要的磁带，软件将显示所需磁带标识符的消息。请执行以下操作：
    a. 加载磁带。
    b. 执行快速清查。
    c. 单击**概述 > 活动**，然后单击具有**需要互动**状态的恢复活动。
    d. 单击**显示详细信息**，然后单击**重试**以继续恢复操作。

在可启动媒体下从连接至存储节点的磁带设备进行恢复

若要在可启动媒体下从连接至存储节点的磁带设备进行恢复：

1. 将进行恢复所需的磁带放入磁带设备中。
2. 从可启动媒体启动计算机。
3. 单击**本地管理此计算机**或单击**应急可启动媒体**两次，具体取决于您要使用的媒体类型。
4. 单击**恢复**。
5. 单击**选择数据**，然后单击**浏览**。

6. 在**路径**方框中，键入 bsp://<存储节点地址>/<集区名称>/，其中 <存储节点地址> 是包含所需备份的存储节点的 IP 地址，<集区名称> 是磁带集区的名称。单击**确定**，然后指定集区的凭据。
7. 选择备份，然后选择要恢复的数据。单击**确定**后，**恢复数据**页面将显示进行恢复所需的磁带列表。丢失的磁带显示为灰色。如果磁带设备的插槽为空，则将这些磁带加载到设备中。
8. 配置其他恢复设置。
9. 单击**确定**来启动恢复。
10. 若由于某种原因未加载任何需要的磁带，软件将显示所需磁带标识符的消息。请执行以下操作：
    a. 加载磁带。
    b. 执行快速清查。
    c. 单击**概述** > **活动**，然后单击具有**需要互动**状态的恢复活动。
    d. 单击**显示详细信息**，然后单击**重试**以继续恢复操作。

磁带管理

检测磁带设备

检测磁带设备时，备份软件会查找连接至计算机的磁带设备并将其相关信息放置到磁带管理数据库中。从 RSM 禁用检测到的磁带设备。

通常，一旦磁带设备连接至安装了产品的计算机，就会自动检测磁带设备。但是，如果发生以下情况，您可能需要检测磁带设备：

- 连接或重新连接磁带设备后。
- 在连接磁带设备的计算机上安装或重新安装备份软件后。

检测磁带设备

1. 单击**设置** > **磁带管理**。
2. 选择磁带设备所连接的计算机。
3. 单击**检测设备**。您将会看到连接的磁带设备及其驱动器和插槽。

磁带集区

备份软件会使用磁带集区(即磁带的逻辑组)。软件包含以下预定义的磁带集区：**未识别的磁带**、**导入的磁带**、**可用磁带**和 **Acronis**。此外，您还可以创建自己的自定义集区。

Acronis 集区和自定义集区也可用作备份位置。

预定义集区

未识别的磁带

该集区包括由第三方应用程序编写的磁带。要写入此类磁带，您需要将其明确移动到**可用磁带**集区。除了**可用磁带**集区，您不能将磁带从该集区移动到任何其他集区。

导入的磁带

该集区包含 Acronis 安克诺斯数据保护软件 在磁带设备中写入的磁带，该磁带设备连接到另一个存储节点或代理程序。要写入此类磁带，您需要将其明确移动到**可用磁带**集区。除了**可用磁带**集区，您不能将磁带从该集区移动到任何其他集区。

可用磁带

该集区包含可用(空)磁带。您可以将磁带从其他集区手动移动到该集区。

将磁带移至**可用磁带**集区时，软件会将其标记为空。如果该磁带包含备份，则它们会标记有 图标。当软件开始覆盖磁带时，会从数据库中删除备份相关的数据。

Acronis

您不想创建自己的集区时，默认使用该集区进行备份。通常适用于具有少数磁带的磁带驱动器。

自定义集区

如果要分开不同数据的备份，需要创建多个集区。例如，可能需要创建自定义集区来分开以下备份：

- 公司不同部门的备份
- 不同计算机的备份
- 系统卷和用户数据的备份。

集区操作

创建集区

创建集区：

1. 单击**设置** > **磁带管理**。
2. 选择您的磁带设备所连接的计算机或存储节点，然后单击此计算机下的**磁带集区**。
3. 单击**创建集区**。
4. 指定集区名称。
5. [可选]取消勾选**从"可用磁带"集区自动选取磁带...**复选框。如果取消勾选，只有在某一时间被纳入新集区的磁带才会用于备份。
6. 单击**创建**。

编辑集区

您可以编辑 **Acronis** 集区或您自己的自定义集区的参数。

编辑集区：

1. 单击**设置** > **磁带管理**。
2. 选择您的磁带设备所连接的计算机或存储节点，然后单击此计算机下的**磁带集区**。
3. 选择所需的集区，然后单击**编辑集区**。
4. 您可以更改集区名称或设置。有关集区设置的更多信息，请参阅"创建集区"部分。
5. 单击**保存**保存更改。

删除集区

您只能删除自定义集区。预定义磁带集区(**未识别的磁带**、**导入的磁带**、**可用磁带**和 **Acronis**)不能删除。

注意
删除一个集区后,请勿忘记编辑将该集区作为备份位置的保护计划。否则,这些保护计划将失败。

删除集区:

1. 单击**设置** > **磁带管理**。
2. 选择您的磁带设备所连接的计算机或存储节点,然后单击此计算机下的**磁带集区**。
3. 选择所需的集区,然后单击**删除**。
4. 选择要删除的磁带集区在删除后要移至的集区。
5. 单击**确定**删除集区。

对磁带进行的操作

移动至另一插槽

在以下情况中执行此操作:

- 需要同时将多个磁带取出磁带设备。
- 磁带设备没有中转槽且要弹出的磁带位于不可拆卸库的插槽中。

您需要将磁带移至一个插槽库的插槽中,然后手动弹出库。

将磁带移至另一插槽

1. 单击**设置** > **磁带管理**。
2. 选择您的磁带设备所连接的计算机或存储节点,然后单击此计算机下的**磁带集区**。
3. 单击包含必需的磁带的集区,然后选择所需的磁带。
4. 单击**移至插槽**。
5. 选择要将所选磁带移动到的新插槽。
6. 单击**移动**开始操作。

移动至另一集区

使用此操作可将一个或多个磁带从一个集区移至另一个集区。

将磁带移至**可用磁带**集区时,软件会将其标记为空。如果该磁带包含备份,则它们会标记有 图标。当软件开始覆盖磁带时,会从数据库中删除备份相关的数据。

关于特定类型磁带的注意事项

- 不能将写保护和一次录制的 WORM(写一次读多次)磁带移至**可用磁带**集区。
- 清理磁带总是显示在**未识别的磁带**集区,无法将其移至任何其他集区。

若要将磁带移至其他集区

1. 单击**设置** > **磁带管理**。
2. 选择您的磁带设备所连接的计算机或存储节点，然后单击此计算机下的**磁带集区**。
3. 单击包含必需的磁带的集区，然后选择所需的磁带。
4. 单击**移至集区**。
5. [可选] 如果要为所选磁带创建其他集区，请单击**创建新集区**。执行"创建集区"章节介绍的操作。
6. 选择要将磁带移至哪个集区。
7. 单击**移动**保存更改。

注意
如果磁带上有可恢复的备份并将磁带移动到另一个池，请确保在完成移动操作后刷新备份存储下的保管库。即使原始备份目标位于第二个池中，备份也将在第二个池中可用。

清查

清查操作可检测加载到磁带设备的磁带并为没有名称的磁带指定名称。

清查方式

有两种清查方式。

快速清查

代理程序或存储节点扫描磁带以获得条形码。通过使用条形码，该软件可将磁带快速返回至其之前使用的集区。

选择此方式以识别附加至同一台计算机上的相同的磁带设备所使用的磁带。其他磁带将发送至**未识别的磁带**集区。

如果磁带库不包含条形码读取器，则所有磁带将发送至**未识别的磁带**集区。要识别磁带，请按本节后面所介绍的方式执行完整清查或结合执行快速清查和完整清查。

完整清查

代理程序或存储节点读取之前写入的标记，分析与加载的磁带内容有关的其他信息。选择此方式以识别任何计算机和任何磁带设备上的空磁带和由相同软件写入的磁带。

下表显示了因执行完整清查而将磁带发送至的集区。

磁带被...使用	磁带由...读取	磁带被发送至集区...
代理程序	同一代理程序	磁带之前的位置
	另一代理程序	**导入的磁带**
	存储节点	**导入的磁带**

存储节点	同一存储节点	磁带之前的位置
	另一存储节点	**导入的磁带**
	代理程序	**导入的磁带**
第三方备份应用程序	代理程序或存储节点	**未识别的磁带**

某些类型的磁带被发送至特定集区：

磁带类型	磁带被发送至集区...
空磁带	**可用磁带**
空的写保护磁带	**未识别的磁带**
清理磁带	**未识别的磁带**

快速清查可应用于整个磁带设备。完整清查可应用于整个磁带设备、单个驱动器或插槽。对于独立磁带驱动器，始终执行完整清查，即使已选中快速清查也如此。

结合执行快速清查和完整清查

对整个磁带设备执行完整清查可能需要很长时间。如果仅需对几盘磁带进行清查，请执行如下操作：

1. 对磁带设备执行快速清查。
2. 单击**未识别的磁带**集区。查找要进行清查的磁带并记录其所占插槽。
3. 对这些插槽执行完整清查。

执行清查之后怎么办

如果您要对放置于**未识别的磁带**或**导入的磁带**集区中的磁带进行备份，则将它们移动至**可用磁带**集区，然后移至 **Acronis** 集区或自定义集区。如果您要备份到的集区为可补充，则可将磁带留在**可用磁带**集区。

如果您要从放置在**未识别的磁带**或**导入的磁带**集区中的磁带恢复，则需要对其进行重新扫描。该磁带将移至您在重新扫描期间选择的集区，且磁带上存储的备份将出现在位置中。

操作顺序

1. 单击**设置** > **磁带管理**。
2. 选择磁带设备所连接的计算机，然后选择要清查的磁带设备。
3. 单击**清查**。
4. [可选] 若要选择快速清查，请关闭**完整清查**。
5. [可选] 打开**将未识别和导入的磁带移至"可用磁带"集区**。

警告！
仅当您绝对确定存储在磁带上的数据可覆盖时，才应该启用此开关。

6. 单击**立即开始清查**开始清查。

重新扫描

有关磁带内容的信息存储在专用数据库中。重新扫描操作会读取磁带内容，如果其中的信息与磁带中存储的数据不匹配，则此操作还将更新数据库。因该操作而检测到的备份放置在指定集区中。

在一个操作中，您可以重新扫描一个集区内的磁带。仅可选择线上磁带进行此操作。

要重新扫描带有多路数据流或兼有多路数据流及多路复用备份的磁带，至少需要与用于创建该备份相同数量的驱动器。无法通过独立磁带驱动器重新扫描此类备份。

运行重新扫描：

- 如果存储节点或受控计算机的数据库丢失或损坏。
- 如果数据库中有关磁带的信息过期(例如，一个磁带的内容被另一存储节点或代理程序修改)。
- 在可启动媒体下操作时，访问磁带上存储的备份。
- 如果您从数据库中错误删除了有关磁带的信息。当您重新扫描已删除磁带时，其中存储的备份将重新出现在数据库中，且可用于数据恢复。
- 如果备份从磁带上手动或通过保留规则删除，但您要使其可用于数据恢复。重新扫描此类磁带之前，请将其弹出，从数据库中删除有关磁带的信息，然后再次将磁带插入磁带设备中。

重新扫描磁带

1. 单击**设置** > **磁带管理**。
2. 选择您的磁带设备所连接的计算机或存储节点，然后单击此计算机下的**磁带设备**。
3. 选择要将磁带加载到其上的磁带设备。
4. 执行快速清查。

注意
在清查期间，请*勿*启用**将未识别和导入的磁带移至"可用磁带"集区**开关。

5. 选择**未识别的磁带**集区。这是因执行快速清查而将大多数磁带发送至的集区。也可以重新扫描任何其他集区。
6. [可选] 若要仅重新扫描个别磁带，请选择它们。
7. 单击**重新扫描**。
8. 选择存放新检测到的备份的集区。
9. 如有必要，选中**启用存储在磁带上的磁盘备份的文件恢复**复选框。

   详细信息。如果选中此复选框，软件将在磁带设备所连接的计算机的硬盘上创建特定辅助文件。只要这些辅助文件保持完好，就可以从磁盘备份进行文件恢复。如果磁带包含应用程序感知备份，请确保选中该复选框。否则，您将无法从这些备份中恢复应用程序数据。

10. 如果磁带包含密码保护的备份，请选中相应的复选框，然后指定该备份的密码。如未指定密码或密码不正确，将不会检测到该备份。请记住这一点，以防在重新扫描之后看不到该备份。

    提示。如果磁带含有由各种密码保护的备份，则需反复重新扫描几次，依次指定每个密码。
11. 单击**开始重新扫描**开始重新扫描。

结果。所选磁带被移至所选集区。该磁带中存储的备份可在此集区中找到。分布于几盘磁带中的备份不会出现在集区中，直至重新扫描到所有这些磁带。

重命名

当软件检测到新磁带时，它将自动按以下格式获得名称分配：**磁带 XXX**，其中 **XXX** 是唯一编号。磁带按顺序编号。重命名操作允许您手动更改磁带的名称。

重命名磁带

1. 单击**设置** > **磁带管理**。
2. 选择您的磁带设备所连接的计算机或存储节点，然后单击此计算机下的**磁带集区**。
3. 单击包含必需的磁带的集区，然后选择所需的磁带。
4. 单击**重命名**。
5. 键入所选磁带的新名称。
6. 单击**重命名**保存更改。

擦除

擦除一个磁带将实际删除该磁带上存储的所有备份并从数据库中移除有关这些备份的信息。然而有关该磁带自身的信息仍保留在数据库中。

擦除后，位于**未识别的磁带**或**导入的磁带**集区的磁带被移至**可用磁带**集区。位于任何其他集区的磁带不会移动。

擦除磁带

1. 单击**设置** > **磁带管理**。
2. 选择您的磁带设备所连接的计算机或存储节点，然后单击此计算机下的**磁带集区**。
3. 单击包含必需的磁带的集区，然后选择所需的磁带。
4. 单击**擦除**。系统提示您确认此操作。
5. 选择擦除方式：快速或完整。
6. 单击**擦除**开始操作。

    详细信息。无法取消擦除操作。

弹出

要从磁带库中成功弹出磁带，此磁带库必须带有中转槽，且此中转槽必须未被用户或其他软件锁定。

弹出磁带

1. 单击**设置** > **磁带管理**。
2. 选择您的磁带设备所连接的计算机或存储节点，然后单击此计算机下的**磁带集区**。
3. 单击包含必需的磁带的集区，然后选择所需的磁带。
4. 单击**弹出**。该软件将提示您提供磁带说明。我们建议您描述磁带存储的物理位置。在恢复期间，软件将显示此描述，这样您就能很轻松地找到这些磁带。
5. 单击**弹出**开始操作。

在手动或自动弹出磁带后，建议在磁带上写下其名称。

删除

删除操作删除所选磁带中存储的备份的相关信息，并从数据库中删除磁带本身的信息。

您只能删除脱机(已弹出的)磁带。

删除磁带

1. 单击**设置** > **磁带管理**。
2. 选择您的磁带设备所连接的计算机或存储节点，然后单击此计算机下的**磁带集区**。
3. 单击包含必需的磁带的集区，然后选择所需的磁带。
4. 单击**删除**。系统提示您确认此操作。
5. 单击**删除**删除磁带。

如果误删磁带该怎么办?

与已擦除的磁带不同，不会实际删除已删除磁带中的数据。因此，您可以再次使用此类磁带中存储的备份。为此：

1. 将磁带加载至您的磁带设备。
2. 执行快速清查以检测磁带。

> **注意**
> 在清查期间，请*勿*启用**将未识别和导入的磁带移至"可用磁带"集区**开关。

3. 执行重新扫描使磁带中存储的数据与数据库匹配。

指定磁带集

此操作允许您为磁带指定磁带集。

磁带集是集区内的一组磁带。

与在备份选项中指定磁带集不同，在备份选项中您可以使用变量，在这里您只可以指定一个字符串值。

如果要根据某些规则将软件备份到*特定*磁带(例如，如果要将周一的备份存储在磁带 1 上，将周二的备份存储在磁带 2 上，以此类推)，请执行此操作。为每个所需的磁带指定一个磁带集，然后在备份选项中指定同一磁带集或使用合适的变量。

对于上述示例，请为磁带 1 指定磁带集 Monday、为磁带 2 指定磁带集 Tuesday，以此类推。在备份选项中，指定 [Weekday]。在这种情况下，在一周的每一天将使用合适的磁带。

为一个或多个磁带指定磁带集

1. 单击**设置** > **磁带管理**。
2. 选择您的磁带设备所连接的计算机或存储节点，然后单击此计算机下的**磁带集区**。
3. 单击包含必需的磁带的集区，然后选择所需的磁带。
4. 单击**磁带集**。
5. 键入磁带集名称。如果已为选定磁带指定其他磁带集，则将取代该磁带集。如果您要在没有指定其他磁带集的情况下从该磁带集中排除这些磁带，则删除现有磁带集名称。
6. 单击**保存**保存更改。

存储节点

存储节点是一个服务器，旨在优化企业数据保护所需的各种资源（如公司的存储容量、网络带宽和生产服务器的 CPU 负载）的使用。此目标是通过组织和管理作为企业备份的专用存储位置（受控位置）的位置而实现的。

Acronis 存储节点的主要目的是实现对磁带驱动器或库的集中式访问；例如，将数据从多个设备备份和恢复到同一个磁带驱动器或库（磁带上的受控保管库）。

另一个用例是启用高级重复数据删除功能，其中需要对跨多个设备的数据进行重复数据删除并将其存储在单个位置（已启用重复数据删除的受控保管库）。

安装存储节点和目录服务

安装存储节点之前，确保计算机满足系统要求。

建议将存储节点和目录服务安装在单独的计算机上。运行目录服务的计算机的系统要求如 "编录最佳方法"（第 535 页）中所述。

安装存储节点和/或目录服务

1. 以管理员身份登录，然后启动 Acronis 安克诺斯数据保护软件 安装程序。
2. [可选] 要更改安装程序的语言，请单击**设置语言**。
3. 接受许可协议和隐私声明的条款，然后单击**继续**。
4. 单机**安装安全保护代理程序**。
5. 单击**自定义安装设置**。
6. 单击**安装内容**旁边的**更改**。
7. 选择要安装的组件：
   - 若要安装存储节点，请勾选**存储节点**复选框。系统会自动勾选**适用于 Windows 的代理程序**复选框。
   - 若要安装目录服务，请勾选**目录服务**复选框。
   - 如果您不希望在此计算机上安装其他组件，请清除相应的复选框。

   单击**完成**以继续。

8. 指定将注册组件的管理服务器：
   a. 在 **Acronis 安克诺斯数据保护软件 管理服务器**旁边，单击**指定**。
   b. 指定安装了管理服务器的计算机的主机名或 IP 地址。
   c. 指定管理服务器管理员的凭据或注册标记。
      有关如何生成注册标记的详细信息，请参阅 "步骤 1：生成注册标记"(第 157 页)。
   d. 单击**完成**。
9. 如果出现系统提示，请选择要将带有存储节点和/或目录服务的计算机添加到组织还是其中一个单位。
   在您管理多个单位或至少有一个单位的组织时，才会出现该提示。否则，会将计算机静默添加到您管理的单位或组织。有关详细信息，请参阅“管理员和单元”。
10. [可选] 更改其他安装设置，如“自定义安装设置”中所述。
11. 单击**安装**以继续安装过程。
12. 安装完成后，单击**关闭**。

使用 Acronis 安克诺斯数据保护软件 15 更新 4 更新目录服务

Acronis 安克诺斯数据保护软件 15 更新 4 使用新版本的目录服务。新版本与由早期版本创建的目录数据不直接兼容。

在更新到 Acronis 安克诺斯数据保护软件 15 更新 4 期间，可以手动将此数据迁移到新版本的目录服务。或者，可以跳过迁移并稍后重新创建目录数据。重新创建目录数据比迁移目录数据需要更多时间。

迁移目录数据

1. 在已安装目录服务的计算机上，运行 Acronis 安克诺斯数据保护软件 安装程序。
2. 接受许可协议和隐私声明的条款，然后单击**继续**。
3. 选中**我了解**复选框，然后单击**更新**。
4. 选中**指定临时文件夹**复选框。
5. 指定将在其中导出目录数据的文件夹。
   导出的数据是加密的。迁移完成后，将自动删除临时文件夹。
6. 单击**完成**。

跳过迁移目录数据

1. 在已安装目录服务的计算机上，运行 Acronis 安克诺斯数据保护软件 安装程序。
2. 接受许可协议和隐私声明的条款，然后单击**继续**。
3. 选中**我了解**复选框，然后单击**更新**。
4. 取消选中**指定临时文件夹**复选框。
5. 单击**完成**。
6. 确认选择。

结果，现有目录数据将在更新到 Acronis 安克诺斯数据保护软件 15 更新 4 后变得不可用。要重新创建目录数据，请运行备份。

注意

如果目录服务、存储节点和管理服务器在不同的计算机上运行，请确保将它们按以下顺序全部都更新到 Acronis 安克诺斯数据保护软件 15 更新 4：

1. 管理服务器
2. 存储节点
3. 目录服务

添加受控位置

可以在以下位置编组受控位置：

- 在本地文件夹中：
  - 在存储节点的本地硬盘上
  - 在向操作系统显示为本地连接设备的 SAN 存储上
- 在网络文件夹中：
  - 在 SMB/CIFS 共享中
  - 在向操作系统显示为网络文件夹的 SAN 存储上
  - 在 NAS 上
- 在本地连接存储节点的磁带设备上

  基于磁带的位置以磁带集区的形式创建。默认存在一个磁带集区。如有必要，您可以创建其他磁带集区，这将在本部分的后面部分进行介绍。

在本地或网络文件夹中创建受控位置

1. 请执行以下任一操作：
   - 依次单击**备份存储** > **添加位置**，然后单击**存储节点**。
   - 创建保护计划时，依次单击**备份位置** > **添加位置**，然后单击**存储节点**。
   - 依次单击**设置** > **存储节点**，选择将管理该位置的存储节点，然后单击**添加位置**。
2. 在**名称**中，为位置指定一个唯一名称。“唯一”意味着不得存在由同一个存储节点管理的具有相同名称的其他位置。
3. [可选] 选择将管理该位置的存储节点。如果您在步骤 1 中选择了最后一个选项，将无法更改存储节点。
4. 选择代理程序将用来访问位置的存储节点名称或 IP 地址。

   默认情况下，存储节点名称已选中。如果 DNS 服务器无法将该名称解析为 IP 地址，导致访问失败，则可能需要更改此设置。若要以后更改此设置，请依次单击**备份存储** > 该位置 > **编辑**，然后更改**地址**字段值。
5. 输入文件夹路径或浏览到所需文件夹。
6. 单击**完成**。软件会检查对指定文件夹的访问权限。
7. [可选] 在该位置启用备份重复数据删除。

   重复数据删除可最大程度减少备份流量，以及通过消除重复磁盘块，减小在位置中存储的备份大小。

   有关重复数据删除限制的详细信息，请参阅“重复数据删除限制”。

8. [仅在启用重复数据删除时]指定或更改**重复数据删除数据库路径**字段值。

   这必须是存储节点的本地硬盘上的文件夹。若要提高系统性能，建议您在不同的磁盘上创建重复数据删除数据库和受控位置。

   有关重复数据删除数据库的详细信息，请参阅"重复数据删除最佳做法"。
9. [可选]选择是否对位置进行加密保护。存储节点将使用保存在存储节点上的位置特定加密密钥对写入位置的任何内容进行加密，并对从位置读取的任何内容进行解密。

   有关加密的更多信息，请参阅"位置加密"。
10. [可选]选择是否对该位置中存储的备份进行编录。使用数据目录可轻松找到所需的数据版本并选择该版本进行恢复。

    如果在管理服务器上注册了多个编录服务，您可选择将对在该位置中存储的备份进行编录的服务。

    可在以后启用或禁用编录，如"如何启用或禁用编录"中所述。
11. 单击**完成**创建位置。

在磁带设备上创建受控位置

1. 依次单击**备份存储** > **添加位置**，或者在创建保护计划时，依次单击**备份位置** > **添加位置**。
2. 单击**磁带**。
3. [可选]选择将管理该位置的存储节点。
4. 遵循"创建集区"中所述的步骤操作，从第 4 步开始。

注意

默认情况下，代理程序使用存储节点名称来访问基于磁带的受控位置。若要使代理程序使用存储节点 IP 地址，请依次单击**备份存储** > 该位置 > **编辑**，然后更改**地址**字段值。

重复数据删除

重复数据删除限制

通用限制

无法对加密的备份进行重复数据删除。如果想要同时使用重复数据删除和加密，请将备份保留为未加密，并将其引导至一个同时启用了重复数据删除和加密的位置。

磁盘级别备份

如果该卷的分配单元大小(也称为簇大小或块大小)不能被 4 KB 整除，则无法对磁盘块执行重复数据删除操作。

注意

大多数 NTFS 和 ext3 卷上的分配单元大小为 4 KB。这允许执行块级重复数据删除操作。允许用于块级重复数据删除的其他分配单元大小的示例包括 8 KB、16 KB 和 64 KB。

文件级备份

如果文件已加密，则不会执行文件的重复数据删除操作。

重复数据删除和 NTFS 数据流

在 NTFS 文件系统中，一个文件可能有一个或多个相关联的其他数据集，这通常称为*交换数据流*。

当备份此类文件时，也同样备份其所有的交换数据流。但是，不能对这些数据流执行重复数据删除，即使文件本身也无法重复数据删除。

重复数据删除最佳实践

重复数据删除是一个受多种因素影响的复杂过程。

影响重复数据删除速度的最重要因素有：

- 重复数据删除数据库的访问速度
- 存储节点的 RAM 容量
- 存储节点中创建的重复数据删除位置的数量。

若要提高重复数据删除性能，请遵循以下建议。

将重复数据删除数据库和重复数据删除位置设置在独立的物理设备上

重复数据删除数据库存储位置中所存储的所有项目的散列值，不能进行重复数据删除的项目（如加密文件）除外。

为了提高重复数据删除数据库的访问速度，数据库和位置必须设置在单独的物理设备上。

最好为位置和数据库分配专用设备。如果这无法实现，至少不要将位置或数据库放置在操作系统的同一磁盘中。原因是操作系统会进行大量的硬盘读/写操作，这将显著降低重复数据删除的速度。

为重复数据删除数据库选择磁盘

- 数据库必须位于固定驱动器中。请勿将重复数据删除数据库放入外部可卸载驱动器中。
- 若要最大程度地减少数据库访问时间，请将其存储在直接连接的驱动器上而不是加载的网络卷上。网络延迟可能会极大地降低重复数据删除性能。
- 可使用以下公式估算重复数据删除数据库所需的磁盘空间：

$$S = U * 90 / 65536 + 10$$

在此，

S 为磁盘大小（以 GB 为单位）

U 是重复数据删除数据存储中唯一数据的计划量（以 GB 为单位）

例如，如果重复数据删除数据存储中唯一数据的计划量为 U=5 TB，则重复数据删除数据库将需要最小可用空间（如下所示）：

$$S = 5000 * 90 / 65536 + 10 = 17 \text{ GB}$$

为重复数据删除位置选择磁盘

为防止数据丢失，建议您使用 RAID 10、5 或 6。不建议使用 RAID 0，因为它不具备容错功能。由于速度相对较慢，不建议使用 RAID 1。可以随意使用本地磁盘或 SAN，两者均可。

40 到 160 MB 的 RAM 可供 1 TB 的唯一数据使用

达到上限时，重复数据删除会停止，但备份和恢复会继续工作。如果您向存储节点添加了更多的 RAM，重复数据删除将在下一次备份后继续运行。通常，拥有的 RAM 越多，可以存储的唯一数据的卷越大。

每个存储节点上仅有一个重复数据删除位置

强烈建议在一个存储节点上仅创建一个重复数据删除位置。否则，整个可用 RAM 卷可能会根据位置的数量按比例分发。

没有应用程序争夺资源

具有此存储节点的计算机不应运行需要大量系统资源的应用程序；例如，数据库管理系统 (DBMS) 或企业资源计划 (ERP) 系统。

多核处理器的时钟频率至少为 2.5 GHz

建议您使用 4 核或 4 核以上且时钟频率不低于 2.5 GHz 的处理器，。

位置中有足够的可用空间

目标重复数据删除需要与将已备份数据保存到位置后立即占用的空间一样多的可用空间。在不对源进行压缩或重复数据删除操作的情况下，此值等于在指定备份操作期间所备份的原始数据的大小。

高速 LAN

建议使用 1Gbit LAN。这将使得软件可以在进行重复数据删除时并行执行 5 到 6 个备份，同时速度不会受很大影响。

先备份一台典型计算机，然后再备份几台内容相似的计算机

备份几台内容相似的计算机时，建议您先备份其中一台计算机，直到已备份数据索引结束。此后，由于进行了有效的重复数据删除，其他计算机的备份速度将更快。由于第一台计算机的备份已建立索引，大部分数据已在重复数据删除数据存储中。

在不同时间备份不同的计算机

如果备份大量计算机，请将备份操作的时间错开。为基于不同时间表创建多个保护计划。

位置加密

对位置进行加密保护后，存储节点将使用保存在存储节点上的位置特定加密密钥对写入位置的任何内容进行加密，并对从位置读取的任何内容进行解密。如果存储媒体被盗或者由未经授权的人员访问，犯罪分子也会因无权访问存储节点而无法解密位置内容。

此加密与由保护计划指定并由代理程序执行的备份加密无关。如果备份已加密，则存储节点端加密将应用于代理程序执行的加密。

对位置进行加密保护

1. 指定并确认要用于生成加密密钥的词语(密码)。
   词语区分大小写。仅当将位置附加到其他存储节点时,系统才会要求您提供此词语。
2. 选择以下加密算法之一:
   - **AES 128** - 位置内容将使用高级加密标准 (AES) 算法通过 128 位密钥进行加密。
   - **AES 192** - 位置内容将使用 192 位密钥的 AES 算法进行加密。
   - **AES 256** - 位置内容将使用 256 位密钥的 AES 算法进行加密。
3. 单击**确定**。

AES 密码算法在密码块链接 (CBC) 模式下运行,并使用带有用户定义的大小 128、192 或 256 位的随机生成的密钥。密钥越大,程序对位置内存储的备份进行加密所需的时间就越长,备份的安全性也越高。

随后加密密钥将使用 AES-256 进行加密,并将所选词语的 SHA-256 哈希作为密钥。该词语本身不会存储在磁盘的任何位置;词语哈希用于验证目的。有了这样的双层安全防护,可防止未经授权访问备份,但是若词语丢失,则无法恢复。

编录

数据目录

使用数据目录可轻松找到所需的数据版本并选择该版本进行恢复。数据目录将显示存储在所有受控位置的数据,在这些位置正在或已启用编录。

只有在管理服务器上注册了至少一个目录服务的情况下,**目录**部分才会显示在**备份存储**选项卡下方。有关安装目录服务的信息,请参阅"安装存储节点和目录服务"。

只有组织管理员才可以看见**目录**部分。

限制

只有物理机的磁盘级别备份和文件级备份以及虚拟机备份才支持编录。

以下数据无法显示在目录中:

- 来自加密备份的数据
- 备份到磁带设备的数据
- 备份到云存储的数据
- Acronis 安克诺斯数据保护软件 12.5 版本之前的产品备份的数据

选择要恢复的备份数据

1. 依次单击**备份存储** > **目录**。
2. 如果在管理服务器上注册了多个编录服务,则选择对该位置中存储的备份进行编录的服务。

注意

要查看哪个服务编录某个位置，请在**备份存储** > **位置** > **位置**中选择该位置，然后单击**详细信息**。

3. 软件会显示已备份到由选定目录服务编录的受控位置的计算机。

   通过浏览或使用搜索，选择要恢复的数据。

   - **浏览**

     双击计算机可查看已备份的磁盘、卷、文件夹和文件。

     要恢复磁盘，请选择标记有以下图标的磁盘： 

     要恢复卷，请双击包含相应卷的磁盘，然后选择该卷。

     要恢复文件和文件夹，请浏览文件和文件夹所在的卷。可以浏览标记有以下文件夹图标的卷： 

   - **搜索**

     在搜索字段中，键入有助于识别所需数据项目的信息(可以是计算机名称、文件或文件夹名称或磁盘标签)，然后单击**搜索**。

     可以将星号 (*) 和问号 (?) 用作通配符。

     搜索结束后，将会看到名称与输入值完全或部分匹配的备份数据项目列表。

4. 默认情况下，数据将尽可能还原至最近的时间点。如果选择了单个项目，可使用**版本**按钮来选择恢复点。
5. 选择所需数据后，请执行以下任一操作：
   - 单击**恢复**，然后如"恢复"中所述配置恢复操作的参数。
   - [仅适用于文件/文件夹] 如果要将文件另存为 .zip 文件，请单击**下载**，选择要将数据保存到的位置，然后单击**保存**。

编录最佳方法

若要提高编录性能，请遵循以下建议。

安装

建议将目录服务和存储节点分别安装在单独的计算机上。否则，这些组件会争用 CPU 和 RAM 资源。

如果在管理服务器上注册多个存储节点，除非索引或搜索性能下降，否则一个目录服务就足够了。例如，如果您注意到编录一直在全天候运行(即，不停地持续执行编录活动)，请在单独的计算机上再安装一个目录服务。然后删除一些受控位置，并用新的目录服务重新创建这些受控位置。这些位置上存储的备份将保持不变。

系统要求

参数	最小值	建议值

CPU 内核数	2	4 个以上 (含 4 个)
RAM	8 GB	16 GB 以上(含 16 GB)
硬盘	7200 rpm HDD	SSD
计算机和存储节点之间以及计算机和目录服务之间的网络连接	100 Mbps	1 Gbps

如何启用或禁用编录

如果为受控位置启用了编录，则每个备份的内容将引导至在创建备份后立即添加数据目录的位置。

您可以在添加受控位置时或在以后启用编录。一旦启用了编录，存储在该位置并且以前未编录的所有备份都在下次备份之后编录到该位置。

编录过程非常耗时，尤其在将大量计算机备份到相同位置时。您可以随时禁用编录。将完成在禁用之前创建的备份编录。新创建的备份将不会进行编录。

为现有位置配置编录

1. 依次单击**备份存储** > **位置**。
2. 单击**位置**，然后选择要为其配置编录的受控位置。
3. 单击**编辑**。
4. 启用或禁用**目录服务**开关。
5. 单击**完成**。

系统设置

这些设置仅适用于本地部署。

要访问这些设置，请依次单击**设置** > **系统设置**。

只有组织管理员才可以看见**系统设置**部分。

电子邮件通知

您可以为所有发送自管理服务器的电子邮件通知配置通用全局设置。

您可在默认备份选项中，覆盖此处针对备份期间发生的事件专门所设的设置。在此情况下，全局设置将会对除备份以外的其他操作有效。

在创建保护计划时，您可以选择使用哪些设置：全局设置或默认备份选项中指定的设置。还可以使用仅特定于该计划的自定义值进行覆盖。

重要事项
当更改全局电子邮件通知设置时，使用全局设置的所有保护计划都会受影响。

在配置这些设置之前，请确保已配置**电子邮件服务器**设置。

配置全局电子邮件通知设置

1. 单击**设置** > **系统设置** > **电子邮件通知**。
2. 在**收件人的电子邮件地址**字段中，键入目标电子邮件地址。您可以输入多个地址，但要用分号隔开。
3. [可选] 在**主题**中，更改电子邮件通知的主题。
   您可以使用下列变量：
   - [Alert] - 警报摘要。
   - [Device] - 设备名称。
   - [Plan] - 生成警报的计划的名称。
   - [ManagementServer] - 安装了管理服务器的计算机的主机名。
   - [Unit] - 计算机所属单位的名称。

   默认主题为 [Alert] **设备：**[Device] **计划：**[Plan]
4. [可选] 选中**活动警告的每日概述**复选框，然后执行以下操作：
   a. 指定发送概述的时间。
   b. [可选] 选中**不发送“无活动警告”消息**复选框。
5. [可选] 选择电子邮件通知中将使用的语言。
6. 选中要接收相关通知的事件的复选框。您可以从按严重性排序的所有可能警告的列表中选择相应事件。
7. 单击**保存**。

电子邮件服务器

您可以指定将用于从管理服务器发送电子邮件通知的电子邮件服务器。

指定电子邮件服务器

1. 依次单击**设置** > **系统设置** > **电子邮件服务器**。
2. 在**电子邮件服务**中，选择以下各项之一：
   - **自定义**
   - **Gmail**
   - **Yahoo Mail**
   - **Outlook.com**
3. [仅适用于自定义电子邮件服务] 指定以下设置：
   - 在 **SMTP 服务器**中，输入发送邮件服务器 (SMTP) 的名称。
   - 在 **SMTP 端口**中，设置发送邮件服务器的端口。默认情况下，端口设为 25。
   - 选择使用 SSL 加密还是使用 TLS 加密。选择**无**以禁用加密。
   - 如果 SMTP 服务器需要身份验证，请选中 **SMTP 服务器需要身份验证**复选框，然后指定将用于发送邮件的帐户的凭据。如果您不确定 SMTP 服务器是否要求身份验证，请联系您的网络管理员或电子邮件服务提供商以获取帮助。
4. [仅用于 Gmail、Yahoo Mail 和 Outlook.com] 指定将用于发送邮件的帐户的凭据。
5. [仅限于自定义电子邮件服务] 在**发件人**中，键入发件人的姓名。此姓名将显示在电子邮件通知的**发件人**字段中。如果将此字段留空，邮件将包含在步骤 3 或4 中指定的帐户。
6. [可选] 单击**发送测试邮件**以检查使用指定的设置时电子邮件通知是否正确工作。输入用于接收测试邮件的电子邮件地址。

安全

这些选项用于提高 Acronis 安克诺斯数据保护软件 本地部署的安全性。

在此时间后，注销非活动用户

此选项可让您指定因用户闲置而自动注销的超时时间。当所设置超时时间还剩余一分钟时，软件会提示用户保持登录状态。否则，将注销用户，并且所有未保存的更改都将丢失。

预设为：**已启用。超时：10 分钟。**

显示关于当前用户上次登录的通知

此选项支持显示用户上次成功登录的日期和时间、自上次成功登录以来的身份验证失败次数以及上次成功登录的 IP 地址。此信息在用户每次登录时显示在屏幕底部。

预设为：**已禁用**。

关于本地或域密码过期的警告

此选项支持显示用户访问 Acronis 安克诺斯数据保护软件 管理服务器的密码何时到期。这是用户登录到安装管理服务器的计算机所用的本地或域密码。密码到期的剩余时间显示在屏幕底部以及右上角的帐户菜单中。

预设为:**已禁用**。

更新

此选项定义 Acronis 安克诺斯数据保护软件 在组织管理员每次登录到 安克诺斯数据保护软件 Web 中控台时检查是否有新版本。

预设为:**已启用**。

如果此选项已禁用,管理员可按"检查软件更新"中所述,手动检查更新。

默认备份选项

对于管理服务器上的所有备份计划,保护选项的默认值是相同的。组织管理员可以对预定义的备份选项更改默认选项值。在默认情况下,新值将用于更改发生后所创建的所有保护计划。

创建保护计划时,用户可以使用仅特定于此计划的自定义值覆盖默认值。

更改默认选项值

1. 以组织管理员身份登录 安克诺斯数据保护软件 Web 中控台。
2. 单击**设置** > **系统设置**。
3. 展开**默认备份选项**部分。
4. 选择该选项,然后做出所需更改。
5. 单击**保存**。

保护设置

要配置保护设置，请在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **保护**。

有关特定设置和步骤的详细信息，请参阅本部分中的相应主题。

更新保护定义

默认情况下，所有保护代理程序都可以连接到 Internet 并下载以下组件的更新：

- 反恶意软件
- 漏洞评估
- 修补程序管理

角色为“更新程序”的代理程序

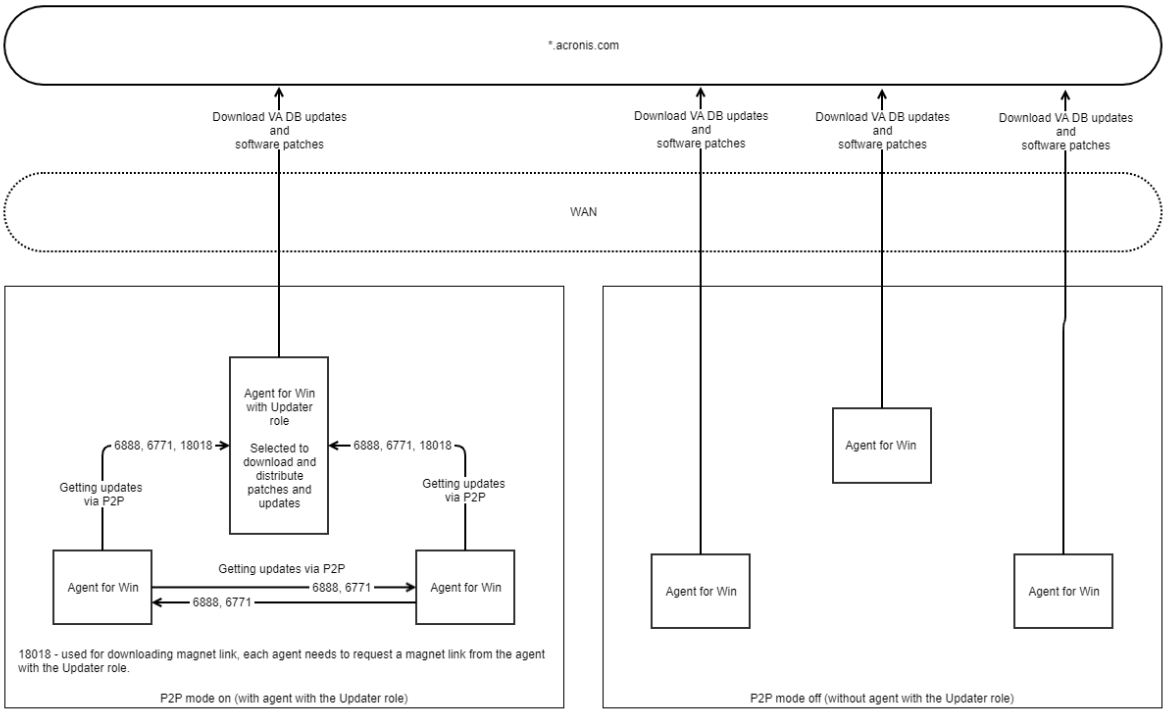
管理员可以通过在环境中选择一个或多个保护代理程序并将“更新程序”角色指派给它们，来最大程度地减少网络带宽流量。这样，专用代理程序将连接到 Internet 并下载更新。通过使用点对点技术，所有其他代理程序将连接到专用更新程序代理程序，然后从中下载更新。

如果环境中没有专用更新程序代理程序，或者如果专用更新程序代理程序的连接不能建立大约五分钟，那么没有“更新程序”角色的代理程序将连接到 Internet。

在将“更新程序”角色指派给代理程序之前，确保运行代理程序的计算机足够强大，并且有稳定的高速 Internet 连接和足够的磁盘空间。

可以将“更新程序”角色指派给环境中的多个代理程序。这样一来，如果角色为“更新程序”的代理程序脱机，则具有此角色的其他代理程序可以充当更新保护定义的源。

下图说明了下载保护更新的选项。在左侧，代理程序已被指派更新器角色。代理程序连接到互联网以下载保护更新，而其对等代理程序则连接到更新器代理程序以获取最新更新。在右侧，无代理程序已被指派更新器角色，因此所有代理程序均连接到互联网以下载保护更新。



为“更新程序”角色准备计算机

1. 在将运行角色为“更新程序”的代理程序的计算机上，请应用以下防火墙规则：
   - 入站（传入）“updater_incoming_tcp_ports”：对于所有防火墙配置文件（公共、专用和域），允许连接到 TCP 端口 18018 和 6888。
   - 入站（传入）“updater_incoming_udp_ports”：对于所有防火墙配置文件（公共、专用和域），允许连接到 UDP 端口 6888。
2. 重新启动 Acronis 代理程序核心服务。
3. 重新启动防火墙服务。

如果不应用这些规则并启用了防火墙，则对等代理程序将从云端下载更新。

要将“更新”角色指派给代理程序

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **代理程序**。
2. 选择要向其指派更新器角色的装有代理程序的计算机。
3. 单击**详细信息**，然后启用**使用此代理程序来下载和分发修补程序与更新**开关。

预定更新

可以在所有代理程序上预定对保护定义的自动更新，也可以在选定代理程序上手动更新保护定义。

预定自动更新

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **保护** > **保护定义更新**。
2. 选择**预定**。

3. 在**预定类型**中，选择以下选项之一：
   - **每日**

     选择周几更新保护定义。

     在**开始时间**中，选择更新开始的时间。
   - **每小时**

     设置更新的粒度预定。

     在**运行间隔**中，设置更新的周期。

     在**从 ... 至**中，设置更新的特定时间范围。

手动更新保护定义

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **代理程序**。
2. 选择要更新其代理程序保护定义的计算机，然后单击**更新定义**。

更改下载位置

保护定义会先下载到计算机上的默认临时文件夹中，然后再存储在 Acronis 程序文件夹中。

更改用于下载的临时文件夹

1. 在管理服务器计算机上，打开 `atp-database-mirror.json` 文件进行编辑。

   可以在以下位置找到此文件：
   - Windows：`%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux：`/var/lib/Acronis/AtpDatabaseMirror/`
2. 将“`enable_user_config`”的值更改为 `true`。

```
{
"sysconfig":
{
...
"enable_user_config": true
}
...
}
```

3. 在管理服务器计算机上，打开 `config.json` 文件进行编辑。

   可以在以下位置找到此文件：
   - Windows：`%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux：`/var/lib/Acronis/AtpDatabaseMirror/`
4. 添加以下行：`"mirror_temp_dir": "<path_to_new_download_location>"`

   例如：

```
{
        "mirror_temp_dir":"C:\\temp"
}
```

该路径可以是指向 AppData 文件夹的绝对路径或相对路径。
如果该文件夹无法创建，或者管理服务器无法写入它，将使用默认位置。

缓存存储选项

缓存的数据存储在以下位置：

- Windows：C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache
- Linux：/opt/acronis/var/atp-downloader/Cache
- macOS：/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache

可以配置清理过时缓存数据的预定，并为其大小设置限制。可以为不装有更新程序代理程序的计算机和装有更新程序代理程序的计算机设置不同的限制。

最新保护定义的源

可以从以下位置下载最新保护定义：

- **云**
  保护代理程序会连接到 Internet 并从 Acronis 云下载最新保护定义。默认情况下，所有代理程序均已在管理服务器上进行注册，检查更新并进行分发。有关角色为“更新程序”的代理程序的详细信息，请参阅 "更新保护定义"(第 540 页)。
- **安克诺斯数据保护软件 管理服务器**
  选中此选项后，代理程序无需访问 Internet。它们只需连接到存储有保护定义的管理服务器。但是，管理服务器需要连接到互联网才能下载最新的保护定义。
- **自定义 Web 服务器**
  此选项专用于故障排除和测试目的，或用于气隙环境。有关详细信息，请参阅 "更新气隙环境中的保护定义"(第 544 页)。通常，仅当 Acronis 支持团队指示执行此操作时，才需要选择此选项。

远程连接

当启用远程连接时，选项**通过 RDP 客户端连接**和**通过 HTML5 客户端连接**选项会出现在 安克诺斯数据保护软件 Web 中控台中右侧菜单中的**网络安全保护桌面**下。当在**设备**选项卡中选择一个工作负载时，右侧菜单即会打开。

启用或禁用远程连接会影响贵组织的所有用户。

启用远程连接

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **保护**。
2. 单击**远程连接**，以启用**远程桌面连接**开关。

此外，还可以启用远程连接共享。使用此选项，可以生成允许远程访问选定工作负载的链接。可以与其他用户共享这些链接。

启用远程连接共享

1. 在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **保护**。
2. 选中**共享远程桌面连接**复选框。

结果，**共享远程连接**选项出现在 安克诺斯数据保护软件 Web 中控台中的右侧菜单中的**网络安全保护桌面**下。

更新气隙环境中的保护定义

Acronis 安克诺斯数据保护软件 支持更新气隙环境中的保护定义。

更新气隙环境中的保护定义

1. 在您的气隙环境之外，安装可以访问 Internet 的第二个管理服务器。
   有关如何执行此操作的详细信息，请参阅 "安装管理服务器"(第 75 页)。
2. 将保护定义从在线管理服务器复制到可移动驱动器，然后将定义传输到气隙环境中的 HTTP 服务器。
   有关此步骤的详细信息，请参阅 "将定义下载到在线管理服务器"(第 544 页) 和 "将定义传输到 HTTP 服务器"(第 545 页)。
3. 在气隙管理服务器上，将 HTTP 服务器配置为更新保护定义的源。
   有关此步骤的详细信息，请参阅 "在气隙管理服务器上配置定义源"(第 546 页)。

将定义下载到在线管理服务器

在安装第二个可以访问 Internet 的管理服务器后，下载最新保护定义并将其复制到可移动驱动器(例如，USB 闪存或外部硬盘驱动器)。

下载和复制保护定义

1. 在管理服务器在线的计算机上，将 `AtpDatabaseMirror` 文件夹复制到您选择的位置(例如，桌面或 `Temp` 文件夹)。
   可以在以下位置找到 `AtpDatabaseMirror` 文件夹：
   - Windows：`%ProgramData%\Acronis\`
   - Linux：`/usr/lib/Acronis/`
2. 打开 `atp_database_mirror.json` 文件以进行编辑。可以在以下位置找到该文件：
   - Windows：`%Program Files%\Acronis\AtpDatabaseMirror`

     注意
     在 Windows 中，此文件夹与上一步中的文件夹不同。

   - Linux：`/usr/lib/Acronis/AppDatabaseMonitor`
3. 编辑 `atp_database_mirror.json` 文件，如下所示：
   a. 将“`enable_appdata_as_root`”的值更改为 `false`。
   b. 将所有“`local_path`”条目的值都更改为要保存保护定义的位置的绝对路径。
4. 将更改保存在 `atp_database_mirror.json` 文件中。
5. 在管理服务器在线的计算机上，使用以下命令停止 **Acronis Management Server** Service：

- Windows(命令提示符) :

```
sc stop AcrMngSrv
```

- Linux(终端) :

```
sudo systemctl stop acronis_ams.service
```

6. 在已复制到您选择的位置的 AtpDatabaseMirror 文件夹中, 使用以下命令启动 AtpDatabaseMirror 工具:
   - Windows(命令提示符) :

```
atp_database_mirror.exe -config atp_database_mirror.json
```

   - Linux(终端) :

```
sudo ./atp_database_mirror -config atp_database_mirror.json
```

   在所有更新都下载到您在“local_path”中指定的文件夹后, 以下行会显示在命令提示符下或终端窗口中:

```
standing by for 1m0s
```

7. 按 CTRL+C 组合键停止 AtpDatabaseMirror 工具。
8. 将在“local_path”中指定的文件夹中的文件复制到可移动驱动器。

接下来, 必须将可移动驱动器中的文件复制到您气隙环境中的 HTTP 服务器。可以将气隙管理服务器用作 HTTP 服务器。有关详细信息, 请参阅 "将定义传输到 HTTP 服务器"(第 545 页)。

将定义传输到 HTTP 服务器

要在气隙环境中分发保护定义, 您需要一个专用 HTTP 服务器。可以将气隙管理服务器用作 HTTP 服务器。

将保护定义传输到 HTTP 服务器

1. 在将运行 HTTP 服务器的计算机上, 将保护定义复制到选定的文件夹中。
2. 从复制其中保护定义的文件夹, 启动 HTTP 服务器。
   例如, 可以使用 Python 并运行以下命令:

```
python -m http.server 8080
```

   注意
   可以使用您偏爱的任何 HTTP 服务器。

3. 在复制其中保护定义的文件夹中, 打开以下 update-index.json 文件进行编辑:
   - ./ngmp/update-index.json
   - ./vapm/update-index.json

4. 在两个 update-index.json 文件中，编辑所有 products > os > arch > components > versions > url 字段，如下所示：
   a. 对于 IP 和 port 值，请设置 HTTP 服务器的 IP 地址和端口。
   b. 请勿更改路径的其他部分。
   例如，"url": "http://192.168.1.10:8080/ngmp/win64/ngmp.zip"，其中192.168.1.10 是 HTTP 服务器的 IP 地址，8080 是其端口。请勿更改 /ngmp/win64/ngmp.zip 部分。
5. 将所做编辑保存在两个 update-index.json 文件中。

接下来，必须在气隙管理服务器上配置保护定义的源。有关详细信息，请参阅 "在气隙管理服务器上配置定义源"(第 546 页)。

在气隙管理服务器上配置定义源

在配置 HTTP 服务器后，必须在气隙管理服务器上将其配置为保护定义的源。

在气隙管理服务器上配置保护定义的源

1. 在气隙管理服务器的 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **保护** > **保护定义更新**。
2. 选择**定义**。
3. 选择**自定义**，然后指定以下路径：

- 对于**防病毒和防恶意软件定义**：
  http://<IP address of your HTTP server>:8080/scanner
- 对于**高级检测定义**：
  http://<IP address of your HTTP server>:8080/ngmp
- 对于**漏洞评估和修补程序管理定义**：
  http://<IP address of your HTTP server>:8080/vapm

结果，气隙环境中的代理程序将从 HTTP 服务器下载保护定义。

管理用户帐户和组织单位

本地部署

本部分中介绍的功能仅对组织管理员可用。

要访问这些设置，请依次单击**设置** > **帐户**。

单位和管理帐户

要管理单位和管理帐户，请在 安克诺斯数据保护软件 Web 中控台中，转到**设置** > **帐户**。**帐户**面板显示**组织**组，包括单位(如有)的树图，以及在选定分层级别上的管理帐户列表。

单元

当安装管理服务器时，系统会自动创建**组织**组。使用 Acronis 安克诺斯数据保护软件 高级许可证，可以创建称为"单位"的子组(通常对应于组织的单位或部门)，而且可以向单位添加管理帐户。通过这种方法，即可将保护管理委派给访问权限严格限制在对应单元内的其他人员。有关如何创建单位的信息，请参阅 "创建单元"(第 550 页)。

每个单位都可以有子单位。父单位的管理帐户在其所有子单位中都有相同的权限。**组织**组是顶级父单位，此级别的管理帐户在所有单位中都有相同的权限。

管理帐户

任何能够登录 安克诺斯数据保护软件 Web 中控台的帐户都是管理帐户。

在 安克诺斯数据保护软件 Web 中控台中，任何管理帐户都可以查看或管理其单位的分层级别上或下的所有内容。例如，*组织*中的管理帐户可以访问此顶级，因此可以访问此组织的所有单位，而特定*单位*中的管理帐户仅可以访问此单位及其子单位。

可以管理哪些帐户?

如果管理服务器安装在包含在 Active Directory 域中的 Windows 计算机上，则可以向本地用户或 Active Directory 域林中的用户和用户组授予管理权限。

默认情况下，管理服务器会与 Active Directory 域控制器建立受 SSL/TLS 保护的连接。如果无法建立这种连接，则不会建立连接。但可以通过编辑 `auth-connector.json5` 文件，来允许建立不安全的连接。

要使用安全连接，请确保为 Active Directory 配置基于 SSL (LDAPS) 的 LDAP。

为 Active Directory 配置 LDAPS

1. 在域控制器上，创建并安装符合 Microsoft 要求的 LDAPS 证书。
   有关如何执行这些操作的详细信息，请参阅 Microsoft 文档中的通过第三方证书颁发机构启用基于 SSL 的 LDAP。

2. 在域控制器上，打开 **Microsoft 管理中控台**，然后验证该证书是否存在于**证书(本地计算机)** > **个人** > **证书**下。
3. 重新启动域控制器。
4. 验证 LDAPS 是否已启用。

允许与域控制器建立不安全的连接

1. 登录到安装了管理服务器的计算机。
2. 打开 `auth-connector.json5` 文件以进行编辑。

   `auth-connector.json5` 文件位于 `%APPDATA%\Acronis\AuthConnector` 中。
3. 导航到 **sync** 部分，然后在**"connectionMode"**的每一行中，将**"ssl_only"**替换为**"auto"**。

   在**自动**模式下，如果无法建立 TLS 连接，则会建立不安全的连接。
4. 重新启动 **Acronis Service Manager 服务**，如 "重新启动 Acronis Service Manager 服务"(第 175 页) 中所述。

注意

如果管理服务器未包含在 Active Directory 域中，或者它安装在 Linux 计算机上，则只能将管理权限授予本地用户和组。

要了解如何将管理帐户添加到管理服务器，请参阅 "添加管理帐户"(第 550 页)。

管理帐户角色

为每个管理帐户指派角色，该角色具有特定任务所必需的预定义权限。管理帐户角色包括：

- **管理员**
  此角色提供对组织或单位的完全管理访问权限。
- **只读**
  此角色提供对 安克诺斯数据保护软件 Web 中控台的只读访问权限。它只允许收集诊断数据，如系统报告。此只读角色不允许浏览备份或浏览备份邮箱的内容。
- **审核者**
  此角色提供对 安克诺斯数据保护软件 Web 中控台中**活动**选项卡的只读访问权限。有关此选项卡的详细信息，请参阅 ""活动"选项卡"(第 503 页)。此角色不允许收集或导出任何数据，包括管理服务器的系统信息。

角色的任何更新显示在**活动**选项卡上。

角色的继承

父单位中的角色由其子单位继承。如果同一用户帐户在父单位和子单位中被指派了不同的角色，则它将同时担扮演这两个角色。

此外，角色可以明确指派给特定的用户帐户或从用户组继承。因此，用户帐户可以同时具有指派的角色和继承的角色。

如果用户帐户具有不同的角色(指派的角色和/或继承的角色)，则它可以访问对象并执行这些角色允许的任何操作。例如，指派了只读角色和继承了管理员角色的用户帐户将具有管理员权限。

重要事项
在 安克诺斯数据保护软件 Web 中控台中，只显示为当前单位明确指派的角色。不会显示继承角色的任何可能差异。强烈建议您将管理员角色、只读角色和审核者角色指派给单独的帐户或组，以避免继承的角色可能出现的问题。

默认管理员

在 Windows 中

当在计算机上安装管理服务器时，会发生以下情况：

- 系统会在计算机上创建 **Acronis Centralized Admins** 用户组。
  在域控制器上，组命名为 *DCNAME* **$ Acronis Centralized Admins**。其中，*DCNAME* 表示域控制器的 NetBIOS 名称。
- **管理员**组的所有成员都会添加到 **Acronis Centralized Admins** 组中。如果计算机在域中但不是域控制器，则会排除本地(非域)用户。在域控制器上，不存在非域用户。
- **Acronis Centralized Admins** 和**管理员**组都会作为**组织管理员**添加到管理服务器中。如果计算机在域中但不是域控制器，则不会添加**管理员**组，因此本地(非域)用户不会成为组织管理员。

您可以从组织管理员列表中删除**管理员**组。但是，无法删除 **Acronis Centralized Admins** 组。在极少数已删除所有组织管理员的情况下，可以在 Windows 中向 **Acronis Centralized Admins** 组添加帐户，然后使用该帐户登录 安克诺斯数据保护软件 Web 中控台。

在 Linux 中

当在计算机上安装管理服务器时，会将**根**用户作为**组织管理员**添加到管理服务器。

可以将其他 Linux 用户添加到管理服务器管理员列表(稍后会介绍)，然后从该列表中删除**根**用户。在极少数已删除所有组织管理员的情况下，可以重新启动 `acronis_asm` 服务。因此，**根**用户将作为组织管理员自动重新添加。

多个单位中的管理帐户

可以向一个帐户授予任意数量单位中的管理权限。对于此类帐户以及组织级别上的管理帐户，安克诺斯数据保护软件 Web 中控台中会显示单位选择器。通过使用此选择器，此帐户可以单独查看和管理每个单位。

具有组织中所有单元权限的帐户并不具有该组织权限。组织级别上的管理帐户在必须明确添加至**组织**组中。

如何为单元填充计算机

当管理员通过 Web 界面添加计算机时，计算机会被添加至相应管理员管理的单元中。如果管理员管理多个单元，则该计算机会被添加至单元选择器中所选的单元中。因此，管理员必须在单击**添加**之前选择相应单元。

当以本地方式安装代理程序时，管理员应提供其凭据。计算机会被添加至相应管理员管理的单元中。如果管理员管理多个单元，则安装程序会提示管理员选择计算机将要添加到的单元。

添加管理帐户

注意
该功能在标准版及 Essential 版中不可用。

若要添加帐户

1. 依次单击**设置** > **帐户**。
   软件将显示管理服务器管理员列表和单元树（如有）。
2. 选择**组织**或选择要添加管理员的单元。
3. 单击**添加帐户**。
4. 在**域**中，选择含有要添加的用户帐户的域。如果管理服务器不属于 Active Directory 域或安装在 Linux 中，则只能添加本地用户。
5. 搜索用户名或用户组名称。
6. 单击用户或组的名称旁边的“+”号。
7. 选择帐户的角色。
8. 对要添加的所有用户或组重复第 4-6 步。
9. 完成后单击**完成**。
10. [仅在 Linux 中] 将用户名添加到 Acronis 模块的嵌入式身份验证模块 (PAM) 配置，如下所述。

将用户名添加到 Acronis 的 PAM 配置

此过程适用于在 Linux 计算机上和 Acronis 安克诺斯数据保护软件 一体式设备中运行的管理服务器。

1. 在运行管理服务器的计算机上，以根用户身份使用文本编辑器打开文件 **/etc/security/acronisagent.conf**。
2. 在此文件中，键入作为管理服务器管理员添加的用户名，一行一个。
3. 保存并关闭文件。

创建单元

1. 依次单击**设置** > **帐户**。
2. 软件将显示管理服务器管理员列表和单元树（如有）。
3. 选择**组织**或为新单元选择父单元。
4. 单击**创建单元**。
5. 为新单元指定名称，然后单击**创建**。

云部署

可在管理门户中管理用户帐户和组织单位。要访问管理门户，请在登录网络安全保护服务时单击**管理门户**，或单击右上角的

 图标，然后单击**管理门户**。仅拥有管理权限的用户可访问此门户。

有关管理用户帐户和组织单位的信息，请参阅“管理门户管理员指南”。要访问该文档，请单击管理门户中的问号图标。

本部分提供了与管理网络安全保护服务相关的其他信息。

限额

配额使您能够限制用户使用服务的能力。要设置配额，请在**用户**选项卡上选择用户，然后在**配额**部分中单击铅笔图标。

当超出配额时，将向用户的电子邮件地址发送一条通知。如果未设置配额超额，则将该配额视为“软配额”。这意味着不会对使用网络安全保护服务施加限制。

还可指定配额超额。超额允许用户超出指定值的配额。当超出超额时，系统会对使用网络安全保护服务施加限制。

备份

可指定云存储空间配额、本地备份的配额以及允许用户保护的最大计算机/设备/邮箱数量。以下配额可用：

- **云存储**
- **工作站**
- **服务器**
- **Windows Server Essentials**
- **虚拟主机**
- **通用**

  此配额可用于替代以上所列的四个配额中任意之一：工作站、服务器、Windows Server Essentials、虚拟主机。
- **移动设备**
- **Microsoft 365 邮箱**
- **本地备份**

只要向计算机/设备/网站应用至少一个保护计划，相应计算机/设备/网站就被视为受到保护。移动设备在第一次备份后进入受保护状态。

超出云存储空间配额超额时，备份失败。当超出许多设备的超额时，用户无法将保护计划应用于更多设备。

本地备份配额可限制使用云基础架构创建的本地备份的总大小。不能为此配额设置超额。

灾难恢复

这些配额由服务提供商应用于整个公司。公司管理员可以在管理门户中查看配额和使用情况，但无法为用户设置配额。

- **灾难恢复存储**

  此存储由主服务器和恢复服务器使用。如果达到此配额的超额，则无法创建主服务器和恢复服务器，或添加/扩展现有主服务器的磁盘。如果超过此配额的超额，则无法启动故障转移或仅启动已停止的服务器。正在运行的服务器继续运行。

  禁用配额后，将删除所有服务器。**云恢复站点**选项卡会从 安克诺斯数据保护软件 Web 中控台中消失。
- **计算点**

  此配额可限制计费期内主服务器和恢复服务器使用的 CPU 和 RAM 资源。如果达到此配额的超额，则所有主服务器和恢复服务器都将关机。在下一个计费期开始之前，无法使用这些服务器。默认计费期为一个完整的日历月。

  当配额禁用时，无论计费期如何，都无法使用服务器。
- **公共 IP 地址**

  此配额限制可以指派给主服务器和恢复服务器的公共 IP 地址的数量。如果达到此配额的超额，则无法为更多服务器启用公共 IP 地址。可以通过在服务器设置中取消选中**公共 IP 地址**复选框，来禁止服务器使用公共 IP 地址。之后，可以允许另一台服务器使用公共 IP 地址，这通常不会是同一个 IP 地址。

  当配额禁用时，所有服务器将停止使用公共 IP 地址，从而无法通过 Internet 进行访问。
- **云服务器**

  此配额可限制主服务器和恢复服务器的总数。如果达到此配额的超额，则无法创建主服务器或恢复服务器。

  当配额禁用后，服务器会在 安克诺斯数据保护软件 Web 中控台中可见，但唯一可进行的操作是**删除**。
- **Internet 访问**

  此配额可启用或禁用主服务器和恢复服务器的 Internet 访问。

  当配额禁用后，主服务器和恢复服务器将立即与 Internet 断开连接。服务器属性中的 **Internet 访问**开关被清除并禁用。

通知

要更改用户的通知设置，请在**用户**选项卡上选择用户，然后在**设置**部分中单击铅笔图标。以下通知设置可用：

- **配额过度使用通知**(默认已启用)

  关于超出配额的通知。
- **预定使用情况报告**

  下面描述的使用情况报告是在每个月的第一天发送。
- **失败通知**、**警告通知**和**成功通知**(默认禁用)

  有关每台设备的保护计划执行结果和灾难恢复操作结果的通知。
- **活动警告的每日概述**(默认启用)

  关于失败的备份、缺少的备份以及其他问题的通知概述。概述于 10:00(数据中心时间)发送。如果当前没有出现任何问题，则不会发送概述。

所有通知都发送到用户的电子邮件地址。

报告

有关使用网络安全保护服务的报告包括组织或单位的以下相关数据：

- 按单位、按用户、按设备类型分类的备份大小。
- 按单位、按用户、按设备类型分类的受保护设备数。
- 按单位、按用户、按设备类型分类的价值。
- 备份的总大小。
- 受保护设备的总数。
- 总价值。

命令行参考

命令行参考是一份单独文档，位于以下位置：https://www.acronis.com/en-us/support/documentation/AcronisCyberProtect_15_Command_Line_Reference/index.html。

疑难解答

本部分介绍如何将代理程序日志保存到 .zip 文件。如果备份由于不明原因而失败，则此文件将帮助技术支持人员识别问题。

收集日志

1. 请执行以下任一操作：
   - 在**设备**下，选择要从中收集日志的计算机，然后单击**活动**。
   - 在**设置** > **代理程序**下，选择要从中收集日志的计算机，然后单击**详细信息**。
2. 单击**收集系统信息**。
3. 如果 Web 浏览器提示您，请指定保存文件的位置。

词汇表

备

备份集

一组可以应用个别保留规则的备份。对于自定义备份方案，备份集对应于备份方法(完整、差异和增量)。在所有其他情况下，备份集为“每月”、“每日”、“每周”和“每小时”。每月备份是一个月开始后创建的第一个备份。每周备份是在每周备份选项(单击齿轮图标，然后依次单击“备份选项”>“每周备份”)中所选日创建的第一个备份。如果每周备份是一个月开始后创建的第一个备份，则该备份视为每月备份。在此情况下，将在下周的所选日创建每周备份。除非每日备份符合每月备份或每周备份的定义，否则每日备份是某日开始后创建的第一个备份。除非每小时备份符合每月备份、每周备份或每日备份的定义，否则每小时备份是某个小时开始后创建的第一个备份。

差

差异备份

差异备份存储对上次完整备份数据的更改。您需要访问相应的完整备份来从差异备份中恢复数据。

单

单文件备份格式

一种新的备份格式，初始完整和后续增量备份使用此格式(而不是文件链)保存到单个 .tib 文件。此格式利用了增量备份方法的速度，同时避免了其主要劣势，即难以删除过期备份。软件将过期备份使用的块标记为“可用”，并将新备份写入这些块。这导致清理速度极快，资源消耗最少。当备份到不支持随机存取读写的位置(例如，SFTP 服务器)时，单文件备份格式不可用。

启

启动恢复管理器

修改系统磁盘上的可启动代理，并配置为在启动时间按下 F11 时启动。启动恢复管理器无需应急媒体或网络连接，即可启动可启动应急实用程序。启动恢复管理器对移动用户特别有用。如果发生故障，用户重新启动计算机、根据提示“按 F11 运行启动恢复管理器...”点击 F11 键，然后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：需要重新激活 Windows 加载程序和 GRUB 以外的加载程序。

受

受控位置

备份位置由存储节点管理。从物理角度看，受控位置可存放在网络共享、SAN、NAS、与存储节点本地连接的硬盘或与存储节点本地连接的磁带库中。存储节点为存储在受控位置中的各备份执行清理和验证操作(如果这些包含在保护计划中)。您可指定存储节点将执行的其他操作(重复数据删除、加密)。

完

完整备份

包含所有选择的备份数据的自足式备份。您无需访问任何其他备份即可从完整备份中恢复数据。

增

增量备份

存储对上次备份数据所作更改的备份。您需要访问其他备份来从增量备份中恢复数据。

索引

按

白

版

包

保

报

备

本

编

变

并

不

步

部

还

忽

缓

恢

获

基

软

扫

删

设

什

升

实

使

准

自

组

最

作