Acronis

acronis.com

网络安全保护

24.09

用户指南

修改：2024/10/10

目录

Cyber Protection 入门指南

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：

- **您的登录名。**这是您用于登录的用户名。您的登录名也会显示在帐户激活页面上。
- **激活帐户**按钮。单击该按钮并为您的帐户设置密码。确保密码的长度至少为九个字符。有关密码的详细信息，请参阅 "密码要求"(第 19 页)。

如果管理员已启用双重身份验证，则系统会提示您为您的帐户设置它。有关它的详细信息，请参阅 "双重身份验证"(第 19 页)。

密码要求

用户帐户的密码长度必须至少为 9 个字符。还会检查密码的复杂性，并分为以下类别之一：

- 弱
- 中
- 强

不会保存弱密码，即使它可能包含 9 个或更多字符也是如此。反复出现用户名、登录名、用户电子邮件地址或用户帐户所属租户的名称的密码始终被视为弱密码。最常见的密码也会被视为弱密码。

要加强密码，请向其中添加更多字符。不强制使用不同类型的字符(例如，数字、大写和小写字母以及特殊字符)，但它会生成长度更短的更强密码。

双重身份验证

双重身份验证 (2FA) 会提供其他保护，以免未经授权访问您的帐户。在设置 2FA 后，您需要输入密码(第一个因素) 和一次性代码(第二个因素) 才能登录到 Cyber Protect 中控台。一次性代码由必须安装在您的手机或其他设备上的特定应用程序生成。即使某人得到您的登录名和密码，如果他们无权访问您的第二因素设备，也无法登录到您的帐户。

为账户设置双重身份验证

如果管理员已为组织启用 2FA，则必须为帐户设置 2FA。如果管理员在您已登录到 Cyber Protect 中控台期间启用 2FA，则您需要在当前会话到期后设置 2FA。

先决条件

- 管理员已为您的组织启用了双重身份验证。

为帐户设置双重身份验证

1. 选择第二重身份验证设备。
   最常见的是手机，但也可以使用平板电脑、笔记本电脑或台式机。
2. 在第二因素设备上安装身份验证器应用程序。

身份验证器应用程序示例：

- Microsoft Authenticator
- Google Authenticator
- Twilio Authy

3. 使用身份验证器应用程序扫描二维码，然后在**设置双重身份验证**窗口中输入身份验证器应用程序上显示的 6 位代码。
4. 单击**下一步**。

   如果丢失 2FA 设备或卸载身份验证器应用程序，则有关如何恢复对您帐户的访问的说明即会显示。
5. 保存或打印 PDF 文件。

   注意

   确保将 PDF 文件保存在安全的地方或打印出来以供进一步参考。这是恢复您的访问的最佳方法。
6. 返回到 Cyber Protect 中控台登录页面，然后输入生成的代码。

   一次性代码在 30 秒内有效。如果等待时间超过 30 秒，请使用生成的下一个代码。

注意

如果您的身份验证器应用程序支持备份，则建议您将配置备份到云。

下次登录时，可以选中**信任此浏览器...**复选框。在这种情况下，在本计算机上使用此浏览器进行后续登录时将不需要该代码。

注意

建议您清除此复选框。否则，您将无法通过 2FA 设置来访问您的帐户。

在新设备上配置双重身份验证 (2FA)

如果您可以访问先前配置的身份验证应用程序，则可使用此过程。

1. 在新设备上安装身份验证器应用程序。
2. 使用在设备上配置 2FA 时保存的 PDF 文件。

   文件的默认名称为 `cyberprotect-2fa-backupcode.pdf`。此文件包含您必须在身份验证器应用程序中输入的 32 位代码，以将身份验证器应用程序再次链接到您的 Acronis 帐户。

   重要事项

   如果代码不起作用，请确保身份验证器移动应用程序中的时间已与您的设备同步。

如果在设置过程中并未保存该 PDF 文件：

1. 单击**重置 2FA**，然后输入在移动身份验证器应用程序中显示的一次性密码。
2. 按照屏幕上的说明操作。

启用双重验证时，若要恢复对您的帐户的访问

当您无法访问先前配置的身份验证器应用程序时，这些选项适用。例如，设备丢失、被盗或被擦除。

- 若要再次设置 TOTP 身份验证器应用程序，请使用初始配置 2FA 时提供的 2FA 代码。文件的默认名称为 `cyberprotect-2fa-backupcode.pdf`。
- 如果您在身份验证器应用程序中有备份，请从备份还原双因素身份验证配置。
- 若要重设双重身份验证设置，请联系可访问云管理门户的管理员账号。
- 请向您的服务提供商请求重设双重身份验证设置。
- 请联系供应商支持团队以寻求协助。

隐私设置

隐私设置可帮助您表明是否同意收集、使用和披露您的个人信息。

根据您使用 Cyber Protect Cloud 所做的国家/地区和为您提供服务的 Cyber Protect Cloud 数据中心，在首次启动推出 Cyber Protect Cloud 时，系统可能会要求您确认是否同意在 Cyber Protect Cloud 中使用 Google Analytics。

Google Analytics 通过收集匿名数据，帮助我们更好地了解用户行为并改善 Cyber Protect Cloud 中的用户体验。

如果在首次启动 Cyber Protect Cloud 时启用或拒绝启用 Google Analytics，可以在以后随时改变您的决定。

启用或禁用 Google Analytics

1. 在 Cyber Protect 中控台中，单击**管理帐户**。
2. 单击右上角的帐户图标。
3. 选择**我的隐私设置**。**我的隐私设置**窗口即会显示。
4. 在 **Google Analytics 数据收集**部分中，单击以下按钮之一：
   - **打开** - 启用 Google Analytics
   - **关闭** - 禁用 Google Analytics

在**如何删除 Cookie** 部分中，可以直接在浏览器中控制和管理 Cookie。

注意
如果您没有看到 Google Analytics 部分，这意味着您所在的国家/地区未使用 Google Analytics。

在试用期最初显示的**产品内引导和交互式帮助**部分中，可以停止或继续将来在程序中接收有关改进和新功能的信息。此功能默认处于启用状态，但可以通过将开关切换到**关闭**来禁用该功能。

访问 Cyber Protection 服务

激活帐户后，可以通过登录到 Cyber Protect 中控台或通过管理门户访问 Cyber Protection 服务。

登录到 Cyber Protect 中控台

1. 转到 Cyber Protection 服务登录页面。
2. 键入登录名，然后单击**下一步**。

3. 键入密码，然后单击**下一步**。
4. [如果您使用多个 Cyber Protect Cloud 服务] 单击**网络安全保护**。
   仅有权访问 Cyber Protection 服务的用户才能直接登录到 Cyber Protect 中控台。

   如果**网络安全保护**不是您有权访问的唯一服务，则可以使用右上角的  图标切换这些服务。
   管理员也可以使用此图标切换到管理门户。

Cyber Protect 中控台的超时时长：活动会话为 24 小时，空闲会话为 1 小时。

单击右上角的帐户图标，可以更改 Web 界面的语言。

通过管理门户访问 Cyber Protect 中控台

1. 在管理门户中，转到**监控** > **使用情况**。
2. 在 **Cyber Protect** 下，选择**保护**，然后单击**管理服务**。
   或者，在**客户端**下，选择一个客户，然后单击**管理服务**。

因此，系统会将您重定向到 Cyber Protect 中控台。

重要事项
如果客户处于**自助服务**管理模式下，则无法为其管理服务。只有客户管理员才能将客户模式更改为**由服务提供商管理**，然后管理服务。

重置密码

1. 转到 Cyber Protection 服务登录页面。
2. 键入登录名，然后单击**下一步**。
3. 单击**忘记密码？**
4. 通过单击**发送**，确认您想要进一步的说明。
5. 按照接收到的电子邮件中的说明进行操作。
6. 设置新密码。

软件要求

支持的 Web 浏览器

Cyber Protect 中控台使用 TLS 1.2 协议并支持以下 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
- 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

以下信息适用于备份和恢复。有关操作系统支持的保护功能的详细信息，请参阅 "操作系统支持的保护功能"(第 42 页)。

适用于 Windows 的代理程序

此代理程序包含支持不同操作系统的 URL 过滤组件的防病毒和防恶意软件保护以及 URL 筛选。请参阅 "支持的防病毒和防恶意软件保护操作系统"(第 728 页)。

注意
下面支持的操作系统列表适用于备份和恢复。

- Windows XP Professional SP1 (x64)、SP2 (x64)、SP3 (x86)
- Windows Server 2003 SP1/2003 R2 及更高版本 – Standard 和 Enterprise 版(x86、x64)
- Windows Small Business Server 2003/2003 R2
- Windows Server 2008、Windows Server 2008 SP2* - 标准版、企业版、Datacenter 版、基础版和 Web 版(x86, x64)
- Windows Small Business Server 2008, Windows Small Business Server 2008 SP2*
- Windows 7 - 所有版本

  注意
  要在 Windows 7 中使用 Cyber Protection，必须在安装保护代理程序之前先安装 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

注意

* 要将 Cyber Protection 与此版本的 Windows 一起使用，必须在安装保护代理程序之前先安装 Microsoft 提供的 SHA2 代码签名支持更新 (KB4474419)。

有关与 SHA2 代码签名支持更新相关问题的信息，请参阅此知识库文章。

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

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。

适用于防止数据丢失的代理程序

设备控制

- Microsoft Windows 7 Service Pack 1 及更高版本
- Microsoft Windows Server 2008 R2 及更高版本
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

注意

面向 macOS 的适用于防止数据丢失的代理程序仅支持 x64 处理器。不支持基于 ARM 的 Apple Silicon 处理器。

数据丢失预防

- Microsoft Windows 7 Service Pack 1 及更高版本
- Microsoft Windows Server 2008 R2 及更高版本

注意

适用于防止数据丢失的代理程序可能安装在不受支持的 macOS 系统上，因为它是适用于 Mac 的代理程序的重要组成部分。在此情况下，Cyber Protect 中控台将指示适用于防止数据丢失的代理程序已安装在计算机上，但设备控制和防止数据丢失功能将不起作用。设备控制功能仅在适用于防止数据丢失的代理程序支持的 macOS 系统上起作用。

适用于 Advanced Data Loss Prevention 的代理程序

- Microsoft Windows 7 Service Pack 1 及更高版本
- Microsoft Windows Server 2008 R2 及更高版本

适用于 File Sync & Share 的代理程序

如需支持的操作系统列表，请参阅《Cyber Files Cloud 用户指南》。

适用于 Exchange 的代理程序(针对邮箱备份)

- 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 Microsoft 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 MySQL/MariaDB 的代理程序

- 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

此代理程序包含支持不同操作系统的 URL 过滤组件的防病毒和防恶意软件保护以及 URL 筛选。请参阅 "支持的防病毒和防恶意软件保护操作系统"(第 728 页)。

注意
下面支持的操作系统列表适用于备份和恢复。

Cyber Protect Cloud 支持使用以下组件的 x86 和 x86_64 Linux 发行版：

- 内核版本从 2.6.9 至 6.9

  根据 www.kernel.org 中的发布版本，列出了支持的内核版本。某些发行版(如 Red Hat Enterprise Linux) 将新功能移植到旧版本内核。即使其版本在支持的范围内，这种特定于发行版的内核也可能不受支持。
- GNU C 库 (glibc) 2.3.4 或更高版本

已经专门测试了以下发行版。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，它们在所有必要的方案中可能仍能正常工作。如果您在使用 Cyber Protect Cloud 时遇到与发行版和内核版本的组合相关的问题，请联系支持团队进行进一步调查。

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*
- 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, 22.10, 23.04, 23.10, 24.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38, 39, 40
- 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, 12
- CentOS 5.x, 6.x, 7.x, 8.x*
- CentOS Stream 8*, 9*
- Oracle Linux 5.x、6.x、7.x、8.x*、9.0*、9.1*、9.2*、9.3*、9.4* - 包括 Unbreakable Enterprise Kernel 和 Red Hat Compatible Kernel

  注意
  在启用了安全引导的 Oracle Linux 8.6 及更高版本上安装保护代理程序，需要手动对内核模块签名。有关如何对内核模块签名的详细信息，请参阅此知识库文章。

- CloudLinux 5.x, 6.x, 7.x, 8.x*, 9.4*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*,9.0*, 9.1*, 9.2*, 9.3*, 9.4*

- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*, 9.4*
- ALT Linux 7.0

* 从 8.4 版本开始，仅支持 4.18 到 5.19 的内核

适用于 Mac 的代理程序

此代理程序包含支持不同操作系统的 URL 过滤组件的防病毒和防恶意软件保护以及 URL 筛选。请参阅 "支持的防病毒和防恶意软件保护操作系统"(第 728 页)。

注意
下面支持的操作系统列表适用于备份和恢复。

支持 x64 和 ARM 架构(在 Apple Silicon 处理器中使用，如 Apple M1 和 M2)。

注意
您不能恢复基于 Intel 的 Mac 对使用 Apple Silicon 处理器的 Mac 的磁盘级别备份，反之亦然。您可以恢复文件和文件夹。

- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13
- macOS Sonoma 14

重要事项
从版本 C23.07 开始，Cyber Protect Cloud 不再支持以下操作系统：OS X Yosemite 10.10、OS X El Capitan 10.11 和 macOS Sierra 10.12。

强烈建议您将操作系统升级到支持的版本，以确保兼容性并能够使用 Cyber Protect Cloud 的全部功能。

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 11(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 - 所有安装选项，Nano Server 除外

适用于 Virtuozzo 的代理程序

- Virtuozzo 6.0.10, 6.0.11, 6.0.12, 7.0.13, 7.0.14
- Virtuozzo Hybrid Server 7.5

适用于 Virtuozzo Hybrid Infrastructure的代理程序

Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0, 6.1, 6.2

适用于 Scale Computing HC3 的代理程序

Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4

适用于 oVirt 的代理程序

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

适用于 Synology 的代理程序

DiskStation Manager 6.2.x、7.x

适用于 Synology 的代理程序仅支持配备 x86_64 处理器的 NAS 设备。不支持 ARM 处理器。请参阅 Synology 知识中心。

Cyber Protect Monitor

- Windows 7 及更高版本
- Windows Server 2008 R2 及更高版本
- 适用于 Mac 的代理程序支持的所有 macOS 版本

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
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

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

注意
仅在 NFTS、REFS 和 FAT32 文件系统上运行的数据库支持 Microsoft SQL 备份。不支持 ExFat。

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

Cyber Protection 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
- Oracle 数据库版本 19c，所有版本
- Oracle 数据库版本 21c，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。

支持的 MySQL 版本

- 5.5.x - Community Server、Enterprise、Standard 和 Classic 版本
- 5.6.x - Community Server、Enterprise、Standard 和 Classic 版本
- 5.7.x - Community Server、Enterprise、Standard 和 Classic 版本
- 8.0.x - Community Server、Enterprise、Standard 和 Classic 版本

支持的 MariaDB 版本

- 10.0.x
- 10.1.x
- 10.2.x
- 10.3.x
- 10.4.x
- 10.5.x
- 10.6.x
- 10.7.x

所支持的虚拟化平台

下表概述了支持何种虚拟化平台。

有关基于代理程序和无代理程序备份之间差异的详细信息，请参阅"基于代理程序备份和无代理程序备份"(第 56 页)。

注意

如果您使用下面未列出的虚拟化平台或版本，**基于代理的备份(从来宾操作系统内部备份)**方法可能仍可在所有所需场景中正常工作。如果您遇到基于代理程序的备份问题，请联系支持团队进行进一步调查。

VMware

平台	无代理程序备份 (虚拟机监控程序级别上备份)	基于代理程序备份 (从来宾操作系统内备份)
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	受支持 **设备 > 添加 > 虚拟化主机 > VMware ESXi > 适用于在 Windows 中安装的代理程序** 或 **设备 > 添加 > 虚拟化主机 > VMware ESXi > 虚拟设备(OVF)**	受支持 **设备 > 添加 > 工作站**或**服务器 > Windows** 或 **Linux**
VMware vSphere Hypervisor (Free ESXi)**	不支持	受支持 **设备 > 添加 > 工作站**或**服务器 > Windows** 或 **Linux**
VMware Server(VMware 虚拟服务器) VMware Workstation VMware ACE VMware Player	不支持	受支持 **设备 > 添加 > 工作站**或**服务器 > Windows** 或 **Linux**

* 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。

注意
Cyber Protect Cloud 在支持的 vSphere 主版本中，正式支持任何更新。

例如，除非另有说明，否则 vSphere 8.0 支持包括支持此版本中的任何更新。例如，vSphere 8.0 Update 1 也与最初发布的 vSphere 8.0 一起受支持。

支持特定的 VMware vSphere 版本意味着也支持相应版本的 vSAN。例如，支持 vSphere 8.0 意味着也支持 vSAN 8.0。

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。
- **来宾 iSCSI 连接**
  适用于 VMware 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。由于 ESXi 虚拟机监控程序不会注意到此类卷，因此这些卷不包含在虚拟机监控程序级快照中，并会在备份中遭忽略，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。
- **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**
  - VMware 虚拟机：(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。此限制适用于 VMware。
  - Hyper-V 虚拟机：对于所有第 2 代虚拟机，在计算机恢复为新虚拟机或现有虚拟机后，将禁用“安全启动”。
- VMware vSphere 7.0 或更高版本不支持 **ESXi 配置备份**。
- **实例 UUID 为空的虚拟机不会出现在 Cyber Protect 中控台中**
  实例 `UUID` vSphere 属性 (`vc.uuid`) 为空的 VMware 虚拟机未在 Cyber Protect 中控台中列出。有关如何解决此问题的更多信息，请参阅此知识库文章。

- **保护代理程序上的网络设置**

  如果保护代理程序无法将 vCenter 中注册的 ESXi 主机的名称解析为 IP 地址，即使可以解析 vCenter 主机名，VMware 虚拟机的备份也可能会失败。会显示以下错误：“您无权访问此文件。”

  若要解决此问题，请通过配置 DNS 或修改`/etc/hosts`文件来编辑保护代理程序的网络设置。若要验证修复情况，请在具有保护代理程序的计算机上运行以下命令：

  ```
  ping <ESXi host name>
  ```

- **具有逻辑卷的计算机支持的操作**

  支持使用逻辑卷备份和恢复工作负载，例如 Windows 中的 LDM（动态磁盘）和 Linux 中的 LVM，但有一些限制。有关限制的更多信息，请参阅 "支持的逻辑卷操作"（第 52 页）。

Microsoft

Hyper-V 运行在超融合集群上的虚拟机 Storage Spaces Direct (S2D) 受支持。Storage Spaces Direct 还支持作为备份存储。

平台	无代理程序备份 （虚拟机监控程序级别上备份）	基于代理程序备份 （从来宾操作系统内备份）
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 11（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	受支持 **设备** > **添加** > **虚拟化主机** > **Hyper-V**	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**

平台	无代理程序备份 (虚拟机监控程序级别上备份)	基于代理程序备份 (从来宾操作系统内备份)
Windows Server 2022(包含 Hyper-V) – 所有安装选项，Nano Server 除外		
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	不支持	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**
Microsoft Virtual Server 2005	不支持	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**

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

限制

- **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 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。由于 Hyper-V 虚拟机监控程序不会注意到此类卷，因此这些卷不包含在虚拟机监控程序级快照中，并会在备份中遭忽略，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。
- **具有 & 符号的 VHD/VHDX 文件名**
  在运行 Windows Server 2016 或更高版本的 Hyper-V 主机上，如果最初使用 Hyper-V 2012 R2 或更早版本创建的旧虚拟机(版本 5.0) 的 VHD/VHDX 文件名包含 & 符号，则不能备份这些旧虚拟机。
  为了能够备份此类虚拟机，请在 Hyper-V Manager 中，从虚拟机拆离相应的虚拟磁盘、通过删除 & 符号编辑 VHD/VHDX 文件名，然后将磁盘重新附加到虚拟机。
- **Microsoft WMI 子系统上的从属关系**

Hyper-V 虚拟机的无代理备份依赖于 Microsoft WMI 子系统，特别是 `Msvm_VirtualSystemManagementService` 类。如果 WMI 查询失败，备份也将失败。有关 `Msvm_VirtualSystemManagementService` 类的更多信息，请参阅 Microsoft 文档。

- **具有 PMEM 磁盘的虚拟机**

  不支持备份具有持久内存 (PMEM) 磁盘的 Hyper-V 虚拟机。
- **跨平台恢复**

  如果 Hyper-V 代理程序将另一个代理程序创建的备份恢复为新的 Hyper-V 虚拟机，则生成的计算机为第一代。
- **安全启动**

  为了保证恢复第 2 代 Hyper-V 虚拟机的启动，已禁用安全启动。可以在 Hyper-V 管理工具中手动重新启用它。有关安全启动和第 2 代虚拟机的更多信息，请参阅Microsoft 文档。
- **Linux 虚拟机的崩溃一致备份**

  由于 Microsoft 的限制(无法为 Linux 虚拟机创建生产检查点)，在 Hyper-V 2019 主机上运行的 Linux 虚拟机的备份会故障转移到崩溃一致的快照。为了避免备份期间出现警告，请在保护计划中禁用虚拟机备份选项的 VSS。
- **从备份运行虚拟机**

  如果备份与为装载的 VM 磁盘选择的路径位于同一卷上，则从 Hyper-V 主机上的备份运行虚拟机将失败。要解决此问题，请为装载的 VM 磁盘的路径选择不同的卷。该空间将仅用于已安装的虚拟机内部生成的更改，并且不会占用虚拟磁盘的整个大小。
- **具有逻辑卷的计算机支持的操作**

  支持使用逻辑卷备份和恢复工作负载，例如 Windows 中的 LDM(动态磁盘)和 Linux 中的 LVM，但有一些限制。有关限制的更多信息，请参阅 "支持的逻辑卷操作"(第 52 页)。

Scale Computing

平台	无代理程序备份 (虚拟机监控程序级别上备份)	基于代理程序备份 (从来宾操作系统内备份)
Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4	受支持 **设备** > **添加** > **虚拟化主机** > **Scale Computing HC3**	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**

限制

具有逻辑卷的计算机支持的操作

支持使用逻辑卷备份和恢复工作负载，例如 Windows 中的 LDM(动态磁盘)和 Linux 中的 LVM，但有一些限制。有关限制的更多信息，请参阅 "支持的逻辑卷操作"(第 52 页)。

Citrix

平台	无代理程序备份 (虚拟机监控程序级别上备份)	基于代理程序备份 (从来宾操作系统内备份)
Citrix XenServer/Citrix Hypervisor 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, 8.0, 8.1, 8.2	不支持	仅支持完全虚拟化的 (aka HVM) 来宾。半虚拟化的 (aka PV) 来宾不受支持。 **设备** > **添加** > **虚拟化主机** > **Citrix XenServer** > **Windows** 或 **Linux**

Red Hat 和 Linux

平台	无代理程序备份 (虚拟机监控程序级别上备份)	基于代理程序备份 (从来宾操作系统内备份)
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	不支持	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**
Red Hat Virtualization(由 oVirt 管理) 4.2、4.3、4.4、4.5	受支持 **设备** > **添加** > **虚拟化主机** > **Red Hat Virtualization (oVirt)**	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**
基于内核的虚拟机 (KVM)	不支持	受支持 **设备** > **添加** > **KVM** > **Windows** 或 **Linux**
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)	受支持 **设备** > **添加** > **虚拟化主机** > **Red Hat Virtualization (oVirt)**	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**
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)	受支持 **设备** > **添加** > **虚拟化主机** > **Red Hat Virtualization (oVirt)**	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**
由在 Red Hat Enterprise Linux 8.x 或 CentOS Stream 8.x 上运行的 oVirt 4.5 管理的基于内核的虚拟机 (KVM)	受支持 **设备** > **添加** > **虚拟化主机** > **Red Hat Virtualization (oVirt)**	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**

限制

具有逻辑卷的计算机支持的操作

支持使用逻辑卷备份和恢复工作负载，例如 Windows 中的 LDM（动态磁盘）和 Linux 中的 LVM，但有一些限制。有关限制的更多信息，请参阅 "支持的逻辑卷操作"（第 52 页）。

Parallels

平台	无代理程序备份 （虚拟机监控程序级别上备份）	基于代理程序备份 （从来宾操作系统内备份）
Parallels Workstation	不支持	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**
Parallels Server 4 Bare Metal	不支持	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**

Oracle

平台	无代理程序备份 （虚拟机监控程序级别上备份）	基于代理程序备份 （从来宾操作系统内备份）
Oracle Virtualization Manager（基于 oVirt）* 4.3	受支持 **设备** > **添加** > **虚拟化主机** > **Red Hat Virtualization (oVirt)**	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**
Oracle VM Server 3.0, 3.3, 3.4	不支持	仅支持完全虚拟化的 (aka HVM) 来宾。半虚拟化的 (aka PV) 来宾不受支持。 **设备** > **添加** > **虚拟化主机** > **Oracle** > **Windows** 或 **Linux**
Oracle VM VirtualBox 4.x	不支持	受支持 **设备** > **添加** > **虚拟化主机** > **Oracle** > **Windows** 或 **Linux**

*Oracle Virtualization Manager 受适用于 oVirt 的代理程序支持。

限制

具有逻辑卷的计算机支持的操作

支持使用逻辑卷备份和恢复工作负载，例如 Windows 中的 LDM（动态磁盘）和 Linux 中的 LVM，但有一些限制。有关限制的更多信息，请参阅 "支持的逻辑卷操作"（第 52 页）。

Nutanix

平台	无代理程序备份 （虚拟机监控程序级别上备份）	基于代理程序备份 （从来宾操作系统内备份）
Nutanix Acropolis Hypervisor (AHV) 20160925.x 到 20180425.x	不支持	受支持 **设备** > **添加** > **虚拟化主机** > **Nutanix AHV** > **Windows** 或 **Linux**

Virtuozzo

平台	无代理程序备份 （虚拟机监控程序级别上备份）	基于代理程序备份 （从来宾操作系统内备份）
Virtuozzo 6.0.10, 6.0.11, 6.0.12	受支持 **设备** > **添加** > **虚拟化主机** > **Virtuozzo**	仅支持虚拟机。容器不受支持。 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**
Virtuozzo 7.0.13, 7.0.14	仅支持 ploop 容器。虚拟机不受支持。 **设备** > **添加** > **虚拟化主机** > **Virtuozzo**	仅支持虚拟机。容器不受支持。 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**
Virtuozzo Hybrid Server 7.5	受支持 **设备** > **添加** > **虚拟化主机** > **Virtuozzo**	仅支持虚拟机。容器不受支持。 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**

限制

具有逻辑卷的计算机支持的操作

支持使用逻辑卷备份和恢复工作负载，例如 Windows 中的 LDM（动态磁盘）和 Linux 中的 LVM，但有一些限制。有关限制的更多信息，请参阅 "支持的逻辑卷操作"（第 52 页）。

Virtuozzo Hybrid Infrastructure

平台	无代理程序备份 （虚拟机监控程序级别上备份）	基于代理程序备份 （从来宾操作系统内备份）
Virtuozzo Hybrid Infrastructure 3.5, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0, 6.1, 6.2	受支持 **设备** > **添加** > **虚拟化主机** >	受支持 **设备** > **添加** > **工作站**或**服务器**

平台	无代理程序备份 (虚拟机监控程序级别上备份)	基于代理程序备份 (从来宾操作系统内备份)
	Virtuozzo Hybrid Infrastructure	> **Windows** 或 **Linux**

限制

- **磁盘位于外部 iSCSI 存储上的 VM 的无代理程序备份**
  如果 VM 磁盘位于外部 iSCSI 卷(已连接到 VHI 簇)上,则无法从 Virtuozzo Hybrid Infrastructure 备份 VM。
- **具有逻辑卷的计算机支持的操作**
  支持使用逻辑卷备份和恢复工作负载,例如 Windows 中的 LDM(动态磁盘)和 Linux 中的 LVM,但有一些限制。有关限制的更多信息,请参阅 "支持的逻辑卷操作"(第 52 页)。

Amazon

平台	无代理程序备份 (虚拟机监控程序级别上备份)	基于代理程序备份 (从来宾操作系统内备份)
Amazon EC2 实例	不支持	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**

Microsoft Azure

平台	无代理程序备份 (虚拟机监控程序级别上备份)	基于代理程序备份 (从来宾操作系统内备份)
Azure 虚拟机	受支持 **设备** > **添加** > **Microsoft Azure 虚拟机**	受支持 **设备** > **添加** > **工作站**或**服务器** > **Windows** 或 **Linux**

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 驱动器加密
- 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，然后安装代理程序。
2. 创建 安全区。
3. 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。

特定于软件的恢复过程

Microsoft BitLocker 驱动器加密

若要恢复由 BitLocker 加密的系统：

1. 从可启动媒体启动。
2. 恢复系统。恢复的数据将不会被加密。
3. 重新启动恢复的系统。
4. 启用 BitLocker。

如果只需要恢复多分区磁盘的一个分区，请在操作系统下执行此操作。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

仅可使用可启动媒体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

可以使用 Dell EMC Data Domain 设备作为备份存储。

对于此存储，我们建议您使用一个会定期创建完整备份的备份方案，例如**始终完整**。若要了解更多关于可用备份方案的信息，请查看"备份方案"(第 372 页)。

保留锁

支持保留锁(治理模式)。支持如果保留锁定已在 Data Domain 存储上启用,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。有关更多信息,请参阅"添加 AR_RETENTION_LOCK_SUPPORT 变量"(第 41 页)。

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。

如果在 Data Domain 存储上启用了保留锁,则保护计划中的保留规则不会删除存储上的备份。不会显示任何错误。当保留锁到期并再次应用保留规则时,备份将被删除。

根据保护计划的配置,保留规则将在备份之前或之后应用于档案。

添加 AR_RETENTION_LOCK_SUPPORT 变量

如果保留锁定已在 Data Domain 存储上启用,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。

添加 AR_RETENTION_LOCK_SUPPORT 环境变量

在 Windows 中

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

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

1. 以管理员身份登录到虚拟设备。
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。

操作系统支持的保护功能

本主题包含有关 Cyber Protect Cloud 的保护功能的信息。它未列出备份和恢复功能。

保护功能仅在已安装保护代理程序的计算机上受支持。例如，它们不适用于在无代理程序模式下由适用于 Hyper-V 的代理程序、适用于 VMware 的代理程序、适用于 Virtuozzo Hybrid Infrastructure 的代理程序、适用于 Scale Computing 的代理程序或适用于 oVirt 的代理程序备份的虚拟机。

某些功能可能需要其他许可，具体取决于所应用的许可模式。

支持的操作系统和版本

Windows

除非对特定功能集另有说明，否则支持以下 Windows 版本：

- Windows 7 Service Pack 1 及更高版本
- Windows Server 2008 R2 Service Pack 1 及更高版本

注意

对于 Windows 7，必须先安装 Microsoft 发布的以下更新，然后再安装保护代理程序。

- 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。

Linux

支持的 Linux 发行版及其版本取决于功能集，显示在每个表的底部。

macOS

支持的 macOS 版本取决于功能集，显示在每个表的底部。

功能集	Windows	Linux	macOS
默认保护计划			
远程工作线程	是	否	否
Office 工作线程(第三方防病毒)	是	否	否
Office 工作线程(Cyber Protect 防病毒)	是	否	否
Cyber Protect Essentials(仅适用于 Cyber Protect Essentials 版)	是	否	否
请参阅 "支持的操作系统和版本"(第 42 页)中受支持的 Windows 版本。			

功能集	Windows	Linux	macOS
取证备份			
正在收集内存转储	是	否	否
正在运行的进程的快照	是	否	否
本地映像取证备份的公证	是	否	否
云映像取证备份的公证	是	否	否
请参阅 "支持的操作系统和版本"(第 42 页)中受支持的 Windows 版本。			

功能	Windows	Linux	macOS
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
请参阅 "支持的操作系统和版本"(第 42 页)中受支持的 Windows 版本。			

功能集	Windows	Linux	macOS
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
请参阅 "支持的操作系统和版本"(第 42 页)中受支持的 Windows 版本。			

功能集	Windows	Linux	macOS
Active Protection			
进程注入检测	是	否	否
自动从本地缓存恢复受影响的文件	是	是	是
安克诺斯 备份文件的自我防御	是	否	否
安克诺斯 软件的自我防御	是	否	是 (仅限 Active Protection 和防恶意软件组件)
受信任/已阻止的进程管理	是	否	是
进程/文件夹排除	是	是	是
基于进程行为的勒索软件检测(基于人工智能 (AI))	是	是	是
基于进程行为的加密挖矿进程检测	是	否	否
外部驱动器保护(HDD、闪存驱动器、SD 卡)	是	否	是
网络文件夹保护	是	是	是
服务器端保护	是	否	否
Zoom、Cisco Webex、Citrix Workspace 和 Microsoft Teams 保护	是	否	否
有关受支持操作系统及其版本的详细信息，请参阅 "支持的防病毒和防恶意软件保护操作系统"(第 728 页)。			

功能集	Windows	Linux	macOS
防病毒和反恶意软件保护			
完全集成的 Active Protection 功能	是	否	否
实时防恶意软件保护	是	是，装有高级防恶意软件包	是，装有高级防恶意软件包
具有本地基于签名检测的高级实时防恶意软件保护	是	是	是
便携式可执行文件的静态分析	是	否	是*

功能集	Windows	Linux	macOS
防病毒和反恶意软件保护			
手动反恶意软件扫描	是	是**	是
网络文件夹保护	是	是	否
服务器端保护	是	否	否
扫描存档文件	是	否	是
扫描可移动驱动器	是	否	是
仅扫描新文件和更改的文件	是	否	是
文件/文件夹排除	是	是	是***
进程排除	是	否	是
行为分析引擎	是	否	是
漏洞利用预防	是	否	否
隔离	是	是	是
隔离区自动清除	是	是	是
URL 过滤 (http/https)	是	否	否
公司范围的白名单	是	否	是
防火墙管理****	是	否	否
Microsoft Defender Antivirus 管理*****	是	否	否
Microsoft Security Essentials 管理	是	否	否
通过 Windows Security Center 注册和管理防病毒和反恶意软件保护	是	否	否
有关受支持操作系统及其版本的详细信息，请参阅 "支持的防病毒和防恶意软件保护操作系统"(第 728 页)。			

* 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。

** 对于 Linux 上的手动扫描，不支持开始条件。

*** 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。

**** Windows 8 及更高版本支持防火墙管理。不支持 Windows Server。

***** Windows 8.1 及更高版本支持 Microsoft Defender Antivirus 管理。

功能集	Windows	Linux	macOS
漏洞评估			
操作系统及其原生应用程序的漏洞评估	是	是******	是
第三方应用程序的漏洞评估	是	否	是
有关受支持操作系统及其版本的详细信息，请参阅 "支持的 Microsoft 和第三方产品"(第 868 页)、"支持的 Linux 产品"(第 870 页) 和 "支持的 Apple 和第三方产品"(第 870 页)。			

****** 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。

功能集	Windows	Linux	macOS
修补程序管理			
修补程序自动批准	是	否	否
修补程序自动安装	是	否	否
修补程序测试	是	否	否
手动修补程序安装	是	否	否
修补预定	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
请参阅 "支持的操作系统和版本"(第 42 页) 中受支持的 Windows 版本。			

功能	Windows	Linux	macOS
数据保护地图			
重要文件的可调整定义	是	否	否
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
可以从“数据保护地图”小部件启动保护操作(**保护所有文件**操作)	是	否	否
请参阅 "支持的操作系统和版本"(第 42 页) 中受支持的 Windows 版本。			

功能集	Windows	Linux	macOS
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
请参阅 "支持的操作系统和版本"(第 42 页) 中受支持的 Windows 版本。			

功能	Windows	Linux	macOS
基于 安克诺斯 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
请参阅 "支持的操作系统和版本"(第 42 页) 中受支持的 Windows 版本。			

功能集	Windows	Linux	macOS
备份扫描			
映像备份的反恶意软件扫描作为备份计划的一部分	是	否	否
在云中扫描映像备份以查找恶意软件	是	否	否
加密备份的恶意软件扫描	是	否	否
请参阅 "支持的操作系统和版本"(第 42 页) 中受支持的 Windows 版本。			

功能集	Windows	Linux	macOS
安全恢复			
在恢复过程中使用“防病毒和反恶意软件保护”进行反恶意软件扫描	是	否	否
加密备份的安全恢复	是	否	否
请参阅 "支持的操作系统和版本"(第 42 页) 中受支持的 Windows 版本。			

功能集	Windows	Linux	macOS
远程桌面连接			
通过 NEAR 连接	是	是	是
通过 RDP 连接	是	否	否
通过 Apple 屏幕共享连接	否	否	是

功能集	Windows	Linux	macOS
远程桌面连接			
通过 Web 客户端连接	是	否	否
通过 Quick Assist 连接	是	是	是
远程协助	是	是	是
文件传输	是	是	是
屏幕截图传输	是	是	是
有关受支持操作系统及其版本的详细信息，请参阅 "支持的平台"(第 916 页) 。			

功能集	Windows	Linux	macOS
#CyberFit 分数			
#CyberFit 分数状态	是	否	否
#CyberFit 分数独立工具	是	否	否
#CyberFit 分数建议	是	否	否
请参阅 "支持的操作系统和版本"(第 42 页) 中受支持的 Windows 版本。			

功能集	Windows	Linux	macOS
数据丢失预防			
设备控制	是	否	在装有 Intel 处理器并运行 macOS 10.15 及更高版本或 macOS 11.2.3 或更高版本的 Mac 上受支持。 在基于 ARM 的 Apple Silicon 处理器(例如 Apple M1/M2) 上不受支持。

功能集	Windows	Linux	macOS
数据丢失预防			
Advanced Data Loss Prevention	是	否	否
请参阅 "支持的操作系统和版本"(第 42 页) 中受支持的 Windows 版本。			

功能集	Windows	Linux	macOS
管理选项			
用于推销 Cyber Protect 版本的追加销售方案	是	是	是
基于 Web 的集中式和远程管理中控台	是	是	是
支持的操作系统和版本:独立于平台。			

功能集	Windows	Linux	macOS
保护选项			
远程擦除	是	否	否
支持 Windows 10 及更高版本。			

功能集	Windows	Linux	macOS
Cyber Protect 监视器			
Cyber Protect 应用程序	是	否	是
Zoom 的保护状态	是	否	否
Cisco Webex 的保护状态	是	否	否
Citrix Workspace 的保护状态	是	否	否
Microsoft Teams 的保护状态	是	否	否
请参阅 "支持的操作系统和版本"(第 42 页) 中受支持的 Windows 版本。 在 macOS 上, 可以安装适用于 Mac 的代理程序的所有版本都支持 Cyber Protect Monitor。有关详细信息, 请参阅 "适用于 Mac 的代理程序"(第 27 页) 。			

功能集	Windows	Linux	macOS
软件清查			
软件清查扫描	是	否	是

功能集	Windows	Linux	macOS
软件清查			
软件清查监控	是	否	是
请参阅 "支持的操作系统和版本"(第 42 页) 中受支持的 Windows 版本。 在 macOS 上, 10.13.x – 13.x 版本支持软件清查。			

功能集	Windows	Linux	macOS
硬件清查			
硬件清查扫描	是	否	是
硬件清查监控	是	否	是
请参阅 "支持的操作系统和版本"(第 42 页) 中受支持的 Windows 版本。 在 macOS 上, 10.13.x – 13.x 版本支持硬件清查。			

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(可启动媒体仅支持恢复)。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	适用于 Windows 和 Linux 的可启动媒体	适用于 Mac 的可启动媒体	
FAT16/32	所有代理程序	+	+	无限制
NTFS	所有代理程序	+	+	
ext2/ext3/ext4	所有代理程序	+	-	
HFS+	适用于 Mac 的代理程序	-	+	

文件系统	受支持			限制
	代理程序	适用于 Windows 和 Linux 的可启动媒体	适用于 Mac 的可启动媒体	
APFS	适用于 Mac 的代理程序	-	+	• 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	+	-	• 文件过滤器(包含/排除)不受支持 • 无法启用快速增量/差异备份
ReiserFS3	适用于 Linux 的代理程序	+	-	
ReiserFS4	适用于 Linux 的代理程序	+	-	• 文件过滤器(包含/排除)不受支持 • 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	+	+	• 文件过滤器(包含/排除)不受支持 • 无法启用快速增量/差异备份 • 无法在恢复期间调整卷大小 • 在从 ReFS 备份恢复文件期间，将仅恢复内容。访问控制列表 (ACL) 和备用流不会恢复。稀疏文件将作为常规文件恢复。
XFS	所有代理程序	+	+	• 文件过滤器(包含/排除)不受支持 • 无法启用快速增量/差异备份 • 无法在恢复期间调整卷大小 • XFS 文件系统不支持快速增量备份模式。XFS 卷到云的增量备份和差异备份可能比使用快速增量模式的可比 ext4 备份慢得多。
Linux Swap	适用于 Linux 的	+	-	无限制

文件系统	受支持			限制
	代理程序	适用于 Windows 和 Linux 的可启动媒体	适用于 Mac 的可启动媒体	
	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 • 文件过滤器(包含/排除)不受支持 • 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(例如，Btrfs)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，使用 安克诺斯 VSS 提供程序时除外。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 安克诺斯 Backup Deduplication 功能无关。

支持的逻辑卷操作

支持使用逻辑卷备份和恢复工作负载，例如 Windows 中的 LDM(动态磁盘)和 Linux 中的 LVM，但有以下限制。

备份

基于代理程序的备份是由安装在工作负载上的保护代理程序或可启动媒体创建的备份。

无代理备份仅适用于虚拟机。无代理备份由可以备份和恢复环境中所有虚拟机的代理程序在虚拟机管理程序级别执行。受保护的虚拟机上未安装单独的代理程序。

有关基于代理程序备份和无代理程序备份之间差异的详细信息，请参阅 "基于代理程序备份和无代理程序备份"(第 56 页) 。

基于代理程序的备份	无代理程序备份
• 逻辑卷以每个卷为基础进行备份的。 • 支持文件筛选器(包含/排除) 。	• 当在磁盘上检测到逻辑卷时，磁盘将以逐扇区 (RAW) 模式备份。不分析磁盘的分区结构，也不单独存储卷镜像。 • 无法通过直接选择或使用策略规则来选择单个 LDM 或 LVM 卷作为备份源。保护计划的**备份内容**部分仅供**整台计算机**使用。 • 不支持文件筛选器(包含/排除) 。任何配置的包含或排除都将被忽略。

恢复

基于代理程序的恢复是由安装在工作负载上的代理程序或可启动媒体执行的恢复。

无代理程序恢复仅支持虚拟机作为目标。无代理程序恢复是由代理程序在虚拟机监控程序级别执行的，可以备份和恢复环境中的所有虚拟机。不必手动创建备份恢复到的目标计算机。

	来自基于代理程序的备份	来自无代理程序备份
基于代理程序的恢复	• 可以按卷恢复。 • 可以进行文件和文件夹恢复。	• 按卷恢复不可用。 • 可以进行文件和文件夹恢复。
无代理程序恢复	• 不支持机器迁移(P2V、V2P 和 V2V) 。要从基于代理程序的备份恢复数据，请使用可启动媒体。 • 不支持**"作为虚拟机运行"**操作。 • 可以进行文件和文件夹恢复。	• 按卷恢复不可用。 • 整个计算机恢复可用。 • 可以进行文件和文件夹恢复。 • 支持**"作为虚拟机运行"**操作。要使虚拟机可引导，您可能需要更改引导顺序。有关更多信息，请参阅此知识库文章。 • 支持转换为以下类型的虚拟机： ◦ VMware ESXi ◦ Microsoft Hyper-V ◦ Scale Computing HC3

安装和部署 Cyber Protection 代理程序

在启动前

准备

步骤 1

根据要备份的内容选择代理程序。有关可能选择的详细信息，请参阅我需要哪个代理程序？

步骤 2

确保硬盘驱动器上有足够的可用空间来安装代理程序。有关所需空间的详细信息，请参阅 "代理程序的系统要求"(第 60 页)。

步骤 3

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 "通过组策略部署保护代理程序"(第 118 页) 中进行介绍。

要下载适用于 Microsoft 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 Microsoft 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 Cyber Protection 服务中注册计算机。如果没有 Internet 连接，安装将失败。

步骤 4

Cyber Protect 功能需要 Microsoft Visual C++ 2017 Redistributable。在安装代理程序之前，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 Microsoft Visual C++ 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。

步骤 5

验证防火墙和网络安全系统的其他组件(如代理服务器)是否允许通过以下 TCP 端口的出站连接。

- 端口 **443** 和 **8443**

  这些端口用于访问 Cyber Protect 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 "配置代理服务器设置"(第 66 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 **2029**

  VMware 代理程序(虚拟设备)在此端口上侦听传入的 NFS 服务器请求，该服务器托管在代理程序上。通过此端口的连接是从备份(即时还原)运行虚拟机所必需的。
- 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。

下载器组件所需的端口

下载器组件负责将更新传送到计算机，然后将更新分发到其他下载器实例。它可以在代理程序模式下运行，从而将其计算机转换为下载器代理程序。下载器代理程序会从 Internet 下载更新，然后用作更新分发到其他计算机的源。下载器需要使用以下端口才能正常运行。

- TCP 和 UDP(传入)端口 **6888**

  由 BitTorrent 协议用于 torrent 点对点更新。

- UDP 端口 **6771**
  用作本地对等发现端口。还参与点对点更新。
- TCP 端口 **18018**
  用于在不同模式下工作的更新程序之间的通信:更新程序和更新程序代理程序。
- TCP 端口 **18019**
  本地端口,用于更新程序和保护代理程序之间的通信。

步骤 6

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。

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`

基于代理程序备份和无代理程序备份

基于代理程序的备份要求在每台受保护的计算机上安装保护代理程序。所有物理机和虚拟机都支持基于代理的备份。有关所需的代理程序及其安装位置的详细信息,请参阅 "我需要哪个代理程序? "(第 57 页)

无代理程序备份受一些虚拟化平台支持,但它不适用于物理机。无代理程序备份只需一个在虚拟环境中的专用计算机上安装的保护代理程序。此代理程序会备份此环境中的所有其他虚拟机。有关每个虚拟化平台支持的备份类型的详细信息,请参阅 "所支持的虚拟化平台"(第 30 页)。

对于某些虚拟化平台,可以使用虚拟设备。虚拟设备 (VA) 是包含保护代理程序的现成虚拟机。可以特定于虚拟机监控程序的格式(例如 .ovf、.ova 或 .qcow) 使用虚拟设备。

我需要哪种备份类型?

如果需要以下功能,我们建议您使用基于代理程序的备份:

- 额外的保护功能,如防病毒和防恶意软件、修补程序管理或远程桌面连接。有关这些功能的详细信息,请参阅 "操作系统支持的保护功能"(第 42 页)。
- 在租户级别上分离虚拟机。例如,因为您仅希望为该租户中的用户提供对其自己备份的访问权

限。

- 可以恢复到来宾操作系统的文件级备份。

  如果需要以下功能，我们建议您使用无代理程序的备份：

  - 仅备份，不需要任何额外的保护功能。
  - 简化管理 - 可以通过仅安装并配置一个代理程序以备份多个虚拟机。
  - 最大程度地减少资源使用量 - 一个专用代理程序比您环境中每个虚拟机上安装的多个代理程序使用较少的 CPU 和 RAM。
  - 特定备份设置，例如无 LAN 备份。有关此功能的详细信息，请参阅 "适用于 VMware 的代理程序 - 无需 LAN 的备份"(第 616 页)。
  - 更少的配置开销。无论来宾操作系统如何，专用代理程序都会在虚拟机监控程序级别备份虚拟机。

我需要哪个代理程序？

选择一个代理程序取决于要备份的内容。下表总结了信息，以帮助您做出决定。

在 Windows 中，适用于 Exchange 的代理程序、适用于 SQL 的代理程序、适用于 Active Directory 的代理程序和适用于 Oracle 的代理程序要求另外安装适用于 Windows 的代理程序。因此，例如，如果安装适用于 SQL 的代理程序，还将能够备份安装了该代理程序的整台计算机。

建议您在安装适用于 VMware 的代理程序 (Windows) 和适用于 Hyper-V 的代理程序时也安装适用于 Windows 的代理程序。

在 Linux 中，适用于 Oracle 的代理程序、适用于 MySQL/MariaDB 的代理程序和适用于 Virtuozzo 的代理程序需要另外安装适用于 Linux 的代理程序(64 位)。这些代理程序将捆绑到适用于 Linux 的代理程序(64 位)安装文件中。

您要备份哪些内容？	要安装哪些代理程序？	在哪里安装它？
物理机		
运行 Windows 的物理机	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	适用于 Linux 的代理程序	
运行 macOS 的物理机	适用于 Mac 的代理程序	
数据库		
SQL 数据库	适用于 SQL 的代理程序	在运行 Microsoft SQL Server 的计算机上。

MySQL 数据库	适用于 MySQL/MariaDB 的代理程序 (已捆绑到适用于 Linux 的代理程序(64 位)安装文件中)	在运行 MySQL Server 的计算机上。
MariaDB 数据库	适用于 MySQL/MariaDB 的代理程序 (已捆绑到适用于 Linux 的代理程序(64 位)安装文件中)	在运行 MariaDB Server 的计算机上。
Exchange 数据库	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。*
Oracle 数据库	适用于 Oracle 的代理程序 (在 Linux 中,已捆绑到适用于 Linux 的代理程序(64 位)安装文件中)	在运行 Oracle 数据库的计算机上。
云到云工作负载		
Microsoft 365 邮箱 (云代理程序或本地代理程序)	云代理程序 (无需安装)	此功能可用于部署在数据中心中的云代理程序。有关详细信息,请参阅 "使用适用于 Microsoft 365 的云代理程序"(第 551 页)。
	适用于 Office 365 的代理程序	在连接到 Internet 的 Windows 计算机上。有关详细信息,请参阅 "使用本地安装的适用于 Office 365 的代理程序"(第 547 页)。
Microsoft 365 OneDrive 文件和 SharePoint Online 站点	云代理程序	此功能可用于部署在数据中心中的云

	(无需安装)	代理程序。有关详细信息，请参阅 "使用适用于 Microsoft 365 的云代理程序" (第 551 页)。
Google Workspace Gmail 邮箱、Google Drive 文件和 Shared Drive 文件	云代理程序 (无需安装)	此功能可用于部署在数据中心中的云代理程序。有关详细信息，请参阅 "保护 Google Workspace 数据" (第 579 页)。
Active Directory		
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。
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(虚拟设备)	在 ESXi 主机上。
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 (虚拟设备)	在 Scale Computing HC3 主机上。
Red Hat Virtualization 虚拟机(由 oVirt 管理)	适用于 oVirt 的代理程序(虚拟设备)	在 Red Hat Virtualization 主机上。
Virtuozzo 虚拟机和容器***	适用于 Virtuozzo 的代理程序 (已捆绑到适用于 Linux 的代理程序 (64 位) 安装文件中)	在 Virtuozzo 主机上。

Virtuozzo Hybrid Infrastructure 虚拟机	适用于 Virtuozzo Hybrid Infrastructure 的代理程序(虚拟设备)	在 Virtuozzo Hybrid Infrastructure主机上。
在 Amazon EC2 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 Windows Azure 上托管的虚拟机		
Citrix XenServer 虚拟机		
Red Hat Virtualization (RHV/RHEV), not managed by oVirt		
基于内核的虚拟机 (KVM), 不受 oVirt 管理		
Oracle 虚拟机, 不受 oVirt 管理		
Nutanix AHV 虚拟机		
Red Hat Virtualization (RHV/RHEV), 由 oVirt 管理	适用于 oVirt 的代理程序(虚拟设备)	在虚拟化主机上。
基于内核的虚拟机 (KVM), 由 oVirt 管理		
Oracle 虚拟机, 由 oVirt 管理		
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 "适用于 VMware 的代理程序 - 无需 LAN 的备份"(第 616 页) 。

***对于 Virtuozzo 7, 仅支持 ploop 容器。虚拟机不受支持。

****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。不过, 如果 Cyber Protection 可以使用 CPUID 指示识别虚拟机, 则对其指派虚拟机服务配额。如果使用直接直通或对 CPU 制造商 ID 使用掩码的其他选项, 则仅可以为物理机指派服务配额。

代理程序的系统要求

代理程序	安装所需磁盘空间

适用于 Windows 的代理程序	1.2 GB
适用于 Linux 的代理程序	2 GB
适用于 Mac 的代理程序	1 GB
适用于 SQL 的代理程序和适用于 Windows 的代理程序	1.2 GB
适用于 Exchange 的代理程序和适用于 Windows 的代理程序	1.3 GB
适用于防止数据丢失的代理程序	500 MB
适用于 Microsoft 365 的代理程序	500 MB
适用于 Active Directory 的代理程序和适用于 Windows 的代理程序	2 GB
适用于 VMware 的代理程序和适用于 Windows 的代理程序	1.5 GB
适用于 Hyper-V 的代理程序和适用于 Windows 的代理程序	1.5 GB
适用于 Virtuozzo 的代理程序和适用于 Linux 的代理程序	1 GB
适用于 Virtuozzo Hybrid Infrastructure的代理程序	700 MB
适用于 Oracle 的代理程序和适用于 Windows 的代理程序	2.2 GB
适用于 Oracle 的代理程序和适用于 Linux 的代理程序	2 GB
适用于 MySQL/MariaDB 的代理程序和适用于 Linux 的代理程序	2 GB

备份操作(包括删除备份)要求每 1 TB 备份大小有大约 1 GB RAM。内存消耗可能会不同,具体取决于代理程序所处理的数据的量和类型。

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。

在使用支持 CET 技术的现代处理器(如第 11 代 Intel Core 或 AMD Ryzen 7)的工作负载上,适用于数据丢失预防的代理程序的一些功能已禁用以避免出现冲突。下表列出了装有此类 CPU 的系统上可用的设备控制和 Advanced DLP 功能。

功能	设备控制	Advanced DLP
本地通道		
可移动存储	不适用	是
加密的可移动存储	是	不适用
打印机	不适用	否

重定向的映射驱动器	不适用	是
重定向的剪贴板	不适用	否
网络通信		
SMTP 电子邮件	不适用	是
Microsoft Outlook (MAPI)	不适用	是
IBM Notes	不适用	否
Webmails	不适用	是
即时消息 (ICQ)	不适用	否
即时消息 (Viber)	不适用	否
即时消息 (IRC、Jabber、Skype、Viber)	不适用	是
文件共享服务	不适用	是
社交网络	不适用	是
本地网络文件共享 (SMB)	不适用	是
Web 访问 (HTTP/HTTPS)	不适用	是
文件传输 (FTP/FTPS)	不适用	是
数据传输白名单		
设备类型的白名单	不适用	是
网络通信的白名单	不适用	是
远程主机的白名单	不适用	是
应用程序的白名单	不适用	是
外围设备		
可移动存储	是	是
加密的可移动存储	是	是
打印机	否	否
MTP 连接的移动设备	否	否
蓝牙适配器	是	是
光盘驱动器	是	是
软盘驱动器	是	是
Windows 剪贴板	否	否

屏幕截图捕获	否	否
重定向的映射驱动器	是	是
重定向的剪贴板	否	否
Cyber Protect 代理程序自我保护		
对普通最终用户的保护	是	是
对本地系统管理员的保护	是	是

下载保护代理程序

在安装代理程序前，必须从 Cyber Protect 中控台下载其安装文件。

在添加要保护的工作负载时下载代理程序的步骤

1. 在 Cyber Protect 中控台中，导航到**设备** > **所有设备**。
2. 在右上角，单击**添加设备**。
3. 在**添加设备**面板中，从**发布渠道**下拉菜单中，选择代理程序版本。
   - **以前的版本** - 从以前的版本下载代理程序版本。
   - **当前** - 下载最新的可用代理程序版本。
4. 选择对应于所添加工作负载的操作系统的代理程序。
   打开**另存为**对话框。
5. [仅限于具有 Apple silicon(例如 Apple M1) 处理器的 Mac] 单击**取消**。在打开的**添加 Mac** 面板中，单击**下载 ARM 安装程序**链接。
6. 选择要保存代理程序安装文件的位置并单击**保存**。

下载代理程序供以后使用的步骤

1. 在 Cyber Protect 中控台的右上角，单击**用户**图标。
2. 单击**下载**。
3. 在**下载**对话框中，从**发布渠道**下拉菜单中，选择代理程序版本。
   - **以前的版本** - 从以前的版本下载代理程序版本。
   - **当前** - 下载最新的可用代理程序版本。
4. 滚动可用安装程序的列表以找到所需的代理程序安装程序，并单击其行末端的下载图标。
   打开**另存为**对话框。
5. 选择要保存代理程序安装文件的位置并单击**保存**。

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。

配置代理服务器设置

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。

由于代理程序在安装过程中将自己注册在云中，因此必须在安装代理程序过程中或事先配置代理服务器设置。

面向 Windows

如果在**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中读取代理服务器设置，并自动使用它们。

如果要执行以下任务，请使用此过程。

- 安装代理程序前配置代理设置。
- 安装代理程序后更新代理设置。

要在代理程序安装期间配置代理设置，请参阅 "在 Windows 中安装保护代理程序"(第 72 页)。

注意
仅当 `http-proxy.yaml` 文件在计算机上不存在时，此过程才适用。如果 `http-proxy.yaml` 文件在计算机上存在，则必须更新该文件中的代理设置，因为它会覆盖 `aakore.yaml` 文件中的设置。

当使用 Cyber Protection Monitor 配置代理服务器设置时，将创建 `%programdata%\Acronis\Agent\var\aakore\http-proxy.yaml` 文件。有关详细信息，请参阅 "在 Cyber Protect Monitor中配置代理服务器设置"(第 260 页)。

要打开 `http-proxy.yaml` 文件，您必须是 Windows 中“管理员”组的成员。

配置代理设置

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. 将以下各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. 如果代理程序尚未安装在此工作负载中，请立即安装。如果代理程序已安装在工作负载中，请继续下一步。
9. 在文本编辑器中打开 `%programdata%\Acronis\Agent\etc\aakore.yaml` 文件。

要打开此文件，您必须是 Windows 中“管理员”组的成员。

10. 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
```

11. 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。
12. 在**开始**菜单中，单击**运行**、键入：**cmd**，然后单击**确定**。
13. 通过运行以下命令，以重新启动 aakore 服务。

```
net stop aakore
net start aakore
```

14. 通过运行以下命令，以重新启动代理程序。

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

适用于 macOS

如果要执行以下任务，请使用此过程。

- 安装代理程序前配置代理设置。
- 安装代理程序后更新代理设置。

要在代理程序安装期间配置代理设置，请参阅 "在 macOS 中安装保护代理程序"(第 76 页)。

配置代理设置

1. 创建 /Library/Application Support/Acronis/Registry/Global.config 文件，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. 如果代理程序尚未安装在此工作负载中，请立即安装。如果代理程序已安装在工作负载中，请继续下一步。
7. 在文本编辑器中打开 `/Library/Application Support/Acronis/Agent/etc/aakore.yaml` 文件。
8. 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
```

9. 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。
10. 转到**应用程序** > **实用程序** > **终端**。
11. 通过运行以下命令，以重新启动 aakore 服务。

```
sudo launchctl stop aakore
sudo launchctl start aakore
```

12. 通过运行以下命令，以重新启动代理程序。

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

面向 Linux

使用 `--http-proxy-host=ADDRESS` `--http-proxy-port=PORT` `--http-proxy-login=LOGIN` `--http-proxy-password=PASSWORD` 参数运行安装文件。在安装保护代理程序后，请使用以下过程来更新代理程序设置。

配置代理设置

1. 在文本编辑器中打开 `/etc/Acronis/Global.config` 文件。
2. 请执行以下任一操作：
   - 如果在代理程序安装过程中已指定代理设置，则找到以下部分。

```
<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>
```

   - 如果在代理程序安装过程中未指定代理设置，则复制以下各行并将其粘贴到文件的 `<registry name="Global">...</registry>` 标记之间。

```
<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>
```

3. 将 ADDRESS 替换为新代理服务器主机名称/IP 地址，将 PORT 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 LOGIN 和 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. 在文本编辑器中打开文件 /opt/acronis/etc/aakore.yaml。
7. 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
```

8. 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。
9. 通过运行以下命令，以重新启动 aakore 服务。

```
sudo service aakore restart
```

10. 通过在任何目录中执行以下命令，以重新启动代理程序。

```
sudo service acronis_mms restart
```

对于可启动媒体

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。要配置代理服务器设置，请依次单击**工具** > **代理服务器**，然后配置代理服务器主机名/IP 地址、端口和凭据。

组件的动态安装和卸载

对于受代理程序版本 15.0.26986(已于 2021 年 5 月发布) 或更高版本保护的 Windows 工作负载，将动态安装以下组件(即仅当保护计划要求时) ：

- URL 过滤代理程序 — 运行 URL 筛选功能所需。
- 适用于防恶意软件保护的代理程序 - 运行防恶意软件保护功能所必需。
- 适用于数据丢失预防的代理程序 - 运行设备控制功能所必需。

默认情况下，这些组件不会安装。如果工作负载变为受计划保护，在该计划中启用了任意以下模块，则自动安装各自的组件：

- 防病毒和反恶意软件保护
- URL 过滤
- 设备控制

同样，如果保护计划不再要求反恶意软件保护、URL 过滤或设备控制功能，则会自动卸载各自的组件。

在更改保护计划后，组件的动态安装或卸载最多需要 10 分钟。但是，如果运行以下任意操作，则动态安装或卸载将在此操作完成后开始：

- 备份
- 恢复
- 备份复制
- 虚拟机复制
- 测试副本
- 从备份运行虚拟机(包括最终确定)
- 灾难恢复故障转移
- 灾难恢复故障恢复
- 运行脚本(对于网络安全脚本功能)
- 修补程序安装
- ESXi 配置备份

为 Connect Agent 授予所需的系统权限

要在 macOS 工作负载上启用远程桌面功能的所有功能，除了全盘访问权限之外，还必须为 Connect Agent 授予以下权限：

- 屏幕录制 - 通过 NEAR 启用 macOS 工作负载的屏幕录制。在授予此权限之前，所有远程控制连接都会被拒绝。
- 可访问性 - 通过 NEAR 在控制模式下启用远程连接。
- 麦克风 - 通过 NEAR 将声音从远程 macOS 工作负载重定向到本地工作负载。要启用声音重定向功能，必须在工作负载上安装声音捕获驱动程序。有关详细信息，请参阅 "远程声音重定向"(第 919 页)。
- 自动化 - 启用清空回收站操作

在 macOS 工作负载上启动代理程序后，它会检查代理程序是否具有这些权限，并在需要时要求您授予相应权限。

授予屏幕录制权限

1. 在 Cyber Protect 代理程序对话框的**授予所需系统权限**中，单击**设置系统权限**。
2. 在**系统权限**对话框中，单击**请求屏幕录制**权限。
3. 单击**打开系统首选项**。
4. 选择 **Connect Agent**。

如果代理程序在您尝试远程访问工作负载时没有权限，它会显示“屏幕录制权限请求”对话框。只有本地用户才可以回答该对话框。

授予可访问性权限

1. 在 Cyber Protect 代理程序对话框的**授予所需系统权限**中，单击**设置系统权限**。
2. 在**系统权限**对话框中，单击**请求可访问性权限**。
3. 单击**打开系统首选项**。

4. 单击窗口左下角的锁定图标，以便将其更改为解锁图标。系统会要求您输入管理员密码，才能使更改生效。
5. 选择 **Connect Agent**。

授予麦克风权限

1. 在 Connect Agent 对话框的**授予所需系统权限**中，单击**设置系统权限**。
2. 在**系统权限**对话框中，单击**请求麦克风权限**。
3. 单击**确定**。

注意
还必须在 macOS 工作负载上安装一个声音捕获驱动程序，以使代理程序能够利用给定的权限并重定向工作负载的声音。有关详细信息，请参阅 "远程声音重定向"(第 919 页)。

授予自动化权限

1. 在 Connect Agent 对话框的**授予所需系统权限**中，单击**设置系统权限**。
2. 在**系统权限**对话框中，单击**请求自动化权限**。

使用图形用户界面安装保护代理程序

在 Windows 中安装保护代理程序

先决条件

在要保护的工作负载上下载所需的代理程序。请参阅 "下载保护代理程序"(第 63 页)。

安装适用于 Windows 的代理程序的步骤

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(例如，禁止安装 Cyber Protection Monitor 或命令行工具，或安装适用于防恶意软件保护的代理程序或适用于 URL 筛选的代理程序)。

     注意
     在 Windows 计算机上，防恶意软件防护功能需要安装防恶意软件防护代理，URL 筛选功能需要安装 URL 筛选代理程序。如果在其保护计划中启用了**防病毒和防恶意软件保护**和/或**URL 筛选**模块，将自动为受保护的工作负载安装这些代理程序。

   - 更改在 Cyber Protection 服务中注册工作负载的方法。可以从**使用服务中控台**(默认设置)切换为**使用凭据**或**使用注册标记**。
   - 更改安装路径。
   - 更改用于运行代理程序服务的用户帐户。有关详细信息，请参阅 "在 Windows 计算机上更改登录帐户"(第 73 页)。

- 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. [仅当安装适用于 VMware 的代理程序时] 指定要备份和恢复其虚拟机的 vCenter 服务器或独立 ESXi 主机的地址和访问凭据，然后单击**完成**。

   建议使用专用帐户来访问 vCenter 服务器或 ESXi 主机，而不是使用角色为管理员的现有帐户。有关详细信息，请参见"Agent for VMware 所需的权限"(第 624 页)。
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 中保留使用默认的注册方法**使用服务中控台**，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. 在客户租户帐户下注册代理。有关注册的详细信息，请参阅"使用图形用户界面注册工作负载"(第 104 页)。
9. [如果代理程序在其租户处于合规模式的帐户下注册] 设置加密密码。

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，不建议您在安装完成后手动更改登录帐户。

在 Linux 中安装保护代理程序

准备

- 在要保护的计算机上下载所需的代理程序。请参阅 "下载保护代理程序"（第 63 页）。
- 确保计算机上已安装必要的 Linux 程序包。
- 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 Cyber Protect 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. 确保计算机连接到 Internet。
2. 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>
   ```

   如果在网络中启用了代理服务器，则在运行安装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 Cyber Protection 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
   - 适用于 Oracle 的代理程序
   - 适用于 MySQL/MariaDB 的代理程序

   适用于 Virtuozzo 的代理程序、适用于 Oracle 的代理程序和适用于 MySQL/MariaDB 的代理程序需要另外安装适用于 Linux 的代理程序(64 位)。
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 Cyber Protection 服务的用户名和密码，或者等到使用标记注册计算机。
5. 在客户租户帐户下注册代理。有关注册的详细信息，请参阅"使用图形用户界面注册工作负载"(第 104 页)。
6. [如果代理程序在其租户处于合规模式的帐户下注册] 设置加密密码。
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
   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。
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 中安装保护代理程序

先决条件

在要保护的工作负载上下载所需的代理程序。请参阅 "下载保护代理程序"(第 63 页) 。

安装适用于 Mac(x64 或 ARM64) 的代理程序的步骤

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. 在客户租户帐户下注册代理。有关注册的详细信息，请参阅"使用图形用户界面注册工作负载" (第 104 页) 。
10. [如果代理程序在其租户处于合规模式的帐户下注册] 设置加密密码。
11. 如果您的 macOS 版本是 Mojave 10.14.x 或更高版本，请授予保护代理程序完整的磁盘访问权限以支持备份操作。

    有关说明，请参阅向网络安全保护代理程序授予“完整磁盘访问”权限 (64657)。
12. 要使用远程桌面功能，请为 Connect Agent 授予所需的系统权限。有关详细信息，请参阅 "为 Connect Agent 授予所需的系统权限"(第 71 页) 。

卸载代理程序

当从工作负载中卸载代理程序时，将从 Cyber Protect 中控台中自动删除该工作负载。例如，如果由于网络问题而导致工作负载在卸载代理程序后仍显示，请从中控台中手动删除该工作负载。有关如何执行该操作的详细信息，请参阅 "从 Cyber Protect 中控台中删除工作负载"(第 280 页) 。

注意
卸载代理程序不会删除任何计划或备份。

卸载代理程序

Windows

1. 以管理员身份登录到装有代理程序的计算机。
2. 在**控制面板**中，转到**程序和功能**(在 Windows XP 中为**添加或删除程序**) 。
3. 右键单击 **安克诺斯 Cyber Protect**，然后选择**卸载**。
4. [对于受密码保护的代理程序] 指定卸载代理程序所需的密码，然后单击**下一步**。
5. [可选] 选中**删除日志和配置设置**复选框。

如果计划重新安装代理程序，请不要选中此复选框。如果选中该复选框，然后重新安装代理程序，则此工作负载可能会在 Cyber Protect 中控台中重复存在，其旧备份可能不会与其相关联。

6. 单击**卸载**。

Linux

1. 在装有代理程序的计算机上，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。
   如果计划重新安装代理程序，请不要选中此复选框。如果选中该复选框，然后重新安装代理程序，则此工作负载可能会在 Cyber Protect 中控台中重复存在，其旧备份可能不会与其相关联。
3. 确认您的决定。

macOS

1. 在装有代理程序的计算机上，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。

卸载与适用于 Windows 的代理程序捆绑的组件

可以卸载与适用于 Windows 的代理程序捆绑的各个组件(如 Cyber Protect Monitor、适用于数据丢失预防的代理程序或可启动媒体生成器)，而不会卸载适用于 Windows 的代理程序。

1. 以管理员身份登录到装有代理程序的计算机。
2. 运行安装程序，然后单击**修改已安装的组件**。
3. 清除要卸载的组件旁边的复选框，然后单击**完成**。

删除适用于 VMware 的代理程序(虚拟设备)

1. 使用 vSphere Client，登录到 vCenter 服务器。
2. [如果虚拟设备已开启] 右键单击虚拟设备，然后依次单击**电源** > **关闭**。确认您的决定。
3. [如果虚拟设备使用虚拟磁盘上本地附加的存储，并希望保留该磁盘上的数据] 从虚拟设备中删除虚拟存储。
   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**。
   c. 在**移除选项**中，单击**从虚拟机移除**。
   d. 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。
5. [可选] [如果您不打算再次使用此设备] 在 Cyber Protect 中控台中，转到**备份存储** > **位置**，然后删除与本地附加的存储相对应的位置。

使用命令行接口安装和卸载保护代理程序

在 Windows 中安装和卸载保护代理程序

在 Windows 中，可以通过以下方式执行无人参与安装或卸载：

- 使用安装程序的 EXE 文件，并在命令行中指定安装参数。
- 使用从安装程序中提取的 MSI 文件，并按以下方式之一指定安装参数：
  - 在 MST 文件中
  - 直接在命令行中

使用 EXE 文件进行无人参与安装和卸载

对于此类无人参与安装，请下载安装程序，然后通过命令行以及所需的安装参数启动无人参与安装。要查看可以使用的参数，请参阅 "无人参与安装的参数 (EXE)"(第 80 页)。

无需事先提取安装包、MSI 和 MST 文件。

安装和卸载代理程序和组件 (EXE)

要使用 EXE 文件执行无人参与安装，请运行安装程序，然后在命令行上指定安装参数。

要下载安装程序，请在 Cyber Protect 中控台中，单击右上角的帐户图标，然后单击**下载**。下载链接也可在**添加设备**窗格中找到。

安装代理程序和组件

1. 以管理员身份启动命令行界面，然后导航到安装程序的 EXE 文件。
2. 要启动安装程序并指定安装参数，请运行以下命令：

   ```
   <file path>/<EXE file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
   ```

   使用空格分隔参数，使用不带空格的逗号分隔参数的值。例如：

   ```
   C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
   components=agentForWindows,agentForSql,commandLine --install-dir="C:\Program
   Files\BackupClient" --reg-address=https://eu2-cloud.company.com --reg-token=34F6-
   8C39-4A5C --quiet
   ```

   要查看可用参数及其值，请参阅 "无人参与安装的参数 (EXE)"(第 80 页)。

示例

- 安装适用于 Windows 的代理程序、防恶意软件代理程序和适用于 URL 筛选的代理程序、命令行工具和 Cyber Protect Monitor。使用用户名和密码在 Cyber Protection 服务中注册工作负载。

  ```
  C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
  components=agentForWindows,agentForAmp,commandLine,trayMonitor --install-
  ```

```
dir="C:\Program Files\BackupClient" --agent-account=system --reg-
address=https://cloud.company.com --reg-login=johndoe --reg-password=johnspassword
```

- 安装适用于 Windows 的代理程序、命令行工具和 Cyber Protect Monitor。在 Windows 中为代理程序服务创建一个新的登录帐户。使用令牌在 Cyber Protection 服务中注册工作负载。

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,commandLine,trayMonitor --install-dir="C:\Program
Files\BackupClient" --agent-account=new --reg-address=https://eu2-cloud.company.com -
-reg-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 Cyber Protect Monitor。使用用户名和密码在 Cyber Protection 服务中注册计算机。

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
dir="C:\Program Files\BackupClient" --language=en --agent-account=system --reg-
address=https://cloud.company.com --reg-login=johndoe --reg-password=johnspassword
```

- 安装适用于 Windows 的代理程序、命令行工具和 Cyber Protect Monitor。将用户界面语言设置为德语。使用标记在 Cyber Protection 服务中注册计算机。设置 HTTP 代理。

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
dir="C:\Program Files\BackupClient"--language=de --agent-account=system --reg-
address=https://eu2-cloud.company.com --reg-token=34F6-8C39-4A5C --http-proxy-
address=https://my-proxy.company.com:80 --http-proxy-login=tomsmith --http-proxy-
password=tomspassword
```

删除已安装的组件

1. 以管理员身份启动命令行界面，然后导航到 `%ProgramFiles%\BackupClient\RemoteInstall`。
2. 运行以下命令：

```
web_installer.exe --remove-components=<value 1>,<value 2> --quiet
```

要查看可用参数及其值，请参阅 "无人参与安装的参数 (EXE)"(第 80 页)。

示例

- 卸载 Cyber Protect Monitor。

```
C:\Program Files\BackupClient\RemoteInstall\web_installer.exe --remove-
components=trayMonitor --quiet
```

卸载代理程序

1. 以管理员身份启动命令行界面，然后导航到 `%Program Files%\Common Files\Acronis\BackupAndRecovery`。
2. 运行以下命令：

```
Uninstaller.exe --quiet --delete-all-settings
```

要查看可用参数及其值，请参阅 "无人参与安装的参数 (EXE)"(第 80 页)。

示例

- 卸载适用于 Windows 的代理程序及其所有组件。删除所有日志、任务和配置设置。

```
C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --quiet --
delete-all-settings
```

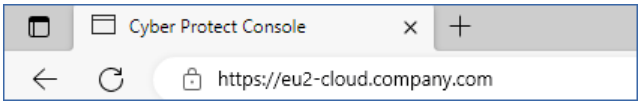
- 卸载受密码保护的适用于 Windows 的代理程序及其所有组件。删除所有日志、任务和配置设置。

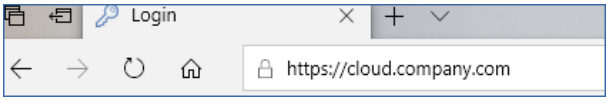
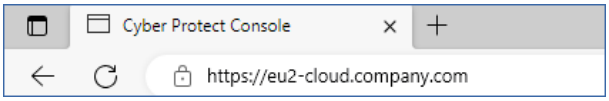
```
C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --anti-
tamper-password=<password> --quiet --delete-all-settings
```

无人参与安装的参数 (EXE)

下表汇总了使用 EXE 文件进行无人参与安装的参数。

参数	描述
通用参数	
--add-components=<component1,component2,...,componentN>	要安装的组件。请参阅 "无人参与安装的组件 (EXE)"(第 84 页) 中可用组件的完整列表。 当指定多个组件时，请使用逗号分隔它们。请勿在逗号前后添加空格。 如果指定已安装的组件，将修复或更新这些组件，具体取决于安装程序的版本和已安装组件的版本。 如果未指定此参数，将安装一组默认组件，具体取决于执行安装的计算机。例如，适用于 SQL 的代理程序仅安装在运行 MS SQL Server 的计算机上。
--install-dir=<path>	选定组件将安装到的文件夹。如果指定的文件夹不存在，将创建该文件夹。 如果未指定此参数，则使用默认文件夹：C:\Program Files\BackupClient。
--log-dir=<path>	安装日志将保存到的文件夹。 如果未指定此参数，则使用默认文件夹：%ProgramData%\Acronis\InstallationLogs。
--language=<code>	产品语言。 以下值可用：en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu,

参数	描述
	ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW.。 如果未指定此参数，并且执行安装的计算机的系统语言如上所列，则使用系统语言。在所有其他情况下，该值都设置为 en。
`--quiet`	使用此参数，可在不显示图形用户界面的情况下运行安装程序。 请勿将该参数与 `--register-only` 参数一起使用。
`--help`	使用此参数，可查看可以在命令行中使用的所有可用参数的列表及其说明。
`--fss-onboarding-auto-start`	将此参数与 `--quiet` 参数一起使用，可在无人参与安装完成后显示 File Sync & Share 登录向导。
注册参数	
`--registration={skip | by-credentials | by-token | device-flow}`	使用此参数，可选择如何在安装完成后注册代理程序。 要跳过注册，请指定 `skip`。可以使用 `--register-only` 参数，以稍后注册代理程序。 要使用凭据注册代理程序，请指定 `by-credentials`，然后使用 `--reg-login` 和 `--reg-password` 参数。此外，只能使用 `--reg-login` 和 `--reg-password` 参数，这使得可选择指定 `--registration=by-credentials`。 要使用注册令牌注册代理程序，请指定 `by-token`，然后使用 `--reg-token` 参数。此外，只能使用 `--reg-token` 参数，这使得可选择指定 `--registration=by-token`。 要使用 OAuth 2.0 协议注册代理程序，请指定 `device-flow`。安装完成后，注册页面即会自动打开。 当使用 `--registration=device-flow` 时，请指定准确的数据中心地址作为 `--reg-address` 参数的值。这是您**登录**到 Cyber Protection 服务后所看到的 URL。例如，`https://eu2-cloud.company.com`。  请勿将 `--registration=device-flow` 与 `--quiet` 参数一起使用。
`--reg-address=<url>`	Cyber Protection 服务的 URL。可以将此参数与 `--reg-login` 和 `--reg-password` 参数一起使用，也可以将此参数与 `--reg-token` 参数一起使用。

参数	描述
	• 当将此参数与 `--reg-login` 和 `--reg-password` 参数一起使用时，请指定用于**登录**到 Cyber Protection 服务的地址。例如，`https://cloud.company.com`：  • 当将此参数与 `--reg-token` 参数一起使用时，请指定准确的数据中心地址。这是您**登录**到 Cyber Protection 服务后所看到的 URL。例如，`https://eu2-cloud.company.com`。  请勿将 `https://cloud.company.com` 与 `--reg-token` 参数一起使用。
`--reg-login=`<login> `--reg-password=`<password>	代理程序将在 Cyber Protection 服务中注册所使用帐户的凭据。这不能是合作伙伴管理员帐户。 当使用这些参数时，可选择指定 `--registration` 参数。 请勿将这些参数与 `--reg-token` 参数一起使用。
`--reg-token=`<token>	注册令牌。 注册令牌由 12 个字符组成，由连字符分为三段。有关如何生成注册令牌的详细信息，请参阅 "生成注册标记"（第 106 页）。 当使用此参数时，可选择指定 `--registration` 参数。 请勿将此参数与 `--reg-login` 和 `--reg-password` 参数一起使用。
`--register-only`	使用此参数，可跳过安装并使用 OAuth 2.0 协议 (device-flow) 注册代理程序。 安装完成后，注册页面即会自动打开。 请勿将 `--register-only` 与 `--quiet` 参数一起使用。
代理程序服务的登录帐户	
`--agent-account=`{system | new | custom} 或 `--agent-account-login=`<login> `--agent-account-password=`<password>	使用此参数，可指定将运行代理程序服务的登录帐户。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"（第 73 页）。 要使用**本地系统**帐户，请指定 `--agent-account=system`，或者在命令中不使用 `--agent-account` 参数。 要使代理程序服务能够在新登录帐户 **Acronis Agent User**（自动创建）下运行，请指定 `new`。

参数	描述
	要使代理程序服务能够在现有帐户下运行，请使用 --agent-account-login 和 --agent-account-password 参数指定帐户凭据。在这种情况下，可选择指定 --agent-account=custom 参数。
vCenter/ESXi 参数	
--esxi-address=<host>	vCenter 服务器或 ESXi 主机的主机名或 IP 地址。 当安装适用于 VMware 的代理程序时，请使用此参数。
--esxi-login=<login> --esxi-password=<password>	vCenter 服务器或 ESXi 主机的访问凭据。 当安装适用于 VMware 的代理程序时，请使用这些参数。
代理参数	
--http-proxy={none | system | custom}	使用此参数，可指定要用于备份到云存储和从云存储恢复的 HTTP 代理服务器。 如果禁用代理服务器连接，请指定 --http-proxy=none。 要使用系统范围的代理服务器，请指定 --http-proxy=system，或者在命令中不使用 --http-proxy 参数。 要使用其他代理服务器，请使用 --http-proxy-address、--http-proxy-login 和 --http-proxy-password 参数指定代理服务器地址和凭据。在这种情况下，可选择指定 --http-proxy=custom 参数。
--http-proxy-address=<host>:<port>	自定义 HTTP 代理服务器的主机名或 IP 和端口。
--http-proxy-login=<login>	自定义 HTTP 代理服务器的登录名。
--http-proxy-password=<password>	自定义 HTTP 代理服务器的密码。
卸载参数	
--remove-components=<component1,component2,...,componentN>	要卸载的组件。请参阅 "无人参与安装的组件 (EXE)"(第 84 页) 中可用组件的完整列表。 当指定多个组件时，请使用逗号分隔它们。请勿在逗号前后添加空格。 **重要事项** 使用此参数，只能卸载组件。要完全卸载产品，请转到“Windows 控制面板”>“程序和功能”、选择产品，然后单击**卸载**。
--delete-all-settings	当使用 --remove-components 参数删除所有产品日志、任务和配置设置时，请使用此可选参数。

参数	描述
--anti-tamper-password=<password>	卸载受密码保护的适用于 Windows 的代理程序或修改其组件所需的密码。

无人参与安装的组件 (EXE)

下表汇总了可以通过 EXE 文件进行无人参与安装的组件。使用值名称指定 --add-components 参数的值。

有关详细信息，请参阅 "无人参与安装的参数 (EXE)"(第 80 页) "无人参与安装的参数 (MSI)"(第 88 页)

值名称	组件描述
agentForWindows	适用于 Windows 的代理程序
agentForSas	适用于 File Sync & Share 的代理程序
agentForAd	适用于 Active Directory 的代理程序
agentForAmp	防恶意软件保护代理程序和 URL 过滤代理程序
agentForDlp	适用于防止数据丢失的代理程序
agentForEsx	适用于 VMware 的代理程序 (Windows)
agentForExchange	适用于 Exchange 的代理程序
agentForHyperV	适用于 Hyper-V 的代理程序
agentForOffice365	适用于 Office 365 的代理程序
agentForOracle	适用于 Oracle 的代理程序
agentForSql	适用于 SQL 的代理程序
commandLine	命令行工具
mediaBuilder	可启动媒体生成器
trayMonitor	Cyber Protect Monitor
all	此值组合所有组件。
allAgents	此值组合所有代理程序。

使用 MSI 文件进行无人参与安装和卸载

对于此类无人参与安装，请使用 Windows 安装程序(Msiexec 程序) 。使用安装程序的图形用户界面，事先提取安装包和 MSI 文件。

当使用 MSI 文件安装组件时，可以使用 MST 转换文件来自定义安装参数。有关如何组合使用 MSI 和 MST 文件的详细信息，请参阅 "安装代理程序和组件(MSI 和 MST 组合) "(第 85 页) 。可以在

Active Directory 域中使用此安装方法，以使用 Windows 组策略安装保护代理程序。有关详细信息，请参阅 "通过组策略部署保护代理程序"(第 118 页)。

或者，也可以在命令行中手动指定安装参数。在这种情况下，不需要 MST 文件。有关详细信息，请参阅 "示例"(第 86 页)。

提取 MSI、MST 和 CAB 文件

通过运行安装程序的图形用户界面，提取安装包中的 MSI、MST 和 CAB 文件。

提取 MSI、MST 和 CAB 文件

1. 运行安装程序的图形用户界面，然后单击**创建 .mst 和 .msi 文件用于无人参与安装**。
2. 在**要安装的内容**中，选择要安装的组件，然后单击**完成**。

   注意
   修改现有安装时，请选择已安装的组件和要添加的组件。

   这些组件的安装包将从安装程序中提取为 CAB 文件。
3. 在**注册设置**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**。

   有关如何生成注册令牌的详细信息，请参阅 "生成注册标记"(第 106 页)。
4. [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。
5. 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**。
6. 选择 MSI、MST 和 CAB 文件将提取到的目标文件夹，然后单击**生成**。

安装代理程序和组件(MSI 和 MST 组合)

使用 MST 文件，自定义 MSI 文件的安装设置。当通过 Windows 组策略在多台计算机上安装代理程序时，请组合使用 MSI 和 MST。有关详细信息，请参阅 "通过组策略部署保护代理程序"(第 118 页)。

使用 MSI 和 MST 文件安装组件

1. 提取 MSI 和 MST 文件，如 "提取 MSI、MST 和 CAB 文件"(第 85 页) 中所述。
2. 在要安装组件的计算机的命令行界面中，运行以下命令：

```
msiexec /i <MSI file> TRANSFORMS=<MST file>
```

例如：

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

安装和卸载代理程序和组件(MSI 和直接选择)

运行 MSI 文件、手动选择要安装的组件，然后在命令行中指定它们的安装参数。在这种情况下，不需要 MST 文件。

安装代理程序和组件

1. 提取 MSI 文件和安装包(CAB 文件)，如 "提取 MSI、MST 和 CAB 文件"(第 85 页) 中所述。
   对于此安装方法，只需要 MSI 和 CAB 文件。不需要 MST 文件。
2. 在计算机的命令行界面中，运行以下命令：

   ```
   msiexec /i <MSI file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
   ```

   使用空格分隔参数，使用不带空格的逗号分隔参数的值。例如：

   ```
   msiexec.exe /i BackupClient64.msi
   ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
   TARGETDIR="C:\Program Files\BackupClient" REGISTRATION_ADDRESS=https://eu2-
   cloud.company.com REGISTRATION_TOKEN=34F6-8C39-4A5C
   ```

   要查看可用参数及其值，请参阅 "无人参与安装的参数 (MSI)"(第 88 页)。

示例

- 安装适用于 Windows 的代理程序、防恶意软件代理程序和适用于 URL 筛选的代理程序、命令行工具和 Cyber Protect Monitor。使用用户名和密码在 Cyber Protection 服务中注册工作负载。

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,AmpAgentFeature,CommandLineTool,Tray
  Monitor 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 Cyber Protect Monitor。在 Windows 中为代理程序服务创建一个新的登录帐户。使用令牌在 Cyber Protection 服务中注册工作负载。

  ```
  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 Cyber Protect Monitor。使用用户名和以 base64 编码的密码在 Cyber Protection 服务中注册计算机。如果密码包含特殊字符或空格，可能需要对该密码进行编码。有关如何对密码进行编码的详细信息，请参

阅 "使用包含特殊字符或空格的密码"(第 110 页)。

```
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 Cyber Protect Monitor。使用标记在 Cyber Protection 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
```

删除已安装的组件

1. 提取 MSI 文件和安装包(CAB 文件) , 如 "提取 MSI、MST 和 CAB 文件"(第 85 页) 中所述。
   对于此安装方法, 只需要 MSI 和 CAB 文件。不需要 MST 文件。
2. 在计算机的命令行界面中, 运行以下命令:

   ```
   msiexec /i <MSI file><REMOVE>=<value 1>,<value 2> REBOOT=ReallySuppress /qn
   ```

   要查看可用参数及其值, 请参阅 "无人参与安装的参数 (MSI)"(第 88 页)。

示例

- 删除 Cyber Protect Monitor。

```
msiexec.exe /i BackupClient64.msi /l*v uninstall_log.txt REMOVE=TrayMonitor
REBOOT=ReallySuppress /qn
```

卸载代理程序

1. 提取 MSI 文件和安装包(CAB 文件) , 如 "提取 MSI、MST 和 CAB 文件"(第 85 页) 中所述。
   对于此安装方法, 只需要 MSI 和 CAB 文件。不需要 MST 文件。
2. 在计算机的命令行界面中, 运行以下命令:

   ```
   msiexec /x <MSI file> /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
   REBOOT=ReallySuppress /qn
   ```

   要查看可用参数及其值, 请参阅 "无人参与安装的参数 (MSI)"(第 88 页)。

示例

- 卸载适用于 Windows 的代理程序及其所有组件。删除所有日志、任务和配置设置。

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
REBOOT=ReallySuppress /qn
```

- 卸载受密码保护的适用于 Windows 的代理程序及其所有组件。删除所有日志、任务和配置设置。

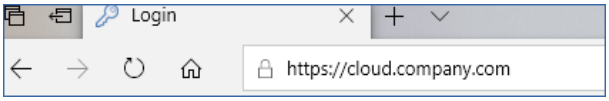
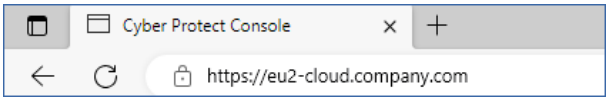
```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt ANTI_TAMPER_
PASSWORD=<password> DELETE_ALL_SETTINGS=1 REBOOT=ReallySuppress /qn
```

无人参与安装的参数 (MSI)

下表汇总了使用 MSI 文件进行无人参与安装的参数。

还可以使用其他 `msiexec` 参数。例如，使用 `/qn` 可阻止显示任何 GUI 元素。要了解有关 `msiexec` 参数的详细信息，请参阅 Microsoft 文档。

参数	描述
通用参数	
`ADDLOCAL=<component1,component2,...,componentN>`	要安装的组件。请参阅 "无人参与安装的组件 (MSI)"(第 91 页) 中可用组件的完整列表。 当指定多个组件时，请使用逗号分隔它们。请勿在逗号前后添加空格。 **注意** 必须提取要安装的所有组件的安装文件。有关如何提取组件的安装文件的详细信息，请参阅 "提取 MSI、MST 和 CAB 文件"(第 85 页) 。
`TARGETDIR=<path>`	选定组件将安装到的文件夹。如果指定的文件夹不存在，将创建该文件夹。 如果未指定此参数，则使用默认文件夹：`C:\Program Files\BackupClient`。
`REBOOT=ReallySuppress`	如果要安装组件但不重新启动计算机，请指定此参数。
`/l*v <log file>`	指定此参数，可保存详细日志。如果必须调查安装问题，需要此日志。
`CURRENT_LANGUAGE=<language ID>`	产品语言。 以下值可用：en、bn、bg、cs、da、de、es、fr、ko、id、it、hi、hu、ms、nl、ja、nb、pl、pt、pt_BR、ru、fi、sr、sv、th、tr、vi、zh、zh_TW。

参数	描述
	如果未指定此参数，并且执行安装的计算机的系统语言如上所列，则使用系统语言。在所有其他情况下，该值都设置为 en。
SKIP_SHA2_KB_CHECK={0,1}	使用此参数，可选择是否检查计算机上是否已安装来自 Microsoft 的 SHA2 代码签名支持更新 (KB4474419)。该检查仅会在需要此更新的操作系统上运行。要查看操作系统是否需要此更新，请参阅 "支持的操作系统和环境" (第 23 页)。 使用值设置为 1 的此参数，可跳过该检查。 如果未指定该参数或将其值设置为 0，并且在计算机上找不到 SHA2 代码签名支持更新，安装会失败。
FSS_ONBOARDING_AUTO_START={0,1}	使用值设置为 1 的此参数，可在无人参与安装完成后显示 File Sync & Share 登录向导。 如果未指定此参数或将其值设置为 0，登录向导不会显示。
注册参数	
REGISTRATION_ADDRESS	Cyber Protection 服务的 URL。可以将此参数与 REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD 参数一起使用，也可以将此参数与 REGISTRATION_TOKEN 参数一起使用。 • 当将此参数与 REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD 参数一起使用时，请指定用于**登录**到 Cyber Protection 服务的地址。例如，https://cloud.company.com:  • 当将此参数与 REGISTRATION_TOKEN 参数一起使用时，请指定准确的数据中心地址。这是您**登录**到 Cyber Protection 服务后所看到的 URL。例如，https://eu2-cloud.company.com。  请勿将 https://cloud.company.com 与 REGISTRATION_TOKEN 参数一起使用。
REGISTRATION_LOGIN REGISTRATION_PASSWORD	代理程序将在 Cyber Protection 服务中注册所使用帐户的凭据。这不能是合作伙伴管理员帐户。 请勿将这些参数与 REGISTRATION_TOKEN 参数一起使用。

参数	描述
REGISTRATION_PASSWORD_ENCODED	代理程序将在 Cyber Protection 服务中注册所使用帐户的密码，以 base64 编码。有关如何对密码进行编码的详细信息，请参阅 "使用包含特殊字符或空格的密码"(第 110 页)。
REGISTRATION_TOKEN	注册令牌。 注册令牌由 12 个字符组成，由连字符分为三段。有关如何生成注册令牌的详细信息，请参阅 "生成注册标记"(第 106 页)。 请勿将此参数与 REGISTRATION_LOGIN 和 REGISTRATION_PASSWORD 参数一起使用。
REGISTRATION_REQUIRED={0,1}	使用此参数，可选择注册失败时该怎么办。 如果将值设置为 1，安装也会失败。如果将值设置为 0 或未指定参数，则即使注册失败，安装也会成功完成。
代理程序服务的登录帐户	
MMS_USE_SYSTEM_ACCOUNT={0,1}	使用值为 1 的此参数，可使服务能够在**本地系统**登录帐户下运行。 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"(第 73 页)。
MMS_CREATE_NEW_ACCOUNT={0,1}	使用值为 1 的此参数，可使代理程序服务能够在新登录帐户 **Acronis Agent User**(自动创建)下运行。
MMS_SERVICE_USERNAME=<user name> MMS_SERVICE_PASSWORD=<password>	使用这些参数，可指定将运行代理程序服务所使用的现有登录帐户。
vCenter/ESXi 参数	
SET_ESX_SERVER={0,1}	当安装适用于 VMware 的代理程序时，请使用此参数。 如果将值设置为 0，则适用于 VMware 的代理程序将不会连接到 vCenter 服务器或 ESXi 主机。 如果将值设置为 1，则指定以下参数：ESX_HOST、EXI_USER、ESX_PASSWORD。
ESX_HOST=<host name>	vCenter 服务器或 ESXi 主机的主机名或 IP 地址。
ESX_USER=<user name> ESX_PASSWORD=<password>	vCenter 服务器或 ESXi 主机的访问凭据。
代理参数	
HTTP_PROXY_ADDRESS=<IP address>	使用这些参数，可指定代理程序将使用的 HTTP 代理服

参数	描述
HTTP_PROXY_PORT=<port>	务器。 如果不使用代理服务器，请不要指定这些参数。
HTTP_PROXY_LOGIN=<login> HTTP_PROXY_PASSWORD=<password>	HTTP 代理服务器的凭据。 如果代理服务器需要身份验证，请使用这些参数。
卸载参数	
REMOVE={<list of components>|ALL}	要卸载的组件。 当指定多个组件时，请使用逗号分隔它们。请勿在逗号前后添加空格。 要删除所有产品组件，请将值设置为 ALL。
DELETE_ALL_SETTINGS={0, 1}	要删除所有产品日志、任务和配置设置，请将值设置为 1。 当使用 REMOVE 时，请使用此可选参数。
ANTI_TAMPER_PASSWORD=<password>	卸载受密码保护的适用于 Windows 的代理程序或修改其组件所需的密码。

无人参与安装的组件 (MSI)

下表汇总了可以通过 MSI 文件进行无人参与安装的组件。使用值名称指定 ADDLOCAL 参数的值。有关详细信息，请参阅 "无人参与安装的参数 (MSI)"(第 88 页)。

值名称	组件描述	必须一起安装	位数
AgentFeature	用于代理程序的核心组件		32 位/64 位
MmsMspComponents	用于备份的核心组件	AgentFeature	32 位/64 位
BackupAndRecoveryAgent	适用于 Windows 的代理程序	MmsMspComponents	32 位/64 位
AmpAgentFeature	Agent for Antimalware protection	BackupAndRecoveryAgent	32 位/64 位
UrlFilteringAgentFeature	Agent for URL Filtering	BackupAndRecoveryAgent	32 位/64 位
DlpAgentFeature	适用于防止数据丢失的代理程序	BackupAndRecoveryAgent	32 位/64 位
SasAgentFeature	适用于 File Sync	TrayMonitor	32 位/64

	& Share 的代理程序		位
ArxAgentFeature	适用于 Exchange 的代理程序	MmsMspComponents	32 位/64 位
ArsAgentFeature	适用于 SQL 的代理程序	BackupAndRecoveryAgent	32 位/64 位
ARADAgentFeature	适用于 Active Directory 的代理程序	BackupAndRecoveryAgent	32 位/64 位
ArxOnlineAgentFeature	适用于 Microsoft 365 的代理程序	MmsMspComponents	32 位/64 位
OracleAgentFeature	适用于 Oracle 的代理程序	BackupAndRecoveryAgent	32 位/64 位
AcronisESXSupport	适用于 VMware ESX(i) 的代理程序 (Windows)	BackupAndRecoveryAgent	64 位
HyperVAgent	适用于 Hyper-V 的代理程序	BackupAndRecoveryAgent	32 位/64 位
CommandLineTool	命令行工具		32 位/64 位
TrayMonitor	Cyber Protect Monitor	AgentFeature	32 位/64 位
BackupAndRecoveryBootableComponents	可启动媒体生成器		32 位/64 位

在 Linux 中安装和卸载保护代理程序

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，<package name> 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"（第 94 页）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中输入敏感信息，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中，后跟该参数的值，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。确保您记住应该使用的密码（根用户的密码或“acronis”）。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。

卸载代理程序

1. 打开终端。
2. 请执行以下任一操作：
   - 要卸载代理程序并删除所有日志、任务和配置设置，请运行以下命令：

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a
     ```

   - 要卸载代理程序但保留其 ID（例如，如果您计划稍后安装代理程序），请运行以下命令：

     ```
     /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a --no-purge
     ```

   - 要使用安装文件卸载代理程序，请运行以下命令：

     ```
     <package name> -a -u
     ```

     此处，<package name> 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"（第 94 页）中所述。

注意

仅当安装程序包与已安装的代理程序版本相同，并且 `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall` 已损坏或无法访问时，才使用此命令。

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
MySQLAgentFeature	适用于 MySQL/MariaDB 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、适用于 Oracle 的代理程序和适用于 MySQL/MariaDB 的代理程序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 Cyber Protection 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`, `vi`, `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 Cyber Protection 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。

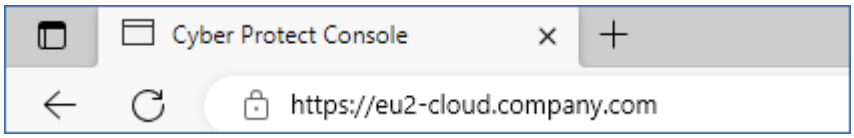
- `--token=<标记>`

  注册标记是由 12 个字符组成的序列,由连字符分为三段。有关详细信息,请参阅 "生成注册标记"(第 106 页)。

  注意
  当您使用 `--token` 参数时,还必须包含 `{-C|--rain=}` 参数并指定确切的数据中心地址。
  不能将 `--token` 参数与 `--login`、`--password` 和 `--register-with-credentials` 参数一起使用。

  - `{-C|--rain=}<服务地址>`

    Cyber Protection 服务的 URL。
    必须使用 `{-C|--rain=}` 参数,并在使用 `--token` 参数时指定准确的数据中心地址。准确的数据中心地址是**您登录 Cyber Protection 中控台后**看到的 URL。例如:

    当您使用 `--login` 和 `--password` 参数进行注册时,可以跳过 `{-C|--rain=}` 参数,因为安装程序默认使用正确的地址。

- `--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 Cyber Protection 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`

  如果想要安装代理程序,但计划稍后在 Cyber Protection 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 "使用命令行接口注册和取消注册工作负载"(第 109 页)。

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。不建议您使用此选项。

`--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=}<路径>`

指定用于 SSL 通信的自定义证书文件的路径。

`{-p|--port=}<端口>`

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
```

在 macOS 中安装和卸载保护代理

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和卸载保护代理程序。

所需权限

在 Mac 工作负载上启动无人参与安装之前，必须修改“隐私首选项策略控制”，以允许应用程序访问工作负载的 macOS 中的内核和系统扩展，从而支持安装 Cyber Protection 代理程序。请参阅 "在 macOS 中进行无人参与安装所需的权限"(第 99 页)。

在部署 PPPC 负载后，可以继续进行以下步骤。

下载安装文件 (.dmg)

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 单击**添加**，然后单击 **Mac**。

安装代理程序

1. 打开终端。
2. 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。
3. 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，**Cyber_Protection_Agent_for_MAC_x64.dmg**。
4. 运行安装程序。
   - 如果使用面向 Mac 的完整安装程序(如 CyberProtect_AgentForMac_x64.dmg 或 CyberProtect_AgentForMac_arm64.dmg)，则运行以下命令。

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

     注意
     如果需要为 File Sync & Share 启用自动登录，则改为运行以下命令。此选项将请求管理员密码。

     ```
     open <dmg_root>/Install.app --args --unattended --fss-onboarding-auto-start
     ```

   - 如果使用面向 Mac 的通用安装程序(如 CyberProtect_AgentForMac_web.dmg)，则运行以下命令。

     ```
     sudo <dmg_root>/Install.app/Contents/MacOS/cyber_installer -a
     ```

5. 卸载安装文件 (.dmg)。

```
hdiutil detach <dmg_root>
```

示例

```
mkdir mydirectory
```

```
hdiutil attach /Users/JohnDoe/Cyber_Protection_Agent_for_MAC_x64.dmg -mountpoint
mydirectory
```

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

```
hdiutil detach mydirectory
```

卸载代理程序

1. 打开终端。
2. 请执行以下任一操作：
   - 要卸载代理程序，请运行以下命令：

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

   - 要卸载代理程序并删除所有日志、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
     ```

在 macOS 中进行无人参与安装所需的权限

在 Mac 工作负载上启动无人参与安装之前，必须修改“隐私首选项策略控制”，以允许应用程序访问工作负载的 macOS 中的内核和系统扩展，从而支持安装 Cyber Protection 代理程序。可以通过部署自定义 PPPC 负载或在工作负载的图形用户界面中配置首选项来实现此操作。需要以下权限。

macOS 11 (Big Sur) 或更高版本的要求

选项卡	节	现场	值
隐私首选项策略控制	应用程序访问	标识符	com.acronis.backup
		标识符类型	捆绑 ID

		规范要求	identifier "com.acronis.backup" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		应用程序或服务	SystemPolicyAllFiles
		访问	允许
	应用程序访问	标识符	com.acronis.backup.aakore
		标识符类型	捆绑 ID
		规范要求	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		应用程序或服务	SystemPolicyAllFiles
		访问	允许
	应用程序访问	已标识	com.acronis.backup.activeprotection
		标识符类型	捆绑 ID
		规范要求	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		应用程序或服务	SystemPolicyAllFiles
		访问	允许
	应用程序	标识符	cyber-protect-service

	访问		
		标识符类型	捆绑 ID
		规范要求	identifier "cyber-protect-service" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		应用程序或服务	SystemPolicyAllFiles
		访问	允许
系统扩展		允许用户批准系统扩展	已启用
	允许的团队 ID 和系统扩展	显示名称	安克诺斯数据保护软件代理程序系统扩展
		系统扩展类型	允许的团队标识符
		团队标识符	ZU2TV78AA6

版本 11 之前的 macOS 版本的要求

选项卡	节	现场	值

隐私首选项策略控制	应用程序访问	标识符	com.acronis.backup

		标识符类型	捆绑 ID
		规范要求	identifier "com.acronis.backup" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		应用程序或服务	SystemPolicyAllFiles
		访问	允许
	应用程序访问	标识符	com.acronis.backup.aakore
		标识符类型	捆绑 ID
		规范要求	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		应用程序或服务	SystemPolicyAllFiles
		访问	允许
	应用程序访问	已标识	com.acronis.backup.activeprotection
		标识符类型	捆绑 ID
		规范要求	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		应用程序或服务	SystemPolicyAllFiles
		访问	允许
	应用程序访问	标识符	cyber-protect-service
		标识符类型	捆绑 ID
		规范要求	identifier "cyber-protect-service" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		应用程序或服务	SystemPolicyAllFiles
		访问	允许

已批准的内核扩展		允许用户批准内核扩展	已启用
		允许标准用户批准旧版内核扩展(macOS 11 或更高版本)	已启用
	已批准的团队 ID 和内核扩展	已批准的团队 ID - 显示名称	安克诺斯数据保护软件代理程序内核扩展
		团队 ID	ZU2TV78AA6
		内核扩展捆绑 ID	• com.acronis.systeminterceptors • com.acronis.ngscan • com.acronis.notifyframework
系统扩展		允许用户批准系统扩展	已启用
	允许的团队 ID 和系统扩展	显示名称	Acronis Cyber Protection Agent System Extensions
		系统扩展类型	允许的团队标识符
		团队标识符	ZU2TV78AA6

工作负载注册

注册是将安装了保护代理程序的工作负载连接到客户租户中的用户帐户。注册完成后，可以在 Cyber Protect中控台的**设备>带代理的计算机**看到工作负载。可以通过将计划应用于已注册的工作负载来管理它们。

使用图形用户界面安装保护代理程序时，注册是安装过程的一部分。

当使用命令行接口时，可以将注册作为独立过程执行。

使用图形用户界面注册工作负载

使用图形用户界面安装保护代理程序时，注册是安装过程的一部分。

有以下注册方法可用：

- 在 Cyber Protect 中控台中注册
- 使用用户帐户凭据注册
- 使用注册令牌注册

当您卸载代理程序时，它将自动取消注册。

使用 Cyber Protect 中控台注册工作负载

此过程适用于使用默认安装设置(**注册设置**>**使用Cyber Protect中控台**)。

若要从 Cyber Protect 中控台注册工作负载

1. 在安装向导中,单击**"注册工作负载"**。
   Cyber Protect中控台会打开。

   注意
   完成注册前请勿关闭安装向导。否则,将不得不重复安装并重新开始注册。

2. 登录到 Cyber Protect 中控台。
3. [如果以管理员身份登录] 在**工作负载注册**屏幕上,选择想要注册工作负载的帐户。
   此帐号必须是客户租户中的帐号。合作伙伴管理员可以查看自己管理的客户租户,并在这些租户中的帐号下注册工作负载。
4. 单击**验证代码**。
5. 单击**注册**。

因此,工作负载会注册在指定的用户帐户下。

使用用户凭据注册工作负载

您可以修改默认的安装程序,并选择使用用户名和密码进行注册,而不是在 Cyber Protect 中控台上进行注册。

若要使用用户名和密码注册工作负载

1. 在安装向导中,单击**自定义安装设置**。
2. 在**注册设置**部分中,单击**更改**。
3. 选择**使用凭据**。
4. 指定要注册工作负载的帐户的用户名和密码。
   此帐户必须是客户租户中的帐户。

   注意
   您只能使用未启用双重身份验证的帐户。

5. 单击**完成**,然后完成安装。

使用注册令牌注册工作负载

您可以修改默认的安装程序,并选择使用注册令牌进行注册,而不是在 Cyber Protect 中控台上进行注册。

若要使用注册标记注册工作负载

1. 在安装向导中,单击**自定义安装设置**。
2. 在**注册设置**部分中,单击**更改**。

3. 选择**使用注册令牌**。
4. 输入注册令牌。
5. 单击**完成**，然后完成安装。

生成注册标记

注册令牌由 12 个字符组成，以连字符分隔为三段。对于Cyber Protect中控台，注册令牌将用户身份传递给代理安装程序，但不存储用户凭据。这使用户无需登录中控台即可在其帐户下注册工作负载或将保护计划应用于工作负载。

注意
工作负载注册期间不会自动应用保护计划。应用保护计划是一项单独的任务。

出于安全原因，令牌的生存期有限，可以对此进行调整。默认生存期为 3 天。

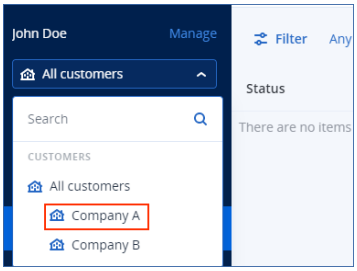
管理员可以为其管理的租户中的所有用户帐户生成注册令牌。用户只能为自己的帐户生成注册令牌。

生成注册标记的步骤

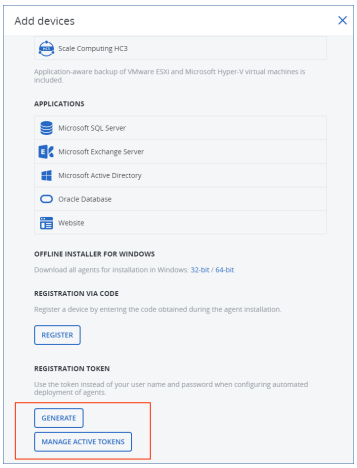
以管理员身份

1. 以管理员身份登录到 Cyber Protect 中控台。
   如果已登录到管理门户，则可以转到 Cyber Protect 中控台，方法是导航到**监视** > **使用情况**，然后在**保护**选项卡下，单击**管理服务**。

   [对于管理客户租户的合作伙伴管理员] 在 Cyber Protect 中控台中，选择要为其生成令牌的用户所在的租户。无法在**所有客户**级别上生成令牌。



2. 在**设备**下，依次单击**所有设备** > **添加**。
   添加设备窗格即会在右侧打开。
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。
5. 选择要为其生成标记的用户。

注意
当使用令牌时，工作负载将注册在此处选择的用户帐户下。

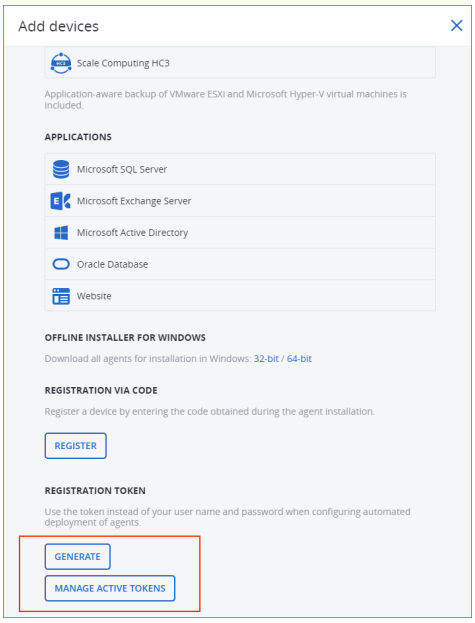
6. [可选] 要使令牌的用户能够在已添加的工作负载上应用和吊销保护计划，请从下拉列表中选择计划。

   请注意，您需要运行一个将在已添加的工作负载上应用或吊销保护计划的脚本。有关更多详细信息，请参阅此知识库文章。
7. 单击**生成标记**。
8. 单击**复制**以将令牌复制到设备剪贴板，或手动记下令牌。

以用户身份

1. 登录到 Cyber Protect 中控台。
2. 依次单击**设备** > **所有设备** > **添加**。

   添加设备窗格即会在右侧打开。
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。
5. 单击**生成标记**。
6. 单击**复制**以将令牌复制到设备剪贴板，或手动记下令牌。

管理注册令牌

您可以查看和删除有效的注册令牌。

若要查看注册令牌

1. 登录到 Cyber Protect 中控台。
2. 依次单击**设备** > **所有设备** > **添加**。
3. 向下滚动到**注册令牌**，然后单击**管理活动令牌**。
   一个包含为租户生成的活动令牌的列表即会在右侧打开。

> **注意**
> 出于安全原因，在**令牌**列中，仅会显示令牌值的前两个字符。

若要删除注册令牌

1. 登录到 Cyber Protect 中控台。
2. 依次单击**设备** > **所有设备** > **添加**。
3. 向下滚动到**注册令牌**，然后单击**管理活动令牌**。
   一个包含为租户生成的活动令牌的列表即会在右侧打开。

> **注意**
> 出于安全原因，在**令牌**列中，仅会显示令牌值的前两个字符。

4. 选择令牌，然后单击**删除**。

使用命令行接口注册和取消注册工作负载

当使用命令行接口时，可以将注册作为独立过程执行。

因此，例如，如果您想在另一个帐户下注册保护代理程序，不必卸载它。

使用用户凭据注册工作负载

使用要注册工作负载的帐户的用户名和密码。此帐户必须是客户租户中的帐户。如果密码包含特殊字符或空格，请参阅"使用包含特殊字符或空格的密码"(第 110 页)。

服务地址是用于**登录**到 Cyber Protection 服务的 URL。

例如，`https://cloud.company.com`。

使用用户名和密码注册工作负载

在 Windows 中

- 在命令提示符中，运行以下命令：

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a <service address> -u <user name> -p <password>
```

例如：

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

在 Linux 中

- 在命令提示符中，运行以下命令：

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
<service address> -u <user name> -p <password>
```

例如：

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

在 macOS 中

重要事项
如果您使用 macOS 10.14 或更高版本，请将完整磁盘访问权限授予保护代理程序。为此，请转到**应用程序 > 实用程序**，然后运行**Cyber Protect 代理程序助手**。接着，按照应用程序窗口中的说明进行操作。

- 在命令提示符中，运行以下命令：

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

例如：

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

使用包含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。

例如，在 Windows 中，运行以下命令：

命令模板：

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -p <"password">
```

命令示例：

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

如果此命令失败，请通过访问 https://www.base64encode.org/，将密码编码为 base64 格式。然后，在命令行中，使用 -b 或 --base64 参数指定编码的密码。

例如，在 Windows 中，运行以下命令：

命令模板：

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -b -p <encoded password>
```

命令示例：

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

使用注册令牌注册工作负载

注册令牌由 12 个字符组成，以连字符分隔为三段。对于Cyber Protect中控台，注册令牌将用户身份传递给代理安装程序，但不存储用户凭据。这使用户无需登录中控台即可在其帐户下注册工作负载或将保护计划应用于工作负载。

有关详细信息，请参阅 "生成注册标记"(第 106 页)。

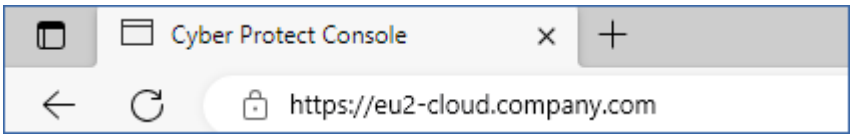
注意

工作负载注册期间不会自动应用保护计划。应用保护计划是一项单独的任务。

有关更多信息，请参阅此知识库文章。

使用注册标记时，必须指定准确的数据中心地址。这是**您登录**到 Cyber Protection 服务后所看到的 URL。

例如，`https://eu2-cloud.company.com`。



使用注册标记注册工作负载

在 Windows 中

- 在命令提示符中，运行以下命令：

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a <service address> --token <registration token>
```

例如：

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

在 Linux 中

- 在命令提示符中，运行以下命令：

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
<service address> --token <registration token>
```

例如：

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

在 macOS 中

重要事项

如果您使用 macOS 10.14 或更高版本，请将完整磁盘访问权限授予保护代理程序。为此，请转到**应用程序 > 实用程序**，然后运行**Cyber Protect 代理程序助手**。接着，按照应用程序窗口中的说明进行操作。

- 在命令提示符中，运行以下命令：

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

例如：

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

虚拟设备

1. 在虚拟设备的中控台中，按 CTRL+SHIFT+F2 组合键以打开命令行界面。
2. 在命令提示符中，运行以下命令：

   ```
   register_agent -o register -t cloud -a <service address> --token <registration token>
   ```

   例如：

   ```
   register_agent -o register -t cloud -a https://eu2-cloud.company.com --token 34F6-
   8C39-4A5C
   ```

3. 要返回设备的图形界面，请按 ALT+F1 组合键。

取消注册工作负载

从命令行接口，可以取消注册保护代理而不卸载它。

注销工作负载

在 Windows 中

- 在命令提示符中，运行以下命令：

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

例如：

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

在 Linux 中

- 在命令提示符中，运行以下命令：

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

在 macOS 中

在命令提示符中，运行以下命令：

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

虚拟设备

1. 在虚拟设备的中控台中，按 CTRL+SHIFT+F2 组合键以打开命令行界面。
2. 在命令提示符中，运行以下命令：

```
register_agent -o unregister
```

3. 要返回设备的图形界面，请按 ALT+F1 组合键。

更改工作负载的注册

可以通过在新租户中或新用户帐户下注册工作负载，来更改工作负载的注册。

重要事项
在更改工作负载的注册后，将吊销应用于该工作负载的所有保护计划。要继续保护工作负载，请将一个新的保护计划应用于该工作负载。

如果在新租户中注册工作负载，则该工作负载将无法访问原始租户的云存储中的备份。非云存储中的备份将仍可访问。

更改工作负载的注册

通过使用命令行接口

1. 注销保护代理程序，如 "取消注册工作负载"(第 112 页) 中所述。
2. 在新租户中或新用户帐户下注册保护代理程序，如 "使用用户凭据注册工作负载"(第 109 页) 或 "使用注册令牌注册工作负载"(第 111 页) 中所述。

通过使用图形用户界面

1. 卸载保护代理程序。
2. 安装保护代理程序，然后在新租户中或新用户帐户下注册该保护代理程序。

有关如何安装和注册代理的详细信息，请参阅 "使用图形用户界面安装保护代理程序"(第 72 页)。

将工作负载转移给另一个租户

原生不支持将工作负载移动到另一个租户。作为一种解决方案，可以注销工作负载，然后将其注册到另一个租户中。所有已应用的保护计划将从该工作负载中撤消，并且该工作负载将无法访问原始

租户的云存储中的其备份。

有关如何在新租户中或新用户帐户下注册工作负载的详细信息，请参阅 "更改工作负载的注册"(第 113 页)。

更新保护代理程序

可以使用 Cyber Protect 中控台或通过下载并运行安装文件，来手动更新所有代理程序。

可以为以下代理程序配置自动更新：

- 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
- Cyber Files Cloud 适用于 File Sync & Share 的代理程序

自动更新代理程序或使用 Cyber Protect 中控台手动更新代理程序时，要求以下位置有 4.2 GB 可用空间：

- 对于 Linux - 根目录
- 对于 Windows – 安装有代理程序的卷

在 macOS 的根目录中，更新代理程序需要 5 GB 可用空间。

注意
[适用于以虚拟设备形式提供的所有代理程序，包括适用于 VMware 的代理程序、适用于 Scale Computing 的代理程序、适用于 Virtuozzo Hybrid Infrastructure 的代理程序、适用于 RHV 的代理程序 (oVirt)]

为了对位于代理之后的虚拟设备执行自动或手动更新，必须按如下所述在每个设备上配置代理服务器。

在 `/opt/acronis/etc/va-updater/config.yaml` 文件中，将以下行添加到该文件末尾并输入特定于您环境的值：

```
httpProxy: http://proxy_login:proxy_password@proxy_address:port
```

手动更新保护代理程序

可以使用 Cyber Protect 中控台或通过下载并运行安装文件来更新代理程序。

以下版本的虚拟设备必须仅使用 Cyber Protect 中控台进行更新：

- 适用于 VMware 的代理程序(虚拟设备)：版本 12.5.23094 及更高版本。
- 适用于 Virtuozzo Hybrid Infrastructure 的代理程序(虚拟设备)：版本 12.5.23094 及更高版本。

以下版本的代理程序也可以使用 Cyber Protect 中控台进行更新：

- 适用于 Windows 的代理程序、适用于 VMware 的代理程序 (Windows)、适用于 Hyper-V 的代理程序：版本 12.5.21670 及更高版本。

- 适用于 Linux 的代理程序:版本 12.5.23094 及更高版本。
- 其他代理程序:版本 12.5.23094 及更高版本。

要查找代理程序版本,请在 Cyber Protect 中控台中选择计算机,然后单击**详细信息**。

若要从这些代理程序的较早代理程序版本更新,请手动下载并安装最新的版本。若要查找下载链接,请依次单击**所有设备** > **添加**。

先决条件

在 Windows 计算机上,Cyber Protect 功能需要 Microsoft Visual C++ 2017 Redistributable。在更新代理程序之前,确保已将其安装在计算机上或先安装它。在安装后,可能需要重新启动。可以在 Microsoft 网站上找到 Microsoft Visual C++ 可再发行程序包:https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows。

使用 Cyber Protect 中控台更新代理程序

1. 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。
2. 选择要更新代理程序的计算机。计算机必须处于联机状态。
3. 单击**更新代理程序**。

注意
在更新过程中,任何正在进行的备份都将失败。

更新版本低于 12.5.23094 的适用于 VMware 的代理程序(虚拟设备)

1. 依次单击**设置** > **代理程序** > 要更新的代理程序 > **详细信息**,然后检查**已指派虚拟机**部分。更新后,您需要重新输入这些设置。
   a. 记下**自动指派**开关的位置。
   b. 要找出手动指派给代理程序的虚拟机,请单击**已指派:**链接。软件将显示已指派虚拟机列表。记下**代理程序**列中代理程序名称后面带有 (M) 的计算机。
2. 删除适用于 VMware 的代理程序(虚拟设备),如"卸载代理程序"中所述。在步骤 5 中,从**设置** > **代理程序**中删除代理程序,即使您计划再次安装代理程序也是如此。
3. 部署适用于 VMware 的代理程序(虚拟设备),如"部署 OVF 模板"中所述。
4. 配置适用于 VMware 的代理程序(虚拟设备),如"配置虚拟设备"中所述。
   如果您要重建本地附加的存储,请在步骤 7 中执行以下操作:
   a. 将包含本地存储的磁盘添加到虚拟设备。
   b. 依次单击**刷新** > **创建存储** > **加载**。
   c. 软件将显示磁盘的原始**代号**和**标签**。请勿更改它们。
   d. 单击**确定**。
5. 依次单击**设置** > **代理程序** > 要更新的代理程序 > **详细信息**,然后重新构建步骤 1 中记下的设置。如果有些虚拟机已手动指派给代理程序,请按照"虚拟机绑定"中所述步骤再次指派它们。
   在完成代理程序配置后,应用于旧代理程序的保护计划即会自动重新应用于新代理程序。

6. 已启用应用程序感知备份的计划需要重新输入访客操作系统凭据。编辑这些计划，然后重新输入凭据。
7. 备份 ESXi 配置的计划需要重新输入“根”密码。编辑这些计划，然后重新输入密码。

要更新计算机上的网络安全保护定义

1. 依次单击**设置** > **代理程序**。
2. 选择要更新网络安全保护定义的计算机，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. 选择要指派“更新”角色的计算机，单击**“详细信息”**，然后在“**网络安全保护定义**”部分启用“**使用此代理程序来下载和分发修补程序与更新**”。

注意
具有“更新”角色的代理程序可以下载并分发仅用于 Windows 第三方产品的修补程序。对于 Microsoft 产品，修补程序分发不受“更新”代理程序的支持。

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”**。

自动更新保护代理程序

要促进多个工作负载的管理，可以为适用于 Windows 的代理程序、适用于 Linux 的代理程序和适用于 Mac 的代理程序配置自动更新。自动更新适用于代理程序版本 15.0.26986（于 2021 年 5 月发布）或更高版本。首先必须将较早的代理程序手动更新至最新版本。

自动更新在运行任意以下操作系统的计算机上受支持：

- Windows XP SP 3 及更高版本
- Red Hat Enterprise Linux 6 及更高版本，CentOS 6 及更高版本
- OS X 10.9 Mavericks 及更高版本

自动更新的设置在数据中心级别预配置。公司管理员可以自定义这些设置 – 为公司或单位中的所有计算机，或为单台计算机。如果应用了自定义设置，将使用较高级别的设置，顺序为：

1. Cyber Protection 数据中心
2. 公司（客户租户）
3. 单元
4. 计算机

例如，单位管理员可以为单位中的所有计算机配置自定义自动更新设置，这可能不同于应用于该公司级别上计算机的设置。管理员还可以为单位中的一台或多台个别计算机配置不同的设置，不对其应用单位设置或公司设置。

启用自动更新后，可以配置以下选项：

- **更新渠道**

  在 **更新通道** 部分，您可以选择要使用哪个版本的保护代理程序：
  - **最新**：始终安装最新版本的保护代理程序。
  - **上一个稳定版**：从之前的版本中安装保护代理程序的最新稳定版。
- **维护时段**

  维护时段定义可以安装更新的时间。如果维护时段已禁用，更新可以随时运行。

  即使在已启用的维护时段内，在代理程序运行以下任意操作时，将不会安装更新：
  - 备份
  - 恢复
  - 备份复制
  - 虚拟机复制
  - 测试副本
  - 从备份运行虚拟机（包括最终确定）
  - 灾难恢复故障转移
  - 灾难恢复故障恢复
  - 运行脚本（对于网络安全脚本功能）
  - 修补程序安装
  - ESXi 配置备份

自定义自动更新设置的步骤

1. 在 Cyber Protect 中控台中，转到**设置** > **代理程序**。
2. 选择设置的范围：
   - 要为所有计算机更改设置，请单击**编辑默认代理程序更新设置**。
   - 要为特定计算机更改设置，请选择所需计算机，然后单击**代理程序更新设置**。
3. 根据您的需要配置设置，然后单击**应用**。

删除自定义自动更新设置的步骤

1. 在 Cyber Protect 中控台中，转到**设置** > **代理程序**。
2. 选择设置的范围：
   - 要删除所有计算机的自定义设置，请单击**编辑默认代理程序更新设置**。
   - 要删除特定计算机的自定义设置，请选择所需计算机，然后单击**代理程序更新设置**。
3. 单击**重置为默认设置**，然后单击**应用**。

检查自动更新状态的步骤

1. 在 Cyber Protect 中控台中，转到**设置** > **代理程序**。
2. 单击表格右上角的齿轮图标，然后确保选中了**自动更新**复选框。
3. 检查显示在**自动更新**列中的状态。

更新 BitLocker 加密工作负载上的保护代理程序

在 BitLocker 和 启动恢复管理器 已启用的工作负载上，引入对 启动恢复管理器 的更改的代理程序更新会干扰 BitLocker。在这种情况下，重新启动后，需要提供 BitLocker 恢复密钥。要缓解此问题，

请在更新代理程序之前暂停或禁用 BitLocker。

受影响的代理程序版本：

- 23.12.36943，发布于 2023 年 12 月

您也可以在保护代理程序的版本说明中检查更新是否对 启动恢复管理器 进行了更改。

更新 BitLocker 和 启动恢复管理器 已启用的工作负载上的代理程序

1. 在要更新代理程序的工作负载上，暂停或禁用 BitLocker。
2. 更新代理程序。
3. 重新启动工作负载。
4. 启用 BitLocker。

通过组策略部署保护代理程序

通过使用 Windows 组策略，可将适用于 Windows 的代理程序集中安装（或部署）到 Active Directory 域的成员计算机上。

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

- 带有运行 Microsoft Windows Server 2003 或更高版本的域控制器的 Active Directory 域。
- 您必须是该域中**域管理员**组的成员。
- 您已下载**适用于 Windows 的所有代理程序**安装程序。
  要下载安装程序，请在 Cyber Protect 中控台中，单击右上角的帐户图标，然后单击**下载**。下载链接也可在**添加设备**窗格中找到。

通过组策略部署代理程序

1. 生成注册令牌，如 "生成注册标记"（第 106 页）中所述。
2. 创建 .mst 文件、.msi 文件和 .cab 文件，如 "创建转换文件和提取安装包"（第 118 页）中所述。
3. 设置组策略对象，如 "设置组策略对象"（第 119 页）中所述。

创建转换文件和提取安装包

要通过 Windows 组策略部署保护代理程序，您需要转换文件 (.mst) 和安装包（.msi 和 .cab 文件）。

注意
下面的过程使用默认注册选项，即通过令牌注册。要了解如何生成注册令牌，请参阅 "生成注册标记"（第 106 页）。

创建 .mst 转换文件和提取安装包（.msi 和 .cab 文件）

1. 以管理员身份登录到 Active Directory 域中的任何计算机上。
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. 运行代理程序安装程序。
4. 单击**创建 .mst 和 .msi 文件用于无人参与安装**。
5. 在**要安装的内容**中，选择要包含在安装中的组件，然后单击**完成**。
6. 在**注册设置**中，单击**指定**、输入注册令牌，然后单击**完成**。
   可以将注册方法从**使用注册令牌**(默认)更改为**使用凭据**或**跳过注册**。**跳过注册**选项假定您稍后将手动注册工作负载。
7. 查看或修改将添加到 .mst 文件中的安装设置，然后单击**继续**。
8. 在**文件的保存位置**中，将路径指定为已创建的共享文件夹。
9. 单击**生成**。

结果，将创建 .mst 文件、.msi 文件和 .cab 文件，并将这些文件复制到指定的共享文件夹。

接下来，设置 Windows 组策略对象。要了解如何操作，请参阅 "设置组策略对象"(第 119 页)。

设置组策略对象

在此过程中，将使用在 "创建转换文件和提取安装包"(第 118 页) 中创建的安装包来设置组策略对象 (GPO)。GPO 会将代理程序部署到域中的计算机。

设置组策略对象

1. 以域管理员身份登录到域控制器。
   如果该域有多个域控制器，请以域管理员身份登录到其中任何一个域控制器。
2. [如果在组织单元中部署代理程序] 请确保要部署代理程序的组织单元存在于在此域中。
3. 在 Windows 的**开始**菜单中，指向**管理工具**，然后单击**组策略管理**(或 Windows Server 2003 中的 **Active Directory 用户和计算机**)。
4. [对于 Windows Server 2008 或更高版本] 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. [对于 Windows Server 2003] 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**。
6. 将新的“组策略”对象命名为**适用于 Windows 的代理程序**。
7. 打开**适用于 Windows 的代理程序**组策略对象以进行编辑：
   - [在 Windows Server 2008 或更高版本中] 在**组策略对象**下，右键单击组策略对象，然后单击**编辑**。
   - [在 Windows Server 2003 中] 单击组策略对象，然后单击**编辑**。
8. 在“组策略”对象编辑器管理单元中，展开**计算机配置**。
9. [对于 Windows Server 2012 或更高版本] 展开**策略 > 软件设置**。
10. [对于 Windows Server 2003 和 Windows Server 2008] 展开**软件设置**。
11. 右键单击**软件安装**、指向**新建**，然后单击**程序包**。
12. 选择已创建共享文件夹中的代理程序的 .msi 安装包，然后单击**打开**。

13. 在**部署软件**对话框中，单击**高级**，然后单击**确定**。
14. 在**修改**选项卡上，单击**添加**，然后选择已创建共享文件夹中的 .mst 文件。
15. 单击**确定**关闭**部署软件**对话框。

部署虚拟设备

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。

为了提高备份性能并避免出现与 RAM 内存不足有关的故障，建议您在要求更高的情况下将这些资源增加到 16 GB RAM 和 4 个 vCPU。例如，当预计备份流量会超过 100 MB/秒（例如，在万兆网络中），或同时备份多个具有较大硬盘驱动器（500 GB 或更多）的虚拟机时，请增加指派的资源。

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。

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 (Windows) 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，建议您不要使用本地连接的存储空间（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"（第 619 页）。

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

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。该文件夹中包含一个 .ovf 文件和三个 .vmdk 文件。
3. 确保这些文件可以从运行 vSphere Client 的计算机进行访问。
4. 启动 vSphere Client，然后登录到 vCenter 服务器。

5. 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。
   - 配置网络连接时，请确保选择允许互联网连接的网络，以便代理程序本身可以在云中正确注册。

配置虚拟设备

在部署虚拟设备后，必须对其进行配置，以使其能够访问 vCenter 服务器或 ESXi 主机和 Cyber Protection 服务。

若要配置虚拟设备

1. 在 vSphere Client 中，打开虚拟设备的中控台。
2. 确保网络连接已配置。

   该连接通过动态主机配置协议 (DHCP) 自动进行配置。

   要更改默认配置，请在**代理程序选项**下的 **eth0** 字段中，单击**更改**，然后指定网络设置。
3. 将虚拟设备连接到 vCenter 服务器或 ESXi 主机。
   a. 在**代理程序选项**下的 **vCenter/ESX(i)** 字段中，单击**更改**，然后指定以下各项。
      - [如果使用 vCenter 服务器] vCenter 服务器名称或 IP 地址。
      - [如果不使用 vCenter 服务器] 要备份和恢复其虚拟机的 ESXi 主机的名称或 IP 地址。要更快地进行备份，请在同一主机上部署虚拟设备。
      - 设备连接到 vCenter 服务器或 ESXi 主机所需的凭据。

        建议使用专用帐户来访问 vCenter 服务器或 ESXi 主机，而不是使用角色为管理员的现有帐户。有关详细信息，请参见"Agent for VMware 所需的权限"（第 624 页）。

   b. 单击**检查连接**，以验证设置是否正确无误。
   c. 单击**确定**。
4. 使用以下方法之一在 Cyber Protection 服务中注册设备。
   - [仅适用于没有双重身份验证的租户] 在其图形界面中注册设备。
     a. 在**代理程序选项**下的**管理服务器**字段中，单击**更改**。
     b. 在**服务器名称/IP** 字段中，选择**云**。

        Cyber Protection 服务地址即会显示。除外另有说明，否则请勿更改此地址。
     c. 在**用户名**和**密码**字段中，指定 Cyber Protection 服务中您帐户的凭据。虚拟设备和该设备管理的虚拟机都注册在此帐户下。
     d. 单击**确定**。
   - 在命令行界面中注册设备。

     注意

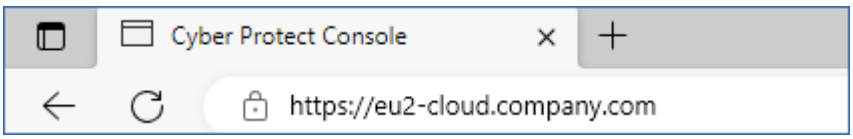
     使用此方法时，需要一个注册令牌。有关如何生成注册令牌的详细信息，请参阅 "生成注册标记"（第 106 页）。

     a. 按 CTRL+SHIFT+F2 组合键以打开命令行界面。
     b. 运行以下命令：

```
register_agent -o register -t cloud -a <service address> --token <registration
token>
```

注意

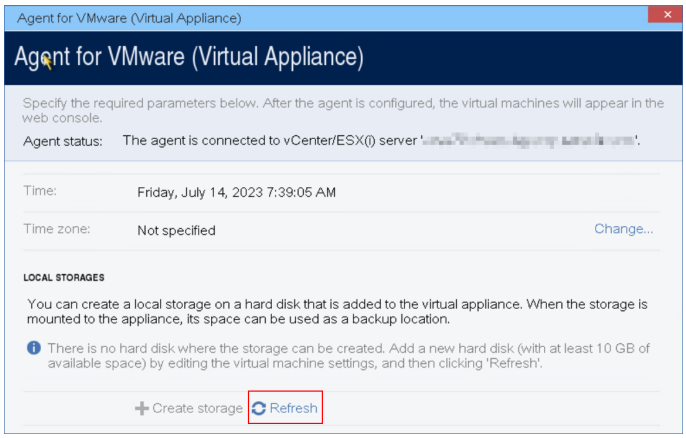
使用注册标记时，必须指定准确的数据中心地址。这是您**登录**到 Cyber Protect 中控台后所看到的 URL。例如，`https://eu2-cloud.company.com`。



请勿在此处使用 `https://cloud.company.com`。

c. 要返回设备的图形界面，请按 ALT+F1 组合键。

5. [可选] 添加本地存储。
   a. 在 vSphere Client 中，将虚拟磁盘附加到虚拟设备。虚拟磁盘必须至少有 10 GB 的可用空间。
   b. 在设备的图形用户界面中，单击**刷新**。



   创建存储按钮变为处于活动状态。
   c. 单击**创建存储**。
   d. 为该存储指定标签，然后单击**确定**。
   e. 单击**是**来确认选择。
6. [如果在网络中启用了代理服务器] 配置代理服务器。
   a. 按 CTRL+SHIFT+F2 组合键以打开命令行界面。
   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 ADDRESS 替换为新代理服务器主机名称/IP 地址，将 PORT 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 LOGIN 和 PASSWORD 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。

注意

为了能够更新部署在代理后面的虚拟设备，请编辑设备文件 config.yaml (/opt/acronis/etc/va-updater/config.yaml)，方法是在该文件的底部添加以下行，然后输入特定于您环境的值：

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

例如：

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

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

默认情况下，带有代理程序的虚拟机使用 2 个 vCPU 和 4 GB RAM。这些设置对大多数操作已够用，但可以通过在 Scale Computing HC3 Web 界面中编辑虚拟机来更改这些设置。

为了提高备份性能并避免出现与 RAM 内存不足有关的故障，建议您在要求更高的情况下将这些资源增加到 4 个 vCPU 和 8 GB RAM。例如，当预计备份流量会超过 100 MB/秒时(例如，在万兆网络中)，或如果同时备份多个具有大型硬盘驱动器(500 GB 或更多) 的虚拟机，请增加指派的资源。

设备虚拟磁盘的大小约是 9 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。

如果在簇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，以便每个代理程序都管理相似数量的计算机。

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。在添加或删除计算机或代理程序后，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。当从管理服务器中删除代理程序时，已指派给该代理程序的计算机会在剩余代理程序之中重新分配。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。仅在从 Cyber Protect 中控台中删除此类代理程序后，才会开始重新分配。

检查哪个代理程序管理特定计算机

1. 在 Cyber Protect 中控台中，单击**设备**，然后选择 **Scale Computing**。
2. 单击表格右上角的齿轮图标，然后在**系统**下，选中**代理程序**复选框。
3. 在出现的列中检查代理程序的名称。

部署 QCOW2 模板

1. 登录到您的 Cyber Protection 帐户。
2. 依次单击**设备** > **所有设备** > **添加** > **Scale Computing HC3**。
   Zip 存档下载到您的计算机。
3. 解压缩 .zip 存档，然后将 .qcow2 文件和 .xml 文件保存到名为 **ScaleAppliance** 的文件夹中。
4. 将 **ScaleAppliance** 文件夹上传到网络共享，然后确保 Scale Computing HC3 簇可以访问它。
5. 以指派有 **VM 创建/编辑**角色的管理员身份登录到 Scale Computing HC3 簇。有关操作 Scale Computing HC3 虚拟机所需角色的详细信息，请参阅 "Scale Computing HC3 的代理程序 – 所需角色"(第 127 页)。
6. 在 Scale Computing HC3 Web 界面中，导入 **ScaleAppliance** 文件夹中的虚拟机模板。
   a. 单击**导入 HC3 VM** 图标。
   b. 在**导入 HC3 VM** 窗口中，指定以下内容：
      - 新虚拟机的名称。
      - **ScaleAppliance** 文件夹所在的网络共享。
      - 访问此网络共享所需的用户名和密码。
      - [可选] 新虚拟机的域标签。
      - 指向网络共享上 **ScaleAppliance** 文件夹的路径。
   c. 单击**导入**。

在部署完成后，必须配置虚拟设备。有关如何配置虚拟设备的详细信息，请参阅 "配置虚拟设备"(第 125 页)。

注意
如果您的簇需要多个虚拟设备，请重复上述步骤并部署其他虚拟设备。请勿使用 Scale Computing HC3 Web 界面中的**克隆 VM** 选项，来克隆现有虚拟设备。

配置虚拟设备

在部署虚拟设备后，需要对其进行配置，以便它可以访问将要保护的 Scale Computing HC3 簇和 Cyber Protection 服务。

若要配置虚拟设备

1. 登录到您的 Scale Computing HC3 帐户。
2. 选择要配置的虚拟设备，然后单击**中控台**图标。
3. 在 **eth0** 字段中，配置设备的网络接口。
   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。根据设备所使用的网络数量，可能要配置一个或多个接口。
4. 在 **Scale Computing** 字段中，单击**更改**以指定 Scale Computing HC3 簇地址和用于访问它的凭据。
   a. 在**服务器名称/IP** 字段中，输入簇的 DNS 名称或 IP 地址。
   b. 在**用户名**和**密码**字段中，输入 Scale Computing HC3 管理员帐户的凭据。
      确保该帐户有操作 Scale Computing HC3 虚拟机所需的角色。有关这些角色的详细信息，请参阅 "Scale Computing HC3 的代理程序 – 所需角色"(第 127 页)。
   c. 单击**检查连接**，以验证设置是否正确无误。
   d. 单击**确定**。
5. 使用以下方法之一在 Cyber Protection 服务中注册设备。
   - [仅适用于没有双重身份验证的租户]在其图形界面中注册设备。
     a. 在**代理程序选项**下的**管理服务器**字段中，单击**更改**。
     b. 在**服务器名称/IP** 字段中，选择**云**。
        Cyber Protection 服务地址即会显示。除外另有说明，否则请勿更改此地址。
     c. 在**用户名**和**密码**字段中，指定 Cyber Protection 服务中您帐户的凭据。虚拟设备和该设备管理的虚拟机都注册在此帐户下。
     d. 单击**确定**。
   - 在命令行界面中注册设备。

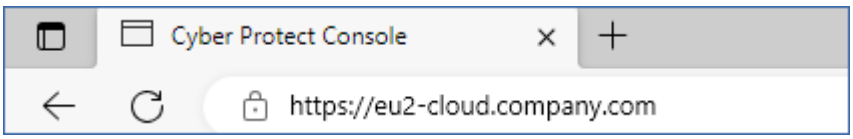
     注意
     使用此方法时，需要一个注册令牌。有关如何生成注册令牌的详细信息，请参阅 "生成注册标记"(第 106 页)。

     a. 按 CTRL+SHIFT+F2 组合键以打开命令行界面。
     b. 运行以下命令：

```
register_agent -o register -t cloud -a <service address> --token <registration
token>
```

注意

使用注册标记时，必须指定准确的数据中心地址。这是您**登录**到 Cyber Protect 中控台后所看到的 URL。例如，`https://eu2-cloud.company.com`。



请勿在此处使用 `https://cloud.company.com`。

c. 要返回设备的图形界面，请按 ALT+F1 组合键。

6. [可选] 在**名称**字段中，单击**更改**以编辑虚拟设备的默认名称，即 **localhost**。此名称会显示在 Cyber Protect 中控台中。
7. [可选] 在**时间**字段中，单击**更改**，然后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。
8. [如果在网络中启用了代理服务器] 配置代理服务器。
   a. 按 CTRL+SHIFT+F2 组合键以打开命令行界面。
   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 `ADDRESS` 替换为新代理服务器主机名称/IP 地址，将 `PORT` 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 `LOGIN` 和 `PASSWORD` 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。

注意

为了能够更新部署在代理后面的虚拟设备，请编辑设备文件 config.yaml (/opt/acronis/etc/va-updater/config.yaml)，方法是在该文件的底部添加以下行，然后输入特定于您环境的值：

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

例如：

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

保护 Scale Computing HC3 簇中的虚拟机

1. 登录到您的 Cyber Protection 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. 选择计算机并为其应用保护计划。

Scale Computing HC3 的代理程序 – 所需角色

本部分介绍操作 Scale Computing HC3 虚拟机所需的角色。

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

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

在启动前

此设备是在 Virtuozzo Hybrid Infrastructure中部署的预配置的虚拟机。它包含的保护代理程序让您可以管理 Virtuozzo Hybrid Infrastructure群集中所有虚拟机的网络安全保护。

注意
为了确保已启用**适用于虚拟机的卷影复制服务 (VSS)** 备份选项的备份正常运行并以应用程序一致状态捕获数据，请验证受保护的虚拟机上是否已安装 Virtuozzo 来宾工具并且其是最新版本。

代理程序的系统要求

部署虚拟设备时，可以在 vCPU 和 RAM(规格) 的不同预定义组合之间进行选择。还可以创建自己的规格。

2 个 vCPU 和 4 GB RAM(中级规格) 是最佳配置，足以应对大多数操作。为了提高备份性能并避免出现与 RAM 内存不足有关的故障，建议您在要求更高的情况下将这些资源增加到 4 个 vCPU 和 8 GB RAM。例如，当预计备份流量会超过 100 MB/秒时(例如，在万兆网络中) ，或如果同时备份多个具有大型硬盘驱动器(500 GB 或更多) 的虚拟机，请增加指派的资源。

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。

如果在簇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，以便每个代理程序都管理相似数量的计算机。

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。在添加或删除计算机或代理程序后，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。当从管理服务器中删除代理程序时，已指派给该代理程序的计算机会在剩余代理程序之中重新分配。如果代理程序损坏或从 Virtuozzo Hybrid Infrastructure节点中手动删除代理程序，则不会发生此情况。仅当从 Cyber Protection Web 界面删除此类代理程序时，才会开始重新分配。

检查哪个代理程序管理特定计算机

1. 在 Cyber Protect 中控台中，单击**设备**，然后选择 **Virtuozzo Hybrid Infrastructure**。
2. 单击表格右上角的齿轮图标，然后在**系统**下，选中**代理程序**复选框。
3. 在出现的列中检查代理程序的名称。

限制

- Virtuozzo Hybrid Infrastructure设备无法远程部署。
- 不支持虚拟机的应用程序感知备份。

配置 Virtuozzo Hybrid Infrastructure中的网络

在部署和配置虚拟设备之前，需要配置 Virtuozzo Hybrid Infrastructure中的网络。

适用于 Virtuozzo Hybrid Infrastructure的代理程序(虚拟设备)的网络要求

- 虚拟设备需要 2 个网络适配器。
- 必须将虚拟设备连接到具有以下网络流量类型的 Virtuozzo 网络：
  - 计算 API
  - VM 备份
  - ABGW 公共
  - VM 公共

有关配置网络的详细信息，请参阅 Virtuozzo 文档中的计算簇要求。

配置 Virtuozzo Hybrid Infrastructure中的用户帐户

要配置虚拟设备，需要一个 Virtuozzo Hybrid Infrastructure 用户帐户。

可以使用以下账号类型之一：

- 系统管理员(在**默认**域或其他域中)
  请确保您已授予此帐户访问选定域中所有项目的权限。由此，虚拟设备将能够备份和恢复选定域的所有子项目中的所有虚拟机。
- 项目管理员
  使用此帐户，虚拟设备将只能备份和恢复创建帐户的项目中的虚拟机。虚拟设备将无法访问域中其他项目的任何信息。

> **注意**
> 若要保护多个项目，则必须为每个项目部署单独的虚拟设备。
> 每个虚拟设备必须使用在相应项目中创建的单独项目管理员帐户。虚拟设备可在 Virtuozzo Hybrid Infrastructure 集群中的任何位置部署，甚至在受保护项目之外。
> 您只能在 Virtuozzo Hybrid Infrastructure 6.2 及更高版本中使用项目管理员帐户。

有关域和项目的更多信息，请参阅 Virtuozzo Hybrid Infrastructure 文档中的 多租户。

使用系统管理员帐户

使用系统管理员帐户，虚拟设备可以备份和恢复 Virtuozzo Hybrid Infrastructure 域中的所有虚拟机。

有关域和项目的更多信息，请参阅 Virtuozzo Hybrid Infrastructure 文档中的 多租户。

先决条件

- 您必须能够使用 OpenStack 命令行接口连接到 Virtuozzo Hybrid Infrastructure 集群。有关详细信息，请参阅 Virtuozzo Hybrid Infrastructure 文档中的 连接到 OpenStack 命令行接口。

若要使用系统管理员帐户

1. 使用 OpenStack 命令行接口连接到 Virtuozzo Hybrid Infrastructure 集群，然后运行以下脚本为系统管理员创建环境文件。

```
su - vstoradmin
kolla-ansible post-deploy
exit
```

2. 使用环境文件来授权其他 OpenStack 命令。

```
. /etc/kolla/admin-openrc.sh
```

3. 在**默认**域中创建管理员帐户。

```
openstack --insecure user set --project admin --project-domain Default --domain
Default <user name>
```

在此及以下，<user name> 是 Virtuozzo Hybrid Infrastructure 帐户。虚拟设备将使用此帐户，以便备份和恢复 **Default** 域中任何子项目中的虚拟机。

4. 将compute角色指派给帐户。

```
openstack --insecure role add --domain Default --user <user name> --user-domain
Default compute --inherited
```

5. [可选] 允许帐户访问 Virtuozzo Hybrid Infrastructure 中的其他域。

```
openstack --insecure role add --domain <domain name> --inherited --user <user name> -
-user-domain Default admin
```

此处的 <domain name> 是此帐户将要访问的域。若域名中包含空格，请将其名字括在引号中。

对于每个要访问的附加域，请重复此步骤。

6. 勾选已指派给帐户的角色。

```
openstack --insecure role assignment list --user <user name> --names
```

7. [可选] 检查帐户的有效角色。

有效角色包括指派角色、继承角色和隐含角色。

```
openstack --insecure role assignment list --user <user name> --names --effective
```

示例

授予对默认域的访问权限

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
```

```
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
```

授予对默认和其他域的访问权限

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
openstack --insecure role add --domain "New Domain"  --user johndoe --user-domain
Default admin --inherited
```

检查已指派的角色

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c
Project -c Domain
```

```
+--------------+-----------------+---------+-------------+
| Role         | User            | Project | Domain      |
+--------------+-----------------+---------+-------------+
| admin        | johndoe@Default |         | New Domain  |
| compute      | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
+--------------+-----------------+---------+-------------+
```

在此示例中，选项 `-c Role`、`-c User`、`-c Project` 和 `-c Domain` 用于缩短命令输出以适配页面。

检查生效的角色

```
openstack --insecure role assignment list --user johndoe --names --effective  -c Role -c
User -c Project -c Domain
```

```
+--------------+-----------------+-----------------+---------+
| Role         | User            | Project         | Domain  |
+--------------+-----------------+-----------------+---------+
| domain_admin | johndoe@Default |                 | Default |
| compute      | johndoe@Default | admin@Default   |         |
| compute      | johndoe@Default | service@Default |         |
| domain_admin | johndoe@Default | admin@Default   |         |
| domain_admin | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | service@Default |         |
| member       | johndoe@Default | service@Default |         |
| reader       | johndoe@Default | service@Default |         |
```

```
| project_user | johndoe@Default | admin@Default   |         |
| member       | johndoe@Default | admin@Default   |         |
| reader       | johndoe@Default | admin@Default   |         |
| project_user | johndoe@Default |                 | Default |
| member       | johndoe@Default |                 | Default |
| reader       | johndoe@Default |                 | Default |
+--------------+-----------------+-----------------+---------+
```

在此示例中，选项 `-c Role`、`-c User`、`-c Project` 和 `-c Domain` 用于缩短命令输出以适配页面。

使用项目管理员帐户

使用此帐户，虚拟设备将只能备份和恢复创建帐户的项目中的虚拟机。虚拟设备将无法访问域中其他项目的任何信息。

注意
若要保护多个项目，则必须为每个项目部署单独的虚拟设备。

每个虚拟设备必须使用在相应项目中创建的单独项目管理员帐户。虚拟设备可在 Virtuozzo Hybrid Infrastructure 集群中的任何位置部署，甚至在受保护项目之外。

您只能在 Virtuozzo Hybrid Infrastructure 6.2 及更高版本中使用项目管理员帐户。

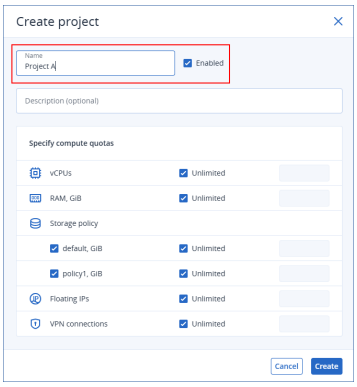
有关域和项目的更多信息，请参阅 Virtuozzo Hybrid Infrastructure 文档中的 多租户。

先决条件

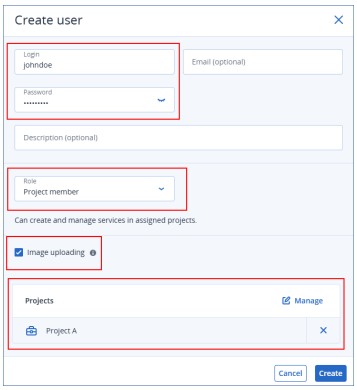
- 您必须能够使用 OpenStack 命令行接口连接到 Virtuozzo Hybrid Infrastructure 集群。有关详细信息，请参阅 Virtuozzo Hybrid Infrastructure 文档中的 连接到 OpenStack 命令行接口。

使用项目管理员帐户

1. 在 Virtuozzo Hybrid Infrastructure 的管理面板中，转到**设置** > **项目和用户**。
2. 选择一个域并在其中创建一个项目。



3. 在同一域中创建用户帐户。将**项目成员**角色指派给此帐户，选择**镜像上传**复选框，然后将用户指派到您创建的项目。



注意

在命令行接口中，**项目成员**角色称为 **project_admin**。

```
+---------------+------------------+-------+--------------------+--------+--------+-----------+
| Role          | User             | Group | Project            | Domain | System | Inherited |
+---------------+------------------+-------+--------------------+--------+--------+-----------+
| project_admin | johndoe@Domain A |       | Project A@Domain A |        |        | False     |
| image_upload  | johndoe@Domain A |       | Project A@Domain A |        |        | False     |
+---------------+------------------+-------+--------------------+--------+--------+-----------+
```

4. 使用 OpenStack 命令行接口连接到 Virtuozzo Hybrid Infrastructure 集群。
   a. 运行以下脚本以创建环境文件。

   ```
   su - vstoradmin
   kolla-ansible post-deploy
   exit
   ```

   b. 使用环境文件来授权其他 OpenStack 命令。

   ```
   . /etc/kolla/admin-openrc.sh
   ```

   c. 将compute角色指派给您在管理面板中创建的用户帐户。

   ```
   openstack --insecure role add --project <project name> --user <user name> --
   project-domain <project domain name> --user-domain <user domain name> compute
   ```

   在此及以下，<project name> 是项目名称，<user name> 是 Virtuozzo Hybrid Infrastructure 帐户，<project domain name> 是项目的父域，<user domain name> 是用户帐户的父域。
   若名称中包含空格，请将其括在引号中。

   d. 将 quota_manager 角色指派给新用户。

   ```
   openstack --insecure role add --project <project name> --user <user name> --
   project-domain <project domain name> --user-domain <user domain name> quota_
   manager
   ```

   e. 勾选已指派给帐户的角色。

   ```
   openstack --insecure role assignment list --names --user <user name> --user-domain
   <user domain name>
   ```

f. [可选] 检查帐户的有效角色。

有效角色包括指派角色、继承角色和隐含角色。

```
openstack --insecure role assignment list --names --effective  --user <user
name> --user-domain <user domain name>
```

示例

在以下示例中，用户帐户为 johndoe，项目为 Project A。用户帐户和项目均在 Domain A中创建。

指派角色

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure role add --project "Project A" --user johndoe --project-domain
"Domain A" --user-domain "Domain A" compute
openstack --insecure role add --project "Project A" --user johndoe --project-domain
"Domain A" --user-domain "Domain A" quota_manager
```

检查已指派的角色

```
openstack --insecure role assignment list --names --user johndoe --user-domain "Domain
A" -c Role -c User -c Project -c Domain
```

```
+--------------+------------------+-------------------+-------------+
| Role         | User             | Project           | Domain      |
+--------------+------------------+-------------------+-------------+
| compute      | johndoe@Domain A | Project A@Domain A|             |
| project_admin| johndoe@Domain A | Project A@Domain A|             |
| image-upload | johndoe@Domain A | Project A@Domain A|             |
| quota_manager| johndoe@Domain A | Project A@Domain A|             |
+--------------+------------------+-------------------+-------------+
```

在此示例中，选项 -c Role、-c User、-c Project 和 -c Domain 用于缩短命令输出以适配页面。

检查生效的角色

```
openstack --insecure role assignment list --names --effective  --user johndoe --user-
domain "Domain A"  -c Role -c User -c Project -c Domain
```

```
+--------------+-----------------+---------------------+---------+
| Role         | User            | Project             | Domain  |
+--------------+-----------------+---------------------+---------+
| compute      | johndoe@Domain A | Project A@Domain A |         |
| project_admin| johndoe@Domain A | Project A@Domain A |         |
| image_upload | johndoe@Domain A | Project A@Domain A |         |
| quota_manager| johndoe@Domain A | Project A@Domain A |         |
```

```
| project_user | johndoe@Domain A | Project A@Domain A |         |
| member       | johndoe@Domain A | Project A@Domain A |         |
| reader       | johndoe@Domain A | Project A@Domain A |         |
+--------------+------------------+--------------------+---------+
```

在此示例中，选项 `-c Role`、`-c User`、`-c Project` 和 `-c Domain` 用于缩短命令输出以适配页面。

部署 QCOW2 模板

1. 登录到您的 Cyber Protection 帐户。
2. 依次单击**设备** > **所有设备** > **添加** > **Virtuozzo Hybrid Infrastructure**。
   Zip 存档下载到您的计算机。
3. 解压缩 .zip 存档。它包含 .qcow2 映像文件。
4. 登录到您的 Virtuozzo Hybrid Infrastructure帐户。
5. 将 .qcow2 映像文件添加到 Virtuozzo Hybrid Infrastructure计算群集，如下所示：
   - 在**计算** > **虚拟机** > **映像**选项卡上，单击**添加映像**。
   - 在**添加映像**窗口中，单击**浏览**，然后选择 .qcow2 文件。
   - 指定映像名称、选择**一般 Linux 操作系统**类型，然后单击**添加**。
6. 在**计算** > **虚拟机** > **虚拟机**选项卡中，单击**创建虚拟机**。将打开一个窗口，需要在其中指定以下参数：
   - 新虚拟机的名称。
   - 在**从以下位置部署**中，选择**映像**。
   - 在**映像**窗口中，选择设备的 .qcow2 映像文件，然后单击**完成**。
   - 在**卷**窗口中，不需要添加任何卷。自动为系统磁盘添加的卷已足够。
   - 在**规格**窗口中，选择所需的 vCPU 和 RAM 组合，然后单击**完成**。通常，2 个 vCPU 和 4 GiB RAM 足够使用。
   - 在**网络接口**窗口中，单击**添加**、选择类型为*公用*的虚拟网络，然后单击**添加**。它将显示在**网络接口**列表中。
     如果使用具有多个物理网络的设置(因此具有多个类型为“公用”的虚拟网络)，请重复此步骤并选择所需的虚拟网络。
7. 单击**完成**。
8. 返回**创建虚拟机**窗口，单击**部署**以创建并启动虚拟机。

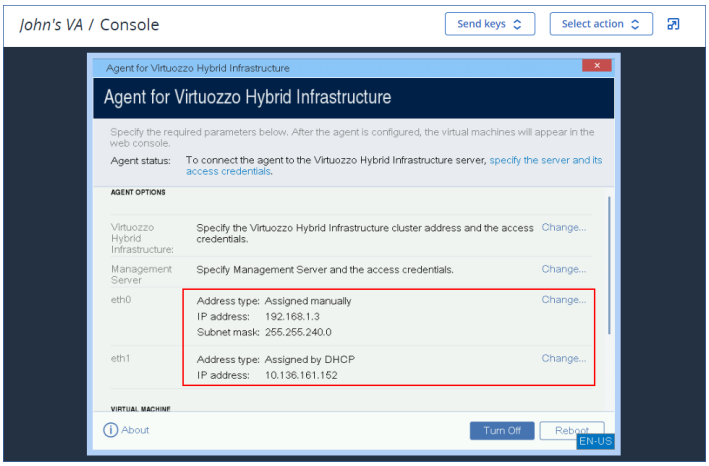
配置虚拟设备

部署适用于 Virtuozzo Hybrid Infrastructure (虚拟设备) 的代理程序后，您必须配置虚拟设备，以便访问 Virtuozzo Hybrid Infrastructure 集群和 Cyber Protection 云服务。

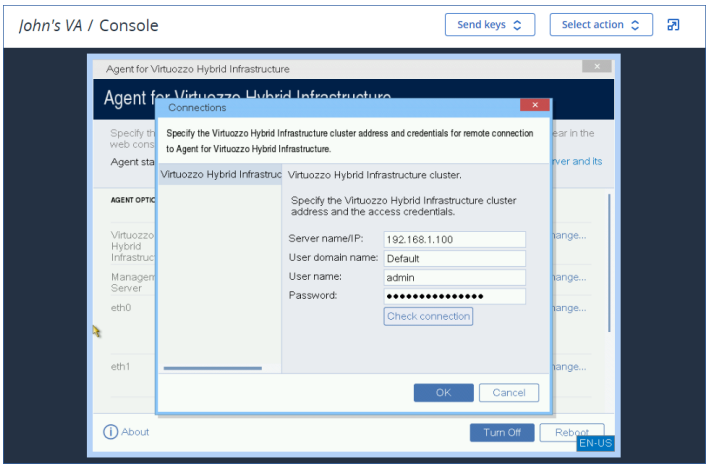
若要配置虚拟设备

1. 登录 Virtuozzo Hybrid Infrastructure 自助服务面板。
2. 转到 **计算** > **虚拟机**，然后在水平菜单中选择 **虚拟机** 选项卡。
3. 单击所创建虚拟机旁的省略号图标 (...)，然后单击 **中控台**。

4. 配置设备的网络接口。可能需要配置一个或多个接口要进行配置，具体取决于设备所使用的虚拟网络数量。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。



5. 指定 Virtuozzo 集群地址和凭据。
   - Virtuozzo Hybrid Infrastructure 集群的 DNS 名称或 IP 地址 - 这是群集的管理节点地址。将自动设置默认端口 5000。如果使用其他端口，则必须手动指定端口。
   - 在**用户名**和**密码**字段中，输入 Virtuozzo Hybrid Infrastructure 用户帐户的凭据。这可以是系统管理员帐户或项目管理员帐户。有关用户、角色和域的详细信息，请参阅配置 Virtuozzo Hybrid Infrastructure 中的用户帐户。
   - 在**用户域名**字段中，指定用户账户的父域。例如，**默认**。域名区分大小写。



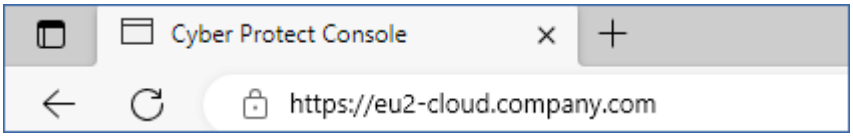
6. 使用以下方法之一在 Cyber Protection 服务中注册设备。
   - [仅适用于没有双重身份验证的租户] 在其图形界面中注册设备。
     a. 在**代理程序选项**下的**管理服务器**字段中，单击**更改**。
     b. 在**服务器名称/IP** 字段中，选择**云**。
        Cyber Protection 服务地址即会显示。除外另有说明，否则请勿更改此地址。
     c. 在**用户名**和**密码**字段中，指定 Cyber Protection 服务中您帐户的凭据。虚拟设备和该设备管理的虚拟机都注册在此帐户下。
     d. 单击**确定**。
   - 在命令行界面中注册设备。

注意
使用此方法时，需要一个注册令牌。有关如何生成注册令牌的详细信息，请参阅 "生成注册标记"(第 106 页)。

a. 按 CTRL+SHIFT+F2 组合键以打开命令行界面。
b. 运行以下命令：

```
register_agent -o register -t cloud -a <service address> --token <registration
token>
```

注意
使用注册标记时，必须指定准确的数据中心地址。这是您**登录**到 Cyber Protect 中控台后所看到的 URL。例如，`https://eu2-cloud.company.com`。



请勿在此处使用 `https://cloud.company.com`。

c. 要返回设备的图形界面，请按 ALT+F1 组合键。

7. [如果在网络中启用了代理服务器] 配置代理服务器。
   a. 按 CTRL+SHIFT+F2 组合键以打开命令行界面。
   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 `ADDRESS` 替换为新代理服务器主机名称/IP 地址，将 `PORT` 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 `LOGIN` 和 `PASSWORD` 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。

注意

为了能够更新部署在代理后面的虚拟设备，请编辑设备文件 config.yaml (/opt/acronis/etc/va-updater/config.yaml)，方法是在该文件的底部添加以下行，然后输入特定于您环境的值：

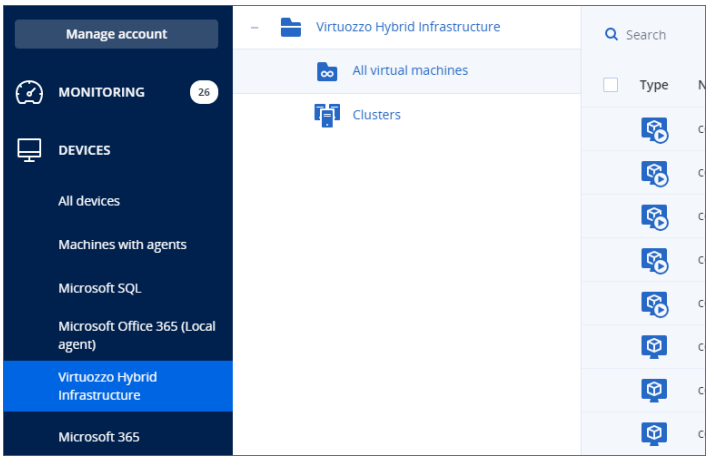
```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

例如：

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

保护 Virtuozzo Hybrid Infrastructure群集中的虚拟机

1. 登录到 Cyber Protection 中控台。
2. 转到到**设备** > **Virtuozo Hybrid Infrastructure** > <您的集群> > **默认项目** > **管理**，或者在**设备** > **所有设备**中找到您的计算机。
3. 选择计算机并为其应用保护计划。



正在部署适用于 oVirt 的代理程序(虚拟设备)

在启动前

此设备是您在 Red Hat Virtualization/oVirt 数据中心中部署的预配置虚拟机。该设备包含的保护代理程序让您可以管理数据中心中所有虚拟机的网络安全保护。

代理程序的系统要求

默认情况下，带有代理程序的虚拟机使用 2 个 vCPU 和 4 GB RAM。这些设置对大多数操作而言已够用，但可以在 Red Hat Virtualization/oVirt 管理门户中编辑这些设置。

为了提高备份性能并避免出现与 RAM 内存不足有关的故障，建议您在要求更高的情况下将这些资源增加到 4 个 vCPU 和 8 GB RAM。例如，当预计备份流量会超过 100 MB/秒时（例如，在万兆网络中），或如果同时备份多个具有大型硬盘驱动器（500 GB 或更多）的虚拟机，请增加指派的资源。

设备虚拟磁盘的大小是 8 GB。

我需要多少个代理程序？

一个代理程序可以保护整个数据中心。如果需要分配备份流量带宽负载，可以在数据中心中放置多个代理程序。

如果在数据中心中放置多个代理程序，则虚拟机将自动在各代理程序之间分配，以便每个代理程序都管理相似数量的计算机。

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。在添加或删除计算机或代理程序后，可能会发生此情况。例如，您意识到需要更多代理程序来帮助提高吞吐量，以及将额外的虚拟设备部署到数据中心。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。当删除代理程序时，已指派给该代理程序的计算机会在剩余代理程序之中重新分配。如果代理程序损坏或从 Red Hat Virtualization/oVirt 管理门户中手动删除代理程序，则不会发生此情况。仅在从 Cyber Protect 中控台中删除此类代理程序后，才会开始重新分配。

检查哪个代理程序管理特定计算机

1. 在 Cyber Protect 中控台中，单击**设备**，然后选择 **oVirt**。
2. 单击表格右上角的齿轮图标，然后在**系统**下，选中**代理程序**复选框。
3. 在出现的列中检查代理程序的名称。

限制

Red Hat Virtualization/oVirt 虚拟机不支持以下操作：

- 应用程序感知备份
- 从备份运行虚拟机
- 虚拟机的复制
- 块更改跟踪

部署 OVA 模板

1. 登录到您的 Cyber Protection 帐户。
2. 依次单击**设备** > **所有设备** > **添加** > **Red Hat Virtualization (oVirt)**。
   Zip 存档下载到您的计算机。
3. 解压缩 .zip 存档。它包含一个 .ova 文件。
4. 将 .ova 文件上传到 Red Hat Virtualization/oVirt 数据中心中要保护的主机。
5. 以管理员身份登录到 Red Hat Virtualization/oVirt 管理门户。有关操作虚拟机所需角色的详细信息，请参阅 "适用于 oVirt 的代理程序 - 所需角色和端口"（第 143 页）。
6. 在导航菜单中，选择**计算** > **虚拟机**。
7. 单击主表上方的垂直省略号图标  ，然后单击**导入**。

8. 在**导入虚拟机**窗口中，请执行以下操作：
   a. 在**数据中心**中，选择要保护的数据中心。
   b. 在**来源**中，选择**虚拟设备(OVA)**。
   c. 在**主机**中，选择其上已上传 .ova 文件的主机。
   d. 在**文件路径**中，指定指向包含 .ova 文件的目录的路径。
   e. 单击**载入**。
      .ova 文件中的 oVirt 虚拟设备模板会显示在**来源上的虚拟机**面板中。
      如果该模板没有出现在此面板中，请确保已指定指向文件的正确路径、文件未损坏，并且可以访问主机。
   f. 在**来源上的虚拟机**中，选择 oVirt 虚拟设备模板，然后单击向右箭头。
      该模板会出现在**要导入的虚拟机**面板中。
   g. 单击**下一步**。
9. 在新窗口中，单击设备名称，然后配置以下设置：
   - 在**网络接口**选项卡上，配置网络接口。
   - [可选] 在**常规**选项卡上，更改带有代理程序的虚拟机的默认名称。

部署现已完成。接下来，需要配置虚拟设备。有关如何配置虚拟设备的详细信息，请参阅 "配置虚拟设备"(第 140 页)。

注意
如果您的数据中心需要多个虚拟设备，请重复上述步骤并部署其他虚拟设备。请勿使用 Red Hat Virtualization/oVirt 管理门户中的**克隆 VM** 选项，来克隆现有虚拟设备。

要将虚拟设备从动态组备份中排除，还必须将其从 Cyber Protect 中控台中的虚拟机列表中排除。要排除它，请在 Red Hat Virtualization/oVirt 管理门户中，选择带有代理程序的虚拟机，然后为其指派标签 `acronis_virtual_appliance`。

配置虚拟设备

在部署虚拟设备后，需要对其进行配置，以便它可以访问 oVirt 引擎和 Cyber Protection 服务。

若要配置虚拟设备

1. 登录到 Red Hat Virtualization/oVirt 管理门户。
2. 选择要配置的虚拟设备，然后单击**中控台**图标。
3. 在 **eth0** 字段中，配置设备的网络接口。
   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。根据设备所使用的网络数量，可能要配置一个或多个接口。
4. 在 **oVirt** 字段中，单击**更改**以指定 oVirt 引擎地址和用于访问它的凭据：
   a. 在**服务器名称/IP** 字段中，输入引擎的 DNS 名称或 IP 地址。
   b. 在**用户名**和**密码**字段中，输入该引擎的管理员凭据。
      确保此管理员帐户有操作 Red Hat Virtualization/oVirt 虚拟机所需的角色。有关这些角色的详细信息，请参阅 "适用于 oVirt 的代理程序 - 所需角色和端口"(第 143 页)。

如果 Keycloak 是 oVirt 引擎的单点登录 (SSO) 提供程序(oVirt 4.5.1 中的默认提供程序) , 则在指定用户名时使用 Keycloak 格式。例如, 将默认管理员帐户指定为 `admin@ovirt@internalsso` 而不是 `admin@internal`。

c. [可选] 单击**检查连接**, 以确保提供的凭据正确无误。

d. 单击**确定**。

5. 使用以下方法之一在 Cyber Protection 服务中注册设备。

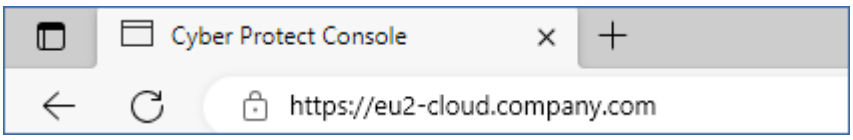
- [仅适用于没有双重身份验证的租户] 在其图形界面中注册设备。
  a. 在**代理程序选项**下的**管理服务器**字段中, 单击**更改**。
  b. 在**服务器名称/IP** 字段中, 选择**云**。
     Cyber Protection 服务地址即会显示。除外另有说明, 否则请勿更改此地址。
  c. 在**用户名**和**密码**字段中, 指定 Cyber Protection 服务中您帐户的凭据。虚拟设备和该设备管理的虚拟机都注册在此帐户下。
  d. 单击**确定**。
- 在命令行界面中注册设备。

  注意
  使用此方法时, 需要一个注册令牌。有关如何生成注册令牌的详细信息, 请参阅 "生成注册标记"(第 106 页)。

  a. 按 CTRL+SHIFT+F2 组合键以打开命令行界面。
  b. 运行以下命令:

  ```
  register_agent -o register -t cloud -a <service address> --token <registration token>
  ```

  注意
  使用注册标记时, 必须指定准确的数据中心地址。这是您**登录**到 Cyber Protect 中控台后所看到的 URL。例如, `https://eu2-cloud.company.com`。

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

  c. 要返回设备的图形界面, 请按 ALT+F1 组合键。

6. [可选] 在**名称**字段中, 单击**更改**以编辑虚拟设备的默认名称, 即 **localhost**。此名称会显示在 Cyber Protect 中控台中。
7. [可选] 在**时间**字段中, 单击**更改**, 然后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。
8. [可选] [如果在网络中启用了代理服务器] 配置代理服务器。
   a. 按 CTRL+SHIFT+F2 组合键以打开命令行界面。
   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 `ADDRESS` 替换为新代理服务器主机名称/IP 地址，将 `PORT` 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 `LOGIN` 和 `PASSWORD` 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。

注意

为了能够更新部署在代理后面的虚拟设备，请编辑设备文件 `config.yaml` (`/opt/acronis/etc/va-updater/config.yaml`)，方法是在该文件的底部添加以下行，然后输入特定于您环境的值：

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

例如：

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

在 Red Hat Virtualization/oVirt 数据中心中保护虚拟机

1. 登录到您的 Cyber Protection 帐户。
2. 导航到**设备** > **oVirt** > <您的簇>，或者在**设备** > **所有设备**中查找您的计算机。
3. 选择计算机并为其应用保护计划。

适用于 oVirt 的代理程序 - 所需角色和端口

所需角色

为了进行部署和操作，适用于 oVirt 的代理程序需要已指派有以下角色的管理员帐户。

oVirt/Red Hat Virtualization 4.2 和 4.3/Oracle Virtualization Manager 4.3

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4、4.5

- SuperUser

所需端口

适用于 oVirt 的代理程序通过使用在配置虚拟设备时指定的 URL，来连接到 oVirt 引擎。通常，引擎 URL 的格式如下所示：`https://ovirt.company.com`。在这种情况下，将使用 HTTPS 协议和端口 443。

非默认的 oVirt 设置可能需要另一个端口。可以通过分析 URL 格式找到确切的端口。例如：

oVirt 引擎 URL	端口	协议
`https://ovirt.company.com/`	443	HTTPS
`http://ovirt.company.com/`	80	HTTP
`https://ovirt.company.com:1234/`	1234	HTTPS

磁盘读/写操作不需要其他端口，因为备份是在 HotAdd 模式下执行的。

部署 Agent for Azure

可以通过设置 Agent for Azure，一个可透明访问 Microsoft Azure 虚拟机数据的单个代理程序，来执行 Microsoft Azure 虚拟机的无代理程序备份。

Agent for Azure 可确保：

- Microsoft Azure 虚拟机（运行 Windows 或 Linux）的备份和还原功能。
- 已减少 Microsoft Azure 虚拟机开销，只需一个代理程序进行管理。
- 可通过 Cyber Protect 中控台进行配置，将任何本地或云计算机备份透明迁移到 Microsoft Azure 虚拟机。
- 已减少 Microsoft Azure 资源成本，虚拟机内只需一个代理程序的 CPU 和 RAM 开销。

在启动前

代理程序的系统要求

默认情况下，为虚拟设备分配 **Standard_B2s** 大小（4 GiB RAM 和 2 个 CPU），这是大多数操作的最佳大小。有关此类属性和其他 Azure 虚拟机属性的详细信息，请参阅 Microsoft Azure 文档。

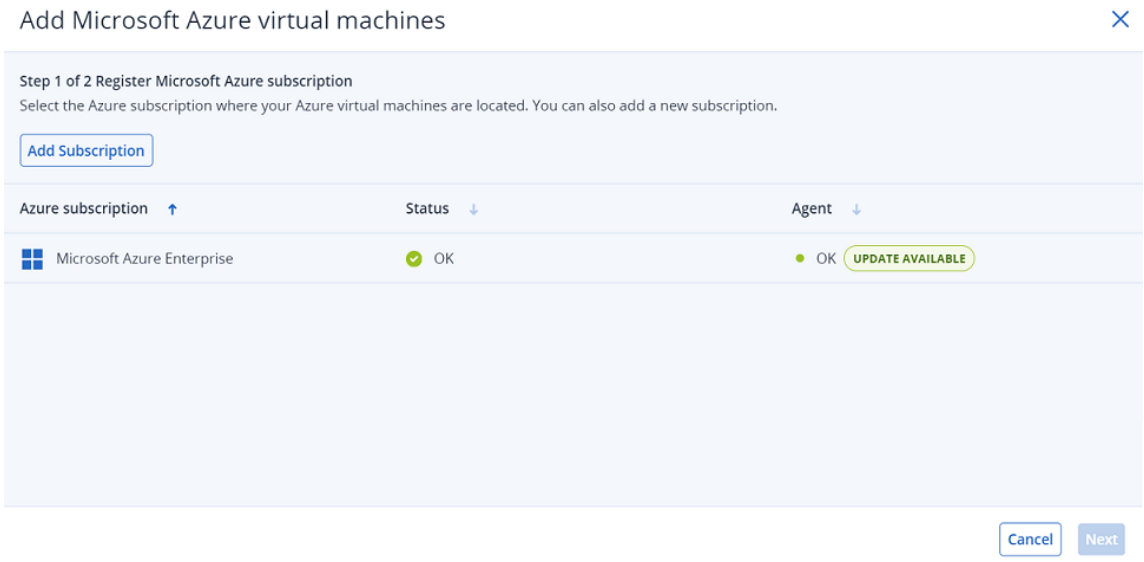
部署 Agent for Azure 虚拟设备

首先，通过连接到相关的 Microsoft Azure 订购许可，然后定义 Azure 部署设置，来部署 Agent for Azure 虚拟设备。

注意
在通过**设备**或**备份存储**菜单创建备份位置时，可以配置与 Microsoft Azure 订购许可的连接，如 "在 Microsoft Azure 中定义备份位置"（第 481 页）中所述。

若要部署 Agent for Azure 虚拟设备

1. 在 Cyber Protect 中控台中，转到**设备** > **所有计算机**。
2. 单击**添加**。
3. 在**云工作负载**部分，选择 **Microsoft Azure 虚拟机**。
   - 如果已使用现有的 Microsoft Azure 订购许可，则会显示“添加 Microsoft Azure 虚拟机”向导，其中列出了您现有的订购许可。可以选择相关的订购许可，然后单击**下一步**。然后，继续执行步骤 8。



   - 如果已使用现有的 Microsoft Azure 订购许可，但想要添加新的订购许可，请单击**添加订购许可**。
   - 若无现有订购许可，请单击**添加**以添加订购许可。
4. 在显示的对话框中，单击**登录**。系统即会将您重定向到 Microsoft 登录页面。

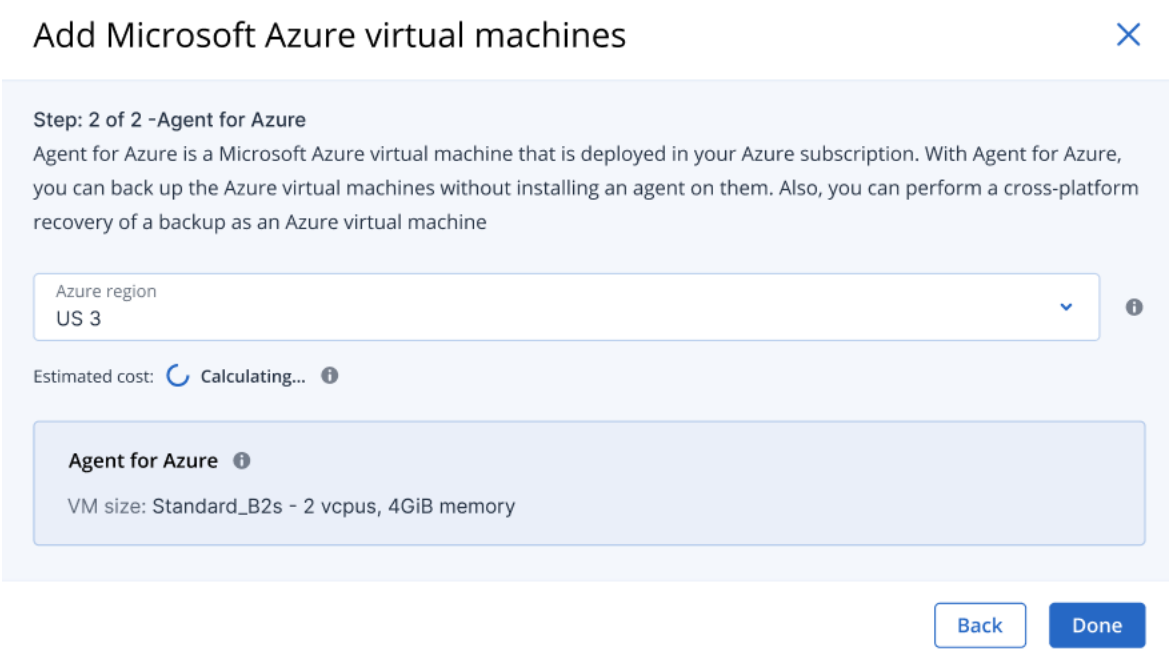
注意

必须在 Microsoft Entra ID 中为您指派以下角色之一，才能完成与订购许可的连接：云应用程序管理员、应用程序管理员或全局管理员。还必须为您指派每个选定订购许可的“所有者”角色。

5. 请输入 Microsoft 登录凭据并接受请求的权限。连接过程将启动，可能需要几分钟的时间。

   有关安全访问 Microsoft Azure 订购许可的详细信息，请参阅文章 Microsoft Azure 连接安全和审核 (72684)。
6. 完成连接后：
   - 若有多个订购许可，请从显示的对话框的下拉列表中选择相关的订购许可，然后单击**添加订购许可**。然后，您将被重定向到主向导屏幕。
   - 若要添加第一个订购许可，系统会将您重定向至主向导屏幕。
7. 选择相关订购许可，然后单击**下一步**。
8. 从**Azure 区域**下拉列表中，选择订购许可的相关区域。为了优化备份性能，您应选择大多数要受保护的虚拟机所部署的 Azure 区域。

   将计算并显示该区域的预估成本。这些成本将计入您的 Microsoft Azure 订购许可，并由 Microsoft 开具账单。



注意

部署的 Agent for Azure 使用 Standard_B2s 大小。

9. 单击**完成**。

   您将会重定向至 **设备** > **Microsoft Azure** 屏幕，屏幕上将显示部署的进度。完成后，即可开始使用新添加的订购许可定义保护计划。

   有关 Microsoft Azure 备份和恢复选项的详细信息，请参阅 "Azure 还原点"(第 398 页) 和 "恢复虚拟机可以从虚拟机的备份中恢复它们。在 Cyber Protect 中控台中，无法为处于合规模式下的租户恢复备份。有关如何恢复此类备份的详细信息，请参阅 Recovering backups for tenants in

the Compliance mode。先决条件在恢复至此计算机时，该虚拟机必须处于停止状态。默认情况下，该软件会在无提示的情况下停止计算机运行。当完成恢复时，您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。步骤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。依次单击恢复 > 整台计算机。如果您希望恢复至物理机，请在恢复至中选择物理机。否则，请跳过此步骤。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，可以恢复至物理机。如果是这种情况，请继续执行“物理机”中的第 4 步。否则，我们建议使用可启动媒体执行 V2P 迁移。[可选] 默认情况下，该软件会自动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：选择虚拟机监控程序(VMware ESXi、Hyper-V、Virtuozzo、Virtuozzo Hybrid Infrastructure、Scale Computing HC3 或 oVirt)。仅 Virtuozzo 虚拟机可恢复至 Virtuozzo。有关 V2V 迁移的详细信息，请参阅“计算机迁移”。请注意，当选择 Microsoft Azure 作为目标时，可以选择相关的 Azure 订购许可、区域和资源组。选择恢复至新计算机还是现有计算机。选择主机并指定新计算机名称，或选择现有目标计算机。单击确定。设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)。要查看每个虚拟磁盘的数据存储(存储)、接口和调配模式，请单击磁盘映射。可以更改这些设置，除非您要恢复 Virtuozzo 容器或 Virtuozzo Hybrid Infrastructure 虚拟机。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。该映射部分也可让您选择个别磁盘进行恢复。对于 Microsoft Azure，可以通过选择相关存储类型(本地冗余存储 (LRS) 或区域冗余存储 (ZRS)) 来更改每个目标磁盘的存储类型。[可用于 VMware ESXi、Hyper-V 和 Virtuozzo] 要更改虚拟机的内存大小、处理器数量和网络连接，请单击 VM 设置。[适用于 Microsoft Azure] 若要更改虚拟机的可用性类型和区域、内存大小以及网络连接(包括子网和安全组)，请单击 VM 设置。[对于 Virtuozzo Hybrid Infrastructure] 要更改虚拟机的内存大小和处理器数量，请选择规格。[仅适用于装有保护代理程序的 Windows 计算机] 启用安全恢复开关，以确保恢复后的数据无恶意软件。有关安全恢复如何工作的详细信息，请参阅 Safe recovery。单击开始恢复。当恢复至现有虚拟机时，请确认您希望覆盖磁盘。恢复进度显示在活动选项卡上。"(第 1 页)。

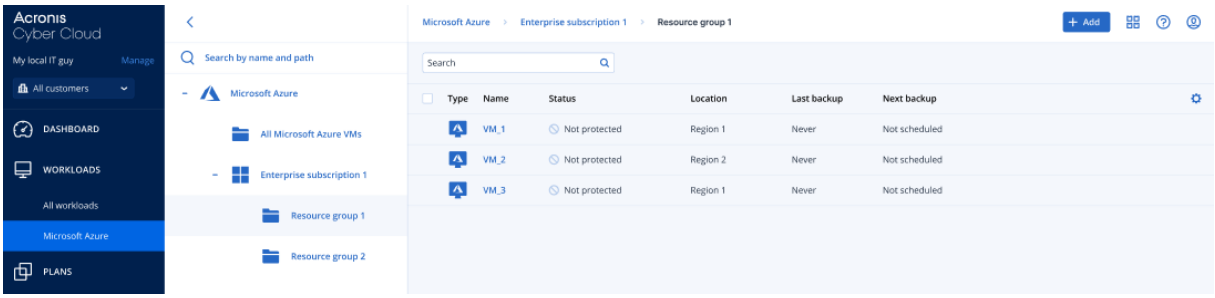
查看和更新已部署的 Agent for Azure

您可以通过以下方式查看和更新 Agent for Azure 部署：

- 通过**设备 > Microsoft Azure** 菜单查看当前的部署。
- 通过**基础架构 > 公共云**菜单查看、更新、访问和重新部署当前的部署。

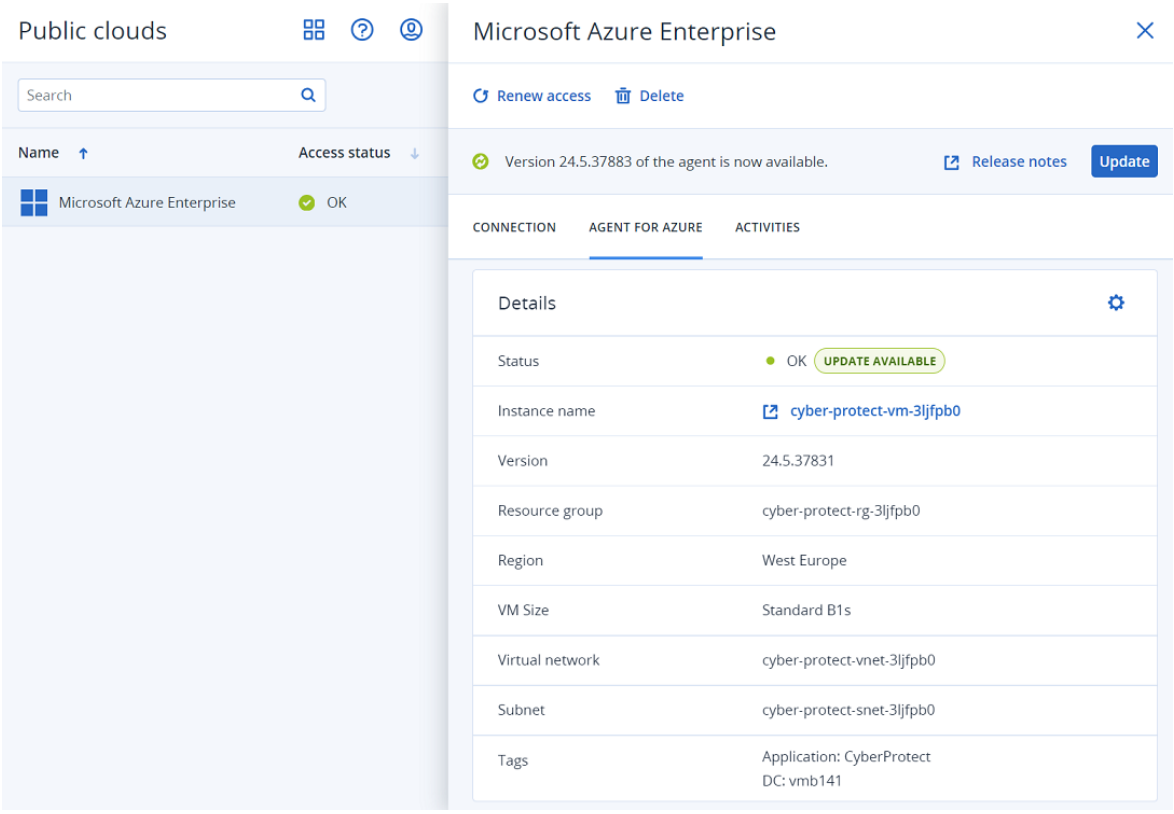
若要通过 Microsoft Azure 菜单查看当前部署

在 Cyber Protect 中控台中，转到 **设备 > Microsoft Azure**。将显示当前的 Agent for Azure 部署列表。请注意，列出的每个订购许可都会在层次结构树中显示其下方的相关资源组。



若要通过基础架构 > 公共云菜单查看和更新当前部署

1. 在 Cyber Protect 中控台中，转到**基础架构 > 公共云**。
   将显示当前的公共云连接列表。
2. 选择部署 Agent for Azure 的有关 Microsoft Azure 订购许可的位置。
3. 在右窗格中，单击 **Agent for Azure** 选项卡。



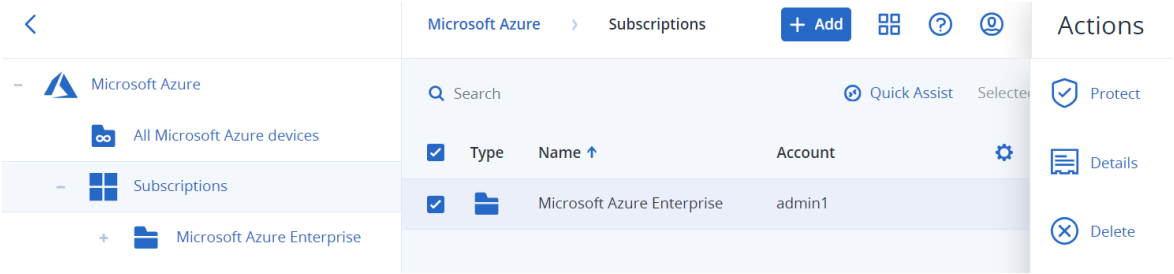
4. 您可以：
   - 查看部署的当前状态。
   - 单击**实例名称**字段中的链接，以访问部署有 Agent for Azure 的实例。请注意，您需要登录 Microsoft Azure 帐户以访问实例。
   - 单击  以重新部署 Agent for Azure。
   - 若有可用的更新，请单击**更新**。

移除 Agent for Azure 虚拟设备

移除对应的 Microsoft Azure 订购许可时，Agent for Azure 虚拟设备会自动移除。

若要移除 Agent for Azure 虚拟设备

1. 在 Cyber Protect 中控台中，转到**设备** > **Microsoft Azure**。
2. 单击分层树中的**订购许可**节点，然后在右侧显示的列表中选择相关的订购许可。



3. 在右侧窗格中，单击**删除**。
4. 在显示的确认对话框中，单击**移除**。

   移除订购许可时，将取消为 Agent for Azure 虚拟设备调配的订购许可，且不会再使用 Microsoft Azure 资源。

注意
如果 Microsoft Azure 虚拟机当前正在使用该订购许可，则无法删除订购许可。

部署适用于 Synology 的代理程序

在启动前

使用适用于 Synology 的代理程序，可以在 Synology NAS 设备之间备份文件和文件夹。将为共享、文件夹和文件保留 NAS 特定的属性和访问权限。

适用于 Synology 的代理程序在 NAS 设备上运行。因此，可以将设备的资源用于脱离主机数据处理操作(如备份复制、验证和清理)。要了解有关这些操作的详细信息，请参阅 "脱离主机的数据保护计划"(第 198 页)。

注意
适用于 Synology 的代理程序仅支持配备 x86_64 处理器的 NAS 设备。不支持 ARM 处理器。请参阅 Synology 知识中心。

可以将备份恢复到 NAS 设备上的原始位置或新位置，并恢复到可通过该设备访问的网络文件夹。云存储中的备份也可以恢复到装有适用于 Synology 的代理程序的非原始 NAS 设备。

下表汇总了可用的备份源和目标。

备份内容	要备份的项目 (备份源)	备份的目标位置 (备份目标)
文件/文件夹	本地文件夹*	云存储
		本地文件夹*
	网络文件夹 (SMB)**	网络文件夹 (SMB)**
		NFS 文件夹
		公有云***

* 包括连接到 NAS 设备的 USB 驱动器。

注意
加密的文件夹不受支持。这些文件夹不会在 Cyber Protection 图形用户界面中显示。

** 通过 SMB 协议使用外部网络共享作为备份源或备份目标仅适用于运行 Synology DiskStation Manager 6.2.3 及更高版本的代理程序。Synology NAS 本身上托管的数据(包括托管网络共享中的数据)可以无限制地进行备份。

*** 仅适用于 Synology 7.x 的代理程序支持备份到公共云,例如 Microsoft Azure、Amazon、Wasabi 或 S3 兼容存储。由于 Synology DSM 6.x 的 Linux 内核限制,适用于 Synology 6.x 的代理程序不支持此备份目标。

限制

- 适用于 Synology 的代理程序仅支持配备 x86_64 处理器的 NAS 设备。不支持 ARM 处理器。请参阅 Synology 知识中心。
- 已备份的加密共享会恢复为未加密共享。
- 已启用**文件压缩**选项的备份共享会在禁用此选项的情况下恢复。
- 只能将由 Agent for Synology 创建的备份恢复到 Synology NAS 设备。

下载安装程序

适用于 Synology 的代理程序的安装程序以 SPK 文件的形式提供。

适用于 Synology 7.x 的代理程序

下载安装程序

1. 在 Cyber Protect 中控台中,导航到**设备** > **所有设备**。
2. 在右上角,单击**添加**。
3. 在**网络附加存储(NAS)**下,单击 **Synology**。
   安装程序即会下载到您的计算机上。

适用于 Synology 6.x 的代理程序

下载安装程序

1. 在 Cyber Protect 中控台中，导航到**设备** > **所有设备**。
2. 在右上角，单击**添加**。
3. 在**网络附加存储(NAS)** 下，单击 **Synology**。
   适用于 Synology 7.x 的代理程序的安装程序即会下载到您的计算机上。
   可以安全地停止下载过程或忽略下载的文件。
4. 单击**下载适用于 Synology 6.x 的代理程序**。
   适用于 Synology 6.x 的代理程序的安装程序即会下载到您的计算机上。

安装适用于 Synology 的代理程序

要安装适用于 Synology 的代理程序，请在 Synology DiskStation Manager 中运行 SPK 文件。

注意
适用于 Synology 的代理程序仅支持配备 x86_64 处理器的 NAS 设备。不支持 ARM 处理器。请参阅 Synology 知识中心。

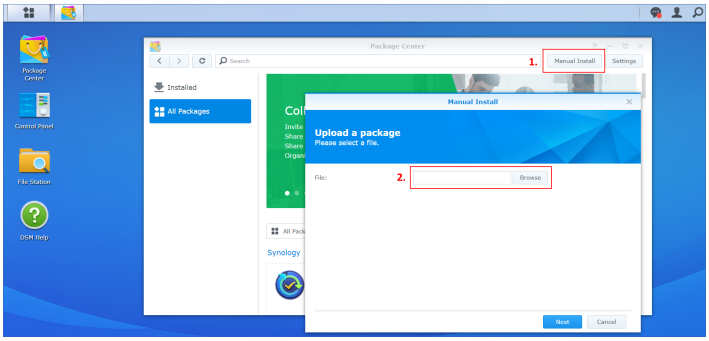
适用于 Synology 7.x 的代理程序

先决条件

- NAS 设备运行 DiskStation Manager 7.x。
- 您是 NAS 设备上**管理员**组的成员。
- 在要安装代理程序的 NAS 卷上，至少有 200 MB 可用空间。
- 一个 SSH 客户端在您的计算机上可用。此文档以 Putty 为例。

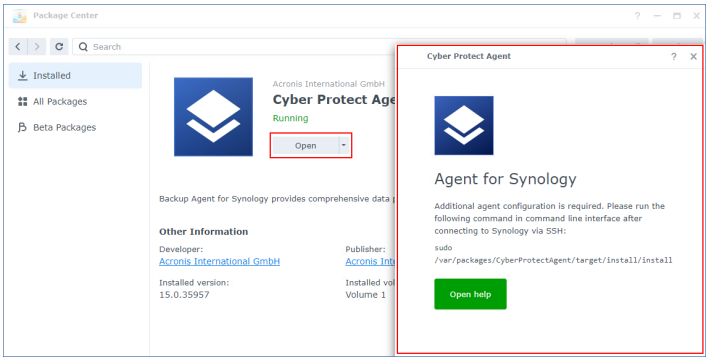
安装适用于 Synology 的代理程序

1. 登录到 Synology DiskStation Manager。
2. 打开**程序包中心**。
3. 单击**手动安装**，然后单击**浏览**。



4. 选择从 Cyber Protect 中控台下载的 SPK 文件，然后单击**下一步**。
   一条表示您将安装第三方软件包的警告即会显示。此消息是标准安装过程的一部分。
5. 要确认您要安装软件包，请单击**同意**。
6. 选择要在其上安装代理程序的卷，然后单击**下一步**。
7. 检查设置，然后单击**完成**。

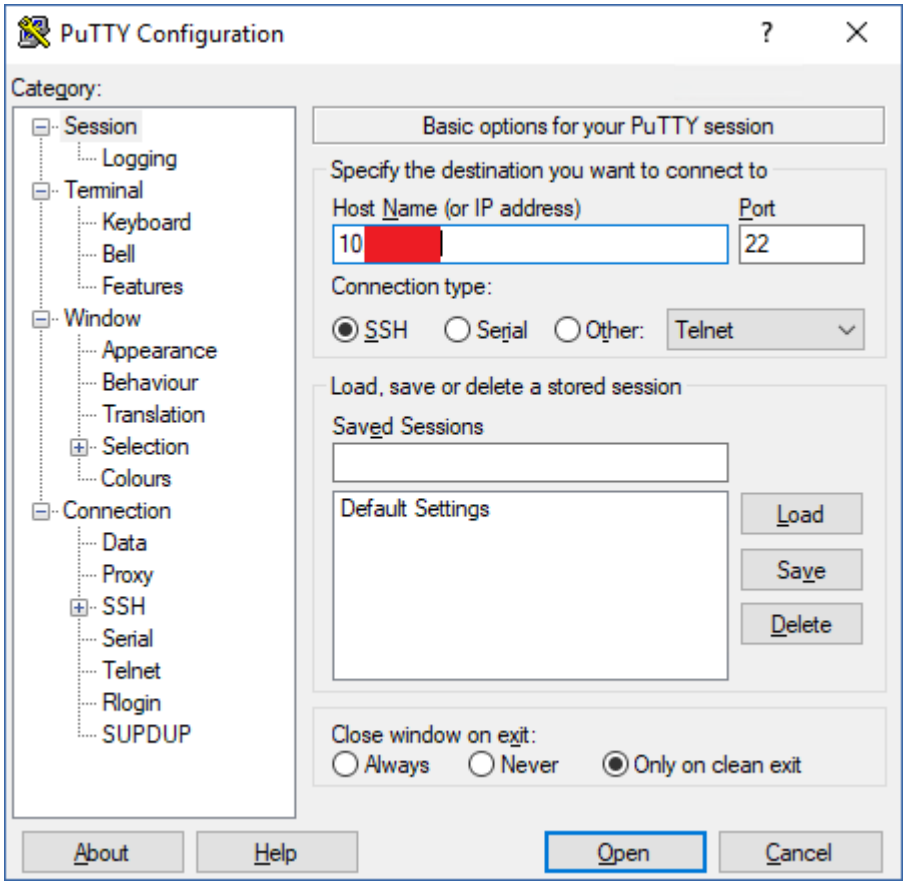
8. 在 Synology DiskStation Manager 的**软件包中心**中，打开适用于 Synology 的 Cyber Protect 代理程序，然后确认您是否看到以下屏幕。



9. 在 Synology DiskStation Manager 的**控制面板**中，转到**终端和 SNMP**，然后启用对 NAS 设备的 SSH 访问。
10. 使用 SSH 客户端(在本例中为 Putty)，在 NAS 设备上运行`install`脚本。

    该脚本允许对 DSM 7.0 或更高版本进行根访问，这是配置代理程序所必需的。

    a. 启动 Putty，然后指定 Synology NAS 设备的 IP 地址或主机名。



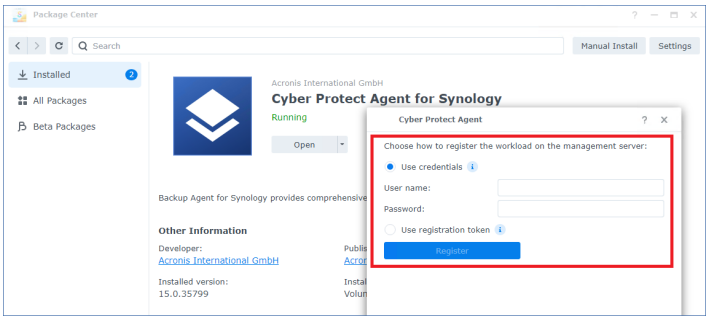
    b. 单击**打开**，然后以 Synology DSM 管理员身份登录。

    c. 运行以下命令。

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

    脚本启动后，请等待 15 秒，在此期间 Cyber Protection 服务会初始化。

11. 在 Synology DiskStation Manager 的**控制面板**中，转到**终端和 SNMP**，然后禁用对 NAS 设备的 SSH 访问。SSH 访问不再需要。
12. 在 Synology DiskStation Manager 的**软件包中心**中，打开适用于 Synology 的 Cyber Protect 代理程序。
13. 选择注册方法。



- [使用凭据注册代理程序]
  - 在**"用户名"**和**"密码"**字段中，指定将注册代理程序的帐户的凭据。该帐户不能是合作伙伴管理员帐户。
- [使用注册令牌注册代理代理程序]
  - 在**注册地址**中，指定确切的数据中心地址。具体的数据中心地址是登录 Cyber Protect 中控台后看到的 URL。例如，`https://us5-cloud.acronis.com`。

    注意
    请勿使用没有数据中心地址的 URL 格式。例如，请勿使用 `https://cloud.acronis.com`。

  - 在**令牌**字段中，指定注册令牌。
    有关如何生成注册令牌的详细信息，请参阅 "生成注册标记"(第 106 页)。
14. 单击**注册**。

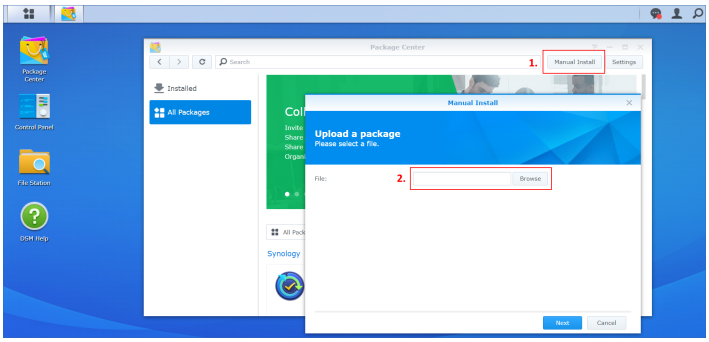
适用于 Synology 6.x 的代理程序

先决条件

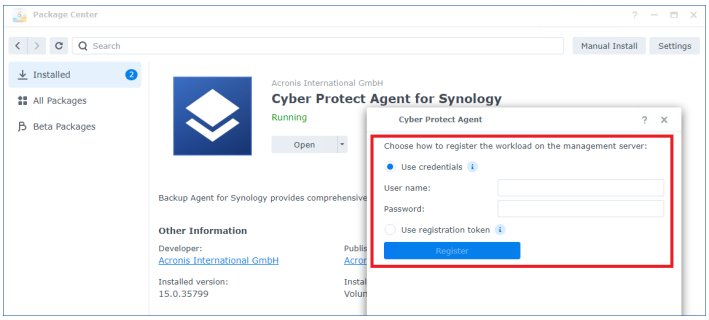
- NAS 设备运行 DiskStation Manager 6.2.x。
- 您是 NAS 设备上**管理员**组的成员。
- 在要安装代理程序的 NAS 卷上，至少有 200 MB 可用空间。

安装适用于 Synology 的代理程序

1. 登录到 Synology DiskStation Manager。
2. 打开**程序包中心**。
3. 单击**手动安装**，然后单击**浏览**。



4. 选择从 Cyber Protect 中控台下载的 SPK 文件，然后单击**下一步**。
   一条表示您将安装没有数字签名的软件包的警告即会显示。此消息是标准安装过程的一部分。
5. 要确认您要安装软件包，请单击**是**。
6. 选择要在其上安装代理程序的卷，然后单击**下一步**。
7. 检查设置，然后单击**应用**。
8. 在 Synology DiskStation Manager 的**软件包中心**中，打开适用于 Synology 的 Cyber Protect 代理程序。
9. 选择注册方法。



   - [使用凭据注册代理程序]
     - 在**"用户名"**和**"密码"**字段中，指定将注册代理程序的帐户的凭据。该帐户不能是合作伙伴管理员帐户。
   - [使用注册令牌注册代理代理程序]
     - 在**注册地址**中，指定确切的数据中心地址。具体的数据中心地址是登录 Cyber Protect 中控台后看到的 URL。例如，`https://us5-cloud.acronis.com`。

       注意
       请勿使用没有数据中心地址的 URL 格式。例如，请勿使用 `https://cloud.acronis.com`。

     - 在**令牌**字段中，指定注册令牌。
       有关如何生成注册令牌的详细信息，请参阅 "生成注册标记"(第 106 页)。
10. 单击**注册**。

在注册完成后，Synology NAS 设备会显示在 Cyber Protect 中控台中的**设备** > **网络附加存储**选项卡上。

要备份 NAS 设备上的数据，请应用保护计划。

更新适用于 Synology 的代理程序

可以将适用于 Synology 6.x 的代理程序更新到适用于 Synology 6.x 的代理程序的更高版本。类似的，可以将适用于 Synology 7.x 的代理程序更新到适用于 Synology 7.x 的代理程序的更新版本。

要更新代理程序，请在 Synology DiskStation Manager 中运行更新版本的安装程序。将保留代理程序的原始注册、其设置以及应用于受保护工作负载的计划。

注意
无法从 Cyber Protect 中控台更新代理程序。

将适用于 Synology 6.x 的代理程序升级到适用于 Synology 7.x 的代理程序仅通过卸载较旧的代理程序并安装更新的代理程序而受支持。在此情况下，所有保护计划都将吊销，而且您必须手动重新应用它们。

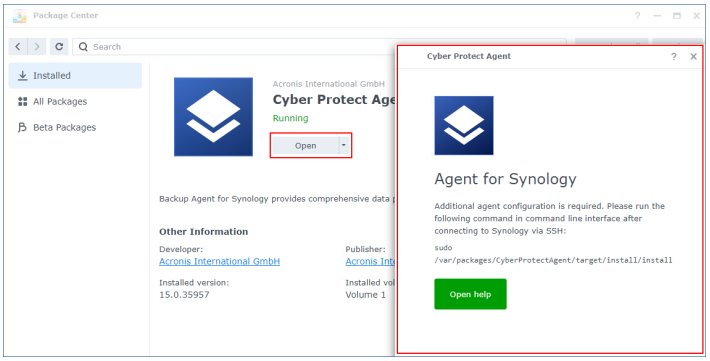
适用于 Synology 7.x 的代理程序

先决条件

- 您是 NAS 设备上**管理员**组的成员。
- 在要安装代理程序的 NAS 卷上，至少有 200 MB 可用空间。
- 一个 SSH 客户端在您的计算机上可用。此文档以 Putty 为例。

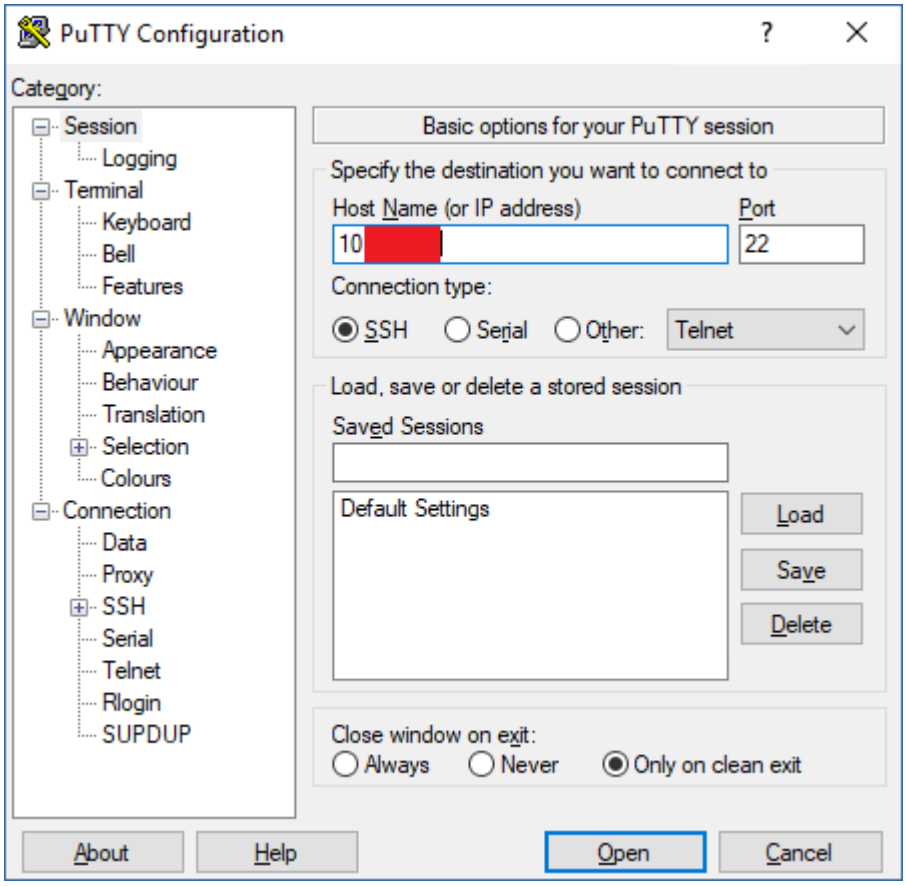
更新适用于 Synology 的代理程序

1. 在 DiskStation Manager 中，打开**程序包中心**。
2. 单击**手动安装**，然后单击**浏览**。
3. 选择从 Cyber Protect 中控台下载的更新的 SPK 文件(适用于 Synology 7.x 的代理程序)，然后单击**下一步**。
   一条表示您将安装第三方软件包的警告即会显示。此消息是标准安装过程的一部分。
4. 要确认您要安装软件包，请单击**同意**。
5. 检查设置，然后单击**完成**。
6. 在 Synology DiskStation Manager 的**软件包中心**中，打开适用于 Synology 的 Cyber Protect 代理程序，然后确认您是否看到以下屏幕。



7. 在 Synology DiskStation Manager 的**控制面板**中，转到**终端和 SNMP**，然后启用对 NAS 设备的 SSH 访问。

8. 使用 SSH 客户端(在本例中为 Putty),在 NAS 设备上运行 `install` 脚本。
   该脚本允许对 DSM 7.0 或更高版本进行根访问,这是配置代理程序所必需的。
   a. 启动 Putty,然后指定 Synology NAS 设备的 IP 地址或主机名。



   b. 单击**打开**,然后以 Synology DSM 管理员身份登录。
   c. 运行以下命令。

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

9. 在 Synology DiskStation Manager 的**控制面板**中,转到**终端和 SNMP**,然后禁用对 NAS 设备的 SSH 访问。SSH 访问不再需要。

适用于 Synology 6.x 的代理程序

先决条件

- 您是 NAS 设备上**管理员**组的成员。
- 在要安装代理程序的 NAS 卷上,至少有 200 MB 可用空间。

更新适用于 Synology 的代理程序

1. 在 DiskStation Manager 中,打开**程序包中心**。
2. 单击**手动安装**,然后单击**浏览**。
3. 选择从 Cyber Protect 中控台下载的更新的 SPK 文件(适用于 Synology 6.x 的代理程序),然后单击**下一步**。

一条表示您将安装没有数字签名的软件包的警告即会显示。此消息是标准安装过程的一部分。

4. 要确认您要安装软件包，请单击**是**。
5. 检查设置，然后单击**应用**。

SSH 连接到虚拟设备

当您远程访问虚拟设备进行维护时，请使用安全套接字外壳 (SSH) 连接。

启动安全外壳守护进程

若要允许 SSH 连接到虚拟设备，需要在设备上启动安全外壳守护进程 (sshd)。

若要启动安全性外壳守护进程

1. 在虚拟机监控程序软件中，打开虚拟设备的中控台。
2. 在该设备的图形用户界面中，按 CTRL+SHIFT+F2 以打开命令行接口。
3. 运行以下命令：

   ```
   /bin/sshd
   ```

4. [仅在首次连接到设备时] 为 root 用户设置密码。

   若要了解如何设置密码，请查看"在虚拟设备上设置根密码"(第 156 页)。

注意

我们建议您在不使用 SSH 连接时停止安全外壳守护进程。

在虚拟设备上设置根密码

在首次建立到虚拟设备的 SSH 连接之前，您必须在设备上设置 root 密码。

若要设置根密码

1. 在虚拟机监控程序软件中，打开虚拟设备的中控台。
2. 在该设备的图形用户界面中，按 CTRL+SHIFT+F2 以打开命令行接口。
3. 运行以下命令：

   ```
   passwd
   ```

4. 指定一个密码，然后按回车键。

   密码必须包含至少九个字符，并且复杂性得分必须为三分或以上。复杂性得分会自动进行计算。若要达到更高的得分，请使用特殊符号、大写和小写符号以及数字的组合。
5. 确认密码，然后按回车键。

通过 SSH 客户端访问虚拟设备

先决条件

- 远程计算机上必须有 SSH 客户端。下面的步骤以 WinSCP 客户端为例。您可以使用任何 SSH 客户端，只需进行相应的步骤调整即可。
- Secure Shell 守护进程 (sshd) 必须在虚拟设备上启动。有关更多信息，请参见"启动安全外壳守护进程"(第 156 页) 。

通过 WinSCP 访问虚拟设备

1. 在远程计算机上，打开 WinSCP。
2. 点击**会话** > **新会话**。
3. 在**文件协议**中，选择 **SCP**。
4. 在**主机名**中，指定虚拟设备的 IP 地址。
5. 在**用户名**和**密码**中，指定root和root用户的密码。
6. 单击**登录**。

显示虚拟设备上所有目录的列表。

设备发现

通过使用设备发现功能，您可以：

- 获得组织网络中可用的网络设备的完整可见性。
- 使用与 Active Directory 同步，以减少在大型 Active Directory 域中调配资源和管理计算机的工作。
- 通过在 Active Directory 域或本地网络中检测计算机，自动安装保护代理程序和注册计算机。
- 在多个工作负载上安装保护代理程序。

可以使用以下方法之一来执行设备发现：

- Active Directory 发现。

  在 Active Directory 发现期间，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。
- 使用 Device Sense ™ 进行本地网络发现。有关详细信息，请参阅 "使用 Device Sense ™ 进行设备发现"(第 164 页) 。
- 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表的计算机。

  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设备发现，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设备发现，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。

还可以使用“Device Sense ™” 配置被动设备发现，并查看组织中公司本地区域网络中可用设备的详细信息。有关详细信息，请参阅 "使用 Device Sense ™ 进行被动设备发现"(第 165 页) 。

发现多个设备

发现多个设备的流程可归纳为以下步骤：

1. 选择发现方法：
   - Active Directory 发现。
   - 使用 Device Sense ™ 进行本地网络发现。
   - 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表的计算机。
2. [对于 Active Directory 发现和手动发现] 选择要添加到租户的计算机。
3. [对于 Active Directory 发现和手动发现] 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 Cyber Protect 中控台中注册它们。
   - 在 Cyber Protect 中控台中注册计算机（如果保护代理程序已安装）。
   - 将计算机作为非托管设备添加到 Cyber Protect 中控台，无需安装保护代理程序。

   还可以将保护计划、监控计划和远程管理计划应用于安装保护代理程序或在 Cyber Protect 中控台注册的计算机。
4. [对于 Active Directory 发现和手动发现] 为所选计算机提供管理员凭据。
5. [对于 Active Directory 发现和手动发现] 验证您是否可以使用提供的凭据连接到计算机。

在 Cyber Protect 中控台中，显示的计算机分为以下几类：

- **已发现的设备** - 已发现但未安装保护代理程序的计算机。
- **带有代理程序的计算机** – 已安装保护代理程序的计算机。
- **已发现的设备 / 无代理程序的设备** – 可在其中安装保护代理程序的计算机。
- **已发现的设备/本地网络** - 使用 Device Sense ™ 扫描本地网络时发现的计算机和网络设备。
- **已发现的设备 / Active Directory** - 通过搜索 Active Directory 发现的计算机。
- **已发现的设备 / 手动 / 从文本文件** - 已手动或从文本文件添加的计算机。

设备发现要求

在使用设备发现功能之前，请确保满足以下要求：

- 您的本地网络或 Active Directory 域中必须至少有一台安装了保护代理程序的计算机。此代理程序将用作发现代理程序。
- 您必须在 Cyber Protection 服务分配有以下角色之一：网络管理员或管理员。

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。

添加多个设备

在添加多个设备之前，请确保满足以下要求。有关详细信息，请参阅 "设备发现要求"（第 158 页）。

注意
由于运行代理程序服务需要额外权限，因此不支持添加域控制器的功能。

搜索 Active Directory

若要在 Active Directory 中添加多个设备

1. 在 Cyber Protect 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**发现设备**。
   将打开发现向导。
4. 选择租户。
5. 选择将执行扫描以检测计算机的发现代理程序。

   注意
   发现代理程序是安装了保护代理程序的工作负载。
   发现代理程序必须是 Active Directory 域的成员。
   您可以选择与所选单位或其子单位相关联的代理程序。

6. 选择**搜索 Active Directory**，然后单击**下一步**。
7. 在**搜索 Active Directory**窗口中，选择计算机搜索方式，然后单击**确定**。

选项	描述
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**筛选器**让您可以指定计算机选择的标准。

8. 在已发现的计算机列表中，选择要添加的计算机，然后单击**下一步**。
9. 在**发现后操作**选项卡上：
   a. 选择处理计算机的方式。

选项	描述
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"(第 162 页)。
注册已安装代理程序的计算机	如果计算机上已经安装了代理程序，则使用此选项，并且只需在 Cyber Protection 中注册它们。如果在计算机上找不到代理程序，则它们将被添加到**无代理程序设备**列表。
添加为非托管计算机	如果选择此选项，该代理程序将不会安装在计算机上。您将能够在中控台中查看它们，并稍后安装或注册代理程序。

   b. 选择要在其下注册计算机的用户帐户。

c. [可选] 若要选择将自动应用于计算机的计划，请在**注册后操作**部分，相应计划类型的计划选择字段中，单击**更改**，选择该计划，然后再次单击**更改**。

注意
仅当为租户配置了双重身份验证 (2FA) 时，才允许选择计划。如果未配置 2FA，则必须首先配置 2FA，然后登录 Cyber Protect 中控台并从头开始执行此过程。

d. 单击**下一步**。

10. 在**凭据**选项卡上，执行以下操作：
    a. 单击**添加凭据**。
    b. 选择具有对所选设备的管理员权限的用户的凭据，然后单击**选择凭据**。

重要事项
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。如果要定义自定义管理员凭据，则必须执行额外的手动准备操作。有关详细信息，请参阅 "准备好计算机以进行远程手动安装"（第 168 页）。

    c. 单击**下一步**。
    系统将对所选设备进行初步检查，以确保其适用并且具有远程安装代理程序和所选组件的正确设置。
11. [如果存在连接问题] 请执行相应的补救操作，解析已识别的连接问题。
12. 单击**安装**。

扫描本地网络

通过扫描本地网络来发现多个设备

1. 在 Cyber Protect 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**发现设备**。
   将打开发现向导。
4. 单击**扫描**。
   将启动主动设备发现扫描。将重定向到**已发现的设备** > **本地区域网络**屏幕。扫描完成后，将显示通知。此通知显示了扫描期间发现的设备数量，并包括设备列表的链接，您可在其中查看有关设备的其他详细信息。

下一步操作：

- 您可以单击通知中的**查看新发现的设备**链接，并在**本地区域网络**选项卡上查看设备及其详细信息。
- 可以在已发现的设备上远程安装保护代理程序并注册它们。有关详细信息，请参阅 "远程安装代理程序并注册设备"（第 171 页）。
- 可以从发现中排除设备。有关详细信息，请参阅 "从发现中排除设备"（第 172 页）。

手动操作或通过导入文件

手动添加多个设备或通过导入文件进行添加

1. 在 Cyber Protect 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**发现设备**。
   将打开发现向导。
4. 单击**手动指定或从文件导入**。
5. 使用以下选项之一添加计算机。
   - 若要手动添加计算机：
     a. 在**添加计算机**字段中，输入计算机的 IPv4 地址或主机名。
     b. 对想要添加的每个计算机重复上一步骤。
   - 若要通过导入文件添加计算机：
     a. 单击**从文件导入计算机**。
     b. 在**从文件导入计算机列表**窗口中，拖放包含计算机列表的文本文件，或单击**浏览**，导航到文件，选择该文件，然后单击**打开**。
     文件必须包含每行一个的 IP 地址或主机名。以下是文件内容示例：

     ```
     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 添加的计算机并检查其可用性。
6. 单击**下一步**。

启动发现计算机后，您将在**监控** > **活动** > **发现基础结构中的设备**活动中找到相应任务。

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 远程限制条件

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，建议您在完成管理操作（例如，远程安装）后，将这两项设置恢复为其原始状态：**EnableLUA=1**，**LocalAccountTokenFilterPolicy = 0**

选择要安装的组件

当添加通过在 Active Directory 中搜索发现的多个设备时，您可以配置以下附加设置：

- 将用于运行服务的帐户。
- 制定您要安装的组件。
- 安装后操作。

若要选择要安装的组件

1. 在**“选择组件”**屏幕上，确保**“在发现的设备上安装保护代理程序”**开关已启用。
2. [可选] 若要更改要在其下运行服务的帐户：
   a. 在**“设置”**窗格中的**“服务登录帐户”**行中，单击**“更改”**。
   b. 选择账户选项。

选项	描述
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”。 确保域安全策略不会影响相关帐户的权限。如果帐户在安装期间被剥夺了分配的用户权限，则组件可能无法正常工作或根本无法工作。
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。 确保域安全策略不会影响相关帐户的权限。如果帐户在安装期间被剥夺了分配的用户权限，则组件可能无法正常工作或根本无法工作。

   c. [如果选择**使用以下帐户**] 输入用户名和密码。
   d. 单击**保存**。
3. [可选] 选择安装后操作

选项	描述
在必要时重新启动设备	如果选择此选项，计算机将根据需要重新启动多次，直到完成安装。 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。
若有用户已登录，请勿重新启动设备	当选择**"在需要时重新启动设备"**时，此选项会变为可编辑。 如果选中此选项，则用户登录系统后计算机将不会自动重新启动。例如，如果用户正在工作，而安装需要重新启动，则系统将不会重新启动。 如果先决条件已安装，但由于用户登录而未重新启动计算机，则若要完成安装，您必须重新启动计算机，然后再次开始安装。 如果已安装代理程序但计算机未重新启动，则必须重新启动计算机。

4. 在**为 Windows 安装附加组件**窗格中，单击箭头图标。
5. 选择您要安装的组件。

组件	描述
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	
适用于防止数据丢失的代理程序	此代理程序使您能够限制用户对本地和重定向的外围设备、端口和保护计划下计算机上剪贴板的访问。如果选择，将安装它。
反恶意软件和 URL 过滤	此组件在保护计划中支持防病毒和反恶意软件保护块以及 URL 过滤模块。即使选择不安装它，如果在该计算机的保护计划中启用了这些模块中的任意一个，那么以后将自动安装它。
适用于 Hyper-V 的代理程序	该代理程序备份 Hyper-V 虚拟机。它会将安装在 Hyper-V 主机上。如果选中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。它将安装在运行 Microsoft SQL Server 的计算机上。如果选中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。它将安装在运行 Microsoft Exchange Server 的"邮箱"角色的计算机上。如果选中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。它将安装在域控制器上。如果选中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。它将安装在对 vCenter 服务器具有网络访问权限的 Windows 计算机上。如果选中，将安装它。
适用于 Microsoft 365 的代理程序	该代理程序会将 Microsoft 365 邮箱备份到本地目标。它将安装在 Windows 计算机上。如果选中，将安装它。
适用于 Oracle 的代理程序	该代理程序备份 Oracle 数据库。它将安装在运行 Oracle 数据库的计算机上。如果选中，将安装它。
Cyber Protection Monitor	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。它将安装在 Windows 计算机上。如果选中，将安装它。 在 Windows 7 Service Pack 1 及更高版本以及 Windows Server 2008 R2 Service Pack 1 及更高版本上受支持。

6. 单击**选择**。

   选择组件屏幕关闭，您会返回到**发现后操作**屏幕/选项卡。

使用 Device Sense™ 进行设备发现

Device Sense™ 使用一种复杂的技术组合来扫描组织的本地网络，以发现和识别设备。除了发现物理和虚拟机器和平板电脑外，Device Sense™ 还可发现其他网络设备，如路由器、交换机、打印机、智能手机和 IP 摄像机。

使用 Device Sense™ 可实现：

- 全面的网络可见性 - 可识别连接到客户网络的每个设备。
  这有助于维护准确的资产清单，并可有效地管理和支持您的 IT 基础结构，这对于资产跟踪和生命周期管理至关重要，也可确保符合许可协议。
- 安全性和合规性 - 检测可能构成安全风险的未经授权或恶意设备。Device Sense™ 可帮助您确保网络中的每个设备符合安全策略和法规要求。
- 资源的高效分配 - 了解客户网络的范围和规模，从而更高效地分配资源并实现更佳的服务计划。

使用 Device Sense™ 进行设备发现包括以下功能：

- 自动智能选择要扫描的发现代理程序和网络
- 防止在家庭或非公司网络中发现设备

注意

使用 Device Sense™ 进行被动发现不会扫描代理程序数量小于在**防止在非公司网络中发现设备**设置中指定的数量的网络。在数据中心层面，此设置的预配置值为 3，但此值会被上限租户继承，且可能不同。若要确保被动发现会扫描所有公司网络，可以根据组织更新设置。有关详细信息，请参阅 "配置被动设备发现"(第 165 页)。

- 按需式主动设备发现
- 按类型进行设备分类
- 浏览已发现设备的高级搜索和筛选选项

- 已发现设备的详细信息
- 在已发现的设备上远程安装保护代理程序，并应用了不同的计划类型
- 有关已发现设备的扩展报告

可以使用 Device Sense ™ 执行被动设备发现扫描或主动设备发现扫描。有关详细信息，请参阅 使用 Device Sense ™ 进行被动设备发现 和 使用 Device Sense ™ 主动设备发现。

注意
数据库中有关已发现设备的信息的保留期为 3 个月。

使用 Device Sense ™ 进行被动设备发现

被动设备发现是一种非侵入式方法，用于识别和编录网络环境中的设备，而无需主动探测或向组织网络中的这些设备发送请求。

被动设备发现会收集以下设备数据：

- 设备名称
- 设备类型
- 操作系统系列
- 厂商
- 型号
- MAC 地址
- IP 地址

被动发现的设置在数据中心级别预配置。公司管理员可以自定义这些设置 – 为公司或单位中的所有设备。如果应用了自定义设置，将使用较高级别的设置，顺序为：

1. Cyber Protection 数据中心
2. 公司（客户租户）
3. 单元

例如，单位管理员可以为单位配置自定义设备发现新设置，这可能不同于应用于该公司级别上的设置。

配置被动设备发现

被动设备发现会持续扫描公司网络中的设备。使用被动设备发现：

- 合作伙伴可以查看客户的网络以及这些网络中可用的设备的数量和类型。
- 客户可以查看其组织的网络，以及这些网络中可用的设备的数量和类型。

若要配置被动设备发现设置

1. 在 Cyber Protect 中控台中，转到**设置** > **保护**。
2. 单击**被动设备发现**选项卡。
3. 请确保已启用 **启用被动设备发现**开关。
   系统会自动将 Windows 代理程序分配为发现代理程序。

4. [可选] 更改默认设置。

设置	描述
智能自动选择发现代理程序	将自动选择的代理程序数量，以在本地网络中执行被动设备发现。默认值为 1。* 最大值为 3。
防止在非公司网络中发现设备	必须在网络中存在的代理程序的最小数量，以便将其分类为公司环境并启用其扫描。默认值为 3。* 最大值为 10。
网络中设备的增强识别	启用或禁用多播信号的使用，以更精确地识别加入本地网络的设备类型。默认情况下，该开关已禁用。*

***** 默认值可能不同，这取决于上一级租户的配置。默认值是继承的，与上一级租户设置的默认值相同。但是，您可以根据组织的需求更改默认值。

5. 单击**保存**。

使用 Device Sense™ 主动设备发现

主动设备发现是网络管理中使用的一种方法，系统会主动探测或与网络中的设备进行通信，以识别并收集有关这些设备的信息。

可以检索网络中设备的全面和准确数据，从而确保所有设备信息清晰可见。

主动设备发现会收集以下设备数据：

- 设备名称
- 设备类型
- 厂商
- 型号
- IP 地址
- MAC 地址

使用 Device Sense™ 运行主动设备发现扫描

可以运行主动扫描，以便全面收集数据并识别连接到本地网络的设备。

若要运行主动扫描

1. 在 保护 中控台中，转到**设备** > **已发现的设备**。
2. 单击**本地网络**选项卡。
3. 单击**运行主动扫描**。
4. 选择要运行主动扫描的网络，然后单击**运行**。
5. 在**租户**字段中，选择租户。
6. 在**发现代理程序**字段中，选择在租户中注册的工作负载。将使用安装在此工作负载上的保护代理程序作为发现代理程序。
7. 单击**运行**。

   将启动主动设备发现扫描。扫描完成后，将显示通知。此通知显示了扫描期间发现的设备数量，并包括设备列表的链接，您可在其中查看有关设备的其他详细信息。

注意

无法同时运行多个主动扫描。若有主动扫描正在进行中，则必须取消它或等待其完成，然后才能启动新的扫描。

查看已发现设备的信息

您可以使用**"已发现的设备"**页上的筛选器，以快速在列表中查找特定设备并查看其详细信息。

查找已发现的设备并查看其详细信息

1. 在 保护 中控台中，单击**已发现的设备**。
   默认情况下，会打开**无代理程序设备**选项卡。
2. [可选] 若要从特定类别搜索设备，请单击相应选项卡。

选项卡	描述
无代理程序的设备	此选项卡会列出所有已发现的计算机，无论使用的是何种发现方法。
Active Directory	此选项卡列出了通过扫描 Active Directory 发现的计算机。
本地网络	此选项卡列出了通过使用 Device Sense™ 扫描本地公司网络而发现的设备(计算机或其他网络设备)。
手动操作/从文本文件	此选项卡列出了手动操作或从文本文件中发现的计算机。
排除	此选项卡列出了已从发现中排除的设备。

3. [可选] 若要按设备名称搜索，请在**搜索**字段中输入设备名称。
   会动态筛选列表中的结果。
4. [可选] 若要使用筛选器搜索结果，请单击**筛选**，选择一个或多个筛选器，然后单击**应用**。

过滤器	描述
设备类型	若要搜索一个或多个设备类型，请单击该字段，然后从列表中选择相关设备类型。 此筛选器不可用于**手动/从文本文件**选项卡。
发现类型	若要根据发现方法筛选结果，请单击字段，然后从以下方法中进行选择。 • **Active Directory** • **手动** • **本地网络被动** • **本地网络主动** 此筛选器仅在**无代理程序的设备**选项卡上可用。
MAC 地址	若要搜索具有特定 MAC 地址的设备，请在此字段中输入 MAC 地址。 此筛选器不可用于**手动/从文本文件**选项卡。

过滤器	描述
IP 地址范围	若要根据设备 IP 地址筛选结果，请在第一个字段中输入起始 IP 地址，在第二个字段中输入结束 IP 地址。
首次发现	若要根据设备首次被发现的日期筛选结果，请单击字段，然后使用预定义范围或自定义范围。
上次发现	若要根据设备上次被发现的日期筛选结果，请单击字段，然后使用预定义范围或自定义范围。
组织单元	设备所属的 Active Directory 组织单元。 此筛选器仅在 **Active Directory** 选项卡上可用。

5. 单击设备，然后单击**详细信息**。
6. 在**原始数据**窗格中，单击箭头图标。
7. 若要下载 JSON 文件中的原始数据，请单击**下载**。
   文件将保存在登录至 保护 中控台的计算机上的默认下载目录中。

远程安装代理程序

完成设备发现过程后，您可以在发现的 Windows 设备上远程安装代理程序。

代理程序的远程安装按以下方式进行：

1. 发现代理程序使用在发现向导中指定的主机名、IP 地址和管理员凭据连接到目标计算机，然后将 `web_installer.exe` 文件上传到这些计算机。
2. 在目标计算机上，`web_installer.exe` 文件在无人参与模式下运行。
3. Web 安装程序从云中检索其他安装包，然后通过 `msiexec` 命令将它们安装到目标计算机上。
4. 安装完成后，组件将在云中注册。

注意
由于运行代理程序服务需要额外权限，因此域控制器不支持远程安装代理程序。

准备好计算机以进行远程手动安装

- 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“用户帐户控制 (UAC) 的要求”>“禁用 UAC”。
- 默认情况下，在任何 Windows 计算机上进行远程安装都需要内置管理员帐户的凭据。要使用另一个管理员帐户的凭据执行远程安装，必须*禁用*用户帐户控制 (UAC) 远程限制。有关如何禁用它们的详细信息，请参阅“用户帐户控制 (UAC) 的要求”>“禁用 UAC 远程限制”。
- 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**。

- Cyber Protection 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。

使用 GPO 为远程安装准备计算机

您可以配置并应用 Active Directory 组策略对象 (GPO) 以准备一组 Active Directory 成员计算机，以便远程安装 保护 代理程序。

先决条件

- 您的用户是“域管理员”组的成员或域管理员。
- 已在登录以创建 GPO 的计算机上安装**组策略管理中控台** (GPMC)。

若要使用 GPO 为远程安装准备计算机

1. 若要打开 GPMC，请按 **Win** + **R**，键入 `gpmc.msc`，然后按 **Enter**。
2. 在中控台树中，右键单击要应用 GPO 的域或组织单元 (OU)。
3. 单击**在此域中创建 GPO 并在此处链接...**。
4. 在**新建 GPO** 弹出窗口中，输入 GPO 的名称，然后单击**确定**。
5. 在中控台树中，右键单击在上一步中创建的 GPO，然后单击 **编辑...**。
6. 请按以下步骤禁用 **使用共享向导**。
   a. 在中控台树中，依次选择 **用户配置** > **首选项** > **Windows 设置** > **注册表**。
   b. 右键单击 **注册表**，然后单击 **新建** > **注册表项**。
   c. 在**新注册表属性**窗口的**常规**选项卡上，配置注册表项如下。

参数	值
操作	更新
Hive	`HKEY_CURRENT_USER`
注册表项路径	Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
值名称	SharingWizardOn
值类型	`REG_DWORD`
值数据	0

   d. 单击**应用**，然后单击**确定**。
7. [仅限 Windows Vista 和更高版本] 请按以下步骤禁用用户帐户控制 (UAC)。

a. 在中控台树中，依次选择 **计算机配置** > **首选项** > **Windows 设置** > **注册表**。
b. 右键单击 **注册表**，然后单击 **新建** > **注册表项**。
c. 在**新注册表属性**窗口的**常规**选项卡上，配置注册表项如下。

参数	值
操作	更新
Hive	HKEY_LOCAL_MACHINE
注册表项路径	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
值名称	EnableLUA
值类型	REG_DWORD
值数据	0

d. 单击**应用**，然后单击**确定**。

8. [仅限 Windows Vista 和更高版本] 请按以下步骤禁用用户帐户控制 (UAC) 远程限制。
a. 在中控台树中，依次选择 **计算机配置** > **首选项** > **Windows 设置** > **注册表**。
b. 右键单击 **注册表**，然后单击 **新建** > **注册表项**。
c. 在**新注册表属性**窗口的**常规**选项卡上，配置注册表项如下。

参数	值
操作	更新
Hive	HKEY_LOCAL_MACHINE
注册表项路径	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
值名称	LocalAccountTokenFilterPolicy
值类型	REG_DWORD
值数据	1

d. 单击**应用**，然后单击**确定**。

9. 请按照以下步骤启用**文件和打印机共享**。
a. 在中控台树中，依次选择**计算机配置** > **策略** > **Windows 设置** > **安全设置** > **Windows Defender 防火墙与 Advanced Security** > **入站规则**。
b. 右键单击**入站规则**，然后单击**新建规则**。
c. 在**新入站规则向导**中，配置规则如下。
d. 在 **规则类型** 选项卡上，选择 **预定义**，选择 **文件和打印机共享**，然后单击 **下一步**。
e. 在**预定义规则**选项卡中，单击**下一步**。
f. 在 **操作** 选项卡上，选择 **允许连接**，然后单击 **完成**。
g. 在中控台树中，依次选择**计算机配置** > **策略** > **Windows 设置** > **安全设置** > **Windows Defender 防火墙与 Advanced Security** > **出站规则**。

h. 右键单击**出站规则**，然后选择**新建规则**。
i. 在**新建传出规则向导**中，执行与步骤 d - f 中相同的操作来配置规则。
10. 按照以下步骤将 GPO 链接到域或 OU。
    a. 在中控台树中，右键单击目标域或 OU，然后单击 **链接现有 GPO...**。
    b. 在 **选择 GPO** 屏幕上，选择您创建的 GPO，然后单击 **确定**。
11. 按照以下步骤，在要准备进行远程代理程序安装的目标计算机上，强制执行组策略更新。
    a. 以管理员身份运行**命令提示符**。
    b. 运行以下命令：

    ```
    gpupdate /force
    ```

远程安装代理程序并注册设备

注意
仅支持 Windows 设备的代理程序的远程安装。

多个设备上的代理程序安装仅适用于位于同一网络中，且由相同的发现方法发现的设备。

若要远程安装代理程序

1. 在 保护 中控台中，转到**设备** > **无代理程序的设备**。
2. 选择设备。
3. 单击**安装并注册**。
4. 在**发现后操作**选项卡上，选择租户帐户。
5. 在**发现代理程序**字段中，选择将用于远程代理程序安装和计算机注册的工作负载。

   注意
   发现代理程序是安装了保护代理程序的工作负载。
   发现代理程序必须是 Active Directory 域的成员。
   您可以选择与所选单位或其子单位相关联的代理程序。

6. 选择要在计算机上执行的操作。

选项	描述
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"(第 162 页)。
注册已安装代理程序的计算机	如果计算机上已经安装了代理程序，则使用此选项，并且只需在 Cyber Protection 中注册它们。如果在计算机上找不到代理程序，则它们将被添加到**无代理程序的设备**列表。

7. 选择要在其下注册计算机的用户帐户。
8. [可选] 若要选择将自动应用于计算机的计划，请在**注册后操作**部分，相应计划类型的计划选择字段中，单击**更改**，选择该计划，然后再次单击**更改**。

注意
仅当为租户配置了双重身份验证 (2FA) 时，才允许选择计划。如果未配置 2FA，则必须首先配置 2FA，然后登录 Cyber Protect 中控台并从头开始执行此过程。

9. 单击**下一步**。
10. 在**凭据**选项卡上，执行以下操作：
    a. 单击**添加凭据**。
    b. 选择凭据，选择具有对所选设备的管理员权限的用户的凭据，然后单击**选择凭据**。

    重要事项
    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。如果要定义自定义管理员凭据，则必须执行额外的手动准备操作。有关详细信息，请参阅 "准备好计算机以进行远程手动安装"（第 168 页）。

    c. 单击**下一步**。
    系统将对所选设备进行初步检查，以确保其适用并且具有远程安装代理程序和所选组件的正确设置。
11. [如果存在连接问题] 请执行相应的补救操作，解析已识别的连接问题。
12. 单击**安装**。

从发现中排除设备

当您从发现中排除设备时，这些设备在运行设备发现扫描时将不会列在已发现设备的结果中。

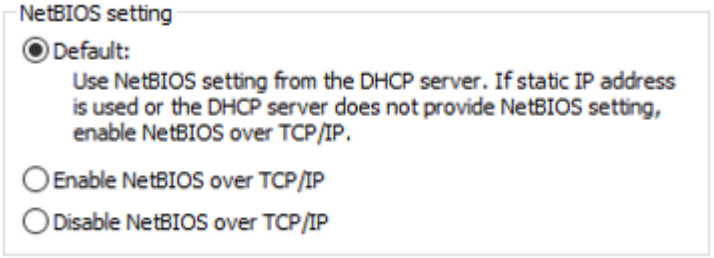
若要从发现中排除设备

1. 在 保护 中控台中，转到**设备**。
2. 单击要从发现中排除的设备，然后单击**排除发现**。
已将设备从发现中排除，并已添加到**"排除"**页面上的设备列表。

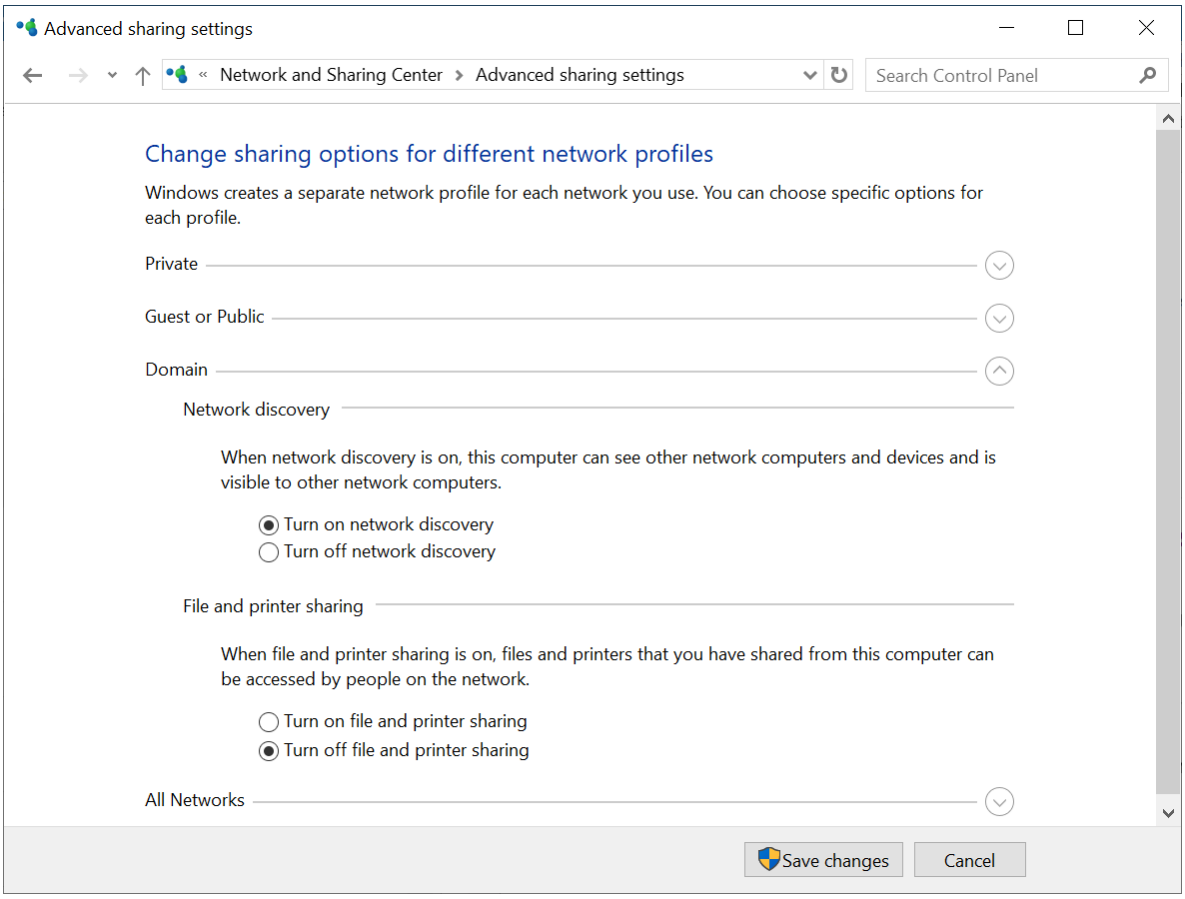
设备发现故障排除

如果遇到与设备发现功能有关的任何问题，请尝试检查以下内容：

- 检查是否已启用基于 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。



- 检查“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。
- 检查“功能发现资源发布”服务是否正在要发现的计算机上运行。

阻止未经授权的卸载或修改代理程序

通过在保护计划中启用**密码保护**，即可保护适用于 Windows 的代理程序免遭未经授权的卸载或修改。仅当**自我保护**设置启用时，该设置才可用。

启用密码保护

1. 在保护计划中，展开**防病毒和反恶意软件保护**模块(即适用于 Cyber Backup 各版本的 **Active Protection** 模块)。
2. 单击**自我保护**，然后确保**自我保护**开关已启用。
3. 启用**密码保护**开关。
4. 在将打开的窗口中，复制卸载或修改受保护的适用于 Windows 的代理程序组件所需的密码。该密码是唯一的，关闭此窗口后将无法恢复它。如果丢失或忘记该密码，可以编辑保护计划并创建新密码。
5. 单击**关闭**。
6. 在**自我保护**窗格中，单击**完成**。
7. 保存该保护计划。

将为应用该保护计划的计算机启用密码保护。密码保护仅可用于适用于 Windows 的代理程序版本 *15.0.25851* 或更高版本。计算机必须处于联机状态。

可以将已启用密码保护的保护计划应用于运行 macOS 的计算机，但不会提供保护。无法将此类计划应用于运行 Linux 的计算机。

同样，无法将多个已启用密码保护的保护计划应用于同一台 Windows 计算机。要了解如何解决可能的冲突，请参阅解决计划冲突。

更改现有保护计划中的密码

1. 在保护计划中，展开**防病毒和反恶意软件保护**模块(即适用于 Cyber Backup 版本的 **Active Protection** 模块)。
2. 单击**自我保护**。
3. 单击**创建新密码**。
4. 在将打开的窗口中，复制卸载或修改受保护的适用于 Windows 的代理程序组件所需的密码。该密码是唯一的，关闭此窗口后将无法恢复它。如果丢失或忘记该密码，可以编辑保护计划并创建新密码。
5. 单击**关闭**。
6. 在**自我保护**窗格中，单击**完成**。
7. 保存该保护计划。

更改计算机的服务配额

首次将保护计划应用于计算机时，将自动指派服务配额。

根据受保护计算机的类型、其操作系统、所需的保护级别和配额可用性，将指派最合适的配额。如果贵组织中没有最合适的配额，则会指派次优配额。例如，如果最合适的配额是 **Web 托管服务器**，但它不可用，则会指派**服务器**配额。

配额指派示例：

- 将向运行 Windows Server 或 Linux 操作系统的物理机指派**服务器**配额。
- 将向运行 Windows 桌面操作系统的物理机指派**工作站**配额。
- 将向运行 Windows 10(已启用 Hyper-V 角色)的物理机指派**工作站**配额。
- 将向在虚拟桌面基础架构上运行且其保护代理程序安装在来宾操作系统(例如，适用于 Windows 的代理程序)中的桌面计算机指派**虚拟机**配额。当**虚拟机**配额不可用时，此类计算机还可以使用**工作站**配额。
- 将向在虚拟桌面基础架构上运行并在无代理程序模式(例如，由适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序)下备份的桌面计算机指派**虚拟机**配额。
- 将向 Hyper-V 或 vSphere 服务器指派**服务器**配额。
- 将向具有 cPanel 或 Plesk 的服务器指派 **Web 托管服务器**配额。如果 Web 托管服务器配额不可用，它还可以使用**虚拟机**或**服务器**配额，具体取决于运行 Web 服务器的计算机类型。
- 应用程序感知备份需要**服务器**配额，即使对于工作站也是如此。

可以稍后手动更改原始指派。例如，要将更高级的保护计划应用于同一台计算机，可能需要升级该计算机的服务配额。如果当前指派的服务配额不支持此保护计划所需的功能，则保护计划将失败。

或者，如果在已指派原始配额后购买了更多适用配额，可以更改服务配额。例如，**工作站**配额已指派给虚拟机。购买**虚拟机**配额后，可以手动将此配额指派给计算机，而不是原来的**工作站**配额。

还可以释放当前指派的服务配额，然后将此配额指派给其他计算机。

可以更改一台计算机的服务配额，也可以更改一组计算机的服务配额。

更改一台计算机的服务配额

1. 在 Cyber Protect 中控台中，转到**设备**。
2. 选择所需计算机，然后单击**详细信息**。
3. 在**服务配额**部分中，单击**更改**。
4. 在**更改配额**窗口中，选择服务配额或**无配额**，然后单击**更改**。

更改一组计算机的服务配额

1. 在 Cyber Protect 中控台中，转到**设备**。
2. 选择多台计算机，然后单击**指派配额**。
3. 在**更改配额**窗口中，选择服务配额或**无配额**，然后单击**更改**。

保护设置

要为 Cyber Protection 配置常规保护设置，请在 Cyber Protect 中控台中转到**设置** > **保护**。

组件的自动更新

默认情况下，所有代理程序都可连接到 Internet 并下载更新。

通过在环境中选择一个或多个代理程序并将“更新程序”角色指派给它们，管理员可以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。

更新程序代理程序会分发用于防病毒和防恶意软件保护、漏洞评估和修补程序管理的更新和修补程序，但不包括代理程序版本的更新。

注意
具有“更新”角色的代理程序可以下载并分发仅用于 Windows 第三方产品的修补程序。对于 Microsoft 产品，修补程序分发不受“更新”代理程序的支持。

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。

为“更新程序”角色准备计算机

1. 在计划启用“更新程序”角色的代理程序计算机上，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 安克诺斯 Agent Core Service。
3. 重新启动防火墙服务。

如果不应用这些规则并且启用了防火墙,则对等代理程序将从云中下载更新。

将“更新器”角色指派给保护代理程序

1. 在 Cyber Protect 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。

点对点更新的工作方式如下。

1. 具有“更新器”角色的代理程序按预定检查服务提供商提供的索引文件,以更新核心组件。
2. 具有“更新器”角色的代理程序开始下载更新并将其分发给所有代理程序。

可以将“更新程序”角色指派给环境中的多个代理程序。这样,如果具有“更新程序”角色的代理程序脱机,具有此角色的其他代理程序可以充当定义更新的源。

按预定更新 Cyber Protection 定义

在 **预定** 选项卡中,可以为自动更新以下每个组件的 Cyber Protection 定义设置预定:

- 反恶意软件
- 漏洞评估
- 修补程序管理

要更改定义更新设置,请导航到**设置** > **保护** > **保护定义更新** > **预定**。

预定类型:

- **每天** - 定义周几更新定义。
  开始时间 - 选择何时更新定义。
- **每小时** - 定义用于执行定义更新的更详细每小时预定。
  运行频率 – 定义运行定义更新的周期。
  从...至 – 指定将执行定义自动定义更新的特定时间范围。

按需要更新 Cyber Protection 定义

要按需要更新特定计算机的 Cyber Protection 定义

1. 在 Cyber Protect 中控台中,转到**设置** > **代理程序**。
2. 选择要更新保护定义的计算机,然后单击**更新定义**。

缓存存储

缓存数据的位置如下所示:

- 在 Windows 计算机上：`C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- 在 Linux 计算机上：`/opt/acronis/var/atp-downloader/Cache`
- 在 macOS 计算机上：`/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

要更改缓存存储设置，请导航到**设置** > **保护** > **保护定义更新** > **缓存存储**。

在**过期的更新文件和修补程序管理数据**中，指定在什么时间过后删除缓存数据。

代理程序的最大缓存存储大小 (GB)：

- **更新器角色** – 定义具有更新器角色的计算机上缓存的存储大小。
- **其他角色** - 定义其他计算机上缓存的存储大小。

注意
Cyber Protection 将收集检测到恶意软件的样本以供进行额外分析，以便我们能够改进软件。通过禁用**收集恶意软件样本并将其上传到 CPOC** 开关，可以随时在**保护**选项卡中更改此设置。

您环境中已安装的 Cyber Protection 服务

Cyber Protection 将安装以下部分或全部服务，具体取决于您使用的 Cyber Protection 选项。

Windows 中已安装的服务

服务名称	目的
安克诺斯 Managed Machine Service	提供备份、恢复、复制、保留、验证功能
安克诺斯 Scheduler2 Service	执行针对特定事件的预定任务
安克诺斯 Active Protection Service	提供针对勒索软件的保护
安克诺斯 Cyber Protection Service	提供反恶意软件保护

macOS 中已安装的服务

服务名称和位置	目的
`/Library/LaunchDaemons/com.acronis.aakore.plist`	提供代理程序和管理组件之间的通信服务
`/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist`	提供恶意软件检测
`/Library/LaunchDaemons/com.acronis.mms.plist`	提供备份和恢复功能
`/Library/LaunchDaemons/com.acronis.schedule.plist`	执行预定任务

保存代理程序日志文件

您可以将代理程序日志保存到 .zip 文件。如果备份因未知原因失败，此文件将帮助技术支持人员识别问题。

默认情况下，日志中的信息针对最近三天进行优化，但您可以更改此时间段。

在线工作负载

收集代理程序日志

1. 请执行以下任一操作：
   - 在**“设备”**下，选择要从中收集日志的工作负载，然后单击**“活动”**。
   - 在**“设置”** > **“代理程序”**下，选择要从中收集日志的工作负载，然后单击**“详细信息”**。
2. [可选] 要更改包含系统信息的默认时间段，请单击**收集系统信息**按钮旁边的箭头，然后选择时间段。
3. 单击**收集系统信息**。
4. 如果 Web 浏览器提示您，请指定保存文件的位置。

离线工作负载和可启动媒体

收集代理程序日志

- 请参阅此 知识库文章 中的步骤。

本地管理服务器的许可证管理

有关如何激活本地管理服务器或如何为其分配许可证的详细信息，请参阅 Cyber Protect 用户指南中的管理许可证部分。

按照计划开展工作

了解计划

注意
某些功能是否可用取决于您帐户启用的服务项目。

计划是一组配置和规则，您可以将其应用于一个或多个工作负载以实现不同的目标，例如备份工作负载、保护工作负载免受恶意软件的侵害、监视工作负载的性能等。

计划由可以启用或禁用的模块组成。每个模块包含与特定功能相关的设置。

创建的所有计划均可在**"管理"**选项卡上看到。

计划	描述
保护计划	保护工作负载上的数据。 保护计划由以下模块组成： • 备份 • "实施灾难恢复"(第 655 页) • 防病毒和反恶意软件保护 • Endpoint Detection and Response (EDR) • URL 过滤 • Windows Defender Antivirus • Microsoft Security Essentials • 漏洞评估 • 修补程序管理 • 数据保护地图 • 设备控制 • Advanced Data Loss Prevention 有关保护计划的更多信息，请参阅"保护计划和模块"(第 192 页)。
远程管理计划	在托管工作负载上启用远程桌面和协助功能。有关更多信息，请参阅"远程管理计划"(第 920 页)。
脚本计划	启用在多个工作负载上执行脚本、计划脚本执行以及配置其他脚本设置。有关详细信息，请参阅"脚本计划"(第 344 页)。
监视计划	监视托管工作负载的性能、硬件、软件、系统和安全参数。有关更多信息，请参阅 "监视计划"(第 976 页)。
云应用程序备份	通过在云中运行的代理备份在云中运行的应用程序，并使用云存储作为备份位置。有关更多信息，请参阅"云应用程序的备份计划"(第 211 页)
备份扫描计划	扫描备份中是否存在恶意软件(包括勒索软件)。

计划	描述
VM 复制	扫描备份中是否存在恶意软件(包括勒索软件)。有关详细信息,请参阅"虚拟机的复制"(第 611 页)。
验证	验证备份并确认是否可以恢复备份中的数据。有关详细信息,请参阅"验证"(第 201 页)。
清理	根据保留规则删除过期的备份。此计划仅适用于代理和工作负载,不适用于云到云备份。有关更多信息,请参阅"清理"(第 207 页)。
转换到虚拟机	该计划仅适用于磁盘级备份。 检查备份是否包括系统卷并包含操作系统启动所需的所有信息,以确保虚拟机可以自行启动。有关详细信息,请参阅"转换为虚拟机"(第 207 页)。
备份复制	将备份复制到另一个位置。有关详细信息,请参阅"备份复制"(第 199 页)。

内建计划

内置计划是预先配置的一些最常用或推荐设置的计划。内置计划可供立即选择。无法更改内置计划,但在将内置计划应用于工作负载后,您可以编辑设置。

内置计划适用于以下计划类型:保护计划、监视计划和远程管理计划。

内置保护计划

下表提供了有关内置保护计划的更多信息。

模块和设置	内置保护计划		
	基本保护	**扩展保护**	**全面防护**
	最大程度地减少停机时间和数据丢失,轻松恢复,RPO 较短且易于维护	**第二层保护:业务连续性、主动降低安全风险和合规性**	**第三级保护:业务连续性、接近零的 RPO、主动降低安全风险、防止数据泄露和合规性**
备份	在(O)	在(O)	在(O)
备份内容 要备份的项目	整台计算机	整台计算机	整台计算机
连续数据保护(CDP)	已禁用	已禁用	已启用
备份位置	云存储	云存储	云存储

模块和设置	内置保护计划		
	基本保护	**扩展保护**	**全面防护**
	最大程度地减少停机时间和数据丢失，轻松恢复，RPO 较短且易于维护	**第二层保护：业务连续性、主动降低安全风险和合规性**	**第三级保护：业务连续性、接近零的 RPO、主动降低安全风险、防止数据泄露和合规性**
预定	周一至周五每天中午 12:00 其他启用选项和启动条件： • 如果计算机关闭，则在计算机启动时运行遗漏的任务 • 从睡眠或休眠模式唤醒以启动预定备份 • 节省电池电量不在使用电池时启动 • 不在使用按流量计费的连接时启动	周一至周五上午 12:00 其他启用选项和启动条件： • 如果计算机关闭，则在计算机启动时运行遗漏的任务 • 从睡眠或休眠模式唤醒以启动预定备份 • 节省电池电量不在使用电池时启动 • 不在使用按流量计费的连接时启动	周一至周五上午 12:00 其他启用选项和启动条件： • 如果计算机关闭，则在计算机启动时运行遗漏的任务 • 从睡眠或休眠模式唤醒以启动预定备份 • 节省电池电量不在使用电池时启动 • 不在使用按流量计费的连接时启动
备份方案	始终增量	始终增量	始终增量
保留期限	保留所有	保留所有备份 90 天	保留所有备份 90 天

模块和设置	内置保护计划		
	基本保护	**扩展保护**	**全面防护**
	最大程度地减少停机时间和数据丢失，轻松恢复，RPO 较短且易于维护	**第二层保护：业务连续性、主动降低安全风险和合规性**	**第三级保护：业务连续性、接近零的 RPO、主动降低安全风险、防止数据泄露和合规性**
	备份 90 天		
备份选项	默认选项	默认选项，外加： • 性能和备份窗口（绿色组）： CPU 优先级：低 输出速度：50%	默认选项，外加： • 性能和备份窗口（绿色组）： CPU 优先级：低 输出速度：50%
EDR	关	关	在(O)
防病毒和反恶意软件保护	在(O)	在(O)	在(O)
Active Protection	在(O)	在(O)	在(O)
高级防恶意软件	在(O)	在(O)	在(O)
网络文件夹保护	在(O)	在(O)	在(O)
服务器端保护	关	关	关
自我保护	在(O)	在(O)	在(O)
Cryptomining 进程检测	在(O)	在(O)	在(O)
隔离	在 30 天之后删除隔离文件	在 30 天之后删除隔离文件	在 30 天之后删除隔离文件
行为引擎	隔离	隔离	隔离
漏洞利用预防	通知并停止过程	通知并停止过程	通知并停止过程

模块和设置	内置保护计划		
	基本保护	**扩展保护**	**全面防护**
	最大程度地减少停机时间和数据丢失，轻松恢复，RPO 较短且易于维护	**第二层保护：业务连续性、主动降低安全风险和合规性**	**第三级保护：业务连续性、接近零的 RPO、主动降低安全风险、防止数据泄露和合规性**
实时保护	隔离	隔离	隔离
预定扫描	快速扫描：隔离 周日至周六晚上 8:00 完整扫描：隔离 周三和周五晚上 9 点 其他启用选项和启动条件： 从睡眠或休眠模式唤醒以启动预定备份	快速扫描：隔离 周日至周六晚上 8:00 完整扫描：隔离 周三和周五晚上 9 点 其他启用选项和启动条件： 从睡眠或休眠模式唤醒以启动预定备份	快速扫描：隔离 周日至周六晚上 8:00 完整扫描：隔离 周三和周五晚上 9 点 其他启用选项和启动条件： 从睡眠或休眠模式唤醒以启动预定备份
排除	无	无	无
URL 过滤	关	在(O)	在(O)
恶意网站访问	阻止	阻止	阻止
要过滤的类别	默认选项	默认选项	默认选项
排除	无	无	无
Microsoft Defender Antivirus	关	关	关

模块和设置	内置保护计划		
	基本保护	**扩展保护**	**全面防护**
	最大程度地减少停机时间和数据丢失，轻松恢复，RPO 较短且易于维护	**第二层保护：业务连续性、主动降低安全风险和合规性**	**第三级保护：业务连续性、接近零的 RPO、主动降低安全风险、防止数据泄露和合规性**
防火墙管理	关	在(O)	在(O)
Microsoft Security Essentials	关	关	关
漏洞评估	在(O)	在(O)	在(O)
漏洞评估范围	Microsoft 产品、Windows 第三方产品、Apple 产品、macOS 第三方产品、扫描 Linux 包	Microsoft 产品、Windows 第三方产品、Apple 产品、macOS 第三方产品、扫描 Linux 包	Microsoft 产品、Windows 第三方产品、Apple 产品、macOS 第三方产品、扫描 Linux 包
预定	上午 11:00 (仅限周三和周五)	上午 11:00(仅限周三和周五)	上午 11:00(仅限周三和周五)
修补程序管理	在(O)	在(O)	在(O)
Microsoft 产品	所有更新	所有更新	所有更新
Windows 第三方产品	所有更新	所有更新	所有更新
预定	中午 12:30，仅限周三和周五	中午 12:30，仅限周三和周五	中午 12:30，仅限周三和周五
更新前备份	在(O)	在(O)	在(O)

模块和设置	内置保护计划		
	基本保护	**扩展保护**	**全面防护**
	最大程度地减少停机时间和数据丢失，轻松恢复，RPO 较短且易于维护	**第二层保护：业务连续性、主动降低安全风险和合规性**	**第三级保护：业务连续性、接近零的 RPO、主动降低安全风险、防止数据泄露和合规性**
数据保护地图	关	关	在(O)
扩展名和例外规则	–	–	默认选项(要检测的 66 个扩展名)
预定	–	–	周一至周五下午 03:40
设备控制	关	关	关
访问设置	已允许:所有	已允许:所有	已允许:所有
设备类型允许列表	允许 1 个 USB HID(鼠标、键盘等)	允许 1 个 USB HID(鼠标、键盘等)	允许 1 个 USB HID(鼠标、键盘等)
USB 设备允许列表	空	空	空
排除	无	无	无
数据丢失预防	关	关	关
模式	–	–	–
高级设置	–	–	–
Disaster Recovery	关	关	关

有关保护计划的更多信息，请参阅 "保护计划和模块"(第 192 页)。

内置监视计划

下表提供了有关内置监视计划的更多信息。

名称	描述	已启用监视器
适用于 Windows 的推荐	监视 Windows 计算机的运行状况和性能	此计划中启用了以下 13 个监视器： • 防恶意软件状态 • 自动运行功能状态 • CPU 温度 • CPU 使用情况 • 磁盘空间 • 磁盘传输速率 • 登录失败 • 防火墙状态 • GPU 温度 • 上次系统重新启动 • 内存使用情况 • 网络使用率 • Windows 更新状态
适用于 macOS 的推荐	监视 macOS 计算机的运行状况和性能	此计划中启用了以下 10 个监视器： • 防恶意软件状态 • CPU 温度 • CPU 使用情况 • 磁盘空间 • 磁盘传输速率 • 防火墙状态 • GPU 温度 • 上次系统重新启动 • 内存使用情况 • 网络使用率
适用于服务器的推荐	监视 Windows 服务器的运行状况和性能	此计划中启用了以下 20 个监视器： • 防恶意软件状态 • CPU 温度，2 个监视器： 80 度，10 分钟，警告 90 度，10 分钟，关键 • CPU 使用率，3 个监视器： 少于 20%，10 分钟，信息 超过 80%，10 分钟，警告 超过 90%，10 分钟，关键 • 磁盘空间，2 个监视器： 少于 20%，30 分钟，警告

名称	描述	已启用监视器
		少于 10%, 30 分钟, 严重 • 磁盘传输速率 • 登录失败, 3 个监视器: 5 次尝试, 1 小时, 信息 10 次尝试, 1 小时, 警告 20 次尝试, 1 小时, 关键 • 防火墙状态 • 硬件更改 • 安装的软件 • 内存使用情况, 3 个监视器: 少于 20%, 10 分钟, 信息 超过 80%, 10 分钟, 警告 超过 90%, 10 分钟, 关键 • 网络使用率 • Windows 更新状态

有关监视计划的更多信息, 请参阅 "监视计划"(第 976 页)。

内置远程管理计划

下表提供了有关内置远程管理计划的更多信息。

名称	描述	设置
必备远程桌面	启用远程桌面和文件传输功能	连接协议 **允许通过 NEAR 连接**:开启 NEAR 安全设置 • **当用户断开与中控台会话的连接时锁定工作负载**:关闭 • **一次只允许一个用户连接 NEAR 或进行文件传输**:关闭 • **允许工作负载管理员连接到任何会话**:开启 • **允许系统会话创建**:关闭 • **允许剪贴板同步**:开启 **允许通过 RDP 连接**:开启 **允许通过 Apple 屏幕共享进行连接**:关闭 安全性设置 • **显示工作负载是否受远程控制**:开启 • **请求用户允许对工作负载进行截图**:开启 工作负载管理

名称	描述	设置
		• **文件传输**:开启 • **截图传输**:关闭 显示设置 • **使用桌面重复数据删除进行桌面捕获**:开启 • **使用 OpenCL 加速**:开启 • **使用硬件 H.264 编码**:开启 工具箱 **显示最后登录的用户**:关闭

有关远程管理计划的详细信息,请参阅 "远程管理计划"(第 920 页)。

默认计划

默认计划是预先选择的计划,并且在计划列表和计划选择字段中首先显示。每个受支持的计划类型每个租户一次只能有一个默认计划。

您将看到的计划列表和默认计划取决于您所使用的 保护 中控台的级别。

例如,如果您在合作伙伴级别使用中控台,则会看到在合作伙伴、客户和单位级别创建的计划,但默认计划将是在合作伙伴级别设置为默认的计划。如果您在客户级别使用中控台,则不会看到在合作伙伴级别创建的任何计划,包括合作伙伴级别的默认计划。同样,如果您在单位级别使用中控台,则不会看到在合作伙伴或客户级别创建的任何计划,包括这些级别的默认计划。

在将另一个计划设为默认计划之前,无法删除默认计划。

默认计划支持以下计划类型:保护计划、监视计划和远程管理计划。

将计划设置为默认计划

您可以将支持的计划类型(保护计划、监视计划或远程管理计划)中的一个计划设置为默认计划。

注意
对于分配了保护服务的只读管理员角色的用户,此功能不可用。

保护计划

先决条件

至少为您的租户创建了一个保护计划。有关详细信息,请参阅"创建保护计划"(第 192 页)。

若要将保护计划设置为默认计划

1. 在**保护计划**屏幕上,找到要设置为默认计划的计划,然后单击它。
2. 单击**"设为默认值"**。
3. 在确认窗口中,单击**"设置"**。
   在**保护计划**屏幕上,计划名称旁边会出现**默认**标签。

远程管理计划

先决条件

- 已为您的用户帐户启用双重身份验证。
- 至少为您的租户创建了一个远程管理计划。有关详细信息，请参阅"创建远程管理计划"(第 921 页)。

将远程管理计划设置为默认

1. 在**远程管理计划**屏幕上，找到您想要设置为默认的计划。
2. 在同一行中，单击**更多操作**图标。
3. 单击**"设为默认值"**。
4. 在确认窗口中，单击**"设置"**。
   在**远程管理计划**屏幕上，计划名称旁边会出现**默认**标签。

监视计划

先决条件

- 已为您的用户帐户启用双重身份验证。
- 至少为您的租户创建了一个监视计划。有关详细信息，请参阅 "创建监视计划"(第 976 页)。

将监视计划设置为默认计划

1. 在**监视计划**屏幕上，找到要设置为默认计划的计划。
2. 在同一行中，单击**更多操作**图标。
3. 单击**"设为默认值"**。
4. 在确认窗口中，单击**"设置"**。
   在**监视计划**屏幕上，计划名称旁边会出现**默认**标签。

收藏计划

收藏夹中的计划将显示在默认计划后的计划列表的顶部。如果您希望确保在组织有很多计划时仍使计划可见且易于查找，则可以将计划添加到收藏夹。

您将看到的计划列表和收藏计划取决于您所使用的 保护 中控台的级别。

例如，如果您在合作伙伴级别使用中控台，则会看到在所有级别(合作伙伴、客户和单位)创建的计划，但收藏计划将是在合作伙伴级别添加为收藏夹的计划。如果您在客户级别使用中控台，则不会看到在合作伙伴级别创建的任何计划，包括合作伙伴级别的收藏计划。同样，如果您在单位级别使用中控台，则不会看到在合作伙伴或客户级别创建的任何计划，包括这些级别的收藏计划。

以下计划类型支持收藏计划：保护计划、监视计划和远程管理计划。

将计划设为收藏

每个租户每个支持的计划类型(保护计划、监视计划或远程管理计划)最多可以设置 10 个收藏计划。

注意
对于分配了保护服务的只读管理员角色的用户，此功能不可用。

保护计划

先决条件

至少为您的租户创建了一个保护计划。有关详细信息，请参阅"创建保护计划"(第 192 页)。

将保护计划设为收藏

1. 在**保护计划**屏幕上，单击要设置为收藏的计划。
2. 单击**"设为收藏"**。
   在**保护计划**屏幕上，计划名称旁边会出现一个星形图标。

远程管理计划

先决条件

- 已为您的用户帐户启用双重身份验证。
- 至少为您的租户创建了一个远程管理计划。有关详细信息，请参阅"创建监视计划"(第 976 页)。

将远程管理计划设置为收藏

1. 在**远程管理计划**屏幕上，找到您想要添加为收藏的计划。
2. 在计划行中，单击**更多操作**图标。
3. 单击**添加到收藏夹**。
   在**远程管理计划**屏幕上，计划名称旁边会出现一个星形图标。

监视计划

先决条件

- 已为您的用户帐户启用双重身份验证。
- 至少为您的租户创建了一个管理计划。有关详细信息，请参阅"创建监视计划"(第 976 页)。

若要若要将监视计划设为收藏

1. 在**监视计划**屏幕上，找到您想要设置为收藏的计划。
2. 在计划行中，单击**更多操作**图标。
3. 单击**添加到收藏夹**。
   在**监视计划**屏幕上，计划名称旁边会出现一个星形图标。

从收藏夹中删除计划

您可以从收藏夹列表中移除收藏的保护计划、监视计划和远程管理计划。

注意
对于分配了保护服务的只读管理员角色的用户，此功能不可用。

保护计划

先决条件

至少有一个保护计划已被设为您租户的收藏。

若要从收藏夹中移除保护计划

1. 在**保护计划**屏幕上，单击要从收藏夹中移除的计划。
2. 单击**"从收藏夹中移除"**。

远程管理计划

先决条件

- 已为您的用户帐户启用双重身份验证。
- 至少有一个远程管理计划已被设为您的租户的收藏计划。

若要从收藏夹中移除远程管理计划

1. 在**远程管理计划**屏幕上，找到要从收藏夹中移除的计划。
2. 在计划行中，单击**更多操作**图标。
3. 单击**"从收藏夹中移除"**。

监视计划

先决条件

- 已为您的用户帐户启用双重身份验证。
- 至少有一个监视计划已被设为您的租户的收藏。

若要从收藏夹中移除监视计划

1. 在**监视计划**屏幕上，找到要从收藏夹中移除的计划。
2. 在计划行中，单击**更多操作**图标。
3. 单击**"从收藏夹中移除"**。

设置收藏计划的顺序

您可以设置显示设为收藏夹的保护计划的顺序，以便在计划选择字段中显示。

先决条件

至少设置了两个计划为收藏夹。

若要设置收藏计划的顺序

1. 在 Cyber Protect 中控台计划屏幕中，转到**管理** > **保护计划**。
2. 单击**管理收藏夹**。
3. 拖放计划以设置它们在计划选择字段中的显示顺序。

注意
若要拖动计划，请单击计划名称前的拖动区域。

4. 单击**保存**。

保护计划和模块

为了保护您的数据，您必须创建保护计划，然后将其应用到您的工作负载。

保护计划由不同的保护模块组成。启用您需要的模块并配置其设置，以创建满足您特定需求的保护计划。

以下模块可用：

- 备份。将数据源备份到本地或云存储。
- "实施灾难恢复"(第 655 页)。在云站点中启动计算机的精确副本，并将工作负载从受损的原始计算机切换到云中的恢复服务器。
- 防病毒和防恶意软件保护。使用内置的防恶意软件解决方案检查工作负载。
- Endpoint Detection and Response (EDR).Detects suspicious activity on the workload, including attacks that have gone unnoticed, and generates incidents to help you understand how an attack happened and how to prevent it from happening again.
- URL 过滤。通过阻止对恶意 URL 和可下载内容的访问，来保护计算机免受来自 Internet 的威胁的侵害。
- Windows Defender Antivirus。管理 Windows Defender Antivirus 的设置来保护您的环境。
- Microsoft Security Essentials。管理 Microsoft Security Essentials 的设置来保护您的环境。
- 漏洞评估。检查计算机上安装的 Windows、Linux、macOS、Microsoft 第三方产品和 macOS 第三方产品，并向您提供有关漏洞的通知。
- 修补程序管理。为计算机上的 Windows、Linux、macOS、Microsoft 第三方产品和 macOS 第三方产品安装修补程序和更新，以解决检测到的漏洞。
- 数据保护地图。发现数据以监视重要文件的保护状态。
- 设备控制。指定允许或禁止用户使用您计算机上的设备。
- Advanced Data Loss Prevention。将根据数据流策略，防止通过外围设备(例如，打印机或可移动存储)或内外网络传输泄露敏感数据。

创建保护计划

可以通过以下方式创建保护计划：

- 在**设备**选项卡上。选择一个或多个要保护的工作负载，然后为它们创建保护计划。
- 在**管理>保护计划**选项卡上。创建保护计划，然后选择一个或多个要应用该计划的工作负载。

当创建保护计划时，仅会显示适用于您的工作负载类型的模块。

可以将保护计划应用于多个工作负载。还可以将多个保护计划应用于同一个工作负载。要了解有关可能冲突的详细信息，请参阅"解决计划冲突"(第 197 页)。

创建保护计划

设备

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 选择要保护的工作负载，然后单击**保护**。
3. [如果已有应用的计划] 单击**添加计划**。
4. 依次单击**创建计划** > **保护**。
   保护计划面板会打开。
5. [可选] 若要重命名保护计划，请单击铅笔图标，然后输入新名称。
6. [可选] 要启用或禁用计划中的模块，请切换模块名称旁边的开关。
7. [可选] 要配置模块，请单击该模块以将其展开，然后根据需要更改设置。
8. 准备就绪后，单击**创建**。

注意
若要创建加密保护计划，请指定加密密码。有关更多信息，请参阅"加密"(第 391 页)。

管理 > 保护计划

1. 在 Cyber Protect 中控台中，转到**管理** > **保护计划**。
2. 单击**创建计划**。
   保护计划的模板即会打开。
3. [可选] 若要重命名保护计划，请单击铅笔图标，然后输入新名称。
4. [可选] 要启用或禁用计划中的模块，请切换模块名称旁边的开关。
5. [可选] 要配置模块，请单击该模块以将其展开，然后根据需要更改设置。
6. [可选] 要选择要应用计划的工作负载，请单击**添加设备**。

注意
您可以创建计划而不将其应用于任何工作负载。您可以稍后通过编辑计划来添加工作负载。有关如何将工作负载添加到计划的更多信息，请参阅 "将保护计划应用于工作负载"(第 194 页)。

7. 准备就绪后，单击**创建**。

注意
若要创建加密保护计划，请指定加密密码。有关更多信息，请参阅"加密"(第 391 页)。

要手动运行模块(例如**备份**、**防病毒和防恶意软件保护**、**漏洞评估**、**修补程序管理**或**数据保护地图**)，请单击**立即运行**。

观看操作方法视频：创建第一个保护计划。

有关灾难恢复模块的更多信息，请参阅 "创建灾难恢复保护计划"(第 660 页)。

有关设备控制模块的更多信息，请参见 "使用设备控制模块"(第 302 页)。

保护计划的操作

在创建保护计划后，可以对其执行以下操作：

- 将计划应用于工作负载或设备组。
- 重命名计划。
- 编辑计划。

  可以启用和禁用计划中的模块，并更改其设置。
- 启用或禁用计划。

  禁用的计划不会在应用该计划的工作负载上运行。

  对于打算以后使用相同计划保护同一工作负载的管理员来说，此操作非常方便。该计划不会从工作负载中撤消，可以通过重新启用该计划来快速恢复保护。
- 从工作负载中撤消计划。

  撤消的计划不会再应用于工作负载。

  对于不再需要使用相同计划快速保护同一工作负载的管理员来说，此操作非常方便。要恢复已撤消计划提供的保护，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相应工作负载。
- 停止计划。

  此操作会停止已应用该计划的所有工作负载上所有正在运行的备份操作。备份将根据计划预定重新开始。

  防恶意软件扫描不受此操作影响，将按预定中的配置继续执行。
- 克隆计划。

  可以创建现有计划的精确副本。该新计划不会指派给任何工作负载。
- 导出和导入计划。

  可以将计划导出为 JSON 文件，之后可以将其重新导入。因此，无需手动创建新计划并配置其设置。

  注意

  可以导入在 Cyber Protection 9.0(于 2020 年 3 月发布) 及更高版本中创建的保护计划。使用早期版本创建的计划与 Cyber Protection 9.0 及更高版本不兼容。
- 查看计划的详细信息。
- 查看与计划相关的活动和警报。
- 删除计划。

将保护计划应用于工作负载

要保护工作负载，必须对其应用保护计划。

可以从**设备**选项卡和**管理** > **保护计划**选项卡应用计划。

设备

1. 选择一个或多个要保护的工作负载。
2. 单击**保护**。
3. [如果另一个保护计划已应用于选定工作负载] 单击**添加计划**。
4. 可用保护计划的列表即会显示。
5. 选择要应用的保护计划，然后单击**应用**。

管理 > 保护计划

1. 在 Cyber Protect 中控台中，转到**管理** > **保护计划**。
2. 选择要应用的保护计划。
3. 单击**编辑**。
4. 单击**管理设备**。
5. 在**设备**窗口中，单击**添加**。
6. 选择要应用计划的工作负载，然后单击**添加**。
7. 在**设备**窗口中，单击**完成**。
8. 在保护计划面板中，单击**保存**。

要了解如何将保护计划应用于设备组，请参阅 "将计划应用于组"(第 301 页) 。

编辑保护计划

当编辑计划时，可以启用和禁用计划中的模块，并更改其设置。

可以为应用保护计划的所有工作负载或仅为选定工作负载编辑保护计划。

您可以从**"设备"**选项卡和**"管理"> "保护计划"**选项卡编辑计划。

设备

1. 选择一个或多个已应用计划的工作负载。
2. 单击**保护**。
3. 选择要编辑的保护计划。
4. 单击计划名称旁边的省略号图标 (...)，然后单击**编辑**。
5. 单击要编辑的模块，然后根据需要配置其设置。
6. 单击**保存**。
7. [如果尚未选择已应用计划的所有工作负载] 选择编辑范围：
   - 要编辑已应用计划的所有工作负载的计划，请单击**将更改应用于此保护计划(这将影响其他设备)**。
   - 要仅更改选定工作负载的计划，请单击**仅为选定设备创建新保护计划**。
     因此，现有计划将从选定工作负载中撤消。将创建一个包含您配置的设置的新保护计划，并将其应用于这些工作负载。

管理 > 保护计划

1. 在 Cyber Protect 中控台中，转到**管理** > **保护计划**。
2. 选择要编辑的保护计划。
3. 单击**编辑**。

4. 单击要编辑的模块，然后根据需要配置其设置。
5. 单击**保存**。

注意
从**"管理" > "保护计划"**选项卡编辑计划会影响应用该计划的所有工作负载。

撤消保护计划

当撤消计划时，将从一个或多个工作负载中删除该计划。该计划仍会保护应用它的其他工作负载。

您可以从**"设备"**选项卡和**"管理" > "保护计划"**选项卡撤销计划。

设备

1. 选择要从中撤消计划的工作负载。
2. 单击**保护**。
3. 选择要撤消的保护计划。
4. 单击计划名称旁边的省略号图标 (...)，然后单击**撤消**。

管理 > 保护计划

1. 在 Cyber Protect 中控台中，转到**管理 > 保护计划**。
2. 选择要撤消的保护计划。
3. 单击**编辑**。
4. 单击**管理设备**。
5. 在**设备**窗口中，选择要从中撤消计划的工作负载。
6. 单击**删除**。
7. 在**设备**窗口中，单击**完成**。
8. 在保护计划模板中，单击**保存**。

启用或禁用保护计划

启用的计划处于活动状态，并在应用该计划的工作负载上运行。禁用的计划处于非活动状态 - 它仍应用于工作负载，但不会在工作负载上运行。

当从**设备**选项卡启用或禁用保护计划时，您的操作仅会影响选定工作负载。

从**管理 > 保护计划**选项卡启用或禁用保护计划时，您的操作会影响已应用该计划的所有工作负载。此外，还可以启用或禁用多个保护计划。

设备

1. 选择要禁用其计划的工作负载。
2. 单击**保护**。
3. 选择要禁用的保护计划。
4. 单击计划名称旁边的省略号图标 (...)，然后相应单击**启用**或**禁用**。

管理 > 保护计划

1. 在 Cyber Protect 中控台中，转到**管理** > **保护计划**。
2. 选择一个或多个要启用或禁用的保护计划。
3. 单击**编辑**。
4. 相应单击**启用**或**禁用**。

注意
此操作不会影响已处于目标状态的保护计划。例如，如果您的选择包括已启用和已禁用的计划，并单击**启用**，则会启用所有选定计划。

删除保护计划

当删除计划时，它会从所有工作负载中撤消，并从 Cyber Protect 中控台中删除。

可以从**设备**选项卡和**管理** > **保护计划**选项卡删除计划。

设备

1. 选择已应用要删除的保护计划的任何工作负载。
2. 单击**保护**。
3. 选择要删除的保护计划。
4. 单击计划名称旁边的省略号图标 (...)，然后单击**删除**。

管理 > 保护计划

1. 在 Cyber Protect 中控台中，转到**管理** > **保护计划**。
2. 选择要删除的保护计划。
3. 单击**删除**。
4. 通过选中**我确认删除计划**复选框来确认您的选择，然后单击**删除**。

解决计划冲突

可以将多个保护计划应用于同一个工作负载。例如，可以应用一个仅启用并配置**防病毒和防恶意软件**模块的保护计划，以及应用另一个仅启用并配置**备份**模块的保护计划。

可以合并已启用不同模块的保护计划。还可以合并多个仅启用**备份**模块的保护计划。但是，如果在多个计划中启用了任何其他模块，则会发生冲突。要应用计划，首先必须解决冲突。

新计划与现有计划之间的冲突

如果新计划与现有计划冲突，可以通过以下方式之一解决冲突：

- 创建新计划、应用它，然后禁用与新计划冲突的现有计划。
- 创建新计划，然后禁用它。

单个计划和组计划之间的冲突

如果单个保护计划与应用于设备组的组计划冲突，可以通过以下方式之一解决冲突：

- 从设备组中删除工作负载，然后对设备组应用单个保护计划。
- 编辑现有组计划，或将一个新组计划应用于设备组。

许可问题

保护计划模块可能要求为受保护的工作负载指派特定的服务配额。如果指派的服务配额不合适，您将无法运行、更新或应用已启用相应模块的保护计划。

要解决许可证问题，请执行以下操作之一：

- 禁用当前指派的服务配额不支持的模块，然后继续使用保护计划。
- 手动更改指派的服务配额。要了解如何执行此操作，请参阅 "更改计算机的服务配额"(第 174 页)。

托管控制面板集成的单独保护计划

在使用 DirectAdmin、cPanel 或 Plesk 的 Web 托管服务器上启用托管控制面板集成后，Cyber Protection 服务会自动在您的用户帐户下为每个工作负载创建一个单独保护计划。此保护计划与启动保护计划创建的特定工作负载相关联，无法吊销或指派给其他工作负载。

要停止使用单独保护计划，可以从 Cyber Protect 中控台删除它。可以通过单独保护计划名称旁边的 标志来识别它们。

如果希望一个保护计划可以保护多个使用托管控制面板集成的 Web 托管服务器，可以在 Cyber Protect 中控台中创建一个常规保护计划，然后将这些工作负载指派给它。然而，对多个 Web 托管控制面板共享的保护计划的任何修改只能在 Cyber Protect 中控台中进行，而不能在集成中进行。

脱离主机的数据保护计划

注意
此功能适用于将**Advanced Backup – 服务器**或**Advanced Backup – NAS** 配额作为 Advanced Backup 包的一部分启用的客户租户。

复制、验证和清理通常由执行备份的保护代理程序执行。即使备份过程完成后，这也会给运行代理程序的计算机带来额外的负载。要卸载计算机，您可以创建脱离主机数据保护计划，即复制、验证、清理和转换到虚拟机的单独计划。

通过脱离主机数据保护计划，可以执行以下操作：

- 为备份和脱离主机数据保护操作选择不同的代理代理程序
- 将脱离主机的数据处理操作安排在非高峰时段，以最大程度地减少网络带宽消耗
- 如果您不想安装用于脱离主机数据处理的专用代理程序，请在非工作时间安排脱离主机数据处理操作

注意
脱离主机数据处理计划根据安装保护代理程序的计算机的时间设置(包括时区)运行。对于虚拟设备(例如,Agent for VMware 或 Agent for Scale Computing HC3),您可以在代理程序的图形用户界面中配置时区。

备份复制

注意
此功能适用于将**Advanced Backup – 服务器**或**Advanced Backup – NAS** 配额作为 Advanced Backup 包的一部分启用的客户租户。

备份复制是将备份复制到另一个位置。作为一种脱离主机数据处理操作,它是在备份复制计划中配置的。

备份复制也可以是保护计划的一部分。有关此选项的详细信息,请参阅 "复制"(第 389 页)。

创建备份复制计划

要以脱离主机数据处理操作的方式复制备份,请创建备份复制计划。

创建备份复制计划

1. 在 Cyber Protect 中控台中,依次单击**管理** > **备份复制**。
2. 单击**创建计划**。
3. 在**代理程序**中,选择将执行复制的代理程序。
   可以选择有权访问源位置和复制位置的任何代理程序。
4. 在**要复制的项目**中,选择要复制的存档或备份位置。
   要在存档和位置之间切换,请使用右上角的**位置/备份**开关。
   如果选择多个加密存档,则它们的加密密码必须相同。对于使用不同加密密码的存档,请创建单独的计划。
5. 在**目标**中,指定复制位置。
6. 在**复制方法**中,选择要复制的备份(也称为恢复点)。
   可使用以下选项:
   - **所有备份**
   - **仅完整备份**
   - **仅上次备份**

   有关这些选项的详细信息,请参阅 "复制内容"(第 200 页)。
7. 在**预定**中,配置复制预定。
   当配置备份复制计划的预定时,确保当备份复制开始时,最后复制的备份在其原始位置仍然可用。如果此备份在原始位置不可用(例如,因为它已被保留规则删除),则整个存档将作为完整备份进行复制。这可能非常耗费时间并且将使用其他存储空间。
8. 在**保留规则**中,指定目标位置的保留规则。
   可使用以下选项:

- **按备份数量**
- **按备份存留时间**(每月、每周、每日和每小时备份的单独设置)
- **按备份的总大小**
- **无限期地保留备份**

  注意
  选择此选项将导致增加存储使用量。必须手动删除不必要的备份。

9. [如果在**要复制的项目**中已选择加密存档]启用**备份密码**开关,然后提供加密密码。
10. [可选]要修改计划选项,请单击齿轮图标,然后根据需要配置选项。
11. 单击**创建**。

复制内容

注意
某些复制操作(例如,复制整个位置或复制备份集中的所有备份)可能非常耗时。

可以复制个别备份集或整个备份位置。复制备份位置时,会复制其中的所有备份集。

备份集由备份(也称为恢复点)组成。必须选择要复制的备份。

可使用以下选项:

- **所有备份**
  每次运行复制计划时,都会复制备份集中的所有备份。
- **仅完整备份**
  仅复制备份集中的完整备份。
- **仅上次备份**
  仅复制备份集中的最新备份,而不考虑其类型(完整、差异或增量)。

根据您的需要和使用的备份方案,选择一个选项。例如,如果您使用**始终增量(单个文件)**备份方案并希望仅复制最新的增量备份,则在备份复制计划中选择**仅上次备份**。

下表汇总了将使用不同备份方案复制的备份。

	始终增量备份(单个文件)	**始终完整备份**	**每周完整,每日增量**	**每月完整备份,每周差异备份,每天增量备份 (GFS)**
所有备份	备份集中的所有备份	备份集中的所有备份	备份集中的所有备份	备份集中的所有备份
仅完整备份	仅第一个完整备份	所有备份	每周备份一次*	每月备份一次*
仅最后一个备份	仅备份集中的最新备份*	仅备份集中的最新备份*	仅备份集中的最新备份,不考虑其类型*	仅备份集中的最新备份,不考虑其类型*

*当配置备份复制计划的预定时，确保当备份复制开始时，最后复制的备份在其原始位置仍然可用。如果此备份在原始位置不可用(例如，因为它已被保留规则删除)，则整个存档将作为完整备份进行复制。这可能非常耗费时间并且将使用其他存储空间。

用于主机外数据处理的受支持位置

以下表格总结了离线主机数据处理备份复制计划中支持的备份位置。

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	+	+
公有云	+	+
NFS 文件夹	–	–
安全区	–	–

验证

注意
此功能适用于将**Advanced Backup – 服务器**或**Advanced Backup – NAS** 配额作为 Advanced Backup 包的一部分启用的客户租户。

可以验证备份以确认是否可以恢复数据。

验证备份时，您会将验证方法应用于备份档案或备份位置。对备份位置的验证会验证此位置中的所有档案。

要以脱离主机数据处理操作的方式验证备份，则必须创建验证计划。有关详细信息，请参阅 "创建验证计划"(第 205 页)。

若要在不创建验证计划的情况下验证备份，请按照 "正在验证备份"(第 474 页) 进行操作。

支持验证的位置

下表总结了支持的备份位置和验证方法。

注意
验证选项不可用于公有云备份，因为从公有云读取整个存档的成本非常高昂。

备份位置	校验和验证	作为虚拟机运行	
		VM 检测信号	屏幕截图验证
云存储	+	+	+
本地文件夹	+	+	+
网络文件夹	+	+	+
NFS 文件夹	–	–	–
安全区	–	–	–

验证方法

可以选择一种或多种验证方法。如果选择了多种验证方法，则按以下顺序应用它们：

- VM 心跳(**作为虚拟机运行**验证选项的一部分)
- 屏幕截图验证(**作为虚拟机运行**验证选项的一部分)
- 校验和验证

作为虚拟机运行验证选项仅适用于包含操作系统的磁盘级别备份。可以在由保护代理程序(适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序)管理的 ESXi 或 Hyper-V 主机上使用它。

VM 检测信号

使用此验证方法时，代理程序会从备份运行虚拟机、连接到 VMware Tools 或 Hyper-V 集成服务，然后检查检测信号响应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。当验证结果变得清晰时，代理程序就会删除该虚拟机，然后运行下一个虚拟机。

注意
仅当在以下情况下才使用此方法：通过在 ESXi 主机上作为虚拟机运行这些备份来验证 VMware 虚拟机的备份，和通过在 Hyper-V 主机上作为虚拟机运行这些备份来验证 Hyper-V 虚拟机的备份。

屏幕截图验证

使用此验证方法时，代理程序会从备份运行虚拟机，并在虚拟机启动时进行屏幕截图。机器智能(MI)模块会检查屏幕截图；如果屏幕截图包含登录屏幕，则备份验证通过。

屏幕截图会附加到恢复点，可以在验证后的一年内在 Cyber Protect 中控台中下载它。有关如何检查屏幕截图的详细信息，请参阅 "检查验证状态"(第 205 页)。

如果已为您的用户帐户启用了通知，则会收到一封有关备份的验证状态的电子邮件。该邮件中附有屏幕截图。有关通知的详细信息，请参阅为用户更改通知设置。

代理程序版本 15.0.30971(已于 2022 年 11 月发布)及更高版本支持屏幕截图验证。

注意
屏幕截图验证最适合用于使用基于 GUI 的登录屏幕的 Windows 和 Linux 系统的备份。对于使用中控台登录屏幕的 Linux 系统，此方法并未进行优化。

校验和验证

通过校验和验证进行的验证会为可以从备份中恢复的每个数据块计算校验和，然后将其与备份过程中写入的该数据块的原始校验和进行比较。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。

通过校验和验证进行验证是一项耗时的操作，即使对于通常较小的增量或差异备份也是如此。验证操作包括必须恢复的所有数据。对于增量和差异备份，这些数据可能包含在多个备份中。

通过校验和验证进行的验证成功会确保较高的数据恢复可能性。但是，通过该方法进行的验证并不会检查可能影响恢复过程的所有因素。

如果备份操作系统，则建议您使用以下一些附加操作：

- 在可启动媒体下测试恢复到备用硬盘驱动器。
- 在 ESXi 或 Hyper-V 环境中，从备份运行虚拟机。
- 运行验证计划，其中启用了**作为虚拟机运行**验证方法。

更改 VM 检测信号和屏幕截图验证的超时

当通过将备份作为虚拟机运行来验证该备份时，可以配置启动虚拟机与发送检测信号请求或拍摄屏幕截图之间的超时。

默认时长如下所示：

- 一分钟 - 用于存储在本地文件夹或网络共享中的备份。
- 五分钟 - 用于存储在云存储中的备份。

更改超时

1. 打开用于编辑的适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序的配置文件。
   可在以下位置找到配置文件：
   - [对于在 Windows 中运行的适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序]`C:\Program Files\BackupClient\BackupAndRecovery\settings.config`
   - [对于适用于 VMware 的代理程序（虚拟设备）]`/bin/mms_settings.config`
     有关如何访问虚拟设备上的配置文件的详细信息，请参阅 "SSH 连接到虚拟设备"（第 156 页）。
2. 转到 `<validation>`，然后根据需要更改本地备份和云备份的值：

```
<validation>
<run_vm>
<initial_timeout_minutes>
<local_backups>1</local_backups>
```

```
<cloud_backups>5</cloud_backups>
</initial_timeout_minutes>
</run_vm>
</validation>
```

3. 保存配置文件。
4. 重新启动代理程序。
   - [对于在 Windows 中运行的适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序] 在命令提示符下运行以下命令：

     ```
     net stop mms
     ```

     ```
     net start mms
     ```

   - [对于适用于 VMware 的代理程序（虚拟设备）] 重新启动虚拟设备。

配置发生错误时的重试次数

为了最大程度地提高成功验证的次数，可以为以错误结束的验证操作配置自动重试。

配置自动重试

1. 创建验证计划时，单击齿轮图标。
2. 在**选项**窗格中，选择**错误处理**。
3. 在**如果发生错误，则重新尝试**下，单击**是**。
4. 在**尝试次数**中，配置发生错误时的最大重试次数。
   验证操作会再次运行，直到成功完成或达到最大重试次数。
5. 在**尝试间隔**中，配置两次连续重试之间的超时。
6. 单击**完成**。

验证状态

将验证状态分配给已完成验证的备份。

若成功完成验证，则备份会标有绿点和标签**已验证**。

如果验证失败，备份会标有红点。

每次验证操作后都会更新验证状态。每个验证方法的状态都会单独更新。如果配置的验证方法之一失败，则验证将失败。在某些情况下，验证失败可能是由于验证计划配置错误造成的。例如，如果在错误的主机上对虚拟机使用 **VM 心跳**方法。

注意
如果配置的多种验证方法之一失败，则备份的验证状态将显示为失败。即使您通过禁用失败的方法重新配置该验证计划，并且通过其他方法成功完成验证，此状态仍将保留。若要获得**已验证**状态，失败的验证方法必须针对同一备份成功完成验证。

检查验证状态

可以在**设备**选项卡或**备份存储**选项卡上，检查备份的验证状态。

可以查看每种验证方法的状态，并在使用屏幕截图验证方法时下载该屏幕截图。

若要检查验证状态

设备

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 选择一个工作负载，然后单击**恢复**。
3. [如果有多个备份位置可用] 选择备份位置。
4. 选择要检查验证状态的备份。

备份存储

1. 在 Cyber Protect 中控台中，转到**备份存储**。
2. 选择备份位置。
3. 选择备份存档，然后单击**显示备份**。
4. 选择要检查验证状态的备份。

验证活动状态

验证计划可能包含多个备份。所有备份均在单个验证活动中按序逐一处理。

保护代理程序一次只能运行一个验证活动。例如，两个同时进行的验证活动需要两个代理程序，三个同时进行的验证活动则需要三个代理程序。

下表总结了验证活动的可能状态。

活动结果	计划包括一个备份	计划包括多个备份
Success	所有验证方法都成功	所有备份中的所有验证方法都成功
成功但有警告	N/A	至少一个备份中至少有一个验证方法失败
失败	至少有一个验证方法失败	所有备份中至少有一个验证方法失败

创建验证计划

要以脱离主机数据处理操作的方式验证备份存档，则必须创建验证计划。

验证计划可能包括多个备份，并且一个备份可以由多个验证计划进行验证。

创建验证计划

1. 在 Cyber Protect 中控台中，转到**管理** > **验证**。
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，然后指定新名称。
4. 在**代理程序**中，选择将执行验证的代理程序，然后单击**确定**。

- 如果要通过从备份运行虚拟机来执行验证，则必须选择具有适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序的计算机。
- 如果不想通过从备份中运行虚拟机来执行验证，请选择任何可访问备份位置的计算机。

5. 在**验证项目**中，选择要验证的备份存档。
   a. 选择验证范围 - 备份存档或备份位置，单击右上角的**备份**或**位置**。
      如果所选存档已加密，则所有存档必须使用相同的加密密码。对于使用不同加密密码的存档，请创建单独的计划。
   b. 单击**添加**。
   c. 根据验证范围，选择一个或多个位置，或一个位置和一个或多个备份存档，然后单击**完成**。
   d. 单击**完成**。
6. 在**验证内容**中，选择选定存档中要验证的备份（也称为恢复点）。可使用以下选项：
   - **所有备份**
   - **仅上次备份**
7. 在**验证方法**中，选择验证方法。
   可以选择以下选项之一或两者皆选：
   - **校验和验证**
   - **作为虚拟机运行**
     作为虚拟机运行选项提供了 **VM 心跳**和**屏幕截图验证**方法。有关详细信息，请参阅 "验证方法"（第 202 页）。
8. [如果已选择**校验和验证**] 单击**完成**。
9. [如果已选择**作为虚拟机运行**]。配置此选项的设置。
   a. 在**目标计算机**中，选择虚拟机类型（ESXi 或 Hyper-V）、主机和计算机名称模板，然后单击**确定**。
      默认名称为 **[Machine Name]_validate**。
   b. 在**数据存储**（适用于 ESXi）或**路径**（适用于 Hyper-V）中，选择虚拟机的数据存储。
   c. 选择一种或两种验证方法：
      - **VM 检测信号**
      - **屏幕截图验证**
   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。
   e. 单击**完成**。
10. [可选] 在验证计划中，单击**预定**，然后配置预定。
11. [如果在**要验证的项目**中选择的存档已加密]启用**备份密码**开关，然后提供加密密码。
12. [可选] 要修改计划选项，请单击齿轮图标。
13. 单击**创建**。

因此，将创建验证计划，并且将根据配置的预定程序运行。若要立即运行计划，请在**管理** > **验证**中选择计划，然后单击**立即运行**。在验证开始后，您可以在 Cyber Protect 中控台中的**监控** > **活动**中检查运行活动并向下钻取其详细信息。

清理

清理是一项根据保留规则删除过时备份的操作。此操作仅适用于代理程序和工作负载，不适用于云到云备份（只能手动删除）。

注意
此功能适用于将**Advanced Backup – 服务器**或**Advanced Backup – NAS**配额作为 Advanced Backup 包的一部分启用的客户租户。

支持的位置

清理计划支持除 NFS 文件夹和 安全区 之外的所有备份位置。

创建清理计划

1. 在 Cyber Protect 中控台中，依次单击**管理** > **清理**。
2. 单击**创建计划**。
3. 在**代理程序**中，选择将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。
4. 在**要清理的项目**中，选择要清理的存档或备份位置。
   要在存档和位置之间切换，请使用右上角的**位置/备份**开关。
   如果选择多个加密存档，则它们的加密密码必须相同。对于使用不同加密密码的存档，请创建单独的计划。
5. 在**预定**中，配置清理预定。
6. 在**保留规则**中，指定保留规则。
   可使用以下选项：
   - **按备份数量**
   - **按备份存留时间**（每月、每周、每日和每小时备份的单独设置）
   - **按备份的总大小**
7. [如果在**要复制的项目**中已选择加密存档] 启用**备份密码**开关，然后提供加密密码。
8. [可选] 要修改计划选项，请单击齿轮图标，然后根据需要配置选项。
9. 单击**创建**。

转换为虚拟机

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。

注意
无法备份通过本机 Scale Computing VM 复制功能复制的 VM。

可以为转换为虚拟机创建单独的计划，然后手动或按预定运行此计划。

有关先决条件和限制的信息，请参阅 "关于转换，您需要知道的内容"（第 209 页）。

注意
此功能适用于将**Advanced Backup – 服务器**或**Advanced Backup – NAS**配额作为 Advanced Backup 包的一部分启用的客户租户。

为转换到虚拟机创建计划

1. 依次单击**管理** > **转换为 VM**。
2. 单击**创建计划**。
   软件显示新的计划模板。
3. [可选] 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 工作站**
   - **VHDX 文件**

     注意
     为了节省存储空间，每个到 VHDX 文件或 VMware 工作站的转换都会覆盖在上一个转换期间创建的目标位置中的 VHDX/VMDK 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，可以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**预定**，然后更改预定。
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] 要修改计划选项，请单击齿轮图标。
14. 单击**创建**。

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。

下表汇总了可以使用**转换为 VM** 操作创建的虚拟机类型。该表中的各行显示转换后的虚拟机类型。列显示执行转换的代理程序。

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	适用于 oVirt 的代理程序 (KVM)	适用于 Virtuozzo Hybrid Infrastructure的代理程序	适用于 Virtuozzo 的代理程序
VMware ESXi	+	–	–	–	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–	–	–	–
VMware Workstation	+	+	+	+	–	–	–	–	–
VHDX 文件	+	+	+	+	–	–	–	–	–
Scale Computing HC3	–	–	–	–	–	+	–	–	–

限制

- 无法转换存储在 NFS 上的备份。
- 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。
- 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。

定期转换为虚拟机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。

定期转换为虚拟机会占用 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。

仅当虚拟机正在运行时，从备份运行虚拟机才会消耗资源。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。

定期转换为虚拟机的工作原理

定期转换的工作方式取决于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：**当转换增量或差异备份时，软件会增量更新现有虚拟机，而不是重新创建它。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。如果该操作成功，将删除旧计算机。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（如本部分前面所述）。
- 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

为了能够安全地更新转换后的虚拟机，该软件会存储此计算机的中间虚拟机监控程序快照。该快照名为 **Replica...**，必须保留。

Replica... 快照对应最近转换的结果。如果要将计算机返回到相应状态，可以转到此快照；例如，如果已使用了计算机，而现在要放弃对它所做的更改。

对于转换后的 Scale Computing HC3 虚拟机，将会额外创建一个**实用工具快照**。只有 Cyber Protection 服务会使用它。

备份扫描计划

要扫描备份以查找恶意软件（包括勒索软件），请创建备份扫描计划。

重要事项
并非所有工作负载和备份存储都支持备份扫描计划。有关详细信息，请参阅 "限制"（第 766 页）。

创建备份扫描计划

1. 在 Cyber Protect 中控台中，转到**管理** > **备份扫描**。
2. 在“**操作**”窗格中，单击“**创建计划**”。
3. [可选] 更改默认计划名称。
4. 在**要扫描的备份**中，单击**指定**。
   a. 若要向该计划添加一个新位置，请单击**添加**，选择一个位置，然后单击**完成**。
   b. 单击**位置**或**备份**以选择计划的范围。
   c. 选择整个位置或位置中的个别存档。
      您可以选择一个或多个项目。
   d. 单击**完成**。
5. [如果所选存档已加密] 在**加密**中，启用切换，然后指定加密密码。
   所有所选存档必须使用相同的加密密码。对于使用不同加密密码的存档，请创建单独的计划。
6. 单击**创建**。

因此，将创建备份扫描计划。云代理程序将每小时自动扫描所选存档。您无法更改计划预定或两次连续扫描之间的时间间隔。

云应用程序的备份计划

管理 > **云应用程序备份**选项卡会显示云到云备份计划。这些计划通过在云中运行并使用云存储作为备份位置的代理，来备份在云中运行的应用程序。

在本部分里，可以执行以下操作：

- 创建、查看、运行、停止、编辑和删除备份计划。
- 查看与每个备份计划相关的活动
- 查看与每个备份计划相关的警告

有关云应用程序备份的详细信息，请参阅：

- 保护 Microsoft 365 数据
- 保护 Google Workspace 数据

手动运行云到云备份

为了防止中断 Cyber Protection 服务，手动云到云备份运行的数量限制为每个 Microsoft 365 或 Google Workspace 组织每小时 10 次运行。达到此数量后，允许的运行数量重置为每小时一次，此后每小时再可运行一次（例如，第 1 小时，10 次运行；第 2 小时，1 次运行；第 3 小时，2 次运行），直到达到每小时 10 次运行。

无法手动运行应用到设备组（邮箱、驱动器、站点）或包含 10 个以上设备的备份计划。

协作和通信应用程序的保护

Zoom、Cisco Webex Meetings、Citrix Workspace 和 Microsoft Teams 现已广泛用于视频/网络会议和通信。Cyber Protection 服务可以助您保护协作工具。

Zoom、Cisco Webex Meetings、Citrix Workspace 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 Cyber Protect 中控台，然后应用保护计划（已启用以下模块之一）：
   - **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 Cyber Protect 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

了解您当前的保护级别

监控

监控选项卡提供了有关当前保护级别的重要信息，并包括以下仪表板：

- **概述**
- **活动**
- **警告**
- **威胁源**（有关更多信息，请参阅 "威胁源"（第 253 页））

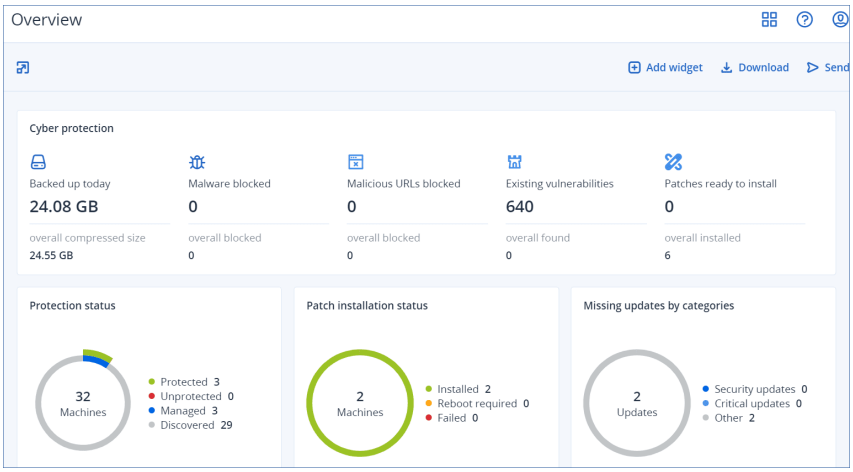
概览仪表板

概述仪表板提供了若干可自定义的小组件，这些小组件会提供与 Cyber Protection 服务相关操作的概述。会在将来的版本中提供适用于其他服务的小部件。

小组件每五分钟更新一次。小部件具有可单击元素，可让您调查和解决问题。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。

可以从各种小部件中进行选择，这些小部件以表格、饼图、条形图、列表和树形图的形式显示。可以使用不同过滤器添加相同类型的多个小部件。

监控 > **概述**中的**下载**和**发送**按钮在 Cyber Protection 服务的 Standard 版中不可用。



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。

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。
- 要在添加小组件之前对其进行编辑，请在选中小组件时单击自定义。在完成编辑小部件后，单击**完成**。

删除小部件的步骤

单击小部件名称旁边的 X 符号。

活动仪表板

活动仪表板提供当前活动和过去活动的概述。默认情况下，保留期为 90 天。

要自定义**活动**仪表板的视图，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。但是，频繁更新多个活动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：

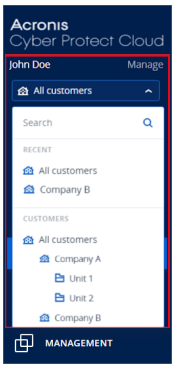
- **状态**
  例如，已成功、失败、进行中、已取消。
- **类型**
  例如，正在应用计划、正在删除备份、正在安装软件更新。
- **时间**
  例如，最近的活动、过去 24 小时的活动或默认保留期内特定时段内的活动。

要查看有关活动的更多详细信息，请从列表中选择该活动，然后在**活动详细信息**面板中单击**所有属性**。有关可用属性的详细信息，请参阅开发者网络门户中的活动和任务 API 参考。

"警报"仪表板

监视 > 警报 仪表板显示您管理的租户的当前警报。根据导航菜单中下拉列表中的选择级别，将显示所有客户租户或特定客户租户的警报。

如果只管理一个租户，则无法使用下拉列表。



每个警报都包含有关其原因或故障排除建议的一般信息。若要获取有关解决潜在问题的进一步帮助，请单击每个警报下的**获取支持**。根据您的角色和在您的租户中启用的服务，可以在知识库中搜索解决方案或提交支持票证。

自定义"警报"仪表板

警报仪表板支持简单视图和表视图。简单视图会显示当前警报的可滚动列表，而表视图会在一个屏幕上显示更多警报和这些警报的其他信息。

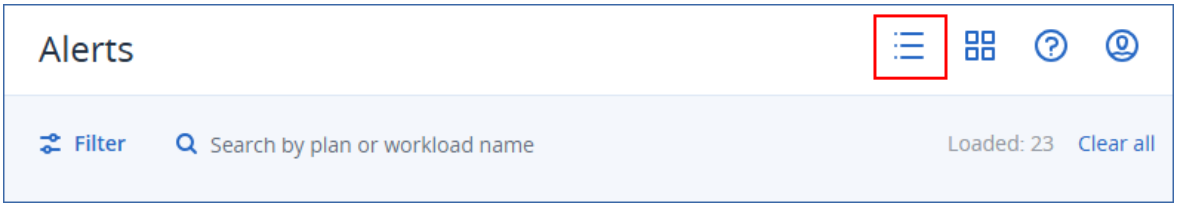
使用表视图时，您可以通过添加或删除列来自定义**警报**仪表板。

在简单视图和表视图中，您都可以隐藏快速筛选器部分。

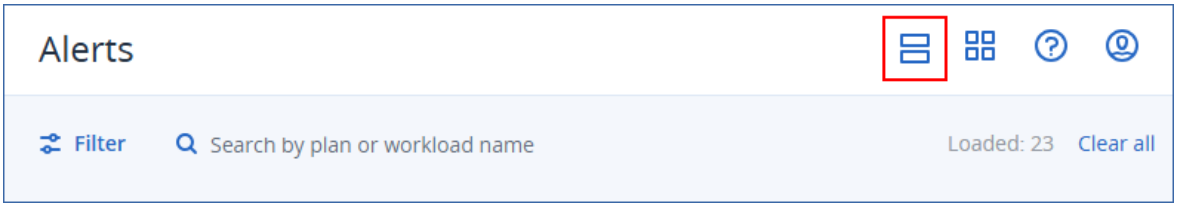
在视图之间切换

若要在简单视图和表视图之间切换

1. 在 Cyber Protect 中控台中，转到**监视** > **警报**。
2. 若要切换至表格视图，请单击表格视图图标。



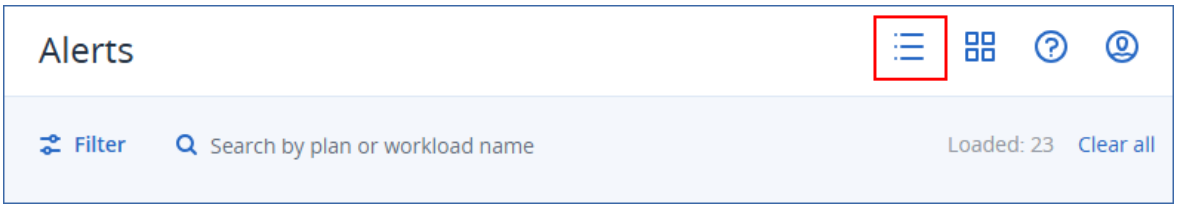
3. 若要切换至简单视图，请单击简单视图图标。



添加或移除列

若要添加或移除列

1. 在 Cyber Protect 中控台中，转到**监视** > **警报**。
2. [如果使用简易视图] 单击表视图图标。



3. 单击右上角的齿轮图标，然后选择要显示的列。

   以下列可用：

列	描述
严重性 （始终可用）	警报的重要性级别。 严重程度可能是以下之一： • 重大 • 错误 • 警告 • 信息
警报类型	警报汇总。有关详细信息，请参阅 "警报类型和类别"（第 218 页）。
消息 （始终可用）	警告详细信息
监视类型	监控类型 – 基于阈值或基于异常。有关详细信息，请参阅 "监视工作负载的运行状况和性能"（第 950 页）。
工作负载	生成警报的工作负载
日期和时间	警报的时间戳
计划	与警报相关的计划（若适用）
警报类别	按功能区域对警报组进行分类。有关详细信息，请参阅 "警报类型和类别"（第 218 页）。
来源	警报来源 – 系统或集成应用程序

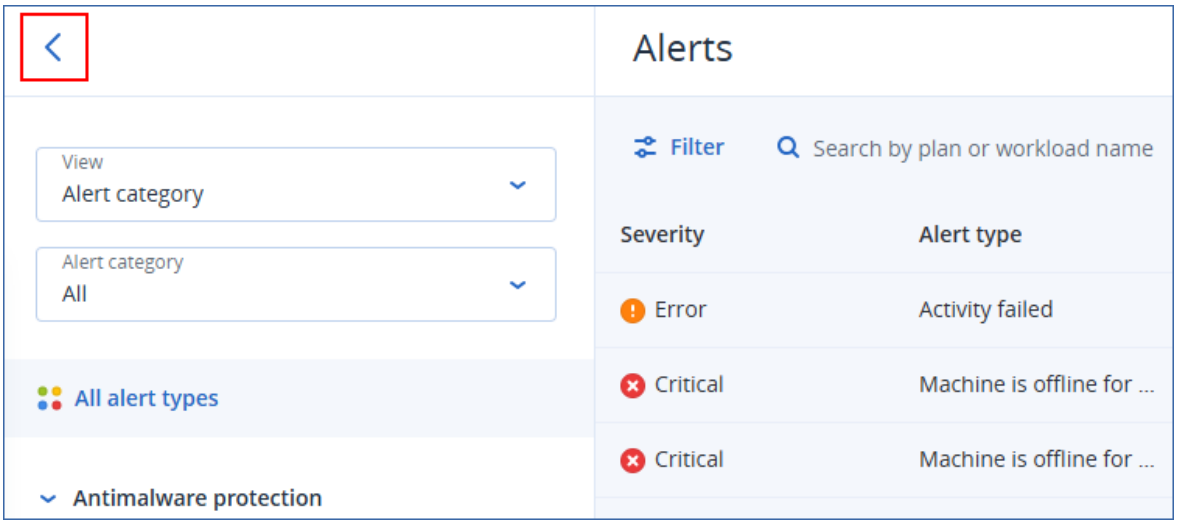
注意

若选择了多个列，则可能需要水平滚动屏幕，以查看所有可用信息。

隐藏快速筛选

若要隐藏快速筛选部分

1. 在 Cyber Protect 中控台中，转到**监视** > **警报**。
2. 单击快速筛选部分顶部的图标。



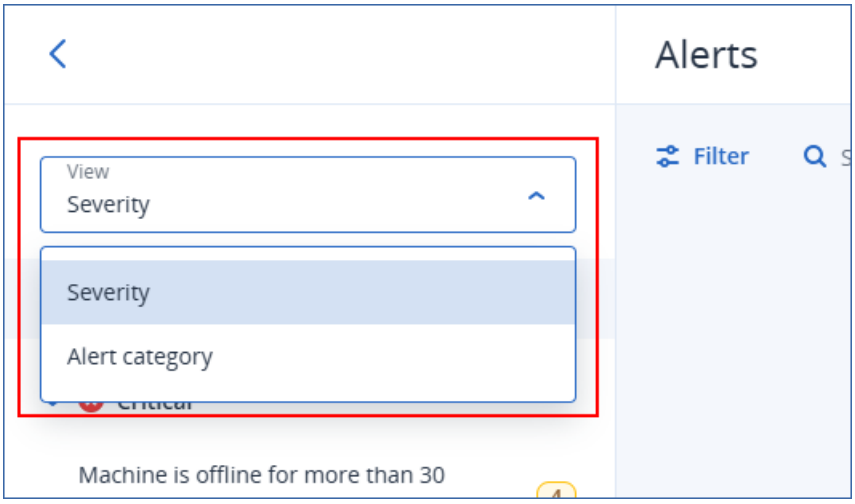
筛选警报

您可以使用快速筛选器或主筛选器。

快速筛选

若要筛选警报

1. 在 Cyber Protect 中控台中，转到**监视** > **警报**。
2. 在**"视图"**下拉列表中，选择筛选条件。



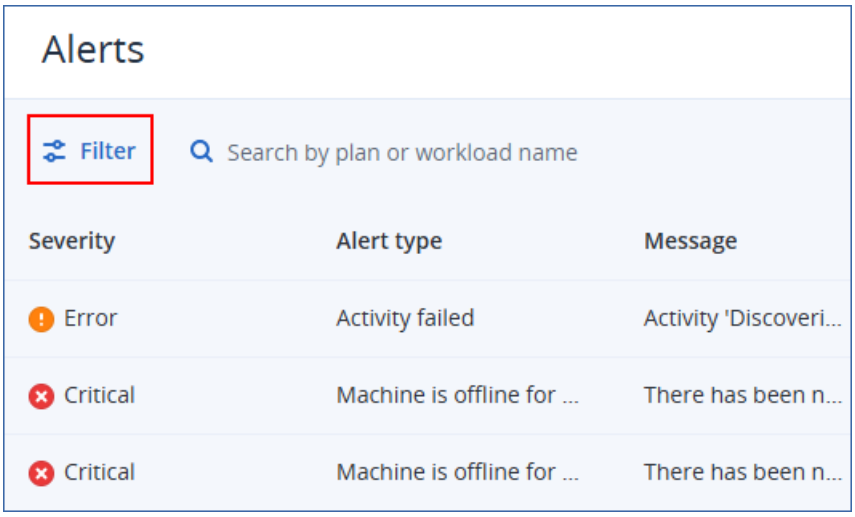
3. [可选] [如果选择了 **警报类别**] 请选择特定的警报类别。
4. [可选] 选择特定的警报类型。

结果是，会列出与筛选条件匹配的警报。

主要筛选

若要筛选警报

1. 在 Cyber Protect 中控台中，转到**监视** > **警报**。
2. 单击**过滤器**。



3. 配置筛选条件，然后单击**应用**。

注意
可用的筛选器条件取决于您可能已配置的快速筛选器设置。

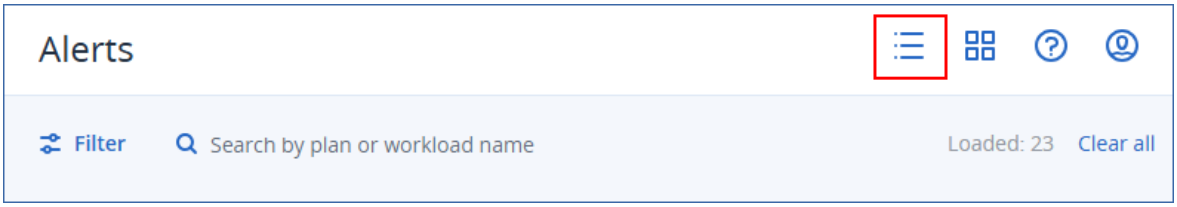
结果是，会列出与筛选条件匹配的警报。

对警报进行排序

使用表视图时，可按降序或升序对警报进行排序。

若要对警报进行排序

1. 在 Cyber Protect 中控台中，转到**监视** > **警报**。
2. [若使用简易视图]单击表视图图标。



3. 单击要对警报进行排序的列名。

注意
您无法通过单击 **消息** 列对警报进行排序。

结果是，警报将被排序，并且会在所选列的名称旁边显示箭头。

警报类型和类别

警报类型会按以下类别分组：

- 备份警报
- 灾难恢复警报
- 防恶意软件保护警报

- 许可警报
- URL 筛选警报
- EDR 警报
- 设备控制警报
- 系统警报
- 设备发现警报
- 软件部署警报

备份警报

警告类型：	描述	解决警报的方法
备份失败	当备份因出现可解决的错误而失败，或因系统关闭而导致中断时，会生成警报。	检查备份操作的日志：单击工作负载以将其选中、单击**活动**，然后在日志中找到警告。该消息应该会将您转到问题的根本原因。
备份成功，但出现警告	当备份成功但出现警告时，会生成警报。	检查转换到 VM、复制或验证计划的日志。这些操作过程中出现的问题会生成“活动失败”或“活动完成，但出现警告”警报。
备份已取消。	每当用户手动取消备份时，都会生成警报。	可以通过单击**“立即运行”**来手动启动备份，也可以等待备份在下一个预定时间开始运行。
备份因备份窗口关闭而导致取消	当因备份活动不适合在备份选项中指定的窗口而导致该备份活动丢失时，会生成警报。	在**性能和备份**窗口中，重新配置预定或编辑备份计划的选项。展开包含您产品的部分，以获取说明。
备份正在等待	当您的预定冲突和两个备份任务同时启动时，就会生成警报。在这种情况下，第二个备份任务会排入队列，直到第一个备份任务完成或停止。	确保备份在预期的时间窗口内根据其预定运行，并避免出现预定冲突。
备份未响应	当备份在一段时间内未显示任何进度，并可能已冻结时，会生成警报。	该问题可能是由锁定引起的。有关更多信息，请参阅 此知识库文章。
备份未启动	当预定备份因未知原因无法启动时，会生成警报。	请确保您正在使用最新版本的 安克诺斯 Backup 产品。 • 如果代理程序计算机在备份开始时间内可用： 1. 编辑备份任务开始时间。 2. 如果警报再次出现，请重新创建备

警告类型：	描述	解决警报的方法
		份任务。 3. 如果新创建的备份任务也触发警报，请联系支持团队以寻求帮助。 • 如果代理程序处于脱机状态： 1. 请勿在备份期间关闭计算机。 2. 如果计算机未关闭，请确保 Acronis Managed Machine Service 正在运行：开始 -> 搜索 -> services.msc -> 找到 Acronis Managed Machine Service。如果需要帮助，请联系支持团队。
备份状态未知	当备份代理程序在预定备份时间开始时处于脱机状态，会生成警报。在备份代理程序重新处于联机状态之前，资源备份的状态将处于未知状态。	1. 检查代理程序预计是否会处于脱机状态(例如，笔记本电脑不在管理服务器网络中)。 2. 如果代理程序不应处于脱机状态，请确保 Acronis Managed Machine Service 正在运行：开始 -> 搜索 -> services.msc -> 找到 Acronis Managed Machine Service 并检查其状态。如果服务已停止，请启动该服务。
备份丢失	当超过 [自上次备份以来的天数] 天没有成功备份时，会生成警报。	
备份已损坏	当验证活动已成功但显示备份损坏时，会生成警报。	请按照对备份损坏问题进行故障排除文章中的步骤进行操作。 如果您需要在确定存档损坏的根本原因时获取帮助，请联系支持团队。
连续数据保护失败	如果备份的连续保护失败，则会生成警报。	验证以下限制： 1. 仅 NTFS 文件系统和以下操作系统支持连续数据保护： • 桌面：Windows 7 及更高版本 • 服务器：Windows Server 2008 R2 及更高版本 2. CDP 不支持将 **Acronis 安全区**作为目标位置。 3. 不支持在 Windows 上加载的 NFS 文件夹。 4. 不支持连续复制：如果保护计划中有两个位置，则仅在第一个目标中创

警告类型：	描述	解决警报的方法
		建 CDP 片段，然后在下一次备份时将更改复制到第二个目标。 5. 如果本地受保护文件夹中的更改应用自网络源（例如，当用户访问网络中的文件夹时），则 CDP 不会检测到它们。 6. 如果文件正在使用（例如，在 Excel 文件中正在进行某些更改），则 CDP 不会检测到这些更改。若要让 CDP 能够检测到更改，请保存这些更改，然后关闭文件。
Hyper-V 主机配置无效	当有 2 个或多个适用于 Hyper-V 的代理程序安装在主机名称相同的 Hyper-V 主机上（在相同的帐户级别上不支持主机名称相同）时，会生成警报。	为了避免出现冲突，请在该帐户的不同子单位下注册这些适用于 Hyper-V 的代理程序。
验证失败	当备份的验证过程无法完成时，会生成警报。	检查错误操作的日志：单击计算机以将其选中、单击**活动**，然后在日志中找到警告。该消息应该会将您转到问题的根本原因。

无法将云存储中的备份迁移到新的格式	当云存储中的备份迁移到新格式失败时会生成警报。	有关迁移 Acronis Cyber Backup Advanced 档案的更多信息，请参阅此知识库文章。
		有关迁移 Acronis Cyber Backup 档案的更多信息，请参阅此知识库文章。
		在联系支持团队之前，请通过运行一下命令，使用 **migrate_archives** 工具收集报告：
		`migrate_archives.exe --account=<Acronis account> --password=<password> --subaccounts=All > report1.txt`
		`migrate_archives.exe --cmd=finishUpgrade --account=<Acronis account> --password=<password> > report2.txt`
		其中 `Acronis account` 是您的 Acronis 帐户，`password` 是该帐户的密码。

加密密码丢失	当数据库加密密钥不正确、损	如果您丢失或忘记密码，则无法恢复加

警告类型：	描述	解决警报的方法
	坏或丢失时，会生成警报。	密备份。必须在受保护的设备上本地设置加密密码。不能在保护计划中设置加密密码。有关详细信息，请参阅设置加密密码。
上传待处理	如果预定检查发现此备份计划的物理数据装运到云存档未上传到存储，则会生成警报。	
备份恢复失败	如果在尝试恢复文件或系统备份时恢复操作失败，则会生成警报。	确定备份失败的确切日期，然后尝试使用上次成功的备份进行恢复。

灾难恢复警报

警告类型：	描述	解决警报的方法
超出存储空间配额	当超出灾难恢复存储的软配额时，就会生成警报。	增加配额或从云存储中移除一些备份。
已达到配额	当以下提供项目的软配额超出时，将生成警报： • 云服务器。 • 计算点。 • 公共 IP 地址。	
已超出存储空间配额	当超出灾难恢复存储的硬配额时，就会生成警报。 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，或添加或扩展现有主服务器的磁盘。如果已超出此配额的超额，则无法执行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。	
已超出配额	当超出以下提供项目的硬配额时，就会生成警报： • 云服务器。 • 计算点。 • 公共 IP 地址。	考虑购买额外的配额，或者禁用不再需要保护的设备的备份任务。
故障转移错误	当启动故障转移后出现系统问题时，就会生成警报。	1. 选择恢复服务器，然后单击**“编辑”**。

警告类型：	描述	解决警报的方法
		2. 减少恢复服务器的 CPU/RAM。 3. 尝试再次执行故障转移。
故障转移测试错误	当启动测试故障转移后出现系统问题时，就会生成警报。	1. 选择恢复服务器，然后单击**"编辑"**。 2. 减少恢复服务器的 CPU/RAM。 3. 尝试再次执行测试故障转移。 **注意** 请确保生产网络中的 IP 地址与 DHCP 服务器中配置的 IP 地址相同。
故障恢复错误	当启动故障恢复后出现系统问题时，就会生成警报。	可以在备份存储列表中看到错误的位置：它有一个编号而不是名称（通常，位置名称与现有最终用户的名称之一匹配），而您尚未创建此位置。移除错误的位置： 1. 在 Cyber Protect 中控台中，转到**备份存储**。 2. 找到该位置，然后单击叉号 (x) 图标以将其删除。 3. 单击**删除**以确认选择。 4. 重试故障转移。
故障恢复已取消	当用户取消故障恢复时，会生成警报。	从中控台中手动忽略警报。
VPN 连接错误	当因与用户操作无关的原因而导致 VPN 连接失败时，会生成警报。来自 VPN 设备的状态报告已过时。	如果您在部署或连接 安克诺斯 VPN 设备时遇到问题，请联系支持团队。 请在您的电子邮件中包含以下信息： • 错误消息的屏幕截图（如果有） • 安克诺斯 VPN 设备 CLI 界面的屏幕截图 • 安克诺斯 Backup Cloud 数据中心和组名称。
（VPN 无法访问）连接网关无法访问	当Disaster Recovery服务无法访问连接网关时，会生成警报。来自连接网关的状态报告已过时。	如果您在部署或连接 安克诺斯 VPN 设备时遇到问题，请联系支持团队。 请在您的电子邮件中包含以下信息： • 错误消息的屏幕截图（如果有） • 安克诺斯 VPN 设备 CLI 界面的屏幕截图 • 安克诺斯 Backup Cloud 数据中心

警告类型：	描述	解决警报的方法
		和组名称
需要重新指派 DR IP	当 VPN 设备检测到网络更改，则会生成警报。	重新指派 IP 地址。有关详细信息，请参阅 "重新指派 IP 地址"(第 688 页)
连接网关出现故障	当云端 VPN 服务器部署失败时，则会生成警报。	使用连接验证工具，并检查其输出以查找错误。 允许 安克诺斯 软件通过防火墙和防恶意软件软件的应用程序控制。
主服务器创建失败	当因出现错误而导致主服务器无法创建时，会生成警报。	
恢复服务器创建失败	当因出现错误而导致服务器无法创建时，会生成警报。	确保恢复服务器符合软件要求。有关详细信息，请参阅 "软件要求"(第 655 页)。
删除主服务器	当删除主服务器时，会生成警报。	
服务器恢复失败	当主服务器或恢复服务器无法恢复时，会生成警报。	查找详细信息。如果错误消息很笼统或不明确(例如，“内部错误”)，请导航到**Disaster Recovery → 服务器**、单击以选择受影响的计算机，然后单击**活动**。单击某活动，按住 Ctrl 键并左键单击该活动。现在，您将能够在每个活动旁边看到省略号图标 (...)。单击并选择**任务活动信息**。
备份失败	当云服务器(主服务器或处于生产故障转移状态下的服务器)的备份失败时，会生成警报。	1. 验证与备份位置的连接。 2. 检查备份存储设备(本地备份)。
超出网络限制	当达到云网络的最大数量(5 个网络)时，会生成警报。	
手册操作失败	当操作手册执行失败时，会生成警报。	这不会影响产品功能，可以安全地忽略它。有关详细信息，请参阅 "创建 Runbook"(第 722 页)。
操作手册警告	当操作手册执行完成但出现警告时，会生成警报。	这不会影响产品功能，可以安全地忽略它。有关详细信息，请参阅 "创建 Runbook"(第 722 页)。
需要操作手册用户交互	当操作手册等待用户交互时，会生成警报。	这不会影响产品功能，可以安全地忽略它。有关详细信息，请参阅 "创建 Runbook"(第 722 页)。

警告类型：	描述	解决警报的方法
Internet 通信被阻止	当管理员阻止 Internet 通信时，会生成警报。	
Internet 通信已取消阻止	当管理员解除阻止 Internet 通信时，会生成警报。	
本地网络重叠	当检测到相同或重叠的本地网络时，会生成警报。	
许可切换不足的服务器配额	当云服务器配额不足时，会生成警报。	• 如果针对物理服务器生成警报，请确保租户和用户对 **Web 托管服务器**或提供项目的**服务器**具有足够的配额。 • 如果警报是针对虚拟服务器生成的，请确保租户和用户对 **Web 托管服务器**或**虚拟机**提供项目具有足够的配额。虚拟服务器不能使用**服务器**提供项的配额。
许可切换不足的产品项目	当禁用**灾难恢复存储**提供项目时，会生成警报。	
许可切换错误	当灾难恢复升级遇到错误时，会生成警报。	
许可切换不足的计算点	当没有可用的计算点时，会生成警报。	增加**计算点**提供项目的硬配额。
许可切换不足的服务器产品项目	当禁用**云服务器**产品项目时，会生成警报。	
策略无法创建恢复服务器	当设置灾难恢复基础架构过程中发生错误时，会生成警报。	手动创建恢复服务器，不带 **Internet 访问**属性。有关详细信息，请参阅 "创建恢复服务器"(第 694 页)。
备份处理器自动测试故障转移已重新预定	当重新预定自动测试故障转移时，会生成警报。	
备份处理器自动测试故障转移超时已达到	当自动测试故障转移取消时，会生成警报。 **注意** 每次自动测试故障转移都会消耗计算点。	
备份处理器自动测试故障转移整体出现故障	上次预定的恢复服务器自动测试故障转移失败时，会生成警报。	• 手动启动恢复服务器的测试故障转移。有关详细信息，请参阅 "执行测试故障转移"(第 706 页)。

警告类型：	描述	解决警报的方法
		• 等待将执行自动测试故障转移的下一个预定日期。
故障恢复数据传输出现错误	当故障恢复的数据传输阶段失败时，会生成警报。	
故障恢复失败	当故障恢复中出现错误时，会生成警报。	可以在备份存储列表中看到错误的位置：它有一个编号而不是名称（通常，位置名称与现有最终用户的名称之一匹配），而您尚未创建此位置。删除错误的位置： 1. 在 Cyber Protection 中，转到**备份存储**。 2. 找到该位置，然后单击叉号 (x) 图标以将其删除。 3. 单击**删除**以确认选择。 4. 再次启动故障转移。
故障恢复确认失败	当故障恢复确认失败时，会生成警报。	
故障恢复计算机已准备好进行切换	当计算机准备好进行切换时，会生成警报。	
故障恢复切换已完成	当切换成功时，会生成警报。	从中控台中手动忽略警报。
故障恢复目标代理程序脱机	当代理程序处于脱机状态时，会生成警报。	

防恶意软件保护警报

警告类型：	描述	解决警报的方法
检测到可疑远程连接活动	当检测到来自远程连接的勒索软件时，会生成警报。	从中控台中手动忽略警报。
检测到可疑活动	当在工作负载中检测到勒索软件时，会生成警报。	从中控台中手动忽略警报。以停用警报。 根据您在 Active Protection 计划中指定的选项，将停止恶意进程、恢复该进程所做的更改，或者尚未采取任何操作，您需要手动解决此问题。 阅读警报的详细信息，以了解哪个进程正在加密文件以及哪些文件受影响。 如果您确定加密文件的进程是准许的（误报警报），请将该进程添加到受信任的进程：

警告类型:	描述	解决警报的方法
		1. 打开 Active Protection 计划。 2. 单击**编辑**以修改设置。 3. 在**受信任的进程**中，指定将永不视为勒索软件的受信任进程。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`
检测到 Cryptomining 活动	当在工作负载中检测到非法加密挖矿程序时，会生成警报。	从中控台中手动忽略警报。
MBR 防御:检测到可疑活动并已将其暂停	当在工作负载中检测到勒索软件(特别是勒索软件会修改 MBR/GPT 分区)时，会生成警报。	从中控台中手动忽略警报。
指定了不受支持的网络路径	当管理员提供的恢复路径不是本地文件夹路径时，会生成警报。	指定网络文件夹保护的本地路径(恢复路径)。在中控台中手动忽略警报。
关键进程添加为对 Active Protection 计划有害的进程	当在“保护排除”列表中将关键进程添加为受阻止的进程时，会生成警报。	从中控台中手动忽略警报。
无法应用 Active Protection 策略	当无法应用 Active Protection 策略时，会生成警报。	请查看错误消息，以了解无法应用 Active Protection 策略的原因。
安全区:未经授权的操作已检测到并被阻止	当在工作负载中检测到勒索软件(勒索软件会修改 ASZ 分区)时，会生成警报。	从中控台中手动忽略警报。
Active Protection 服务未运行	Active Protection 服务已崩溃或不在运行时，会生成警报。	请查看错误消息，以了解 Active Protection 服务不在运行的原因。
Active Protection 服务不可用	当因驱动程序不兼容或丢失而导致 Active Protection 服务不可用时，会生成警报。	请查看 Windows 事件日志，以了解 Acronis Active Protection 服务 (acronis_protection_service.exe) 是否崩溃。
与另一个安全解决方案冲突	如果因检测到与另一个安全解决方案冲突而导致 Active Protection 不可用于计算机“{{resourceName}}”时，会生成警报。要启用 Active Protection，请禁用或卸载冲突的安全解决方案。	**解决方案 1**:如果想使用 安克诺斯 实时保护，请从从工作负载中卸载第三方防病毒软件。 **解决方案 2**:如果想使用第三方防病毒软件，请在应用于工作负载的保护计划中禁用 Acronis 实时保护、URL 过滤和 Windows Defender 防病毒软件。
隔离操作失败	当防恶意软件无法隔离检测到的恶意软件时，会生成警报。	请查看错误消息，以了解隔离失败的原因。

警告类型：	描述	解决警报的方法
检测到恶意进程	当行为引擎检测到恶意软件(进程类型)时，会生成警报。检测到的恶意软件已隔离。	从中控台中手动忽略警报。
检测到恶意进程，但未隔离	当行为引擎检测到恶意软件(进程类型)时，会生成警报。检测到的恶意软件未隔离。	从中控台中手动忽略警报。
恶意软件已检测到并被阻止 (ODS)	当预定扫描检测到恶意软件时，会生成警报。检测到的恶意软件已隔离。	从中控台中手动忽略警报。
恶意软件已检测到并被阻止(RTP)	当实时保护检测到恶意软件时，会生成警报。检测到的恶意软件已隔离。	从中控台中手动忽略警报。
在备份中检测到恶意软件	当在备份扫描期间检测到恶意软件时，就会生成警报。	从中控台中手动忽略警报。
在反恶意软件实时保护和安全产品之间检测到的冲突	当防恶意软件无法在 Windows Security Center 中注册时，会生成警报。	禁用或卸载第三方安全产品，或在保护计划中禁用实时防恶意软件保护。
无法运行 Microsoft Security Essentials 模块	当 Microsoft Security Essentials 模块运行失败时，则会生成警报。	请查看错误消息，以了解 Microsoft Security Essentials 模块无法运行的原因。
由于安装了第三方防病毒软件，因此实时保护不可用	当因第三方防病毒已启用实时保护而导致无法打开实时保护时，则会生成警报。	禁用或卸载第三方安全产品，或在保护计划中禁用实时防恶意软件保护。
由于驱动程序不兼容或丢失，因此实时保护不可用	当因驱动程序不兼容或丢失而导致实时保护不可用时，会生成警报。	检查错误消息以了解工作负载上驱动程序安装失败的原因。
网络安全保护(或 Active Protection)服务不响应	当网络安全保护服务从中控台响应运行状况检查 ping 时，会生成警报。	在中控台中手动忽略警报。
安全定义更新失败	当安全定义更新失败时，会生成警报。	请查看错误消息，以了解安全定义更新失败的原因。
防篡改保护已启用	当由于防篡改保护已启用而导致无法更改 Microsoft Defender 设置时，会生成警报。	禁用 Windows 工作负载上的防篡改保护设置。
Windows Defender 模块执行失败	当 Windows Defender 模块执行失败时，会生成警报。	请查看错误消息，以了解 Windows Defender 模块无法运行的原因。

警告类型：	描述	解决警报的方法
Windows Defender 被第三方防病毒软件阻止	当因在计算机上安装第三方防病毒软件而导致阻止 Windows Defender 时，会生成警报。	禁用或卸载第三方安全产品。
组策略冲突	当因 Microsoft Defender 设置受控于组策略而导致无法更改该设置时，会生成警报。	禁用 Windows 工作负载上的组策略设置。
Microsoft Security Essentials 已采取措施来保护此计算机免受恶意软件的侵害	当 Microsoft Security Essentials 删除或隔离恶意软件时，会生成警报。	从中控台中手动忽略警报。
Microsoft Security Essentials 检测到恶意软件	当 Microsoft Security Essentials 检测到恶意软件或其他潜在不受欢迎的软件时，会生成警报。	从中控台中手动忽略警报。

许可警报

警告类型：	描述	解决警报的方法
几乎已达到存储空间配额	当使用率降至 80% 以下(在清理或配额升级后)时，会生成警报。	购买额外的存储空间，或释放云存储中的空间。
已超出存储空间配额	当所有 100% 的存储空间配额都已使用时，会生成警报。	购买更多存储空间。有关更多信息，请参阅此知识库文章。
已达到工作负载配额	当产品项目的使用量 > 0 且使用量 > 配额，但使用量 <= 配额 + 超额时，会生成警报。	
已超出工作负载配额	当产品项目的使用量 > 配额 + 超额时，会生成警报。	
工作负载没有用于应用备份计划的配额(资源没有服务配额)	在以下情况下，会生成警报： • 手动删除配额：**设备** > **详细信息** > **服务配额**、单击**更改**，然后选择**无配额**选项。 • **管理中控台**提供项目已禁用。 • 产品项目的**管理中控台**配额+超额值降至低于当前使用量。	
无法保护已指派配额的工作负载	当产品项目不足时会生成警报，您需要： • 动态组。	

警告类型：	描述	解决警报的方法
	• 将备份计划指派给该组。 • 一个属于该动态组的资源，但其某些特性禁止对其应用相同的备份计划。	
订购许可证到期	许可证过期时，会生成警报。	在订购许可到期后，将阻止除恢复外的所有产品功能，直到续订订购许可为止。备份数据仍可以访问以进行恢复。 购买新的许可证。 **注意** 如果您最近购买了新订购许可，但仍收到订购许可已过期的消息，请从 安克诺斯 账户：在管理中控台中，进入**设置->许可证**，点击右上角**同步**以导入新的订购许可。订购许可将会同步。
订购许可即将过期	如果许可证将在 30 天内到期，则会生成警报。	购买新的订购许可。

URL 筛选警报

警告类型：	描述	解决警报的方法
恶意 URL 已阻止	当 URL 过滤阻止恶意 URL 时，会生成警报。	检查 URL 过滤设置。URL 过滤将根据 URL 过滤设置，来阻止应该被阻止的页面。有关详细信息，请参阅 "URL 过滤"(第 751 页) 。
恶意 URL 警告已忽略	当选择继续处理由 URL 过滤阻止的恶意 URL 时，会生成警报。	检查 URL 筛选设置。
在 URL 过滤和安全产品之间检测到的冲突	当由于与另一个安全产品冲突而导致无法启用 URL 过滤时，会生成警报。	检查 URL 筛选设置。
网站 URL 已阻止	当 URL 满足在 URL 过滤的受阻止类别中指定的所有条件时，会生成警报。	检查 URL 筛选设置。

EDR 警报

警告类型：	描述	解决警报的方法
检测到事件	当创建事件或更新现有事件的	此警报会通知您新事件或旧事件

警告类型：	描述	解决警报的方法
	状态时，会生成警报。	是否已更新。可以查看警报并将其关闭。如果需要，可以选择打开事件以进行进一步调查。
检测到危害指标 (IOC)	当 EDR IOC 威胁搜索服务检测到新的危害指标时，会生成警报。	此警报会通知您在一个或多个工作负载上检测到 IOC。您将查看警报，然后单击警报中的链接以查看有关 IOC 的详细信息。
无法将工作负载与网络隔离	当用户触发将计算机与网络隔离的操作，但隔离操作失败时，会生成警报。	采取必要操作。
无法将工作负载重新连接到网络	当用户触发将计算机重新连接回网络的操作，但该操作失败时，会生成警报。	采取必要操作。
Windows Defender 防火墙设置已修改	当在隔离的计算机上修改防火墙设置时，会生成警报。	此警报会通知您已在隔离的计算机上修改了防火墙详细信息。它仅供参考，可以在查看后关闭警报。

设备控制警报

警告类型：	描述	解决警报的方法
设备控制和数据丢失预防将运行，但功能受限(检测到不兼容的 CPU)。	当 DeviceLock 代理程序在装有支持 CET 技术的 CPU 的物理机上启动时，会生成警报。	禁用受影响计算机上的该选项，可避免出现这些警报。
设备控制功能在 macOS Ventura 上尚不受支持	当 DeviceLock 代理程序在物理 macOS Ventura 计算机上启动，并将带有设备控制的保护计划应用于该代理程序，会生成警报。仅适用于因 DeviceLock 驱动程序而导致出现内核死机问题时的版本。	
允许的敏感数据传输	如果允许传输敏感度内容，则会生成警报。	
正当的敏感数据传输	如果传输敏感内容是合理的，则会生成警报。	
拒绝的敏感数据传输	如果传输敏感内容被阻止，则会生成警报。	
审核数据丢失预防观测模式的结果	当要审核观察结果时，会生成警报： • Advanced DLP 包许可证未应用。	

警告类型：	描述	解决警报的方法
	• 自在已应用于至少一个工作负载的任何保护计划中启用观察模式以来已过去一个月。 • 自上次发出类似警报以来已过去一个月，并且在观察模式下检测到 DLP 的一些使用。	
用户的安全标识符已更改	当已知用户名的 SID 更新时会生成警报。在非域工作负载上重新安装操作系统时可能会发生这种情况。	
外围设备访问已被阻止	当支持设备的某些操作(读/写操作)受阻止时，会生成警报。	
无法连接到远程 SSL 资源。	当对远程 SSL 资源的访问由于资源上使用的额外握手预防而被阻止时，会生成警报。	将资源添加到远程主机的白名单中。

系统警报

警告类型：	描述	解决警报的方法
代理程序已过期	当代理程序版本过时时，会生成警报。	转到代理程序列表，并启动更新代理程序。
自动更新失败	当代理自动更新失败时，则会生成警报。	尝试执行手动更新。
安装新代理程序后，需要重新启动设备	当远程安装成功后需要重新启动时，则会生成警报。	重新启动工作负载。
活动失败	当活动失败时，则会生成警报。	重新启动工作负载上的所有 Acronis 服务。
活动已成功，但带有警告	当活动成功但生成了一些警告时，会生成警报。	
活动未响应	当正在进行的活动不响应时，会生成警报。	
计划部署失败	当保护计划部署失败时，会生成警报。	
无法将用户名转换为 SID	当预定 SID 转换失败时，会生成警报。	

设备发现警报

警告类型：	描述
发现新设备	这是一个信息警报，当本地网络的设备发现扫描发现新的未注册设备时，将生成该警报。 警报包含**查看已发现的设备**链接，可打开新发现的设备列表。

软件部署警报

警告类型：	描述
检测到软件包不兼容	这是一个关键警报，当无法安装软件包，因为它与目标工作负载的操作系统不兼容时，将生成此警报。
尝试安装缺失的软件	这是一个关键警报，当软件部署计划尝试安装存储库中未找到的软件包时，将生成此警报。
尝试卸载丢失的软件	这是一个关键警报，当软件部署计划尝试卸载存储库中未找到的软件包时，将生成此警报。
安装软件后需要重新启动	这是警告警报，当安装软件包需要重新启动目标工作负载的操作系统时，将生成此警告。
软件卸载后需要重新启动	这是警告警报，当卸载软件包需要重新启动目标工作负载的操作系统时，将生成此警告。

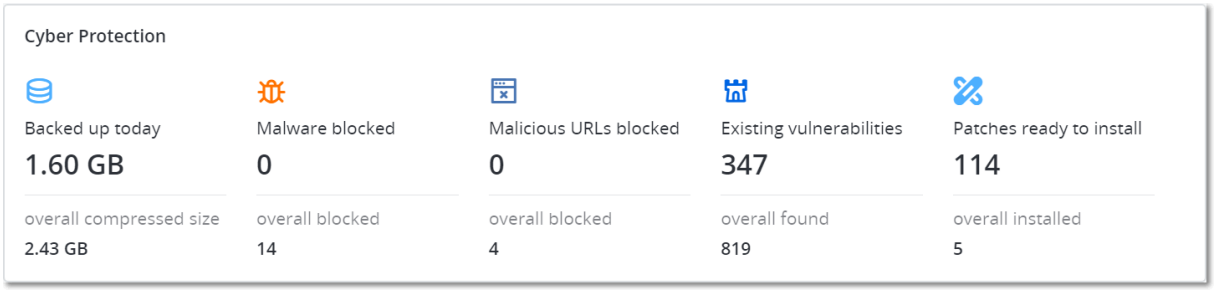
警报小组件

在警报小组件中，可以查看与工作负载相关的警报的以下详细信息：

现场	描述
5 个最新警报小组件	五个最新警报的列表。
历史警报摘要	一个图形小组件，按警报严重性、警报类型和时间范围显示警报。
活动警报摘要	一个图形小组件，按警报严重性和警报类型以及活动警报的总和显示活动警报。
警报历史记录	一个历史警报的表视图。
活动警报详细信息	一个活动警报的表视图。

网络安全保护

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

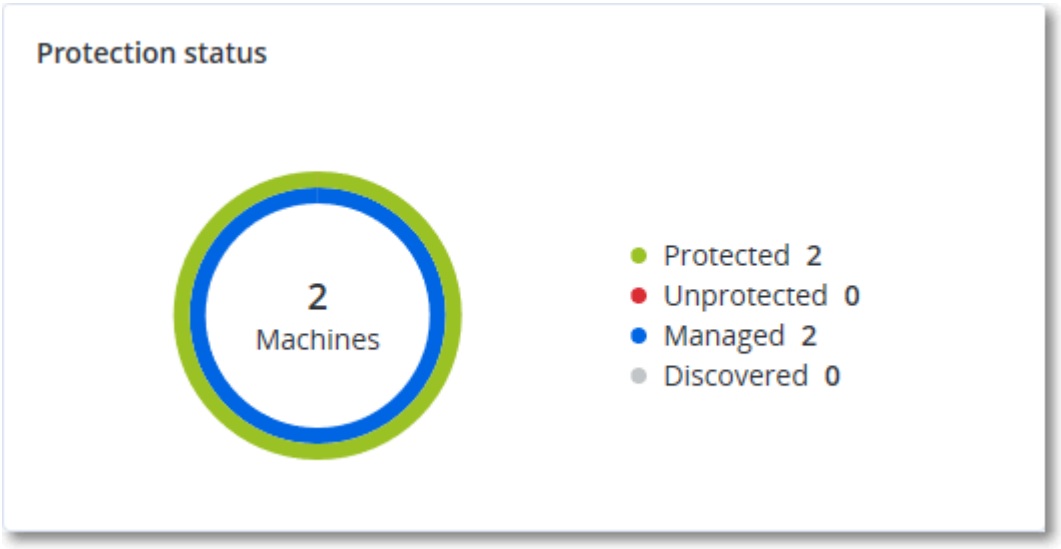
保护状态

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：

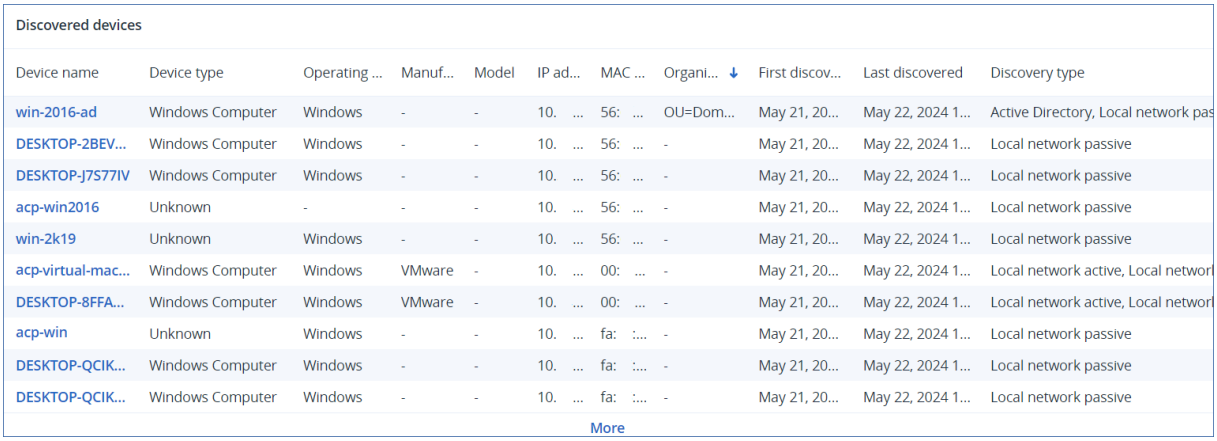
- **受保护** - 计算机已应用保护计划。
- **不受保护** - 计算机未应用保护计划。这包括未应用保护计划的已发现计算机和受控计算机。
- **受控** - 计算机已安装保护代理程序。
- **已发现** - 计算机未安装保护代理程序。

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。



已发现的设备

此小组件显示有关在组织网络中发现的设备的详细信息。



Endpoint Detection and Response (EDR) 小组件

Endpoint Detection and Response (EDR) 包括七个小组件，所有这些小组件都可以从**概述**仪表板进行访问；其中的三个小组件也会默认显示在 EDR 功能内（请参阅 "查看事件"（第 797 页））。

可用的七个小组件包括：

- 每个工作负载的主要事件分发
- 威胁状态（显示在 EDR 中）
- 事件严重性历史记录（显示在 EDR 中）
- 安全性事件 MTTR
- 安全性事件刻录
- 战术检测（显示在 EDR 中）
- 工作负载网络状态

每个工作负载的主要事件分发

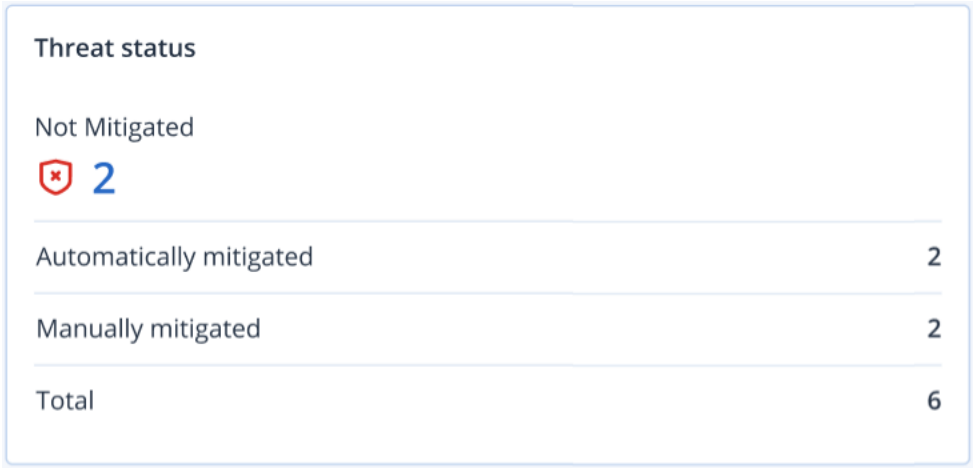
此小组件显示具有最多事件的前五个工作负载(单击**全部显示**以重定向到事件列表,这可根据小组件设置进行过滤)。

将鼠标悬停在工作负载行上以查看事件的当前调查状态明细;调查状态有**未启动**、**正在调查**、**已关闭**和**误报**。然后,单击要进一步分析的工作负载;事件列表会根据小组件设置进行刷新。

威胁状态

此小组件会显示所有工作负载的当前威胁状态,同时亮显当前未缓解并需要调查的事件数量。小组件还指示已缓解的事件数(由系统手动和/或自动)。

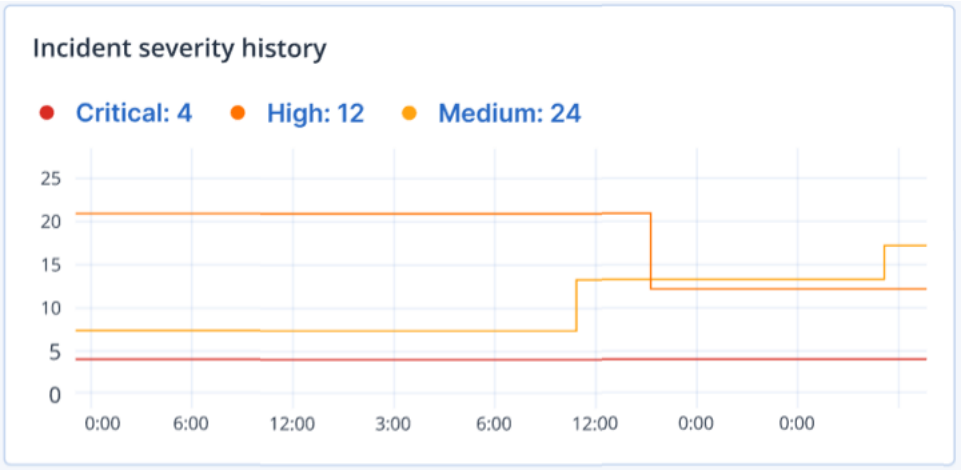
单击**未缓解**的数量,可显示事件列表,该列表已过滤为显示未缓解的事件。



事件严重性历史记录

此小组件会按严重性显示攻击的演变,并有助于指示攻击活动。当尖峰可见时,这可能指示组织正遭受攻击。

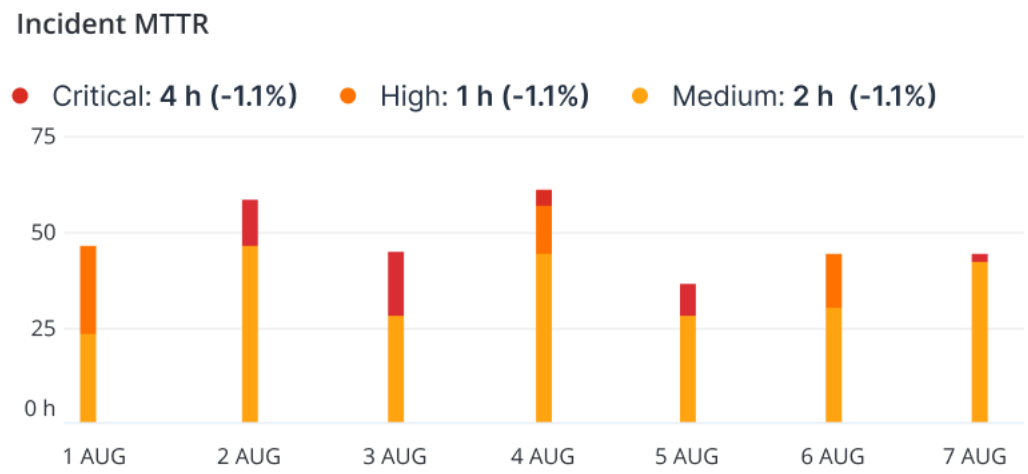
将光标悬停在图形上，可查看过去 24 小时(默认时间段)内某一特定时间点的事件历史记录明细。如果要查看相关事件的列表，请单击严重级别(**严重**、**高**或**中**)；系统会将您重定向到事件列表，该列表已预先过滤出与选定严重级别匹配的事件。



安全性事件 MTTR

此小组件显示用于安全性事件的平均解决时间。它指示调查和解决事件的快速程度。

单击某个列以根据严重性(**严重**、**高**和**中**)查看事件明细，并可查看解决不同严重性级别花费多少时间的指示。在括号中显示的 % 值表示与以前时间段比较的上升或下降。

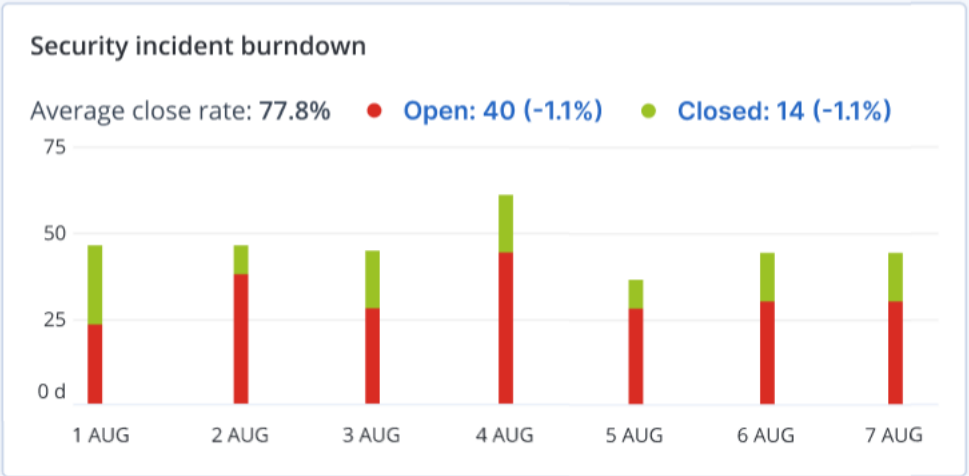


安全性事件刻录

此小组件显示关闭事件中的效率；针对一段时间的关闭事件的数量测量打开事件数。

将鼠标悬停在某列上可以查看在选定日发生的关闭和开放事件的明细。如果单击“未解决”值，相应事件列表即会显示，并过滤为显示当前未解决的事件(处于**正在调查**或**未启动**状态)。如果单击“已解决”值，相应事件列表即会显示，并过滤为显示不再处于未解决状态的事件(处于**已关闭**或**误报**状态)。

在括号中显示的 % 值表示与以前时间段比较的上升或下降。



战术检测

此小组件会显示在选定时间段内在事件中发现特定攻击技术的次数。

绿色值和红色值指示相较于上一时间段是增加还是减少。在下面的示例中，发现“特权提升”和“命令和控制”攻击相较于上一时间段有所增加；这可能指示您的凭证管理需要进行分析并增强安全性。

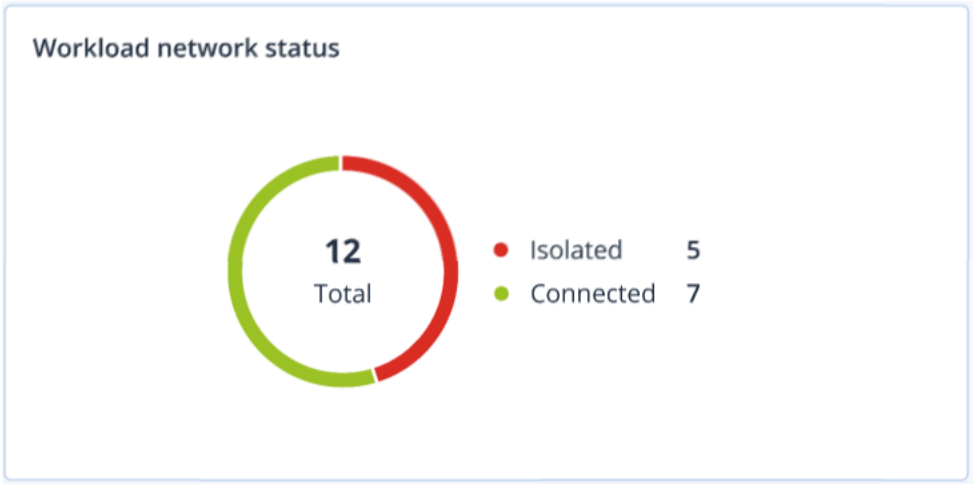
Detection by tactics

Initial Access	3	Discovery	3
Execution	7	Lateral Movement	0
Persistence	15	Collection	15
Priviledge Escalation	31	Command and Control	31
Defense Evasion	23	Exfiltration	23
Credential Access	7	Discovery	0
Impact	0	Resouce Development	0

工作负载网络状态

此小组件显示工作负载的当前网络状态，并指示隔离和连接了多少工作负载。

单击“已隔离”值可查看“装有代理程序的工作负载”列表（在 中控台中的**工作负载**菜单下），该列表会过滤为显示隔离的工作负载。单击“已连接”值可查看“装有代理程序的工作负载”列表，该列表过滤为显示连接的工作负载。



#CyberFit 分数(按计算机)

此小组件显示每台计算机的 #CyberFit 总分、其复合分数以及每个评估指标的发现:

- 反恶意软件
- 备份
- 防火墙
- VPN
- 加密
- NTLM 流量

要提高每个指标的分数,可以查看报告中提供的建议。

有关 #CyberFit 分数的更多详细信息,请参阅"计算机的 #CyberFit 分数"。

#CyberFit Score by machine

Metric	#CyberFit Score	Findings
DESKTOP-2N2TRE8	625 / 850	
Anti-malware	275 / 275	You have anti-malware protection enabled
Backup	175 / 175	You have a backup solution protecting your data
Firewall	175 / 175	You have a firewall enabled for public and private networks
VPN	0 / 75	No VPN solution was found, your connection to public and shared networks is n...
Encryption	0 / 125	No disk encryption was found, your device is at risk from physical tampering
NTLM traffic	0 / 25	Outgoing NTLM traffic to remote servers is not denied, your credentials may be ...

磁盘运行状况监控

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。
- 只可以监控物理计算机的磁盘。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。磁盘运行状况小组件不包括任何有关 RAID 已实现的计算机的信息。
- 不支持 NVMe SSD。
- 不支持外部存储设备。

磁盘运行状况可以表示为以下状态之一：

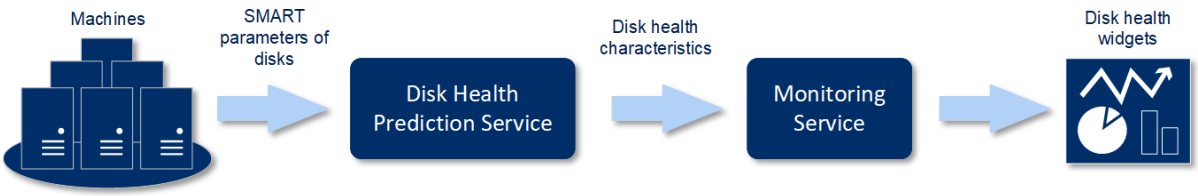
- **正常**
  磁盘运行状况为 70% 和 100% 之间。
- **警告**
  磁盘运行状况为 30% 和 70% 之间。
- **严重**
  磁盘运行状况为 0% 和 30% 之间。
- **计算磁盘数据**
  正在计算当前磁盘状态和预测。

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，然后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）。

   预测期为一个月。
3. 监视服务会收到这些特征，然后在 Cyber Protect 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

磁盘运行状况监视的结果显示在 Cyber Protect 中控台中可用的以下小组件中。

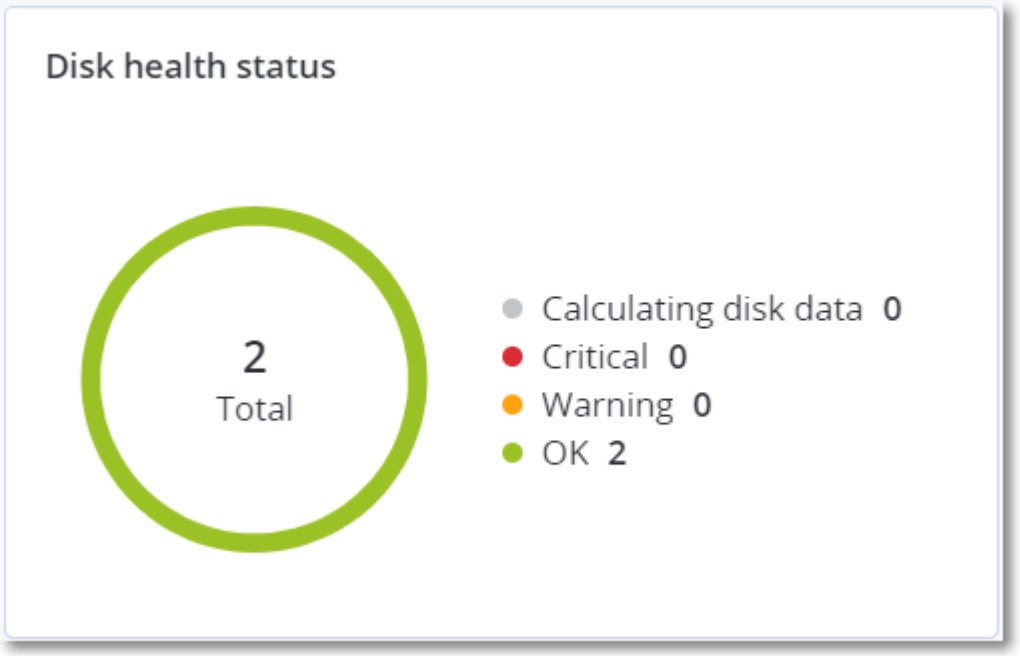
- **磁盘运行状况概述**是一个树形图小部件，具有可以通过向下钻取来切换的两个级别的详细信息。
  - 计算机级别
    显示有关每个选定客户计算机的磁盘运行状况状态的概要信息。仅显示最严重的磁盘状态。将光标悬停在特定块上时，其他状态会显示在工具提示中。计算机块的大小取决于该计算机所有磁盘的总大小。计算机块的颜色取决于找到的最严重磁盘状态。

  - 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	描述
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	严重	(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。此时，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

注意
该功能随 Advanced Backup 包提供。

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。

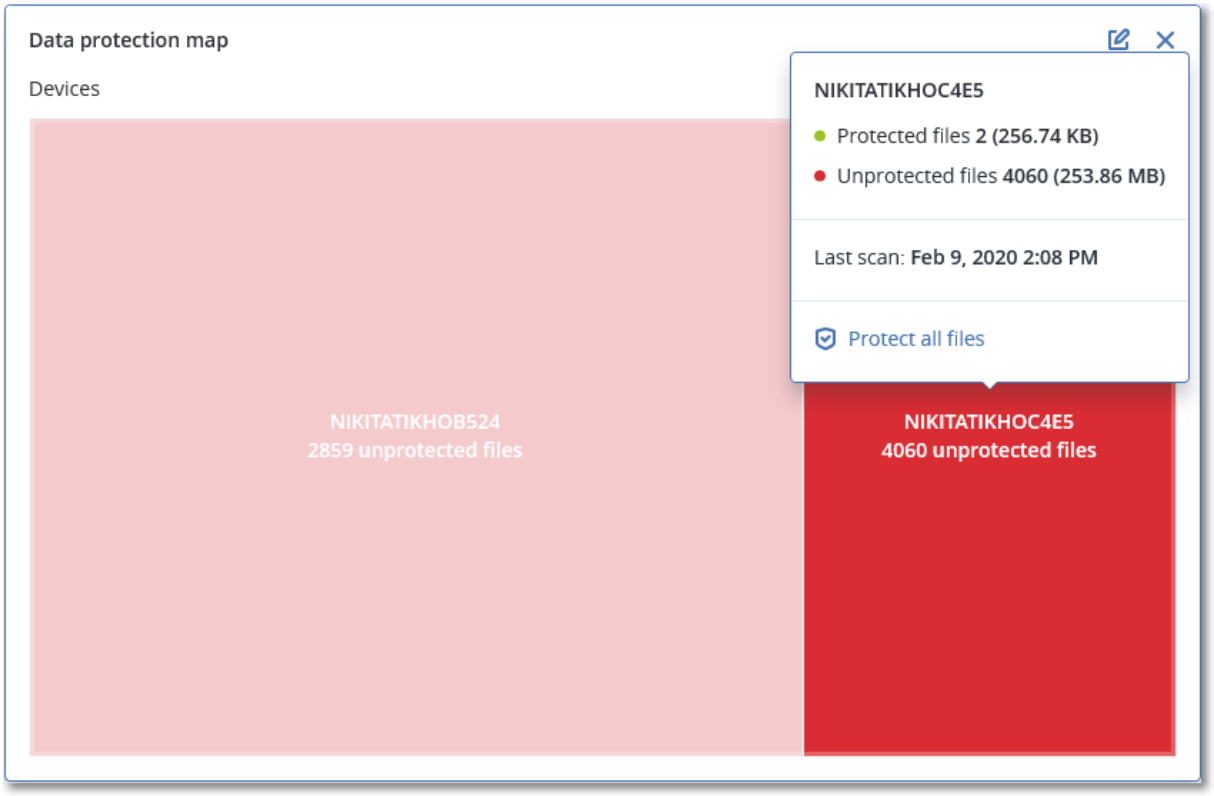
每个块的大小取决于属于客户/计算机的所有重要文件的总数/大小。

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”小组件（一个在计算机级别上显示详细信息的树形图小组件）的“监视”仪表板上找到：

- 计算机级别 - 显示有关选定客户的每台计算机的重要文件保护状态的信息。

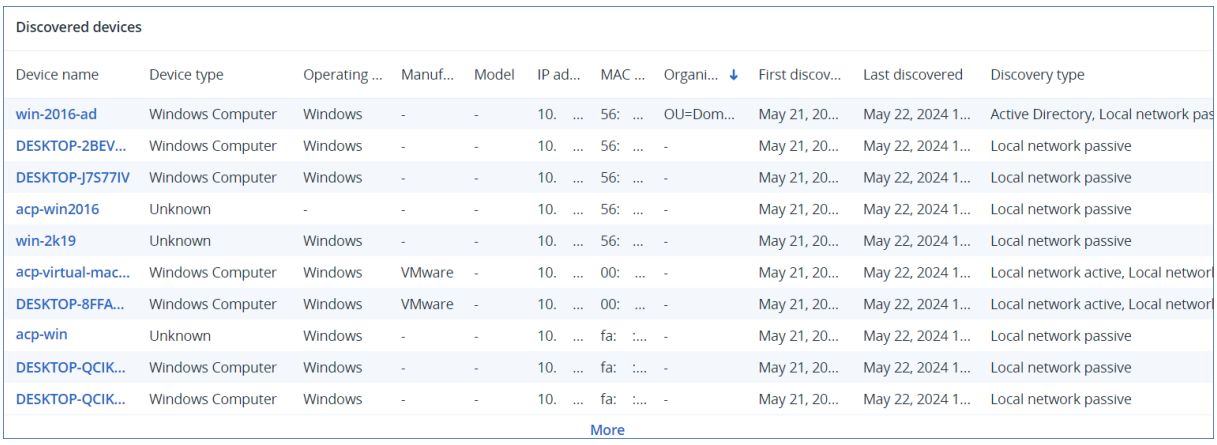


要保护不受保护的文件，请将光标悬停在相应块上，然后单击**保护所有文件**。在该对话框窗口中，可以找到有关不受保护文件数量及其位置的信息。要保护它们，请单击**保护所有文件**。

还可以下载 CSV 格式的详细报告。

已发现设备小组件

已发现设备表小组件显示了组织网络中通过主动和被动扫描发现的设备的详细信息。设备信息包括设备类型、制造商、操作系统、IP 地址、MAC 地址、发现日期等。



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。

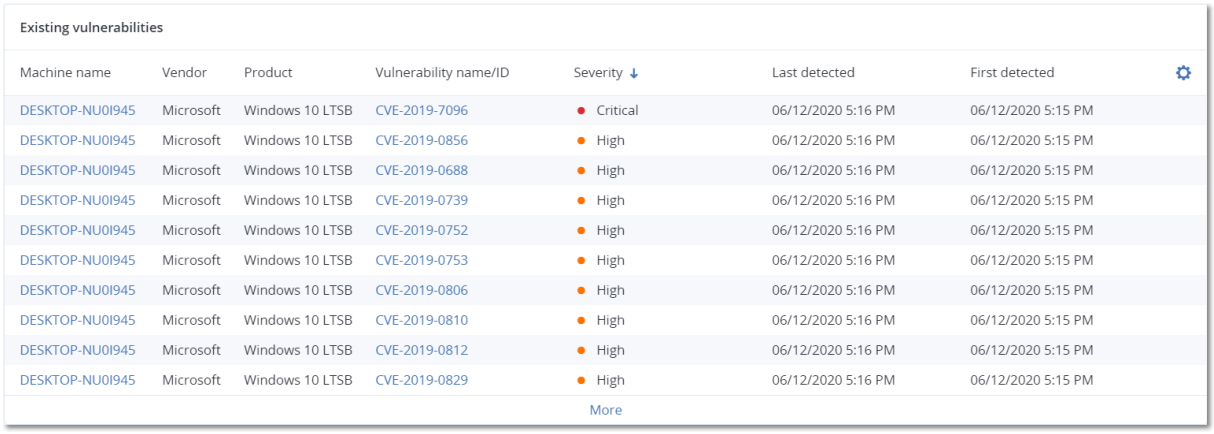
根据通用漏洞评分系统 (CVSS) v3.0, 发现的漏洞可能具有以下严重级别之一:

- 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。



Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

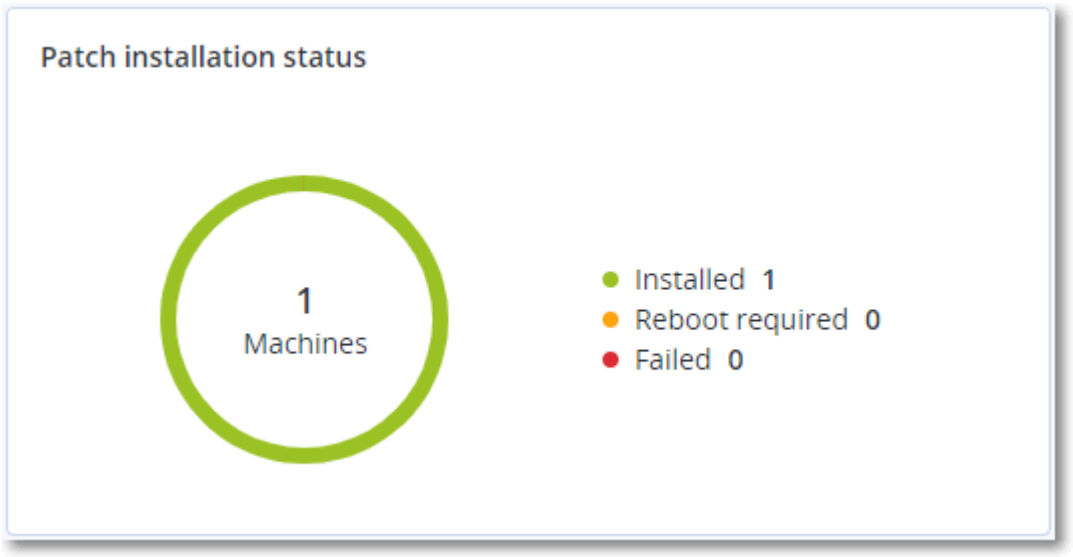
修补程序安装小部件

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

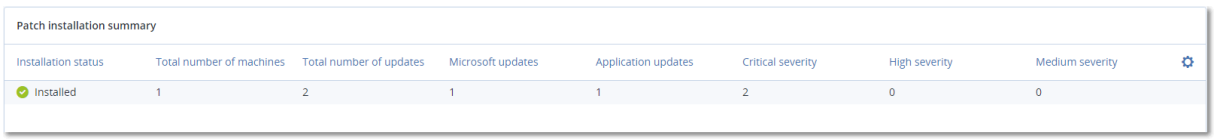
该小部件显示按修补程序安装状态分组的计算机数量。

- **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。



Patch installation summary

Installation status	Total number of machines	Total number of updates	Microsoft updates	Application updates	Critical severity	High severity	Medium severity
Installed	1	2	1	1	2	0	0

修补程序安装历史记录

该小部件显示有关计算机上修补程序的详细信息。

Patch installation history

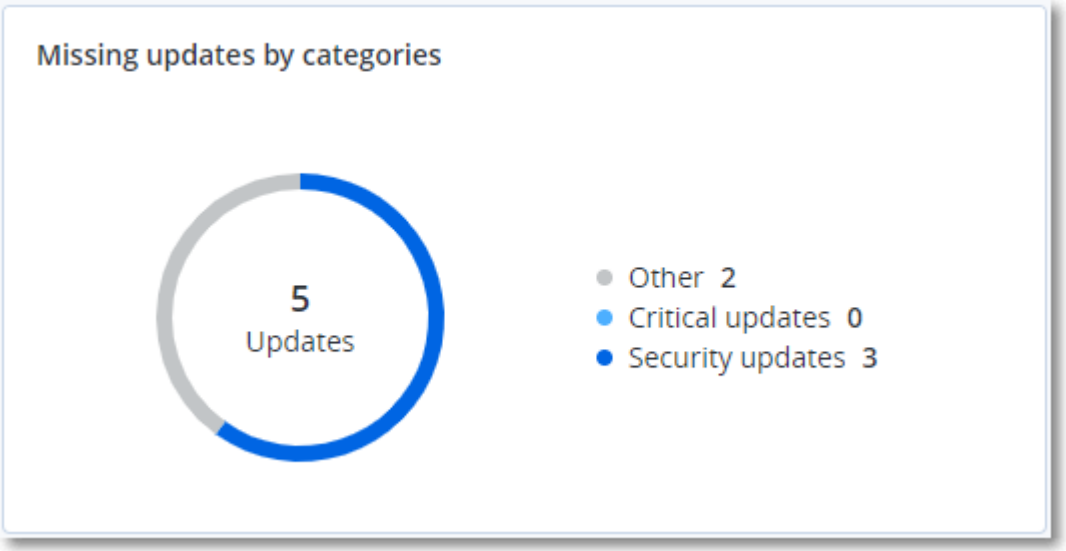
Machine name	Update name	Version	Severity	Approval status	Installation status	Installation date
NIKITATIKHOC4E5	FastStone Soft FastStone I...	5.9	Medium	New	Installed	02/05/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOB524	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Oracle Java Runtime Envir...	8.0.2410.7	High	New	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Installed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020
NIKITATIKHOC4E5	Mozilla Firefox	72.0.1	Critical	Approved	Failed	02/04/2020

More

按类别划分的缺少更新

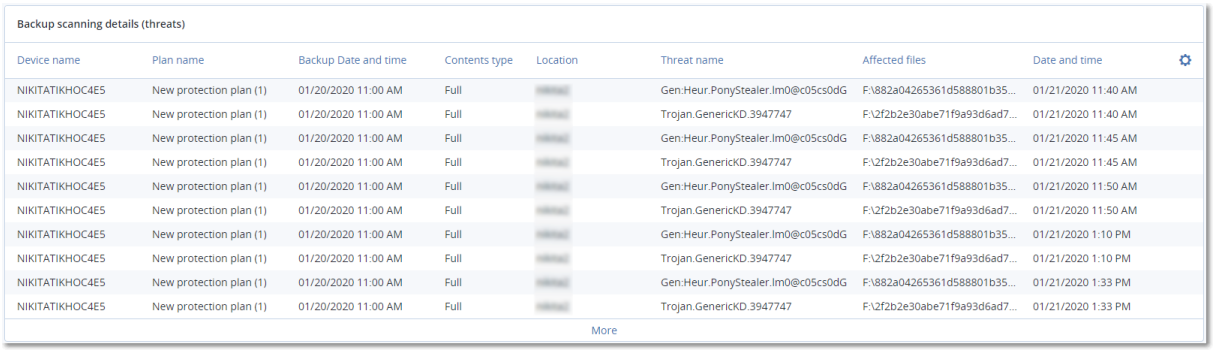
该小部件显示每个类别缺少的更新数量。显示以下类别：

- 安全更新
- 重要更新
- 其他



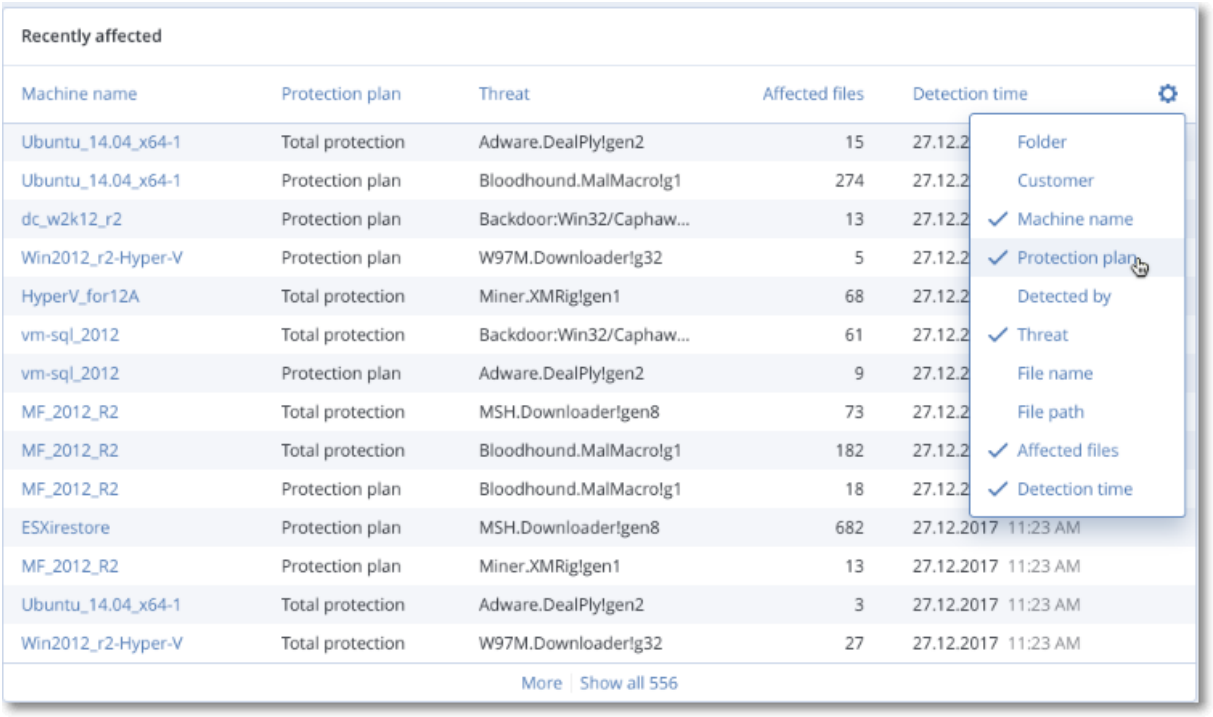
备份扫描详细信息

该小部件显示有关备份中检测到威胁的详细信息。



最近受影响

该小组件会显示有关受病毒、恶意软件和勒索软件等威胁影响的工作负载的详细信息。可以找到有关检测到的威胁、检测到威胁的时间以及受影响的文件数量的信息。



下载最近受影响工作负载的数据

可以下载最近受影响工作负载的数据、生成 CSV 文件，然后将其发送给指定的收件人。

下载最近受影响工作负载的数据

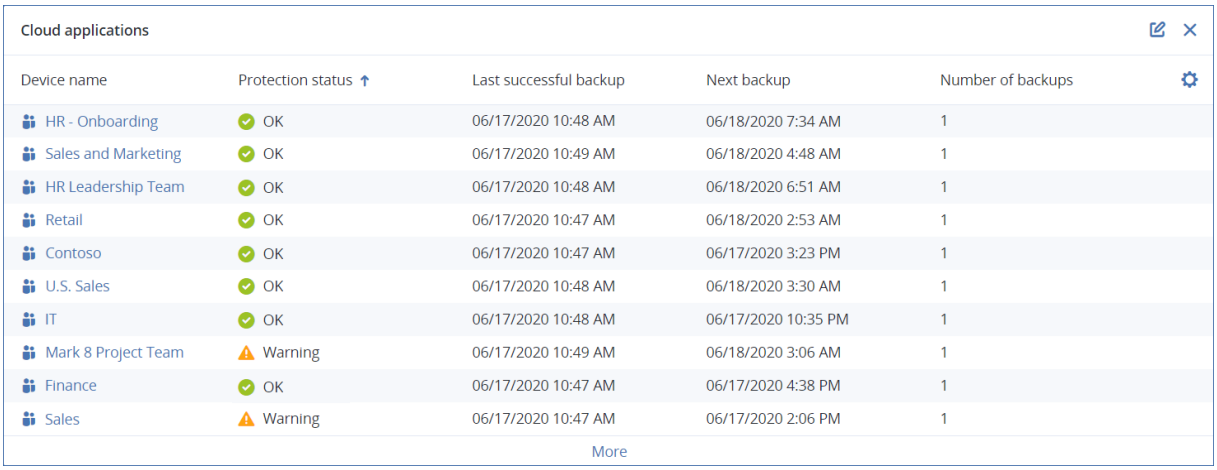
1. 在**最近受影响**小组件中，单击**下载数据**。
2. 在**时间段**字段中，输入要下载数据的天数。可以输入的最大天数为 200。
3. 在**收件人**字段中，输入将接收电子邮件（内含下载 CSV 文件的链接）的所有人员的电子邮件地址。
4. 单击**下载**。

系统开始生成 CSV 文件，其中包含指定的时间段内受影响工作负载的数据。CSV 文件准备完成后，系统会向收件人发送一封电子邮件。然后，每个收件人都可以下载该 CSV 文件。

云应用程序

此小组件显示有关云到云资源的详细信息：

- Microsoft 365 用户（邮箱、OneDrive）
- Microsoft 365 组（邮箱、组站点）
- Microsoft 365 公用文件夹
- Microsoft 365 站点集合
- Microsoft 365 Teams
- Google Workspace 用户（Gmail、Google Drive）
- Google Workspace Shared Drive



以下小组件中还提供了有关云到云资源的其他信息：

- 活动
- 活动列表
- 5 个最新警告
- 警告历史记录
- 活动警告摘要
- 历史警告摘要
- 活动警告详细信息
- 位置汇总

软件小组件

软件清查小组件

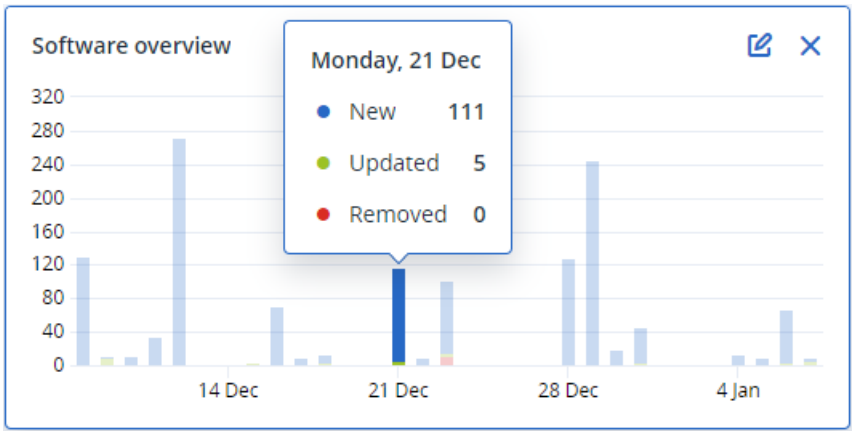
软件盘点表小组件会显示有关贵组织中 Windows 和 macOS 设备上安装的所有软件的详细信息。

Software inventory

Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User
Ivelins-Mac-mini-2.local									
Ivelins-Mac-mini-2.local	-	15.0.26046	-	No change	-	12/12/2020, 3:26 AM	12/14/2020, 10:24 AM	/Library/Application Supp...	root
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Pages.app	root
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Keynote.app	root
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Numbers.a...	root
Ivelins-Mac-mini-2.local	Canon IJScanner2	4.0.0	Canon Inc. (XE2XNRRXZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root
Ivelins-Mac-mini-2.local	Canon IJScanner4	4.0.0	Canon Inc. (XE2XNRRXZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root
Ivelins-Mac-mini-2.local	Canon IJScanner6	4.0.0	Canon Inc. (XE2XNRRXZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root
Ivelins-Mac-mini-2.local	commandFilter	1.71	EPSON (TXAEAV5RN4)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Printers/EPSON/...	root
Ivelins-Mac-mini-2.local	Cyber Protect Agent Assis...	1	Acronis International Gm...	No change	-	12/12/2020, 10:01 AM	12/14/2020, 10:24 AM	/Applications/Utilities/Cy...	root
Ivelins-Mac-mini-2.local	Cyber Protect Agent Unin...	1	Acronis International Gm...	No change	-	12/12/2020, 3:28 AM	12/14/2020, 10:24 AM	/Library/Application Supp...	root

More

软件概述小组件会显示特定时段(7 天、30 天或当月)内贵组织中 Windows 和 macOS 设备上新的、已更新和已删除应用程序的数量。



将光标悬停在图表上的某一栏上时,将显示带有以下信息的工具提示:

新的 - 新安装应用程序的数量。

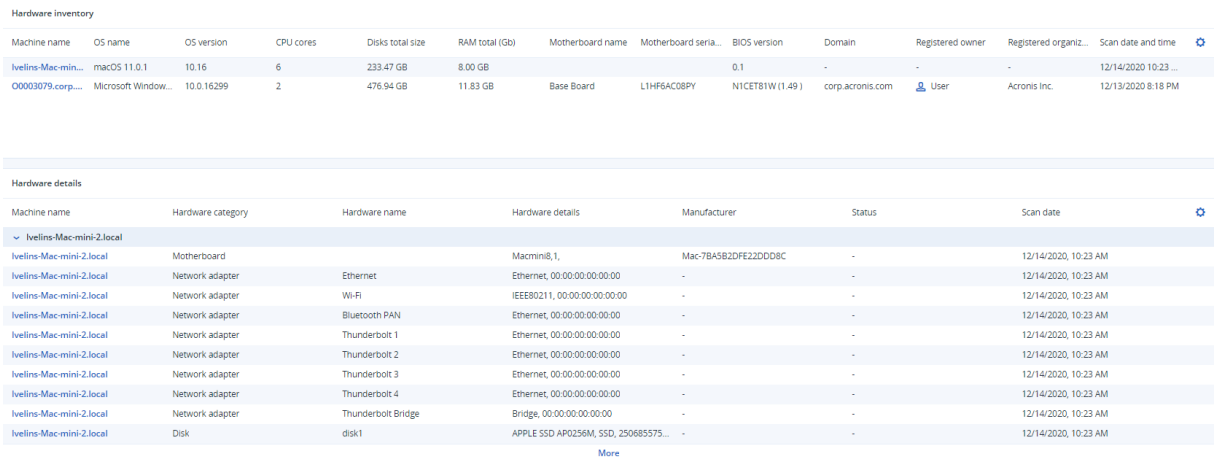
已更新 - 已更新应用程序的数量。

已删除 - 已删除应用程序的数量。

单击栏上特定状态的部分时,系统会将您重定向到**软件管理** -> **软件清查**页面。将针对相应日期和状态过滤该页面中的信息。

硬件清查小组件

硬件清查和**硬件详细信息**表小组件会显示有关贵组织中物理和虚拟 Windows 及 macOS 设备上安装的所有硬件的信息。



Hardware inventory

Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-min...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
O0003079.corp....	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Hardware details

Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local						
Ivelins-Mac-mini-2.local	Motherboard		Macmini8,1,	Mac-7BA5B2DFE22DDD8C	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt Bridge	Bridge, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Disk	disk1	APPLE SSD AP0256M, SSD, 250685575...	-	-	12/14/2020, 10:23 AM

More

硬件更改表小组件会显示有关特定时段(7 天、30 天或当月)内贵组织中物理和虚拟 Windows 及 macOS 设备上已添加、已删除和已更改硬件的信息。

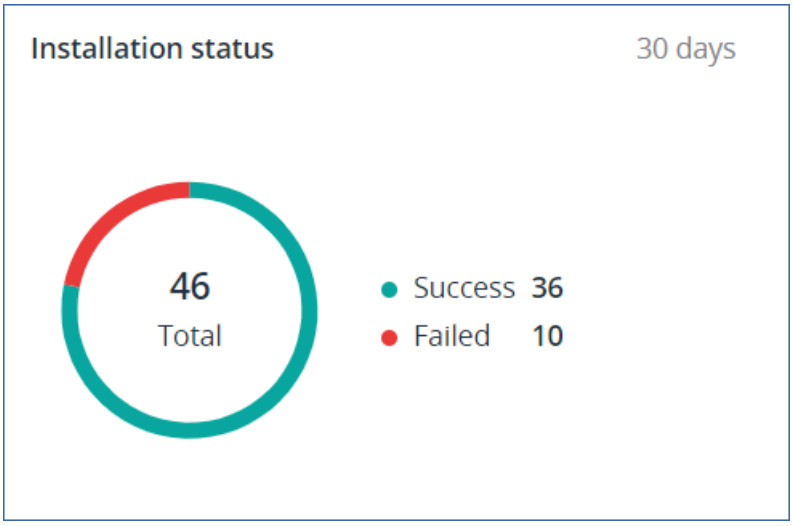
Hardware changes

Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF					
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, PF0PJB10	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM

More

程序安装小组件

安装状态小组件按状态显示已安装的活动总数。单击圆环图的某个部分,将重定向到**活动**页面,该页面仅显示具有相应状态的活动,按时间顺序排列。



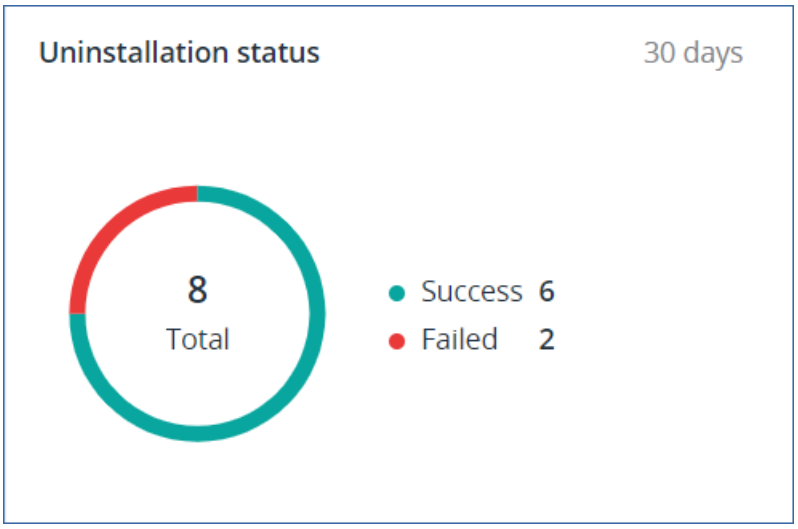
软件安装历史小组件提供有关受控设备上远程软件安装的详细状态信息。单击**安装状态**列中的状态,将重定向到**活动**页面,该页面将按时间顺序显示具有相应状态的活动。

Software installation history — 30 days

Machine name	Software name	Vendor name	Version	Installation date	Software plan	Signature check st...	Installation status
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	15.08.2024	15AugInstallNotep...	Verified	Failed
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	15.08.2024	15AugInstallNotep...	Verified	Failed
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	15.08.2024	15AugInstallNotep...	Verified	Failed
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	15.08.2024	15AugInstallNotep...	Verified	Failed
DESKTOP-0SKJ...	Tableau	Tableau Software	24.2.544	16.08.2024	16RebbotIfRequir...	Verified	Success
DESKTOP-0SKJ...	Tableau	Tableau Software	24.2.544	16.08.2024	16RebbotIfRequir...	Verified	Success
DESKTOP-0SKJ...	Notepad++	Notepad++ Team	8.6.9	22.08.2024	22AugInstallNotep...	Verified	Success

软件卸载小组件

卸载状态小组件按状态显示卸载的活动总数。单击圆环图的某个部分，将重定向到**活动**页面，该页面仅显示具有相应状态的活动，按时间顺序排列。



软件卸载历史小组件提供有关受控设备上远程软件卸载的详细状态信息。单击**卸载状态**列中的状态，将重定向到**活动**页面，该页面将按时间顺序显示具有相应状态的活动。

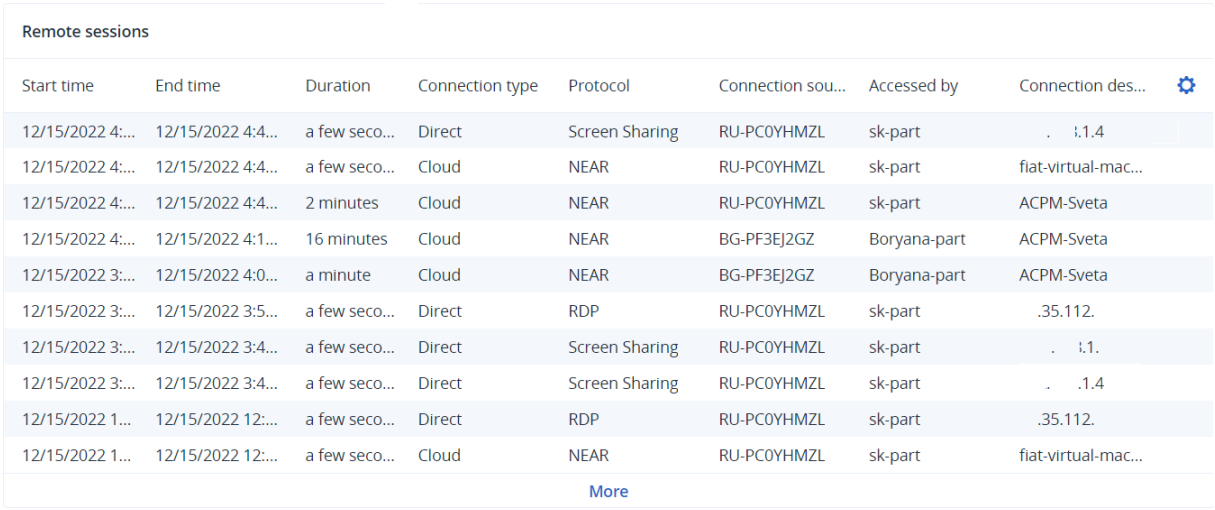
Software uninstallation history — 30 days

Machine name	Software name	Vendor name	Uninstallation date	Uninstallation status	Software plan
DESKTOP-0SKJMF9	Firefox	Mozilla	22.08.2024	Success	22AugFirefoxUninstall2
DESKTOP-0SKJMF9	Firefox	Mozilla	22.08.2024	Success	22AugFirefoxUninstall2
DESKTOP-0SKJMF9	Tableau	Tableau Software	21.08.2024	Success	Quick uninstall action
DESKTOP-0SKJMF9	Notepad++	Notepad++ Team	21.08.2024	Success	Quick uninstall action
DESKTOP-0SKJMF9	Tableau	Tableau Software	21.08.2024	Success	Quick uninstall action
DESKTOP-0SKJMF9	Tableau	Tableau Software	21.08.2024	Success	Quick uninstall action
DESKTOP-0SKJMF9	KeePass	Dominik Reichl	21.08.2024	Failed	Quick uninstall action
DESKTOP-0SKJMF9	KeePass	Dominik Reichl	20.08.2024	Failed	Quick uninstall action
DESKTOP-0SKJMF9	MySQLInstaller	Oracle Corporation	14.08.2024	Cancelled	Quick uninstall action
DESKTOP-0SKJMF9	Tableau	Tableau Software	14.08.2024	Cancelled	Quick uninstall action

More

远程会话小组件

此小组件会显示有关远程桌面和文件传输会话的详细信息。



智能保护

威胁源

安克诺斯 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。

注意
此功能的可用性取决于为您的帐户启用的服务配额。

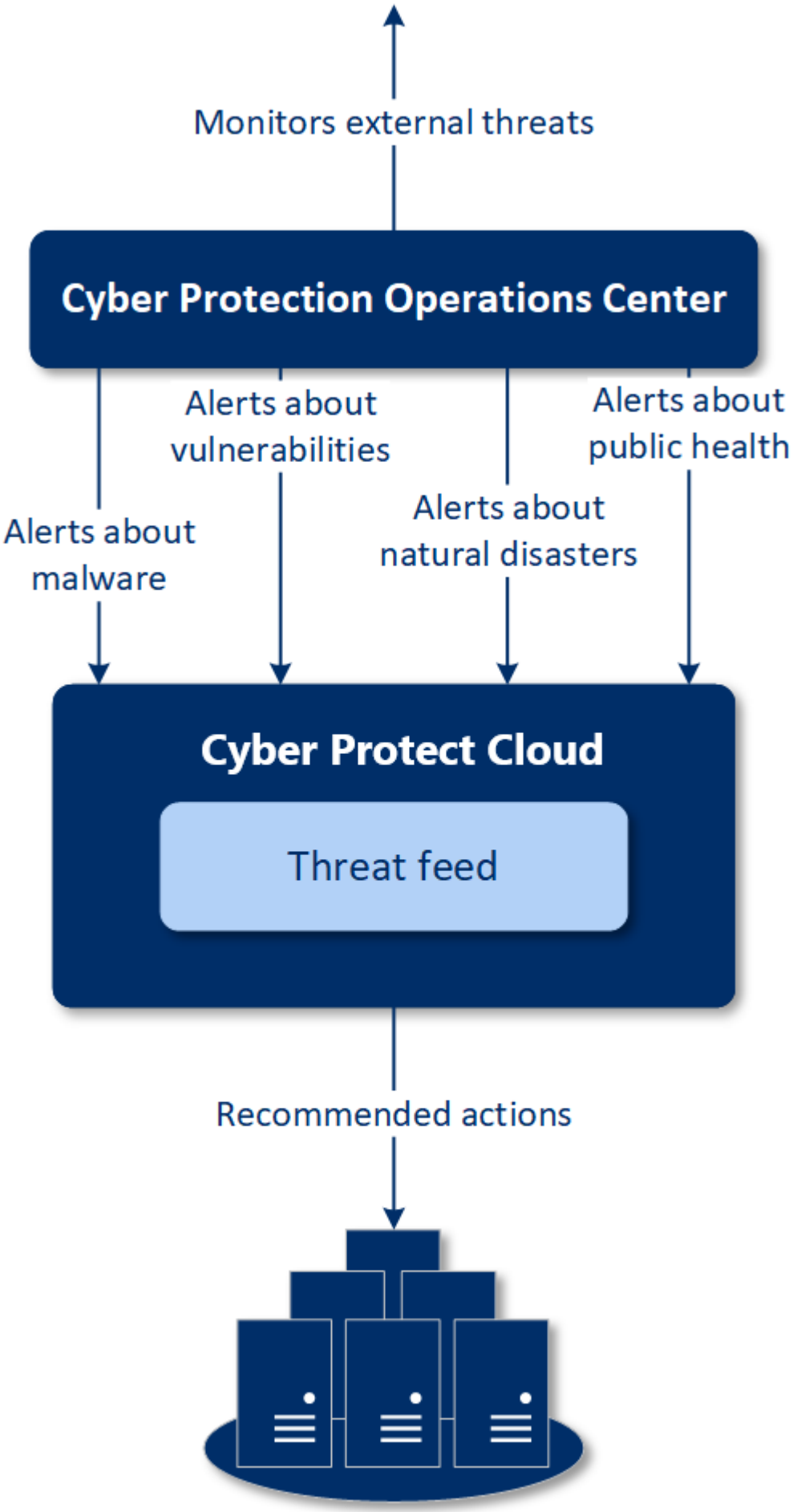
可以通过遵循安全专家提供的一组特定操作来解决某些安全警报。其他安全警报仅通知您即将到来的威胁，但不提供建议操作。

注意
恶意软件警报仅针对安装有适用于反恶意软件保护的代理程序的计算机生成。

工作方式

安克诺斯 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 Cyber Protect 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 安克诺斯 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 Cyber Protect 中控台中，转到**监视** > **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** – 对选定计算机运行全面扫描

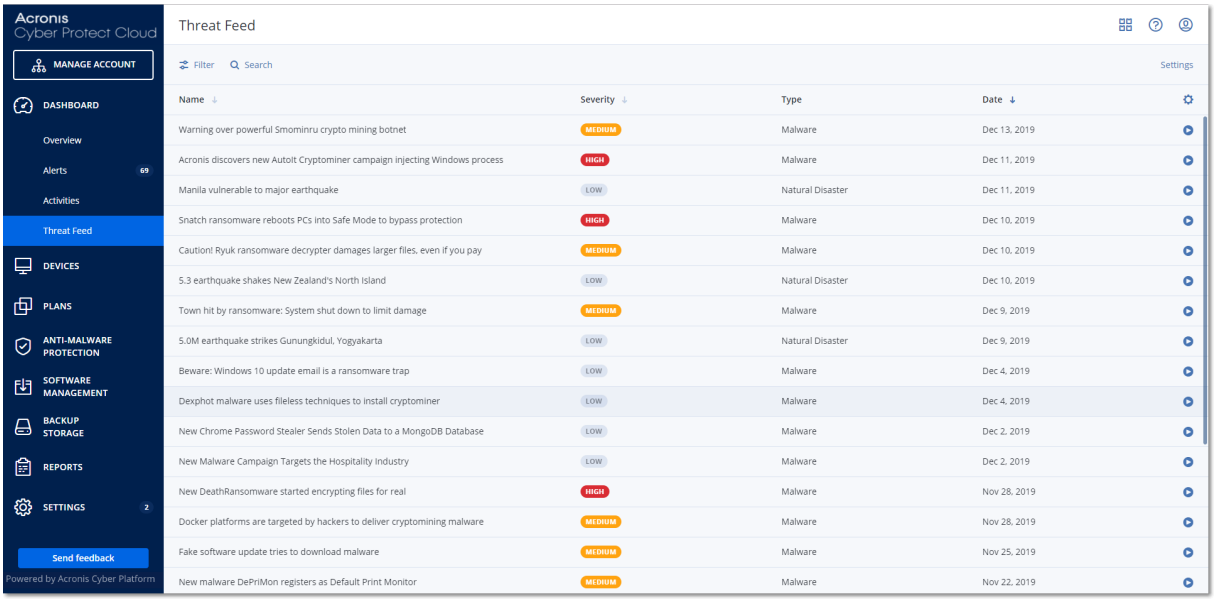
     注意
     此操作仅可用于安装有适用于反恶意软件保护的代理程序的计算机。

   - **受保护或不受保护计算机的备份** - 备份受保护和不受保护的工作负载。
     如果工作负载还没有备份(在所有可访问的位置、云和本地)或现有备份已加密，则系统会按以下名称格式创建完整备份：

     `%workload_name%-Remediation`

     默认情况下，备份的目标是 Cyber Protect Cloud 存储，但可以在开始操作之前配置其他位置。

     如果未加密备份已存在，则系统会在现有存档中创建增量备份。
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

在以下时间段后执行从威胁馈送自动清理：

- 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 Cyber Protect 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。

   您将看到每个扩展和每个位置上不受保护文件的数量。在搜索字段中定义扩展,您想要为其获取有关不受保护文件的信息。
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。

现场	描述
使用以下事件预定任务运行	此设置定义任务将何时运行。 以下值可用： • **按时间预定** - 这是默认设置。任务将根据指定的时间运行。 • **用户登录系统时** - 默认情况下，任何用户登录都会触发任务。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，任何用户注销都会触发任务。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。
预定类型	如果在**使用以下事件预定任务运行**中选择了**按时间预定**，则该字段会显示。 以下值可用： • **月** – 选择运行任务的月份和月份中的特定周或特定天。 • **每日** - 这是默认设置。选择任务将在星期几运行。 • **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。
启动时间	如果在**使用以下事件预定任务运行**中选择了**按时间预定**，则该字段会显示。 选择任务将运行的确切时间。
在日期范围内运行	如果在**使用以下事件预定任务运行**中选择了**按时间预定**，则该字段会显示。 设置配置的预定将有效的日期范围。
指定登录到操作系统将启动任务的用户帐户	如果在**使用以下事件预定任务运行**中选择了**用户登录系统时**，则该字段会显示。 以下值可用： • **任何用户** - 如果希望任何用户的登录触发任务，请使用此选项。 • **以下用户** - 如果仅希望特定用户帐户的登录触发任务，请使用此选项。
指定从操作系统注销将启动任务的用户帐户	如果在**使用以下事件预定任务运行**中选择了**用户注销系统时**，则该字段会显示。 以下值可用： • **任何用户** - 如果希望任何用户的注销触发任务，请使用此选项。 • **以下用户** - 如果仅希望特定用户帐户的注销触发任务，请使用此选项。

现场	描述
开始条件	定义为了任务能够运行而必须同时满足的所有条件。 防恶意软件扫描的开始条件类似于“开始条件”中所述的**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 10:00 点，延迟时间为 60 分钟，则任务将在上午 10:00 点到上午 11:00 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。

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系统文件和文件夹。

“活动”选项卡

活动选项卡会提供过去 90 天的活动概述。

在仪表板上过滤活动

1. 在**设备名称**字段中，指定在其上执行活动的计算机。
2. 从**状态**下拉列表中，选择状态。例如，已成功、失败、进行中、已取消。
3. 从**远程操作**下拉列表中，选择操作。例如，正在应用计划、正在删除备份、正在安装软件更新。
4. 在**最近**字段中，设置活动的时间段。例如，最近的活动、过去 24 小时的活动或过去 90 天中特定时段内的活动。
5. 如果您以合作伙伴管理员身份访问**活动**选项卡，则可以过滤您管理的特定客户的活动。

要自定义**活动**选项卡的视图，请单击齿轮图标，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。

要取消正在运行的活动，请单击其名称，然后在**详细信息**屏幕上单击**取消**。

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。

可以通过以下属性过滤远程桌面活动：

- 正在创建计划
- 正在应用计划
- 正在吊销计划
- 删除计划
- 远程连接
  - 通过 RDP 进行云远程桌面连接
  - 通过 NEAR 进行云远程桌面连接
  - 通过 Apple 屏幕共享进行云远程桌面连接
  - 通过 Web 客户端进行远程桌面连接
  - 通过 Quick Assist 进行远程桌面连接
  - 通过 RDP 进行直接远程桌面连接
  - 通过 Apple 屏幕共享进行直接远程桌面连接
  - 文件传输
  - 通过 Quick Assist 进行文件传输
- 远程操作
  - 正在关闭工作负载
  - 正在重新启动工作负载
  - 正在注销工作负载上的远程用户
  - 正在清空工作负载上用户的回收站
  - 正在让工作负载进入睡眠状态

Cyber Protect Monitor

Cyber Protect Monitor会显示有关计算机(已安装适用于 Windows 的代理程序或适用于 Mac 的代理程序)的保护状态的信息，并允许其用户配置备份加密和代理服务器设置。

当适用于 File Sync & Share 的代理程序安装在计算机上时，Cyber Protect Monitor提供对 File Sync & Share 服务的访问。File Sync & Share 是强制加入后即可访问的功能，在此期间用户需登录自己的 File Sync & Share 帐户并选择个人同步文件夹。有关适用于 File Sync & Share 的代理程序的更多信息，请参阅 Cyber Files Cloud用户指南。

重要事项
Cyber Protect Monitor可供可能没有 Cyber Protection 或 File Sync & Share 服务管理权限的用户访问。

下表总结了没有管理权限的用户可以执行的操作。

已安装代理程序	用户可以	用户无法
适用于 Windows 的代理程序或适用于 Mac 的代理程序	• 将默认保护计划应用于他们的计算机 • 检查他们的计算机的保护状态 • 接收 Active Protection 通知 • 暂时暂停他们的计算机的备份 • 配置代理服务器设置 • 更改备份加密设置 **警告！** 更改 Cyber Protect Monitor中的加密设置会覆盖保护计划中的设置并影响计算机的所有备份。此操作可能会导致某些保护计划失败。有关详细信息，请参阅 "加密"(第 391 页)。 如果您丢失或忘记密码，则无法恢复加密备份。	• 应用自定义保护计划 • 管理已应用的保护计划
Windows 代理程序和Sync and Share 代理程序 适用于 Mac 的代理程序和Sync and Share代理程序	• 同步他们的本地同步文件夹和他们的 File Sync & Share 帐户之间的内容 • 暂停同步操作 • 更改同步文件夹 • 检查无法同步的文件类型	• 编辑无法同步的文件类型

在 Cyber Protect Monitor中配置代理服务器设置

可以在 Cyber Protect Monitor中配置代理服务器设置。该配置会影响安装在计算机上的所有代理程序。

配置代理服务器设置

1. 打开 Cyber Protect Monitor，然后单击右上角的齿轮图标。
2. 单击**设置**，然后单击**代理**。
3. 启用**使用代理服务器**开关，然后输入代理服务器地址和端口。
4. [如果代理服务器访问受密码保护] 启用**需要密码**开关，然后输入用于访问代理服务器的用户名和密码。
5. 单击**保存**。

   代理服务器设置即会保存在 `http-proxy.yaml` 文件中。

报告

注意
此功能的可用性取决于为您的帐户启用的服务配额。

操作的相关报告可以包括任何一组仪表板小组件。所有小组件都会显示整个公司的概要信息。

根据小组件类型，报告包括时间范围内的数据或者浏览或报告生成时的数据。请参阅 "根据小组件类型报告的数据"(第 264 页) 。

所有历史小组件都会显示同一时间范围内的数据。可以在报告设置中更改此范围。

可以使用默认报告，也可以创建自定义报告。

可以下载报告，也可以通过电子邮件以 XLSX (Excel) 或 PDF 格式发送该报告。

默认报告集取决于所拥有的 Cyber Protection 服务版本。默认报告如下所示：

报告名称	描述
#CyberFit 分数 (按计算机)	根据对每台计算机的安全指标和配置的评估，显示 #CyberFit 分数和改进建议。
警告	显示某一指定时间段内发生的警告。
备份扫描详细信息	显示有关备份中检测到威胁的详细信息。
每日活动	显示有关某一指定时间段内已执行活动的概要信息。
数据保护地图	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	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	显示在组织网络中发现的所有计算机。
磁盘运行状况预测	显示 HDD/SSD 故障发生时间预测和当前磁盘状态。
现有漏洞	显示您组织中操作系统和应用程序的现有漏洞。该报告还会显示您网络中受影响计算机的每个列出产品的详细信息。
软件库存记录	显示有关贵公司设备上安装的软件的信息。
硬件清查	显示有关贵公司设备上可用的硬件的信息。
修补程序管理摘要	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	显示有关某一指定时间段内受保护设备的概要信息。
每周活动	显示有关某一指定时间段内已执行活动的概要信息。
远程会话	显示有关远程桌面和文件传输会话的信息。

对报告的操作

添加

添加新报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在可用报告列表下，单击**添加报告**。
3. [添加预定义报告] 单击预定义报告的名称。
4. [添加自定义报告] 单击**自定义**，然后为报告添加小组件。
5. [可选] 拖放小组件，可重新排列它们。

查看

若要查看报告

- 要查看报告，请单击其名称。

编辑

若要编辑报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择要编辑的报告。
3. 在屏幕的右上角，单击**设置**。
4. 编辑报告，然后单击**保存**。

删除

删除报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择要删除的报告。
3. 在屏幕的右上角，单击省略号图标 (...)，然后单击 **删除报告**。
4. 在确认窗口中，单击**删除**。

预定

若要安排报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择要预定的报告。
3. 在屏幕的右上角，单击**设置**。
4. 在 **已预订** 旁边，启用开关。
   - 指定收件人的电子邮件地址。
   - 选择报告的格式。

   - **注意**
     可以在 PDF 文件中导出多达 1,000 个项目，在 XLSX 文件中导出多达 10,000 个项目。PDF 和 XLSX 文件中的时间戳使用计算机的本地时间。

   - 选择报告的语言。
   - 配置预定。
5. 单击**保存**。

下载

下载报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择报告。
3. 请在屏幕的右上角单击**下载**。
4. 选择报告的格式。

因此，所选格式的文件将下载到您的计算机。

如果您选择了 **Excel 和 PDF**，则会将 ZIP 文件下载到您的计算机。

发送

发送报告

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择报告。
3. 在屏幕的右上角，单击**发送**。
4. 指定收件人的电子邮件地址。
5. 选择报告的格式。
6. 单击**发送**。

导出结构

导出报告结构

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择报告。
3. 在屏幕的右上角，单击省略号图标 (...)，然后单击 **导出**。

因此，报告结构将作为 JSON 文件保存在计算机上。

转储数据

转储报告数据

您可以将自定义期间的所有数据导出到 CSV 文件，而无需对其进行筛选，并将 CSV 文件发送至电子邮件收件人。CSV 文件仅包含报告中包含的小组件的数据。

注意
可以在一个 CSV 文件中导出多达 150,000 个项目。CSV 文件中的时间戳使用协调世界时 (UTC)。

1. 在 Cyber Protect 中控台中，转到**报告**。
2. 在报告列表中，选择要转储其数据的报告。
3. 在屏幕的右上角，单击省略号图标 (...)，然后单击 **转储数据**。
4. 指定收件人的电子邮件地址。
5. 在**时间范围**中，指定要转储数据的自定义时间段。

   注意
   准备较长时间段的 CSV 文件需要花费更多时间。

6. 单击**发送**。

根据小组件类型报告的数据

根据它们所显示的数据范围，仪表板上的小组件分为两类：

- 在浏览或报告生成时显示实际数据的小组件。
- 显示历史数据的小组件。

在报告设置中配置日期范围以转储特定时间段的数据时，所选时间范围将仅适用于显示历史数据的小组件。对于浏览时显示实际数据的小组件，时间范围参数不适用。

下表列出了可用的小组件及其数据范围。

小组件名称	小组件和报告中显示的数据
#CyberFit 分数(按计算机)	实际
5 个最新警告	实际
活动警告详细信息	实际
活动警告摘要	实际
活动	历史
活动列表	历史
警告历史记录	历史
攻击战术统计数据	历史
备份扫描详细信息(威胁)	历史
备份状态	历史 - 在**运行总计**和**成功运行次数**列中 实际 - 在其他所有列中
已阻止 URL	实际
云应用程序	实际
Cyber protection	实际
数据保护地图	历史
设备	实际
已发现的设备	实际
磁盘运行状况概述	实际
磁盘运行状况(按物理设备)	实际
现有漏洞	历史

硬件更改	历史
硬件详细信息	实际
硬件清查	实际
历史警告摘要	历史
事件严重性历史记录	历史
位置汇总	实际
按类别划分的缺少更新	实际
未保护	实际
修补程序安装历史记录	历史
修补程序安装状态	历史
修补程序安装摘要	历史
保护状态	实际
最近受影响	历史
远程会话	历史
安全性事件刻录	历史
安全性事件 MTTR	历史
软件库存记录	实际
软件概述	历史
威胁状态	实际
易受攻击的计算机	实际
工作负载网络状态	实际

在 Cyber Protect 中控台中管理工作负载

本部分介绍如何在 Cyber Protect 中控台中管理工作负载。

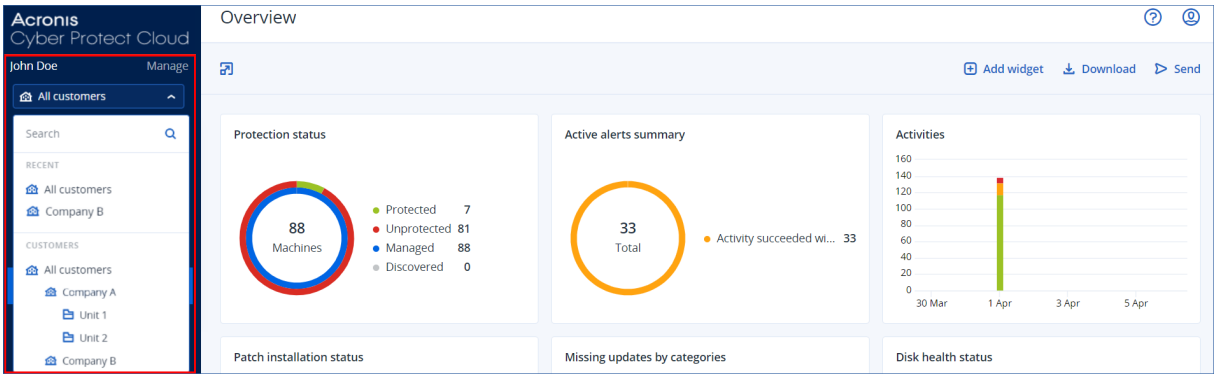
Cyber Protect 中控台

在 Cyber Protect 中控台中，可以管理工作负载和计划、更改保护设置、配置报告，或检查备份存储。

通过 Cyber Protect 中控台，可以访问其他服务或功能，例如“File Sync & Share”、防病毒和防恶意软件保护、修补程序管理、设备控制以及漏洞评估。这些服务和功能的类型和数量会因您的 Cyber Protection 许可证而异。

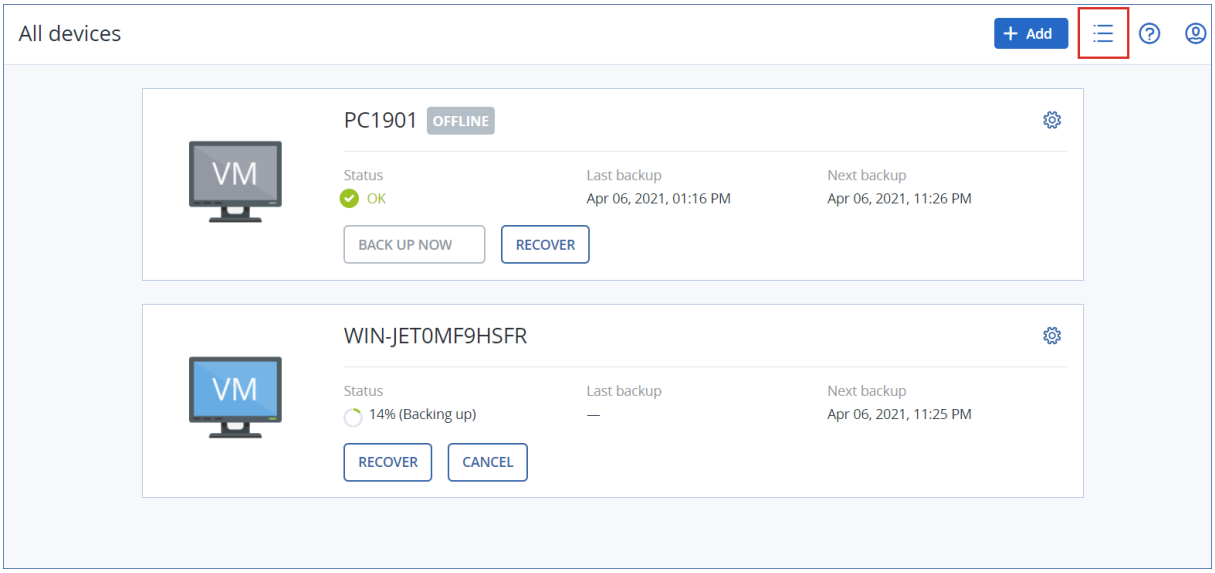
要查看包含有关您保护的最重要信息的仪表板，请转到**监控** > **概述**。

根据您的访问权限，可以为一个或多个客户租户或者一个租户中的单位管理保护。要切换层次结构级别，请使用导航菜单中的下拉列表。仅显示您有权访问的级别。要转到管理门户，请单击**管理**。

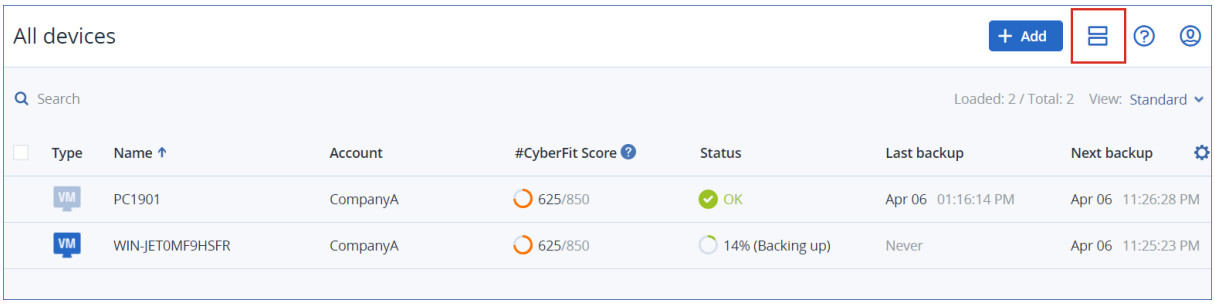


设备部分在简单视图和表视图中可用。若要在不同视图之间切换，请单击右上角的相应图标。

简单视图仅显示少数工作负载。



当工作负载数量变大时，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。

当一个工作负载联机或脱机时，该工作负载在 Cyber Protect 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工作负载状态。如果安装在相应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，则该工作负载会显示为“脱机”。当工作负载应答状态检查或开始传输数据时，该工作负载会重新显示为“联机”。

Cyber Protect 中控台中的新增功能

在 Cyber Protect Cloud 的新功能可用后，您会在登录到 Cyber Protect 中控台时看到一个弹出窗口，其中简要描述了这些功能。

还可以通过单击主 中控台窗口左下角的**新增功能**链接，来查看新功能的描述。

如果没有新功能，则不会显示**新增功能**链接。

以合作伙伴管理员身份使用 Cyber Protect 中控台

作为合作伙伴管理员，您可以使用合作伙伴租户(**所有客户**)级别或客户租户级别的 Cyber Protect 中控台。

合作伙伴租户(**所有客户**)级别

在合作伙伴租户(**所有客户**)级别，您可以执行以下操作：

- 管理所有托管客户租户的工作负载的脚本编写计划。
  可以将相同的脚本计划应用于不同客户中的工作负载，并创建包含来自不同客户的工作负载的设备组。要了解如何在合作伙伴级别上创建静态或动态设备组，请参阅 "在合作伙伴级别创建静态设备组"(第 270 页) 和 "在合作伙伴级别上创建动态设备组"(第 270 页)。有关脚本和脚本计划的详细信息，请参阅 "网络安全脚本"(第 333 页)。
- 为所有托管客户租户的工作负载创建监控计划。
- 为所有托管客户租户的工作负载创建远程管理计划。
- 查看在受管理的客户租户中使用的保护计划，并按状态、客户和创建日期筛选计划。
- 在一个事件管理界面中查看和管理所有客户租户的 Endpoint Detection and Response (EDR) 事件，而不是访问每个客户的事件屏幕。
- 为所有托管客户租户执行计算机自动发现。

客户租户级别

在此级别上，您拥有与您所代表的公司管理员相同的权限。

选择租户级别

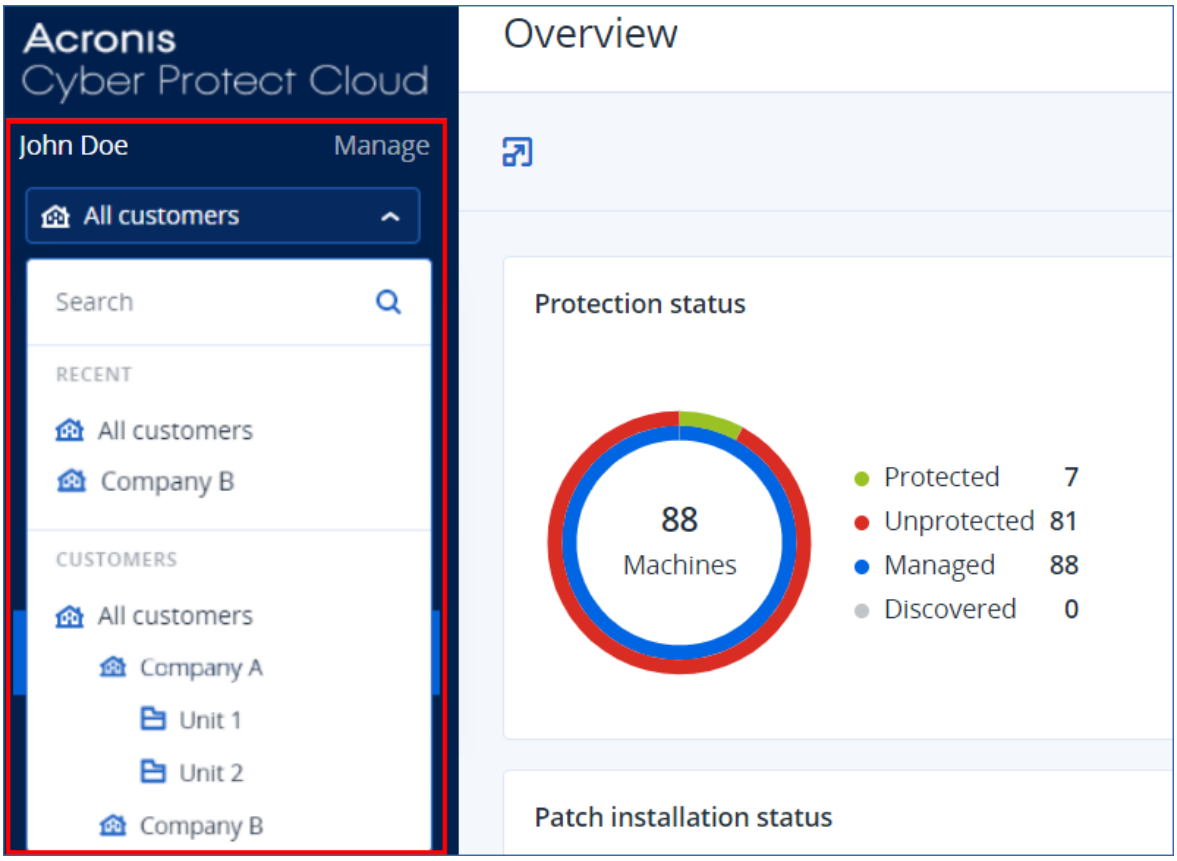
可以在 Cyber Protect 中控台中选择要在其中工作的租户级别。

先决条件

- 您有权访问 Cyber Protect 中控台并管理门户。
- 您可以管理多个租户或单位。

若要在 Cyber Protect 中控台中选择租户级别

1. 在左侧的导航菜单中，单击客户租户名称旁边的箭头。
2. 选择下列选项之一：
   - 要在合作伙伴级别上工作，请选择**所有客户**。
   - 要在客户或单位级别上工作，请选择该客户或单位的名称。



Cyber Protect 中控台中的合作伙伴租户级别

当在合作伙伴租户(**所有客户**)级别上使用 Cyber Protect 中控台时，可以使用自定义视图。

警告和**活动**选项卡提供其他与合作伙伴相关的过滤器，而**设备**和**管理**选项卡仅提供对合作伙伴管理员可访问的功能或对象的访问。

"警报"选项卡

在此处，可以查看您管理的所有客户的警报、搜索它们并根据以下条件过滤它们：

- 设备
- 客户
- 计划

可以为其中的每个条件选择多个项目。

"活动"选项卡

在此处，可以查看您管理的所有租户的活动或特定客户租户中的活动。

可以按客户、状态、时间和类型过滤活动。

将在此级别上自动预先选择以下类型的活动：

- 正在应用计划
- 创建保护计划
- 保护计划
- 正在吊销计划
- 脚本

"设备"选项卡

在此，您可以查看受管理的客户租户的所有工作负载。

您可以从不同租户中选择工作负载并创建设备组。

重要事项
在合作伙伴（**所有客户**）级别，可以使用设备执行有限数量的操作。例如，您不能执行以下任何操作：

- 创建新的保护计划。
- 编辑客户设备上现有的保护计划。
- 恢复备份。
- 使用Disaster Recovery。
- 访问 Cyber Protection 桌面功能。

若要执行任何这些操作，请在客户级别进行工作。

"管理"选项卡

可用计划按类型分组。

注意
在 **管理** > **保护计划**中，您可以查看受管理的客户租户中使用的计划，并按状态、客户和创建日期筛选这些计划。您无法创建新计划或编辑现有计划。

"软件管理"选项卡

如果为客户工作负载启用了软件清单扫描，则可以看到软件扫描结果。

查看特定客户的工作负载

作为合作伙伴管理员，您可以查看属于所管理的客户租户的工作负载。

若要查看特定客户的工作负载

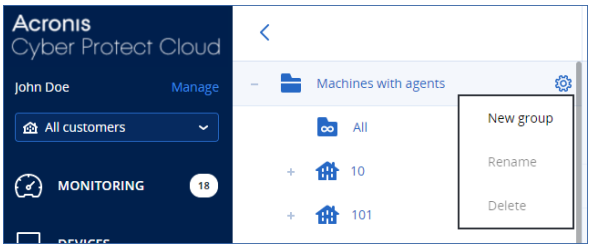
1. 在 Cyber Protect 中控台中，转到**设备** > **装有代理程序的计算机**。
2. 在树中，单击**装有代理程序的计算机**以展开列表。
3. 单击要查看和管理其工作负载的客户的姓名。

在合作伙伴级别创建静态设备组

可以在合作伙伴(**所有设备**)级别创建静态设备组。

在合作伙伴级别上创建静态设备组

1. 在 Cyber Protect 中控台中，转到**设备** > **装有代理程序的计算机**。
2. 单击**装有代理程序的计算机**旁边的齿轮图标，然后单击**新组**。



3. 指定组名称。
4. [可选]添加说明。
5. 单击**确定**。

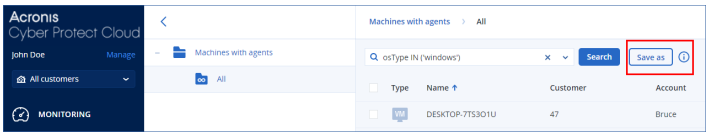
在合作伙伴级别上创建动态设备组

可以在合作伙伴(**所有设备**)级别创建动态设备组。

在合作伙伴级别上创建动态设备组

1. 在 Cyber Protect 中控台中，转到**设备** > **装有代理程序的计算机**。
2. 在树中，单击**装有代理程序的计算机**以展开列表。
3. 单击**全部**。
4. 在搜索字段中，指定要创建动态设备组所依据的条件，然后单击**搜索**。

   若要了解有关可用搜索条件的更多信息，请参阅 "非云到云工作负载的搜索属性"(第 289 页) 和 "云到云工作负载的搜索属性"(第 288 页)。
5. 单击**另存为**，然后指定组名称。



6. [可选]添加说明。
7. 单击**确定**。

在合作伙伴租户级别执行计算机自动发现

可以在合作伙伴租户(**所有客户**)级别执行计算机自动发现。

先决条件

客户的本地网络或 Active Directory 域中至少有一台装有保护代理程序的计算机。

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。如果您的客户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。

由于运行代理程序服务需要额外权限,因此添加域控制器不支持自动发现。

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)。若要在运行 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。

若要在合作伙伴租户级别执行计算机自动发现

1. 在 Cyber Protect 中控台中,选择**所有客户**。
2. 转至**设备**>**所有设备**。
3. 单击**添加**。
4. 在**多个设备**中,单击**仅限 Windows**。将打开发现向导。
5. 选择客户租户,然后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**。确保安装发现代理程序的计算机是 Active Directory 域的成员。
   - **扫描本地网络**。将使用 Device Sense 来扫描本地网络。如果所选的发现代理程序找不到任何机器,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**筛选器**让您可以指定计算机选择的标准。

8. 根据您选择的发现方法，执行以下操作之一：

发现方法	操作
搜索 Active Directory	在已发现的计算机列表中，选择要添加的计算机。
扫描本地网络	在已发现的计算机列表中，选择要添加的计算机。

手动指定或从文件导入	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. 选择在发现后必须执行的操作：

选项	描述
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"(第 162 页)。
代理程序服务的登录帐户	此设置在**"选择组件"**屏幕上可用。 该设置定义了将运行服务的帐户。 可选择下列选项之一： • **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完全不工作。
注册已安装代理程序的计算机	如果计算机上已经安装了代理程序，则使用此选项，并且只需在 Cyber Protection 中注册它们。如果在计算机上找不到代理程序，则它们将被添加为**非托管**计算机。
添加为非托管计算机	如果选择此选项，该代理程序将不会安装在计算机上。您将能够在中控台中查看它们，并稍后安装或注册代理程序。

选项	描述
如有必要，重新启动计算机	当选择**安装代理程序和注册计算机**时，会出现此选项。 如果选择此选项，计算机将根据需要重新启动多次，直到完成安装。 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。
如果用户已登录，则不重新启动	当选择**"根据需要重新启动计算机"**时，会出现此选项。 如果选中此选项，则用户登录系统后计算机将不会自动重新启动。例如，如果用户正在工作，而安装需要重新启动，则系统将不会重新启动。 如果先决条件已安装，但由于用户登录而未重新启动计算机，则若要完成安装，您必须重新启动计算机，然后再次开始安装。 如果已安装代理程序但计算机未重新启动，则必须重新启动计算机。
用户在哪里注册计算机	[如果组织中有单位]选择要在其下注册计算机的单位或下属单位的用户帐户。 [在合作伙伴租户级别执行自动发现时]在您管理的客户租户列表中，展开树结构，然后选择要在其下注册计算机的用户帐户。 [以客户管理员身份执行自动发现时]如果您选择了**安装代理程序并注册计算机**或**使用已安装的代理程序注册计算机**，则还可以选择将保护计划应用到计算机。如果您有多个保护计划，可以选择要使用哪一个。

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
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，则必须按 "先决条件"(第 271 页) 中所述执行额外的准备操作。

11. 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，将在**监控 > 活动 > 发现计算机**活动中看到相应任务。

多租户支持

Cyber Protection 服务支持多租户，这意味着在以下级别上进行管理：

- [对于服务提供商]合作伙伴租户(**所有客户**)级别
  此级别仅适用于管理客户租户的合作伙伴管理员。
- 客户租户级别
  此级别由公司管理员管理。
  合作伙伴管理员也可以在他们管理的客户租户中在此级别上工作。在此级别上，合作伙伴管理员与他们所代表的客户管理员具有相同的权限。
- 单位级别
  此级别由单位管理员和来自父客户租户的公司管理员管理。

管理父客户租户的合作伙伴管理员也可以访问单位级别。在此级别上，他们与他们所代表的客户管理员具有相同的权限。

管理员可以管理他们自己的租户及其子租户中的对象。他们无法查看或访问上级管理级别的对象（如果有）。

例如，公司管理员可以在客户租户级别和单位级别上管理保护计划。单位管理员只能在单位级别上管理他们自己的保护计划。他们无法在客户租户级别上管理任何保护计划，也无法管理客户管理员在单位级别上创建的保护计划。

此外，合作伙伴管理员可以在他们所管理的客户租户中创建和应用脚本计划。此类租户中的公司管理员对合作伙伴管理员应用于其工作负载的脚本计划仅有“只读”访问权限。但是，客户管理员可以创建和应用他们自己的脚本或保护计划。

工作负载

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。在 Cyber Protect 中控台中，工作负载显示为您可以对其应用计划（保护计划、备份计划或脚本计划）的对象。

某些工作负载要求安装保护代理程序或部署虚拟设备。通过使用图形用户界面或使用命令行界面（无人参与安装），可以安装代理程序。您可以使用无人参与安装使安装步骤自动化。有关如何安装保护代理程序的详细信息，请参阅 "安装和部署 Cyber Protection 代理程序"（第 54 页）。

虚拟设备 (VA) 是包含保护代理程序的现成虚拟机。通过虚拟设备，您可以在相同的环境中备份其他虚拟机，无需在其中安装保护代理程序（无代理程序备份）。可以特定于虚拟机监控程序的格式（例如 .ovf、.ova 或 .qcow）使用虚拟设备。有关哪些虚拟化平台支持无代理程序备份的详细信息，请参阅 "所支持的虚拟化平台"（第 30 页）。

重要事项
代理程序必须至少每 30 天在线一次。否则，其计划将被吊销，并且工作负载将变得不受保护。

下表总结了工作负载类型及其各自的代理程序。

工作负载类型	代理程序	示例（非详尽列表）
物理机	保护代理程序已安装在每台受保护计算机上。	工作站 笔记本电脑 服务器
虚拟机	根据虚拟化平台，以下备份方法可能可用： • 基于代理程序的备份 - 保护代理程序安装在每台受保护计算机上。 • 无代理程序备份 - 保护代理程序仅安装在虚拟机监控程序主机上、专用虚拟机上或作为虚拟设备部署。此代理程序备份环境中的所有虚拟机。	VMware 虚拟机 Hyper-V 虚拟机 基于内核的虚拟机 (KVM)，由 oVirt 管理 VMware Cloud

工作负载类型	代理程序	示例 (非详尽列表)
		Director (vCD) 虚拟机*
Microsoft 365 Business 工作负载 Google Workspace 工作负载	这些工作负载由云代理程序备份，无需安装该代理程序。 要使用云代理程序，需要将 Microsoft 365 或 Google Workspace 组织添加到 Cyber Protect 中控台。 此外，还提供 Office 365 本地代理程序。它需要安装并且只能用于备份 Exchange Online 邮箱。有关本地代理程序和云代理程序之间差异的详细信息，请参阅 "保护 Microsoft 365 数据"(第 543 页)。	Microsoft 365 邮箱 Microsoft 365 OneDrive Microsoft Teams SharePoint 站点 Google 邮箱 Google Drive
应用程序	特定应用程序的数据由专用代理程序备份，例如适用于 SQL 的代理程序、适用于 Exchange 的代理程序、适用于 MySQL/MariaDB 的代理程序或适用于 Active Directory 的代理程序。	SQL Server 数据库 MySQL/MariaDB 数据库 Oracle 数据库 Active Directory
移动设备	移动应用程序已安装在受保护设备上。	Android 或 iOS 设备
网站	这些网站由云代理程序备份，无需安装该代理程序。	通过 SFTP 或 SSH 协议访问的网站

有关所需的代理程序及其安装位置的详细信息，请参阅 "我需要哪个代理程序？"(第 57 页)

* 有关将 VMware Cloud Director 与 Cyber Protect Cloud 集成，请参阅合作伙伴管理员指南。

将工作负载添加到 Cyber Protect 中控台

要开始保护工作负载，请先将它们添加到 Cyber Protect 中控台。

注意

可以添加的工作负载类型取决于您帐户的服务配额。如果缺少特定工作负载类型，则它在**添加设备**窗格中处于灰显状态。

合作伙伴管理员可以在管理门户中启用所需的服务配额。有关详细信息，请参阅 "合作伙伴管理员的信息"(第 279 页)。

添加工作负载

1. 登录到 Cyber Protect 中控台。
2. 转到**设备** > **所有设备**，然后单击**添加**。

添加设备窗格即会在右侧打开。

3. 选择发布渠道。
4. 单击要添加的工作负载类型，然后按照所选特定工作负载的说明进行操作。

下表汇总了工作负载类型和所需操作。

要添加的工作负载	所需操作	要遵循的步骤
多台 Windows 计算机	在您的环境中执行“自动发现”。 要执行“自动发现”，在本地网络或 Active Directory 域中需要至少有一台装有保护代理程序的计算机。该代理程序将用作发现代理程序。	"添加多个设备"(第 158 页)
Windows 工作站 Windows 服务器	安装适用于 Windows 的代理程序。	"在 Windows 中安装保护代理程序"(第 72 页) 或 "在 Windows 中安装和卸载保护代理程序"(第 78 页)
macOS 工作站	安装适用于 macOS 的代理程序。	"在 macOS 中安装保护代理程序"(第 76 页) 或 "在 macOS 中安装和卸载保护代理"(第 98 页)
Linux 服务器	安装适用于 Linux 的代理程序。	"在 Linux 中安装保护代理程序"(第 74 页) 或 "在 Linux 中安装和卸载保护代理程序"(第 92 页)
移动设备 (iOS、Android)	安装移动应用程序。	"保护移动设备"(第 537 页)
云到云工作负载		
Microsoft 365 企业	将 Microsoft 365 组织添加到 Cyber Protect 中控台，然后使用云代理程序来保护 Exchange Online 邮箱、OneDrive 文件、Microsoft Teams 和 SharePoint 站点。 或者，可以安装适用于 Office 365 的本地代理程序。它仅提供 Exchange Online 邮箱的备份。	"保护 Microsoft 365 数据"(第 543 页)

要添加的工作负载	所需操作	要遵循的步骤
	有关本地代理程序和云代理程序之间差异的详细信息，请参阅 "保护 Microsoft 365 数据"(第 543 页) 。	
Google Workspace	将 Google Workspace 组织添加到 Cyber Protect 中控台，然后使用云代理程序来保护 Gmail 邮箱和 Google Drive 文件。	"保护 Google Workspace 数据"(第 579 页)
虚拟机		
VMware ESXi	在您的环境中部署适用于 VMware 的代理程序(虚拟设备) 。	"部署适用于 VMware 的代理程序(虚拟设备) "(第 120 页)
	安装适用于 VMware 的代理程序 (Windows)。	"在 Windows 中安装保护代理程序"(第 72 页) 或 "在 Windows 中安装和卸载保护代理程序"(第 78 页)
Virtuozzo Hybrid Infrastructure	在您的环境中部署适用于 Virtuozzo Hybrid Infrastructure 的代理程序(虚拟设备) 。	"部署适用于 Virtuozzo Hybrid Infrastructure 的代理程序(虚拟设备) "(第 128 页)
Hyper-V	安装适用于 Hyper-V 的代理程序。	"在 Windows 中安装保护代理程序"(第 72 页) 或 "在 Windows 中安装和卸载保护代理程序"(第 78 页)
Virtuozzo	安装适用于 Virtuozzo 的代理程序。	"在 Linux 中安装保护代理程序"(第 74 页) 或 "在 Linux 中安装和卸载保护代理程序"(第 92 页)
KVM	安装适用于 Windows 的代理程序。	"在 Windows 中安装保护代理程序"(第 72 页) 或 "在 Windows 中安装和卸载保护代理程序"(第 78 页)
	安装适用于 Linux 的代理程序。	"在 Linux 中安装保护代理程序"(第 74 页) 或 "在 Linux 中安装和卸载保护代理

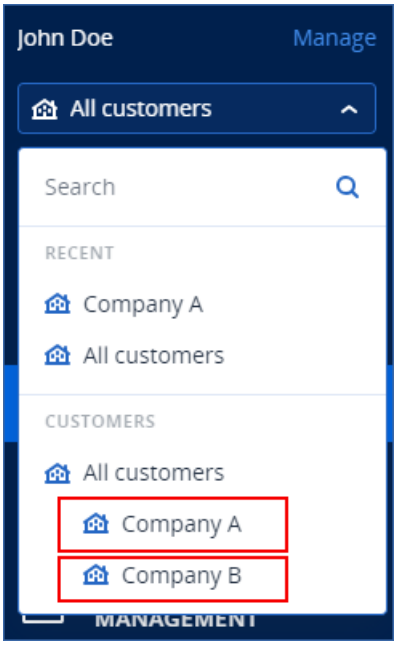
要添加的工作负载	所需操作	要遵循的步骤
		程序"(第 92 页)
Red Hat Virtualization (oVirt)	在您的环境中部署适用于 oVirt 的代理程序(虚拟设备)。	"正在部署适用于 oVirt 的代理程序(虚拟设备)"(第 138 页)
Citrix XenServer	安装适用于 Windows 的代理程序。	"在 Windows 中安装保护代理程序"(第 72 页) 或 "在 Windows 中安装和卸载保护代理程序"(第 78 页)
	安装适用于 Linux 的代理程序。	"在 Linux 中安装保护代理程序"(第 74 页) 或 "在 Linux 中安装和卸载保护代理程序"(第 92 页)
Nutanix AHV	安装适用于 Windows 的代理程序。	"在 Windows 中安装保护代理程序"(第 72 页) 或 "在 Windows 中安装和卸载保护代理程序"(第 78 页)
	安装适用于 Linux 的代理程序。	"在 Linux 中安装保护代理程序"(第 74 页) 或 "在 Linux 中安装和卸载保护代理程序"(第 92 页)
Oracle VM	安装适用于 Windows 的代理程序。	"在 Windows 中安装保护代理程序"(第 72 页) 或 "在 Windows 中安装和卸载保护代理程序"(第 78 页)
	安装适用于 Linux 的代理程序。	"在 Linux 中安装保护代理程序"(第 74 页) 或 "在 Linux 中安装和卸载保护代理程序"(第 92 页)
Scale Computing HC3	在您的环境中部署适用于 Scale Computing HC3 的代理程序(虚拟设	"正在部署适用于 Scale Computing HC3 的代理程序(虚拟设备)"(第

要添加的工作负载	所需操作	要遵循的步骤
	备)。	123 页)
网络附加存储		
Synology	在您的环境中部署适用于 Synology 的代理程序(虚拟设备)。	"部署适用于 Synology 的代理程序"(第 148 页)
应用程序		
Microsoft SQL Server	安装适用于 SQL 的代理程序。	"在 Windows 中安装保护代理程序"(第 72 页) 或 "在 Windows 中安装和卸载保护代理程序"(第 78 页)
Microsoft Exchange Server	安装适用于 Exchange 的代理程序。	
Microsoft Active Directory	安装适用于 Active Directory 的代理程序。	
Oracle 数据库	安装适用于 Oracle 的代理程序。	"保护 Oracle 数据库"(第 599 页)
网站	配置与网站的连接。	"保护网站和托管服务器"(第 605 页)

有关可用保护代理程序及其安装位置的详细信息,请参阅 "我需要哪个代理程序?"(第 57 页)

合作伙伴管理员的信息

- 如果在管理门户中未启用所需服务配额,则**添加设备**窗格中可能缺少工作负载类型。有关哪些工作负载需要哪些服务配额的详细信息,请参阅《合作伙伴管理员指南》中的启用或禁用产品项目。
- 作为合作伙伴管理员,您无法在**所有客户**级别上添加工作负载。要添加工作负载,请选择单个客户租户。



从 Cyber Protect 中控台中删除工作负载

可以从 Cyber Protect 中控台中删除不再需要保护的工作负载。该过程取决于工作负载类型。

或者，可以卸载受保护工作负载上的代理程序。卸载代理程序时，受保护工作负载会自动从 Cyber Protect 中控台中删除。

重要事项

从 Cyber Protect 中控台中删除工作负载时，将吊销已应用于该工作负载的所有计划。删除工作负载不会删除任何计划或备份，也不会卸载保护代理程序。

下表汇总了工作负载类型和所需操作。

要删除的工作负载	所需操作	要遵循的步骤
物理机和虚拟机		
装有保护代理程序的物理机或虚拟机	1. 从 Cyber Protect 中控台删除工作负载。 2. [可选] 卸载保护代理程序。	"从 Cyber Protect 中控台中删除工作负载"(第 281 页) (装有保护代理程序的工作负载)
在虚拟机监控程序级别上备份的虚拟机(无代理程序备份)	1. 在 Cyber Protect 中控台中，删除装有保护代理程序的计算机。此代理程序备份的所有虚拟机都将自动从中控台中删除。 2. [可选] 卸载保护代理程序。	"从 Cyber Protect 中控台中删除工作负载"(第 281 页) (未装有保护代理程序的工作负载)
云到云工作负载		
Microsoft 365 Business 工作负载 Google Workspace 工作负载	从 Cyber Protect 中控台中删除 Microsoft 365 或 Google Workspace 组织。该组织中的所有资源都将自动从中控台中删除。	"从 Cyber Protect 中控台中删除工作负载"(第 281 页) (云到云工作负载)
移动设备		
Android 设备	1. 从 Cyber Protect	"从 Cyber Protect 中控台中删除工作负载"(第 281 页)

要删除的工作负载	所需操作	要遵循的步骤
iOS 设备	中控台中删除移动设备。 2. [可选] 在移动设备上，卸载应用程序。	(移动设备)
网络附加存储		
Synology	1. 从 Cyber Protect 中控台删除工作负载。 2. [可选] 卸载保护代理程序。	"从 Cyber Protect 中控台中删除工作负载"(第 281 页) (装有保护代理程序的工作负载)
应用程序		
Microsoft SQL Server Microsoft Exchange Server Microsoft Active Directory Oracle 数据库	1. 在 Cyber Protect 中控台中，删除装有保护代理程序的计算机。此代理程序备份的对象将自动从中控台中删除。 2. [可选] 卸载保护代理程序。	"从 Cyber Protect 中控台中删除工作负载"(第 281 页) (未装有保护代理程序的工作负载)
网站	从 Cyber Protect 中控台中删除网站。	"从 Cyber Protect 中控台中删除工作负载"(第 281 页) (网站)

从 Cyber Protect 中控台中删除工作负载

装有保护代理程序的工作负载

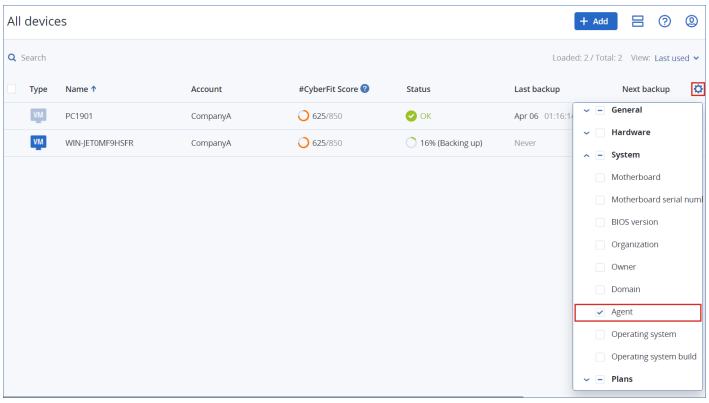
可以直接删除此类工作负载。

1. 在 Cyber Protect 中控台中，导航到**设备** > **所有设备**。
2. 选中一个或多个要删除的工作负载旁边的复选框。
3. 在**操作**窗格中，单击**删除**。
4. 单击**删除**以确认选择。
5. [可选] 卸载代理程序，如 "卸载代理程序"(第 76 页) 中所述。

未装有保护代理程序的工作负载

要删除此类工作负载，需要删除装有保护代理程序的计算机。

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 在右上角，单击齿轮图标，然后选中**代理程序**复选框。



代理程序列即会显示。

3. 在**代理程序**列中，选中装有保护代理程序的计算机的名称。
4. 在 Cyber Protect 中控台中，选中装有保护代理程序的计算机旁边的复选框。
5. 在**操作**窗格中，单击**删除**。
6. 单击**删除**以确认选择。
7. [可选] 卸载代理程序，如 "卸载代理程序"(第 76 页) 中所述。

云到云工作负载

要删除由云代理程序备份的工作负载，请从 Cyber Protect 中控台中删除 Microsoft 365 或 Google Workspace 组织。

1. 在 Cyber Protect 中控台中，导航到**设备** > **Microsoft 365** 或**设备** > **Google Workspace**。
2. 单击 Microsoft 365 或 Google Workspace 组织的名称。
3. 在**操作**窗格中，单击**删除组**。
4. 单击**删除**，以确认您的操作。

移动设备

1. 在 Cyber Protect 中控台中，导航到**设备** > **所有设备**。
2. 选中要删除的工作负载旁边的复选框。
3. 在**操作**窗格中，单击**删除**。
4. 单击**删除**以确认选择。
5. [可选] 从移动设备中卸载应用程序。

网站

1. 在 Cyber Protect 中控台中，导航到**设备** > **所有设备**。
2. 选中要删除的工作负载旁边的复选框。
3. 在**操作**窗格中，单击**删除**。
4. 单击**删除**以确认选择。

设备组

通过设备组，可以使用一个组计划保护多个类似的工作负载。该计划作为一个整体应用于该组，不能从该组的成员中撤消。

一个工作负载可以是多个组的成员。包含在设备组中的工作负载仍然可以受个别计划的保护。

只能向一个设备组添加类型相同的工作负载。例如，在 **Hyper-V** 下，只能创建 Hyper-V 虚拟机组。在**装有代理程序的计算机**下，只能创建装有代理程序的计算机组。

无法在以下任何**全部**型组中创建设备组：例如，根组**全部设备**，或诸如**装有代理程序的计算机** > **全部**、**Microsoft 365** > 您的组织 > **用户** > **所有用户**之类的内建组。

内建组和自定义组

内建组

在 Cyber Protect 中控台中注册工作负载后，该工作负载将显示在**设备**选项卡上的一个内建根组中，例如**装有代理程序的计算机**、**Microsoft 365** 或 **Hyper-V**。

所有注册的非云到云工作负载也将列在**所有设备**根组中。以您的租户命名的独立内建根组包含此租户中的所有非云到云工作负载和所有单位。

无法删除或编辑根组，也无法对其应用计划。

某些根组包含一个或多个级别的内建子组，例如，**装有代理程序的计算机** > **全部**、**Microsoft 365** > 您的组织 > **团队** > **全部团队**、**Google Workspace** > 您的组织 > **共享驱动器** > **全部共享驱动器**。

无法编辑或删除内建子组。

自定义组

由于可能存在需要不同保护设置或不同保护预定的工作负载，因此保护内建组中的所有工作负载可能并不方便。

在某些根组中（例如，在**装有代理程序的计算机**、**Microsoft 365** 或 **Google Workspace** 中），可以创建自定义子组。这些子组可以是静态组，也可以是动态组。

可以编辑、重命名或删除任何自定义组。

静态组和动态组

可以创建以下类型的自定义组：

- 静态
- 动态

静态组

静态组包含手动添加的工作负载。

仅当显式添加或删除工作负载时，静态组的内容才会发生变化。

示例：为公司的会计部创建静态组，然后将会计员的计算机手动添加到此组。应用组计划时，该组中的计算机将受到保护。如果聘用了一名新的会计员，则需要手动向该静态组添加会计员的计算机。

动态组

动态组包含符合特定条件的工作负载。通过创建包含属性（例如，osType）、其值（例如，Windows）和搜索运算符（例如，IN）的搜索查询，可以预先定义这些条件。

因此，可以为操作系统为 Windows 的所有计算机创建一个动态组，也可以创建一个包含 Microsoft 365 组织中所有用户（其电子邮件地址以 john 开头）的动态组。

有必填属性和值的所有工作负载都会自动添加到组中，并且任何失去必填属性或值的工作负载都会自动从组中删除。

示例 1：属于会计部的计算机的主机名称包含会计一词。搜索名称包含会计的计算机，然后将搜索结果保存为动态组。然后，将保护计划应用于该组。如果聘用了一名新的会计员，则会计员计算机的名称中会有会计一词，并在 Cyber Protect 中控台中注册该计算机后，就会自动将会计员的计算机添加到动态组中。

示例 2：财务部成立了一个独立的活动目录组织单位 (OU)。将会计 OU 指定为必填属性，然后将搜索结果保存为动态组。然后，将保护计划应用于该组。如果聘用了一名新的会计员，则只要将会计员的计算机添加到 Active Directory OU 并在 Cyber Protect 中控台中注册（不分先后顺序），就会将会计员的计算机添加到动态组。

云到云组和非云到云组

云到云组包含由云代理程序备份的 Microsoft 365 或 Google Workspace 工作负载。

非云到云组包含所有其他工作负载类型。

支持的设备组计划

下表汇总了可以应用于设备组的计划。

组	可用的计划	计划位置
云到云工作负载 （Microsoft 365 和 Google Workspace 工作负载）	备份计划	**管理 > 云应用程序备份**
非云到云工作负载	保护计划	**管理 > 保护计划**
	远程管理计划	**管理 > 远程管理计划**
	脚本计划	**管理 > 脚本计划**

云资源（如 Microsoft 365 或 Google Workspace 用户、OneDrive 和 Google Drive 共享、Microsoft Teams 或 Azure AD 组）将在向 Cyber Protect 中控台添加 Microsoft 365 或 Google Workspace 组织后立即同步到该中控台。在组织中所做的任何进一步更改将每天同步一次。

如果需要立即同步更改，请在 Cyber Protect 中控台中，分别导航到**设备** > **Microsoft 365** 或**设备** > **Google Workspace**、选择所需的组织，然后单击**刷新**。

创建静态组

可以创建一个空的静态组并向其中添加工作负载。

或者，可以选择工作负载并基于选择内容创建一个新的静态组。

无法在以下任何**全部**型组中创建设备组：例如，根组**全部设备**，或诸如**装有代理程序的计算机** > **全部**、**Microsoft 365** > 您的组织 > **用户** > **所有用户**之类的内建组。

创建静态组

在主窗口中

1. 单击**设备**，然后选择包含要为其创建静态组的工作负载的根组。
2. [可选] 要创建嵌套组，请导航到现有的静态组。

   注意
   创建嵌套静态组不适用于云到云工作负载。

3. 单击组树下方的 **+ 新静态组**，或单击**操作**窗格中的**新静态组**。
4. 为新组指定名称。
5. [可选] 为组添加注释。
6. 单击**确定**。

在组树中

1. 单击**设备**，然后选择包含要为其创建静态组的工作负载的根组。
2. 单击要在其中创建新静态组的组名称旁边的齿轮图标。

   注意
   创建嵌套静态组不适用于云到云工作负载。

3. 单击**新静态组**。
4. 为新组指定名称。
5. [可选] 为组添加注释。
6. 单击**确定**。

从选择内容

1. 单击**设备**，然后选择包含要为其创建静态组的工作负载的根组。

   注意
   无法在以下任何**全部**型组中创建设备组：例如，根组**全部设备**，或诸如**装有代理程序的计算机** > **全部**、**Microsoft 365** > 您的组织 > **用户** > **所有用户**之类的内建组。

2. 选中要为其创建新组的工作负载旁边的复选框，然后单击**添加到组**。

3. 在文件夹树中，选择新组的父级，然后单击**新静态组**。

> **注意**
> 创建嵌套静态组不适用于云到云工作负载。

4. 为新组指定名称。
5. [可选] 为组添加注释。
6. 单击**确定**。
   新组将显示在文件夹树中。
7. 单击**完成**。

向静态组添加工作负载

可以先选择目标组，然后向其添加工作负载。

或者，可以先选择工作负载，然后将其添加到某个组中。

向静态组添加工作负载

先选择目标组

1. 单击**设备**，然后导航到您的目标组。
2. 选择目标组，然后单击**添加设备**。
3. 在文件夹树中，选择包含所需工作负载的组。
4. 选中要添加的工作负载旁边的复选框，然后单击**添加**。

先选择工作负载

1. 单击**设备**，然后选择包含所需工作负载的根组。
2. 选中要添加的工作负载旁边的复选框，然后单击**添加到组**。
3. 在文件夹树中，选择目标组，然后单击**完成**。

创建动态组

通过搜索有特定属性的工作负载(在搜索查询中定义属性值)，来创建一个动态组。然后，将搜索结果保存为动态组。

对于云到云工作负载和非云到云工作负载，支持搜索和创建动态组的属性有所不同。有关支持属性的详细信息，请参阅 "非云到云工作负载的搜索属性"(第 289 页) 和 "云到云工作负载的搜索属性"(第 288 页)。

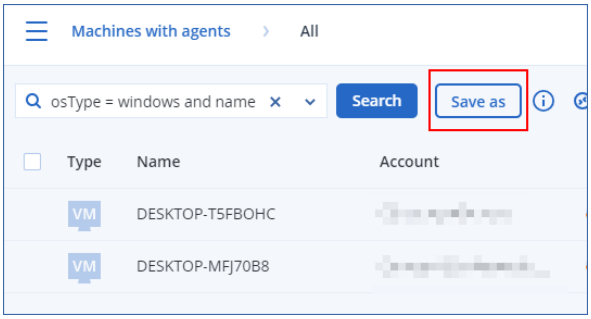
动态组在其各自的根组中创建。不支持嵌套的动态组。

无法在以下任何**全部**型组中创建设备组：例如，根组**全部设备**，或诸如**装有代理程序的计算机** > **全部**、**Microsoft 365** > 您的组织 > **用户** > **所有用户**之类的内建组。

创建动态组

非云到云工作负载

1. 单击**设备**，然后选择包含要为其创建新动态组的工作负载的组。
2. 使用支持的搜索属性和运算符来搜索工作负载。
   您可以在单个查询中使用多个属性和运算符。有关支持的属性的更多信息，请参阅 "非云到云工作负载的搜索属性"(第 289 页)。
3. 单击搜索字段旁边的**另存为**。

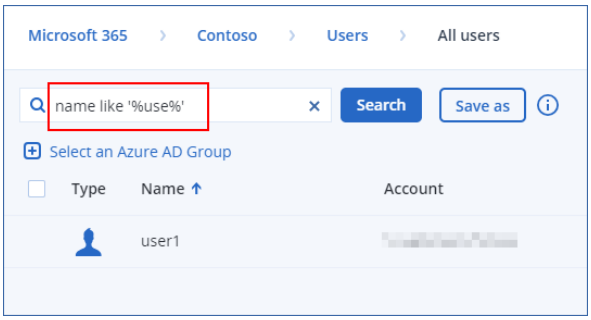


注意
当不允许在特定级别上创建动态组时，**"另存为"**按钮将不可用。例如，在根组**"设备"** > **"所有设备"**中。
选择另一个级别(例如，**设备>具有代理程序的计算机>全部**)，然后重复上述步骤。通过此搜索，您可以在**具有代理程序的计算机**中创建动态组，而不是在**具有代理程序的计算机>全部**中创建动态组。

4. 为新组指定名称。
5. [可选]在**注释**字段中，为新组添加说明。
6. 单击**确定**。

云到云工作负载

1. 单击**设备**，然后选择 **Microsoft 365** 或 **Google Workspace**。
2. 选择包含要为其创建新动态组的工作负载的组，例如**用户>所有用户**。
3. 通过使用支持的搜索属性和运算符来搜索工作负载，或从特定 Active Directory 组中选择 Microsoft 365 用户来搜索工作负载。
   您可以在单个查询中使用多个属性和运算符。有关支持的属性的更多信息，请参阅 "云到云工作负载的搜索属性"(第 288 页)。

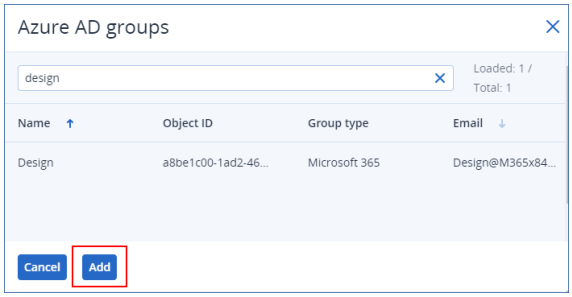


4. [仅适用于 **Microsoft 365** > **用户**]要从特定 Active Directory 组中选择用户，请执行以下操作：
   a. 导航到**用户** > **所有用户**。
   b. 单击**选择 Azure AD 组**。

组织中 Active Directory 组的列表即会打开。

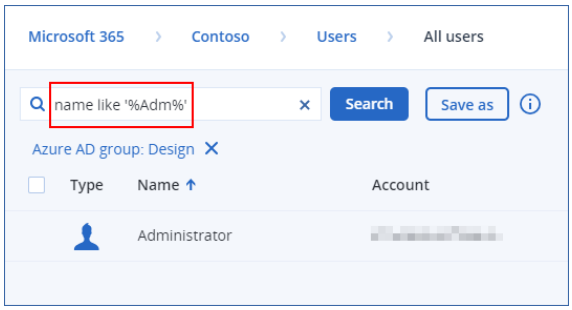
在此列表中，可以搜索特定组，也可以按名称或电子邮件地址对组进行排序。

c. 选择所需的 Active Directory 组，然后单击**添加**。



d. [可选] 要在选定的 Active Directory 组中包含或排除特定用户，请使用支持的搜索属性和运算符创建搜索查询。

您可以在单个查询中使用多个属性和运算符。有关支持的属性的更多信息，请参阅 "云到云工作负载的搜索属性"(第 288 页)。



5. 单击搜索字段旁边的**另存为**。

注意

如果不允许您在特定级别上创建动态组，则**"另存为"**按钮将不可用。例如，在**Microsoft 365** > 你的组织 >**用户**中。

选择另一个级别(例如，**Microsoft 365** > 你的组织 >**用户**>**全部**)，然后重复上述步骤。通过此搜索，您可以在**Microsoft 365**>您的组织>**用户**> 中创建动态组，而不是在**用户**>**全部**中。

6. 为新组指定名称。
7. [可选] 在**注释**字段中，为新组添加说明。
8. 单击**确定**。

云到云工作负载的搜索属性

下表总结了可以在 Microsoft 365 和 Google Workspace 工作负载的搜索查询中使用的属性。

要查看可以在其他类型的工作负载的搜索查询中使用的属性，请参阅 "非云到云工作负载的搜索属性"(第 289 页)。

属性	含义	可用于	搜索查询示例	支持用于组创建
name	Microsoft 365 或 Google Workspace 工作负载的显示名称	所有云到云资源	name = 'My Name' name LIKE '*nam*'	是
email	Microsoft 365 用户或组的电子邮件地址，或 Google Workspace 用户的电子邮件地址	Microsoft 365 > 组 Microsoft 365 > 用户 Google Workspace > 用户	email = 'my_group_email@mycompany.com' email LIKE '*@company*' email NOT LIKE '*enterprise.com'	是
siteName	与 Microsoft 365 组关联的站点的名称	Microsoft 365 > 组	siteName = 'my_site' siteName LIKE '*company.com*support*'	是
url	Microsoft 365 组或 SharePoint 站点的网址	Microsoft 365 > 组 Microsoft 365 > 站点集	url = 'https://www.mycompany.com/' url LIKE '*www.mycompany.com*'	是

非云到云工作负载的搜索属性

下表汇总了可以在非云到云工作负载的搜索查询中使用的属性。

要查看可以在云到云工作负载的搜索查询中使用的属性，请参阅 "云到云工作负载的搜索属性"(第 288 页)。

属性	含义	搜索查询示例	支持用于组创建
一般			
name	工作负载名称，如： • 物理机的主机名称 • 虚拟机的名称 • 数据库名称 • 邮箱的电子邮件地址	name = 'en-00'	是
id	设备 ID。	id != '4B2A7A93-A44F-4155-BDE3-	是

属性	含义	搜索查询示例	支持用于组创建
	要查看该设备 ID，请在**设备**下，选择该设备、依次单击**详细信息** > **所有属性**。 ID 会显示在 id 字段中。	A023C57C9431'	
resourceType	工作负载类型。 可能的值： • 'machine' • 'exchange' • 'mssql_server' • 'mssql_instance' • 'mssql_database' • 'mssql_database_folder' • 'msexchange_database' • 'msexchange_storage_group' • 'msexchange_mailbox.msexchange' • 'msexchange_mailbox.office365' • 'mssql_aag_group' • 'mssql_aag_database' • 'virtual_machine.vmww' • 'virtual_machine.vmwesx' • 'virtual_host.vmwesx' • 'virtual_cluster.vmwesx' • 'virtual_appliance.vmwesx' • 'virtual_application.vmwesx' • 'virtual_resource_pool.vmwesx' • 'virtual_center.vmwesx' • 'datastore.vmwesx' • 'datastore_cluster.vmwesx' • 'virtual_network.vmwesx' • 'virtual_data_center.vmwesx' • 'virtual_machine.vmww' • 'virtual_cluster.mshyperv' • 'virtual_machine.mshyperv' • 'virtual_host.mshyperv'	resourceType = 'machine' resourceType in ('mssql_aag_database', 'mssql_database')	是

属性	含义	搜索查询示例	支持用于组创建
	• 'virtual_network.mshyperv' • 'virtual_folder.mshyperv' • 'virtual_data_center.mshyperv' • 'datastore.mshyperv' • 'virtual_machine.msvs' • 'virtual_machine.parallelsw' • 'virtual_host.parallelsw' • 'virtual_cluster.parallelsw' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen' • virtual_machine.vcd • 'bootable_media'		
chassis	底座类型。 可能的值： • laptop • desktop • server • other • unknown	chassis = 'laptop' chassis IN ('laptop', 'desktop')	是
ip	IP 地址(仅适用于物理机)。	ip RANGE ('10.250.176.1','10.250.176.50')	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** 如果注释字段中有手动添加的文本，将禁用自动同步。要再次启用同步，请清除此文本。	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

	要刷新工作负载的自动同步注释，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**。
	对于已安装保护代理程序的设备，有两个单独的注释字段：
	• 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
	如果注释字段中有手动添加的文本，将禁用自动同步。要再次启用同步，请清除此文本。
	• 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。
	设备可以指定其中一个或两个注释，也可以将它们都保留为空		

属性	含义	搜索查询示例	支持用于组创建
	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**。		
isOnline	工作负载可用性。 可能的值： • true • false	isOnline = true	否
hasAsz	安全区可用性。 可能的值： • true • false	hasAsz = true	是
tzOffset	与协调世界时 (UTC) 的时区偏移量，以分钟为单位。	tzOffset = 120 tzOffset > 120 tzOffset < 120	是
CPU、内存、磁盘			
cpuArch	CPU 架构。 可能的值： • 'x64' • 'x86'	cpuArch = 'x64'	是
cpuName	CPU 名称。	cpuName LIKE '%XEON%'	是
memorySize	RAM 大小，以 MB 为单位。	memorySize < 1024	是
diskSize	硬盘驱动器大小(以千兆字节或兆字节为单位，仅适用于物理	diskSize < 300GB diskSize >= 3000000MB	否

属性	含义	搜索查询示例	支持用于组创建
	机)。		
操作系统			
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 = 'windows' osType IN ('linux', 'macosx')	是
osArch	操作系统架构。 可能的值: • 'x64' • 'x86'	cpuArch = 'x86'	是
osProductType	操作系统产品类型。 可能的值: • 'dc' 代表域控制器。 **注意** 当在 Windows 服务器上已指派域控制器角色时,osProductType 会从 server 更改为 dc。此类计算机不会包括在 osProductType='server' 的搜索结果中。 • 'server' • 'workstation'	osProductType = 'server'	是
osSp	操作系统的服务包。	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。	osVersionMinor > 1	是
代理程序			
agentVersion	已安装的保护代理程序的版本。	agentVersion LIKE '12.0.*'	是

属性	含义	搜索查询示例	支持用于组创建
hostId	保护代理程序的内部 ID。 要查看保护代理程序 ID，请在**设备**下，选择该设备、依次单击**详细信息** > **所有属性**。查看 agent 属性的 id 值。	hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	是
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 • 'vcd' VMware Cloud Director 虚拟机	virtualType = 'vmwesx'	是
insideVm	内部附带代理程序的虚拟机。 可能的值： • true • false	insideVm = true	是
位置			
tenant	设备所属租户的名称。	tenant = 'Unit 1'	是
tenantId	设备所属租户的标识符。 要查看该租户 ID，请在**设备**下，选择该设备、依次单击**详细信息** > **所有属性**。ID 会显示在 ownerId 字段中。	tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'	是

属性	含义	搜索查询示例	支持用于组创建
ou	属于指定 Active Directory 组织单元的计算机。	`ou IN ('RnD', 'Computers')`	是
状态			
state	设备状态。 可能的值： • 'idle' • 'interactionRequired' • 'canceling' • 'backup' • 'recover' • 'install' • 'reboot' • 'failback' • 'testReplica' • 'run_from_image' • 'finalize' • 'failover' • 'replicate' • 'createAsz' • 'deleteAsz' • 'resizeAsz'	`state = 'backup'`	否
状态	保护状态。 可能的值： • ok • warning • error • critical • protected • notProtected	`status = 'ok'` `status IN ('error', 'warning')`	否
protectedByPlan	设备受具有给定 ID 的保护计划保护。 要查看计划 ID，请在**管理** > **保护计划**中选择一个计划、单击**状态**列中的栏，然后单击状态名称。系统将创建一个具有该计划 ID	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	否

属性	含义	搜索查询示例	支持用于组创建
	的新搜索。		
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**状态。	errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	否
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
lastBackupTime*	上次成功备份的日期和时间。 格式为“YYYY-MM-DD HH:MM”。	lastBackupTime > '2023-03-11' lastBackupTime <= '2023-03-11 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 >= '2023-03-11'	否
nextBackupTime*	下次备份的时间。 格式为“YYYY-MM-DD HH:MM”。	nextBackupTime >= '2023-08-11'	否
lastVAScanTime*	上次成功进行漏洞评估的日期和时间。 格式为“YYYY-MM-DD HH:MM”。	lastVAScanTime > '2023-03-11' lastVAScanTime <= '2023-03-11 00:15' lastVAScanTime is null	是
lastVAScanTryTime*	上次漏洞评估尝试的时间。 格式为“YYYY-MM-DD HH:MM”。	lastVAScanTimeTryTime >= '2022-03-11'	是
nextVAScanTime*	下次漏洞评估的时间。 格式为“YYYY-MM-DD HH:MM”。	nextVAScanTime <= '2023-08-11'	是
network_status	Endpoint Detection and Response (EDR) 的网络隔离状态。 可能的值：	network_status= 'connected'	是

属性	含义	搜索查询示例	支持用于组创建
	• connected • isolated		

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 = 2023-01-20`，表示搜索结果将包括间隔 `lastBackupTime >= 2023-01-20 00:00` 和 `lastBackupTime <= 2023-01-20 23:59:59` 之间的所有备份。

搜索运算符

下表汇总了可用于搜索查询的运算符。

可以在单个查询中使用多个运算符。

运算符	支持用于	含义	示例
AND	所有工作负载	逻辑与运算符	`name like 'en-00' AND tenant = 'Unit 1'`
OR	所有工作负载	逻辑或运算符	`state = 'backup' OR state = 'interactionRequired'`
NOT	所有工作负载	逻辑非运算符	`NOT(osProductType = 'workstation')`
IN (<value1>,... <valueN>)	所有工作负载	此运算符会检查表达式是否与值列表中的任何值匹配。	`osType IN ('windows', 'linux')`
NOT IN	所有工作负载	此运算符与 IN 运算符的作用相反。	`NOT osType IN ('windows', 'linux')`

LIKE 'wildcard pattern'	所有工作负载	此运算符会检查表达式是否与通配符模式匹配。
		可以使用以下通配符运算符：
		• * 或 % 星号和百分
			`name LIKE 'en-00'`
			`name LIKE '*en-00'`
			`name LIKE '*en-00*'`
			`name LIKE 'en-00_'`

运算符	支持用于	含义	示例
		比符号代表零个、一个或多个字符 • _ 下划线代表单个字符	
NOT LIKE 'wildcard pattern'	所有工作负载	此运算符与 LIKE 运算符的作用相反。 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	NOT name LIKE 'en-00' NOT name LIKE '*en-00' NOT name LIKE '*en-00*' NOT name LIKE 'en-00_'
RANGE (<starting_value>, <ending_value>)	所有工作负载	此运算符会检查表达式是否在一个值(值包含在内)范围内。 使用字母数字字符串的搜索查询会使用 ASCII 排序顺序，但不区分大小写。	ip RANGE('10.250.176.1','10.250.176.50') name RANGE('a','d') 通过使用此查询，可以过滤所有以 A、B 和 C 开头的名称(如 Alice、Bob、Claire)。但是，只有一个字母 D 符合要求，因此包含更多字母的名称(如 Diana 或 Don)将不包括在内。 要获得相同的结果，还可以使用以下查询： name >= 'a' AND name <= 'd'
= 或 ==	所有工作负载	等于运算符	osProductType = 'server'
!= 或 <>	所有工作负载	不等于运算符	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'
<	非云到云工作负载	小于运算符	memorySize < 1024
>	非云到云工作负载	大于运算符。	diskSize > 300GB
<=	非云到云	小于或等于运算符	lastBackupTime <= '2022-03-11 00:15'

运算符	支持用于	含义	示例
	工作负载		
>=	非云到云工作负载	*大于或等于*运算符	`nextBackupTime >= '2022-08-11'`

编辑动态组

通过更改定义组内容的搜索查询，可以编辑动态组。

在基于 Active Directory 的动态组中，还可以更改 Active Directory 组。

编辑动态组

通过更改搜索查询

1. 单击**设备**、导航到要编辑的动态组，然后选择它。
2. 单击组名称旁边的齿轮图标，然后单击**编辑**。或者，单击**操作**窗格中的**编辑**。
3. 通过修改搜索属性、其值或搜索运算符来更改搜索查询，然后单击**搜索**。
4. 单击搜索字段旁边的**保存**。

通过更改 Active Directory 组

注意
此过程适用于基于Active Directory 的动态组。基于 Active Directory 的动态组仅在 **Microsoft 365** > **用户**中可用。

1. 单击**设备**，导航到**设备** > **Microsoft 365** > 您的组织 > **用户**。
2. 选择要编辑的动态组。
3. 单击组名称旁边的齿轮图标，然后单击**编辑**。或者，单击**操作**窗格中的**编辑**。
4. 通过执行以下任一操作更改组内容：
   - 更改已选定的 Active Directory 组，方法是单击其名称，然后从打开的列表中选择新的 Active Directory 组。
   - 编辑搜索查询，然后单击**搜索**。
     搜索查询仅限于当前选定的 Active Directory 组。
5. 单击搜索字段旁边的**保存**。

还可以保存所做的编辑，而不覆盖当前组。要将编辑的配置保存为一个新组，请单击搜索字段旁边的箭头按钮，然后单击**另存为**。

删除组

当删除设备组时，将撤消应用于该组的所有计划。如果没有其他计划应用于组中的工作负载，则这些工作负载会失去保护。

删除设备组

1. 单击**设备**，然后导航到要删除的组。
2. 单击组名称旁边的齿轮图标，然后单击**删除**。
3. 单击**删除**以确认选择。

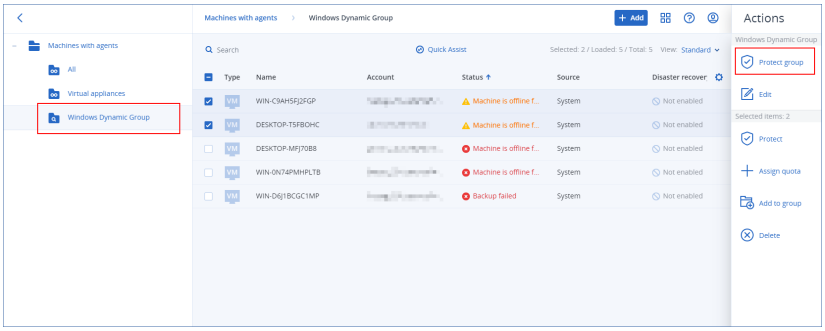
将计划应用于组

通过先选择组，然后将计划指派给该组，可以将计划应用于组。

或者，可以打开计划以进行编辑，然后向其中添加组。

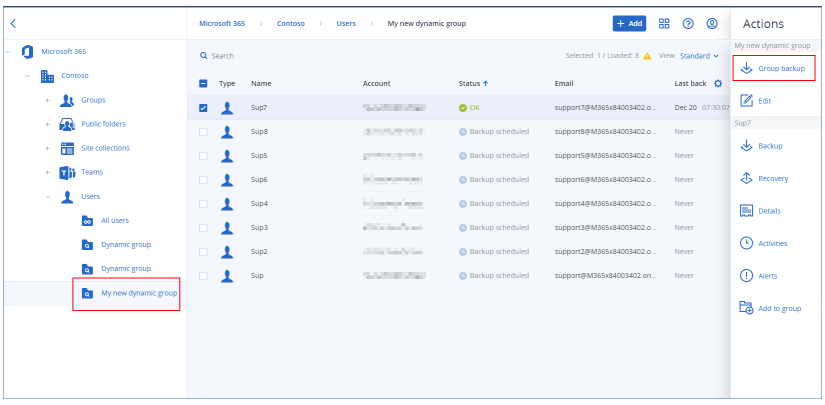
将计划应用于组

1. 单击**设备**，然后导航到要应用计划的组。
2. [对于非云到云工作负载] 单击**保护组**。



可以应用的计划列表即会显示。

3. [对于云到云工作负载] 单击**组备份**。



可以应用的备份计划列表即会显示。

4. [应用现有计划] 选择计划，然后单击**应用**。
5. [创建新计划] 单击**创建计划**、选择计划类型，然后创建新计划。

   有关可用计划类型以及如何创建计划的详细信息，请参阅 "支持的设备组计划"(第 284 页)。

注意
应用于云到云设备组的备份计划将自动预定为每天运行一次。无法通过单击**立即运行**，来手动运行这些计划。

从组中撤消计划

可以从组中撤消计划，方法是先选择组，然后从该组中撤消计划。

或者，可以打开计划进行编辑，然后从中删除组。

从组中撤消计划

1. 单击**设备**，然后导航到要撤消计划的组。
2. [对于非云到云工作负载] 单击**保护组**。
   应用于该组的计划列表即会显示。
3. [对于云到云工作负载] 单击**组备份**。
   应用于该组的备份计划列表即会显示。
4. 选择要撤消的计划。
5. [对于非云到云工作负载] 单击省略号图标 (...)，然后单击**撤消**。
6. [对于云到云工作负载] 单击齿轮图标，然后单击**撤消**。

使用设备控制模块

作为 Cyber Protection 服务保护计划的一部分，设备控制模块[1]利用每台受保护计算机上的适用于防止数据丢失的代理程序[2]的功能子集，来检测和防止通过本地计算机通道对数据进行未经授权的访问和传输。它提供了对广泛数据泄漏途径的精细控制，这些途径包括使用可移动媒体、打印机、虚拟和重定向的设备以及 Windows 剪贴板进行的数据交换。

该模块可用于 Cyber Protect Essentials、Cyber Protect Standard 和 Cyber Protect Advanced 版本，这些版本都按工作负载给予许可。

注意
在 Windows 计算机上，设备控制功能要求安装适用于防止数据丢失的代理程序。如果在其保护计划中启用了**设备控制**模块，它将自动安装以用于受保护的工作负载。

[1]作为保护计划的一部分，设备控制模块利用每台受保护计算机上的数据丢失保护代理程序的功能子集，来检测和防止通过本地计算机通道对数据进行未经授权的访问和传输。这包括用户访问外围设备和端口、文档打印、剪贴板复制/粘贴操作、媒体格式和弹出操作，以及与本地连接的移动设备的同步。设备控制模块提供对以下对象的精细化相关控制：受保护计算机上允许用户访问的设备类型和端口，以及用户可以在这些设备上执行的操作。

[2]通过应用上下文和内容分析技术的组合，并强制集中管理数据丢失预防策略，数据丢失预防系统的客户端组件保护其主机计算机避免未授权使用、传输和存储机密、受保护或敏感数据。Cyber Protection 提供全功能的数据丢失预防代理程序。但是，受保护计算机上的代理程序功能受限于可用于 Cyber Protection 中的许可的数据丢失预防功能集，并取决于应用于该计算机的保护计算。

设备控制模块依赖于代理程序的数据丢失保护[1]功能，来强制执行对受保护计算机上的数据访问和传输操作的相关控制。这包括用户访问外围设备和端口、文档打印、剪贴板复制/粘贴操作、媒体格式和弹出操作，以及与本地连接的移动设备的同步。适用于防止数据丢失的代理程序包括设备控制模块的所有集中管理和管控组件，因此它必须安装在要通过设备控制模块进行保护的每台计算机上。代理程序根据它从应用于受保护计算机的保护计划接收的设备控制设置，允许、限制或拒绝用户操作。

设备控制模块控制对各种外围设备的访问，不管是直接在受保护的计算机上使用，还是在受保护计算机上托管的虚拟环境中重定向。它识别在 Microsoft Remote Desktop Server、Citrix XenDesktop / XenApp / XenServer 和 VMware Horizon 中重定向的设备。它还控制以下两个剪贴板之间的数据复制操作：运行在 VMware Workstation / Player、Oracle VM VirtualBox 或 Windows Virtual PC 上的来宾操作系统的剪贴板，以及运行在受保护计算机上的主机操作系统的剪贴板。

设备控制模块可以保护运行以下操作系统的计算机：

设备控制

- Microsoft Windows 7 Service Pack 1 及更高版本
- Microsoft Windows Server 2008 R2 及更高版本
- macOS 10.15 (Catalina)
- macOS 11.2.3 (Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

注意
面向 macOS 的适用于防止数据丢失的代理程序仅支持 x64 处理器。不支持基于 ARM 的 Apple Silicon 处理器。

数据丢失预防

- Microsoft Windows 7 Service Pack 1 及更高版本
- Microsoft Windows Server 2008 R2 及更高版本

注意
适用于防止数据丢失的代理程序可能安装在不受支持的 macOS 系统上，因为它是适用于 Mac 的代理程序的重要组成部分。在此情况下，Cyber Protect 中控台将指示适用于防止数据丢失的代理程序已安装在计算机上，但设备控制和防止数据丢失功能将不起作用。设备控制功能仅在适用于防止数据丢失的代理程序支持的 macOS 系统上起作用。

使用 Hyper-V 的适用于防止数据丢失的代理程序的使用限制

不要在 Hyper-V 簇中的 Hyper-V 主机上安装适用于防止数据丢失的代理程序，因为它可能导致 BSOD 问题，主要在使用群集共享卷 (CSV) 的 Hyper-V 簇中。

[1]集成技术和公司措施系统，旨在检测和预防意外的或有意的泄漏/公司内外未经授权的实体访问机密、受保护或敏感数据，或将此类数据传输给不受信任的环境。

如果您使用以下任意版本的适用于 Hyper-V 的代理程序，则需要手动删除适用于防止数据丢失的代理程序：

- 15.0.26473 (C21.02)
- 15.0.26570 (C21.02 HF1)
- 15.0.26653 (C21.03)
- 15.0.26692 (C21.03 HF1)
- 15.0.26822 (C21.04)

要删除适用于防止数据丢失的代理程序，则在 Hyper-V 主机，手动运行安装程序，并清除“适用于防止数据丢失的代理程序”复选框，或运行以下命令：

```
<installer_name> --remove-components=agentForDlp -quiet
```

可以在 Cyber Protect 中控台中的保护计划的**设备控制**部分中，启用和配置设备控制模块。有关说明，请参见启用或禁用设备控制的步骤。

设备控制部分显示模块配置的概要：

- 访问设置 - 显示具有受限(拒绝或只读)访问权限的设备类型和端口的概要(如果有)。否则，表示允许所有设备类型。单击此概要以查看或更改访问权限设置(请参见查看或更改访问权限设置的步骤)。
- 设备类型允许列表 - 显示通过从设备访问控制中排除所允许的设备子类数量(如果有)。否则，表示允许列表为空。单击此概要以查看或更改允许的设备子类的选择(请参见从访问控制排除设备子类的步骤)。
- USB 设备允许列表 - 显示通过从设备访问控制中排除所允许的 USB 设备/型号的数量(如果有)。否则，表示允许列表为空。单击此概要以查看或更改允许的 USB 设备/型号的列表(请参见从访问控制排除单个 USB 设备的步骤)。
- 排除 - 显示已为 Windows 剪贴板、屏幕截图捕获、打印机和移动设备设置了多少个访问控制排除。

使用设备控制

本部分包括在使用设备控制模块时，基本任务的分步说明。

启用或禁用设备控制

在创建保护计划时，可以启用设备控制。可以更改现有保护计划以启用或禁用设备控制。

启用或禁用设备控制

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 执行以下任一操作以打开保护计划面板：
   - 如果想要创建新的保护计划，请选择要保护的计算机、单击**保护**，然后单击**创建计划**。
   - 如果想要更改现有保护计划，请选择受保护的计算机、单击**保护**、单击保护计划名称旁边的省略号 (...)，然后单击**编辑**。
3. 在保护计划面板中，导航到**设备控制**区域，然后启用或禁用**设备控制**。
4. 执行以下任一操作以应用更改：
   - 如果创建保护计划，请单击**创建**。
   - 如果编辑保护计划，请单击**保存**。

还可以从"管理"选项卡访问保护计划面板。但是，此功能在 Cyber Protection 服务的所有版本中不可用。

在 macOS 上启用设备控制模块的使用

仅在受保护的工作负载上加载设备控制驱动程序后，保护计划的设备控制设置才生效。本部分介绍如何加载设备控制驱动程序以在 macOS 上启用设备控制模块的使用。这是一次性操作，需要在端点计算机上具有管理员权限。

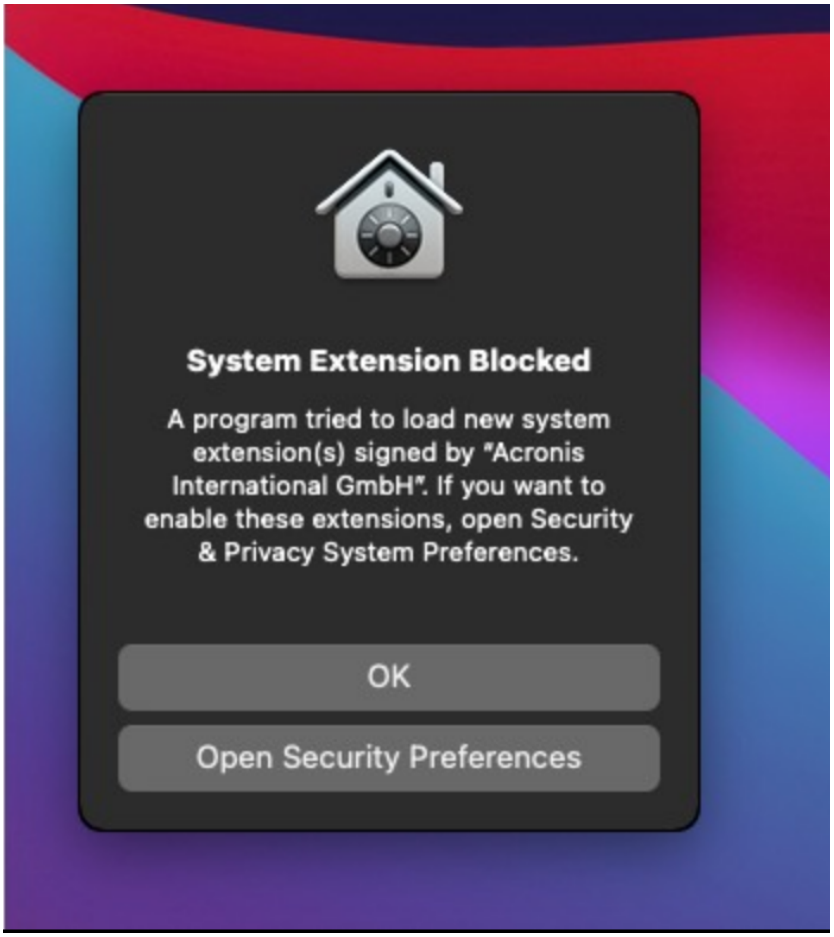
支持的 macOS 版本：

- macOS 10.15 (Catalina) 及更高版本
- macOS 11.2.3 (Big Sur) 及更高版本
- macOS 12.2 (Monterey) 及更高版本
- macOS 13.2 (Ventura) 及更高版本

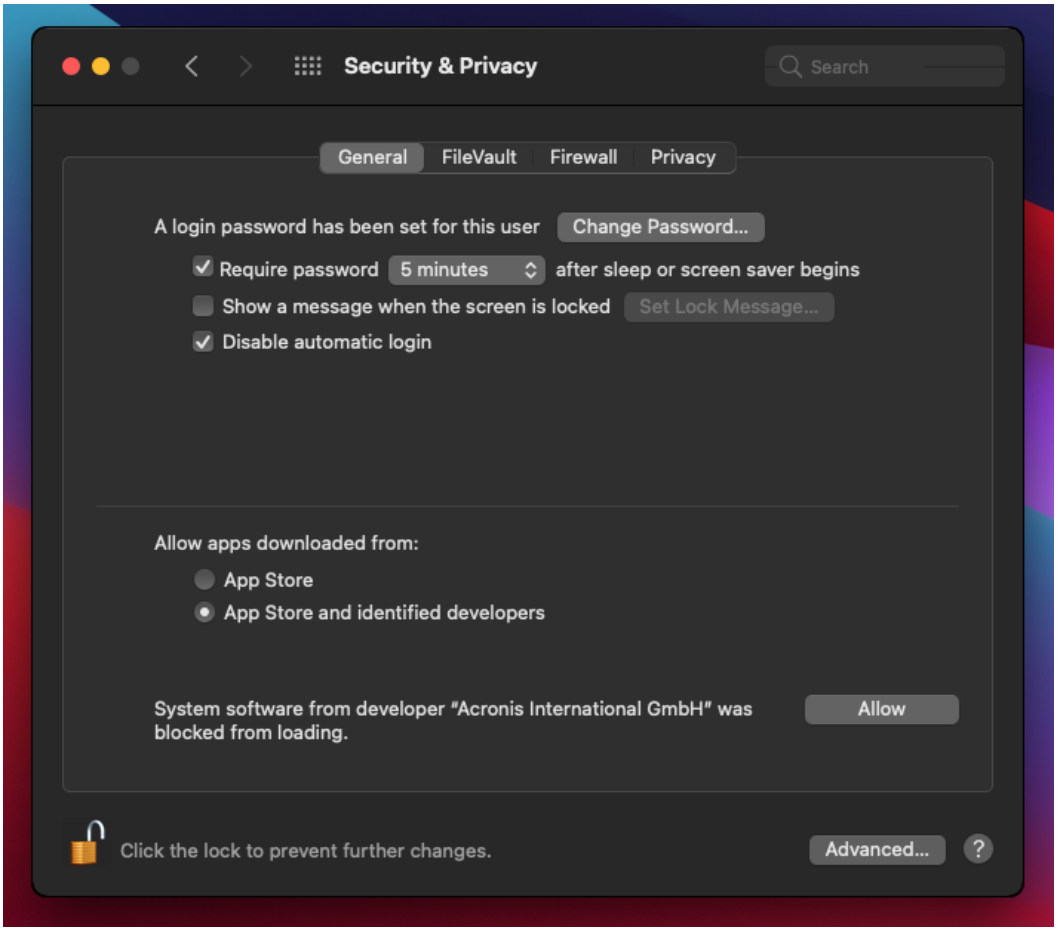
在 macOS 上启用设备控制模块的使用的步骤

1. 在想要保护的计算机上安装适用于 Mac 的代理程序。
2. 在保护计划中启用设备控制设置。
3. 应用保护计划。

4. “系统扩展已阻止”警告将显示在受保护的工作负载上。单击**打开安全首选项**。



5. 在显示的**安全性和隐私**窗格中，选择**应用程序商店和标识的开发者**，然后单击**允许**。



6. 在显示的对话框中，单击**重新启动**以重新启动工作负载，并激活设备控制设置。

注意
如果设备控制设置已禁用，然后重新启用，则不必重复这些步骤。

查看或更改访问设置

从保护计划面板上，可以管理设备控制模块的访问设置。通过此方法，可以允许或拒绝访问特定类型的设备，以及启用或禁用通知和警报。

查看或更改访问设置

1. 打开保护计划的保护计划面板，并在该计划中启用设备控制(请参见启用或禁用设备控制的步骤)。
2. 单击**设备控制**开关旁边的箭头图标以展开设置，然后单击**访问设置**旁边的链接。
3. 在显示的管理访问设置页上，查看或更改适当的访问设置。

注意
在使用设备控制和 Advanced DLP 来保护工作负载时，设备控制中配置的访问设置可能会被覆盖。请参见"在保护计划中启用 Advanced Data Loss Prevention"(第 777 页)。

启用或禁用 OS 通知和服务警报

当管理访问设置时，可以启用或禁用 OS 通知和服务警报，通知用户尝试执行不允许的操作。

启用或禁用 OS 通知

1. 遵循查看或更改访问设置的步骤。
2. 在管理访问设置页上，选择或清除**如果最终用户试图使用被阻止的设备类型或端口，显示 OS 通知**复选框。

启用或禁用设备警报

1. 遵循查看或更改访问设置的步骤。
2. 在管理访问设置页上，针对所需的设备类型选择或清除**显示警报**复选框。

显示警报复选框仅适用于访问受限(只读或拒绝访问)的设备类型(屏幕截图捕获除外)。

从访问控制排除设备子类

从保护计划面板上，可以选择要从访问控制中排除的设备子类。结果是，将允许访问这些设备，而不管设备控制访问设置如何。

从访问控制排除设备子类

1. 打开保护计划的保护计划面板，并在该计划中启用设备控制(请参见启用或禁用设备控制的步骤)。
2. 单击**设备控制**开关旁边的箭头图标以展开设置，然后单击**设备类型允许列表**旁边的链接。
3. 在显示的管理允许列表页上，查看或更改要从访问控制中排除的设备子类。

从访问控制排除单个 USB 设备

在保护计划面板中，可以指定要从访问控制中排除的单个 USB 设备或 USB 设备型号。结果是，将允许访问这些设备，而不管设备控制访问设置如何。

从访问控制排除 USB 设备

1. 打开保护计划的保护计划面板，并在该计划中启用设备控制(请参见启用或禁用设备控制的步骤)。
2. 单击**设备控制**开关旁边的箭头图标以展开设置，然后单击 **USB 设备允许列表**旁边的链接。
3. 在显示的管理允许列表页上，单击**从数据库添加**。
4. 在显示的选择 USB 设备页上，从在 USB 设备数据库中注册的设备中选择所需的设备。
5. 单击**添加到允许列表**按钮。

停止从访问控制排除 USB 设备

1. 打开保护计划的保护计划面板，并在该计划中启用设备控制(请参见启用或禁用设备控制的步骤)。
2. 单击**设备控制**开关旁边的箭头图标以展开设置，然后单击 **USB 设备允许列表**旁边的链接。
3. 在显示的管理允许列表页上，单击代表所需 USB 设备的列表项末尾的删除图标。

从数据库添加或删除 USB 设备

要从访问控制中排除特定 USB 设备，需要将其添加到 USB 设备数据库。然后，通过从该数据库中选择，可以将设备添加到允许列表。

以下步骤适用于启用了设备控制功能的保护计划。

将 USB 设备添加到数据库

1. 打开设备的保护计划以进行编辑：
   单击保护计划名称旁边的省略号 (...)，然后选择**编辑**。

   注意
   必须在计划中启用设备控制，以便可以访问设备控制设置。

2. 单击**设备控制**开关旁边的箭头图标以展开设置，然后单击 **USB 设备允许列表**旁边的链接。
3. 在显示的 **USB 设备允许列表**页上，单击**从数据库添加**。
4. 在显示的 USB 设备数据库管理页上，单击**添加到数据库**。
5. 在出现的**添加 USB 设备**对话框中，单击要连接 USB 设备的计算机。
   仅联机的计算机会显示在计算机列表中。
   USB 设备列表仅会针对已安装适用于数据丢失预防的代理程序的计算机显示。
   USB 设备会以树状视图列出。树的第一层表示设备模型。第二层表示该模型的特定设备。
   设备描述旁边的蓝色图标表示该设备当前已连接到计算机。如果设备未连接到计算机，该图标将灰显。
6. 选中要添加到数据库的 USB 设备的复选框，然后单击**添加到数据库**。
   选定的 USB 设备会添加到数据库中。
7. 关闭或保存保护计划。

从计算机详细信息面板将 USB 设备添加到数据库

注意
该步骤仅适用于已安装适用于数据丢失预防的代理程序的联机设备。无法查看脱机或未安装数据丢失预防代理程序的计算机的 USB 设备列表。

1. 在 Cyber Protect 中控台中，转到**设备 > 所有设备**。
2. 选择所需 USB 设备曾连接到的计算机，然后在右侧菜单中单击**清查**。
   计算机详细信息面板将打开。
3. 在计算机详细信息面板上，单击 **USB 设备**选项卡。
   将打开选定计算机上已知的 USB 设备列表。
   USB 设备会以树状视图列出。树的第一层表示设备模型。第二层表示该模型的特定设备。
   设备描述旁边的蓝色图标表示该设备当前已连接到计算机。如果设备未连接到计算机，该图标将灰显。
4. 选中要添加到数据库的 USB 设备的复选框，然后单击**添加到数据库**。

从服务警报将 USB 设备添加到数据库

1. 在 Cyber Protect 中控台中，转到**监视** > **警报**。
2. 定位设备控制警报，该警报通知拒绝访问 USB 设备。
3. 在警报简单视图中，单击**允许此 USB 设备**。
   这将从访问控制中排除 USB 设备，并将其添加到数据库以供将来参考。

通过将设备列表导入到数据库来添加 USB 设备

可以将一个包含 USB 设备列表的 JSON 文件导入到数据库。请参阅 "将 USB 设备列表导入到数据库"(第 318 页)。

从数据库删除 USB 设备

1. 打开设备的保护计划以进行编辑：
   单击保护计划名称旁边的省略号 (...)，然后选择**编辑**。

   注意
   必须在计划中启用设备控制，以便可以访问设备控制设置。

2. 单击**设备控制**开关旁边的箭头以展开设置，然后单击 **USB 设备允许列表**行。
3. 在显示的管理允许列表页上，单击**从数据库添加**。
4. 在从数据库选择 USB 设备页面上，单击表示设备的列表项末尾的省略号 (...)、单击**删除**，然后确认删除。
   USB 设备会从数据库中删除。
5. 关闭或保存保护计划。

查看设备控制警报

设备控制模块可以配置为引发警报，该警报通知拒绝用户尝试使用特定设备类型(请参阅启用或禁用 OS 通知和服务警报)。使用以下步骤查看这些警报。

查看设备控制警报

1. 在 Cyber Protect 中控台中，转到**监视** > **警报**。
2. 查找具有以下状态的警报：“外围设备访问已被阻止”。

请参见设备控制警报获取详细信息。

访问设置

在**访问设置**页上，可以允许或拒绝访问特定类型的设备，以及启用或禁用 OS 通知和设备控制警报。

注意
在使用设备控制和 Advanced DLP 来保护工作负载时，设备控制中配置的访问设置可能会被覆盖。请参见"在保护计划中启用 Advanced Data Loss Prevention"(第 777 页)。

访问设置允许您限制用户访问以下设备类型和端口：

- **可移动**(按设备类型的访问控制) - 具有连接到计算机的任意接口的设备(USB、FireWire、PCMCIA、IDE、SATA、SCSI 等),操作系统将其识别为可移动存储设备(例如,记忆棒、卡读取器、磁光光驱等)。设备控制将所有通过 USB、FireWire 和 PCMCIA 连接的硬盘分类为可移动设备。如果某些硬盘(通常具有 SATA 和 SCSI)支持热插拔功能并且没有安装正在运行的操作系统,也会将这些硬盘分类为可移动设备。

  可以对可移动设备允许完全访问、允许只读访问或拒绝访问,以控制与受保护计算机上任何可移动设备之间进行的数据复制操作。访问权限不会影响使用 BitLocker 或 FileVault(仅限于 HFS+ 文件系统)加密的设备。

  此设备类型在 Windows 和 macOS 上受支持。
- **加密的可移动设备**(按设备类型的访问控制) - 使用 BitLocker(在 Windows 上)或 FileVault(在 macOS 上)驱动器加密进行加密的可移动设备。

  在 macOS 上,仅支持使用 HFS+(也称为 HFS Plus 或 Mac OS Extended,或 HFS Extended)文件系统的加密可移动驱动器。使用 APFS 文件系统的加密可移动驱动器被当作可移动驱动器。

  可以对加密的可移动设备允许完全访问、允许只读访问或拒绝访问,以控制与受保护计算机上任何加密的可移动设备之间进行的数据复制操作。访问权限仅影响使用 BitLocker 或 FileVault(仅限于 HFS+ 文件系统)加密的设备。

  此设备类型在 Windows 和 macOS 上受支持。
- **打印机**(按设备类型的访问控制) - 具有连接到打印机的任何接口(USB、LPT、蓝牙等)的物理打印机,以及从网络上的计算机访问的打印机。

  可以允许或拒绝访问打印机,以控制在受保护计算机中的任何打印机上打印文档。

  注意

  当将打印机的访问设置更改为**拒绝**时,必须重新启动访问打印机的应用程序和进程,才能强制执行新配置的访问设置。为了确保已正确强制执行访问设置,请重新启动受保护的工作负载。

  此设备类型仅在 Windows 上受支持。
- **剪贴板**(按设备类型的访问控制) - Windows 剪贴板。

  可以允许或拒绝访问剪贴板,以控制通过受保护计算机上的 Windows 剪贴板进行的复制和粘贴操作。

  注意

  当将剪贴板的访问设置更改为**拒绝**时,必须重新启动访问剪贴板的应用程序和进程,才能强制执行新配置的访问设置。为了确保已正确强制执行访问设置,请重新启动受保护的工作负载。

  此设备类型仅在 Windows 上受支持。
- **屏幕截图捕获**(按设备类型的访问控制) - 支持捕获整个屏幕、活动窗口或屏幕选定部分的屏幕截图。

  可以允许或拒绝访问屏幕截图捕获,以控制在受保护计算机上进行的屏幕截图捕获。

注意
当将屏幕截图捕获的访问设置更改为**拒绝**时，必须重新启动访问屏幕截图捕获的应用程序和进程，才能强制执行新配置的访问设置。为了确保已正确强制执行访问设置，请重新启动受保护的工作负载。

此设备类型仅在 Windows 上受支持。

- **移动设备**（按设备类型的访问控制）- 通过媒体传输协议 (MTP) 与计算机通信的设备（例如基于 Android 的智能手机等），具有用于连接计算机的任何接口（USB、IP、Bluetooth）。
  可以对移动设备允许完全访问、允许只读访问或拒绝访问，以控制与受保护计算机上任何基于 MTP 的移动设备之间进行的数据复制操作。

  注意
  当将移动设备的访问设置更改为**只读**或**拒绝**时，必须重新启动访问移动设备的应用程序和进程，才能强制执行新配置的访问设置。为了确保已正确强制执行访问设置，请重新启动受保护的工作负载。

  此设备类型仅在 Windows 上受支持。
- **蓝牙**（按设备类型的访问控制）- 具有连接到计算机的任何接口（USB、PCMCIA 等）的外部和内部蓝牙设备。此设置控制使用此类型的设备而不是使用此类设备的数据交换。
  可以允许或拒绝访问蓝牙，以对在受保护计算机上使用任何蓝牙设备进行控制。

  注意
  在 macOS 上，蓝牙的访问权限不影响蓝牙 HID 设备。始终允许对这些设备的访问权限，以防止无线 HID 设备（鼠标和键盘）在 iMac 和 Mac Pro 硬件上被禁用。

  此设备类型在 Windows 和 macOS 上受支持。
- **光驱**（按设备类型的访问控制）- 具有连接到计算机的任何接口（IDE、SATA、USB、FireWire、PCMCIA 等）的外部和内部 CD/DVD/BD 驱动器（包括写入器）。
  可以对光盘驱动器允许完全访问、允许只读访问或拒绝访问，以控制与受保护计算机上任何光盘驱动器之间进行的数据复制操作。
  此设备类型在 Windows 和 macOS 上受支持。
- **软驱**（按设备类型的访问控制）- 具有连接到计算机的任何接口（IDE、USB、PCMCIA 等）的外部和内部软驱。有一些操作系统识别为可移动驱动器的软驱型号，在此情况下，设备控制也会将这些驱动器标识为可移动设备。
  可以对软盘驱动器允许完全访问、允许只读访问或拒绝访问，以控制与受保护计算机上任何软盘驱动器之间进行的数据复制操作。
  此设备类型仅在 Windows 上受支持。
- **USB**（按设备接口的访问控制）- 连接到 USB 端口的任何设备，除了集线器。
  可以对 USB 端口允许完全访问、允许只读访问或拒绝访问，以控制与受保护计算机上任何 USB 端口连接的设备之间进行的数据复制操作。
  此设备类型在 Windows 和 macOS 上受支持。
- **FireWire**（按设备接口的访问控制）- 连接到 FireWire (IEEE 1394) 端口的任何设备，除了集线器。

可以对 FireWire 端口允许完全访问、允许只读访问或拒绝访问，以控制与受保护计算机上任何 FireWire 端口连接的设备之间进行的数据复制操作。

此设备类型在 Windows 和 macOS 上受支持。

- **重定向的设备**（按设备接口的访问控制）- 映射的驱动器（硬盘、可移动驱动器和光驱）、USB 设备以及重定向到虚拟应用程序/桌面会话的剪贴板。

  设备控制识别通过 Microsoft RDP、Citrix ICA、VMware PCoIP 和 HTML5/WebSockets 远程协议重定向的设备，这些协议位于受保护 Windows 计算机上托管的 Microsoft RDS、Citrix XenDesktop、Citrix XenApp、Citrix XenServer 和 VMware Horizon 虚拟环境中。它还控制以下两个剪贴板之间的数据复制操作：运行在 VMware Workstation、VMware Player、Oracle VM VirtualBox 或 Windows Virtual PC 上的来宾操作系统的 Windows 剪贴板，以及运行在受保护 Windows 计算机上的主机操作系统的剪贴板。

  此设备类型仅在 Windows 上受支持。

  可以按以下步骤配置对重定向设备的访问：

  - **映射的驱动器** - 允许完全访问、允许只读访问或拒绝访问，以控制与重定向到受保护计算机上托管的会话的任何硬盘驱动器、可移动驱动器或光盘驱动器之间进行的复制数据操作。
  - **剪贴板传入** - 允许或拒绝访问，以控制通过剪贴板到受保护计算机上托管的会话进行的数据复制操作。

    注意

    当将剪贴板传入的访问设置更改为**拒绝**时，必须重新启动访问剪贴板的应用程序和进程，才能强制执行新配置的访问设置。为了确保已正确强制执行访问设置，请重新启动受保护的工作负载。

  - **剪贴板传出** - 允许或拒绝访问，以控制通过剪贴板从受保护计算机上托管的会话进行的数据复制操作。

    注意

    当将剪贴板传出的访问设置更改为**拒绝**时，必须重新启动访问剪贴板的应用程序和进程，才能强制执行新配置的访问设置。为了确保已正确强制执行访问设置，请重新启动受保护的工作负载。

  - **USB 端口** - 允许或拒绝访问，以控制与连接到任何 USB 端口（重定向到受保护计算机上托管的会话）的设备之间进行的复制数据操作。

设备控制设置平等地影响所有用户。例如，如果拒绝访问可移动设备，就会阻止任何用户与受保护计算机上的此类设备之间复制数据。通过将单个 USB 设备从访问控制中排除，可以有选择地允许访问（请参阅设备类型允许列表和 USB 设备允许列表）。

当对设备的访问由其类型及其接口进行控制时，在接口级别上拒绝访问将优先。例如，如果拒绝了对 USB 端口的访问（设备接口），那么将拒绝对连接到 USB 端口的移动设备的访问，而不管是允许还是拒绝访问移动设备（设备类型）。要允许访问此类设备，必须允许其接口和类型。

注意
如果用在 macOS 上的保护计划具有仅在 Windows 上受支持的设备类型的设置，那么这些设备类型的设置在 macOS 上将被忽略。

重要事项
当可移动设备、加密的可移动设备、打印机或蓝牙设备已连接到 USB 端口时，允许访问该设备将替代在 USB 接口级别上设置的访问拒绝。如果允许此类设备类型，将允许对该设备的访问，不管是否拒绝对 USB 端口的访问。

OS 通知和服务警报

如果最终用户试图在受保护的计算机上使用被阻止的设备类型，可以配置设备控制以显示 OS 通知。当在访问设置中选中了**如果最终用户试图使用被阻止的设备类型或端口，显示 OS 通知**复选框时，如果发生任何以下事件，代理程序会在受保护计算机的通知区域显示一条弹出消息：

- 拒绝在 USB 或 FireWire 端口上尝试使用设备。当用户插入在界面级别（例如，当拒绝对 USB 端口的访问时）或在类型级别（例如，当拒绝使用可移动设备时）拒绝的 USB 或 FireWire 设备时，显示此通知。该通知的内容是不允许此用户访问指定的设备/驱动器。
- 拒绝尝试从特定设备复制数据对象（例如文件）。当拒绝对以下设备的读取访问时将显示此通知：软盘驱动器、光盘驱动器、可移动设备、加密的可移动设备、移动设备、重定向的映射驱动器以及重定向的剪贴板传入数据。该通知的内容是不允许此用户从指定的设备获取指定的数据对象。

  当拒绝对蓝牙、FireWire 端口、USB 端口和重定向的 USB 端口的访问时，还会显示拒绝的读取通知。
- 将数据对象（例如文件）复制到特定设备的尝试被拒绝。当拒绝对以下设备的写入访问时将显示此通知：软盘驱动器、光盘驱动器、可移动设备、加密的可移动设备、移动设备、本地剪贴板、屏幕截图捕获、打印机、重定向的映射驱动器以及重定向的剪贴板传出数据。该通知的内容是不允许此用户将指定的数据对象发送到指定的设备。

用户尝试访问受保护计算机上的被阻止设备类型可能会引发记录在 Cyber Protect 中控台中的警报。通过在访问设置中选中**显示警报**复选框，可以单独为每个设备类型（不包括屏幕截图捕获）或端口启用警报。例如，如果对可移动设备的访问限制为只读，并且为该设备类型选中了**显示警报**复选框，则每当受保护计算机上的用户尝试将数据复制到可移动设备时，都会记录警报。请参见设备控制警报获取详细信息。

另请参见启用或禁用 OS 通知和服务警报的步骤。

设备类型允许列表

在**设备类型允许列表**页面上，可以选择要从设备访问控制中排除的设备子类。结果是，将允许对这些设备的访问，而不管设备控制模块中的访问设置如何。

设备控制模块提供了选项，以允许访问被拒绝设备类型中特定子类的设备。此选项允许您拒绝特定类型的所有设备，除了此类型设备的某些子类。它是有用的，例如，当您需要拒绝所有 USB 端口，同时允许使用 USB 键盘和鼠标时。

当配置设备控制模块时，可以指定要从设备访问控制中排除哪些设备子类。当设备属于排除的子类时，允许访问该设备，不管是否拒绝该设备类型或端口。可以从设备访问控制中有选择地排除以下设备子类：

- **USB HID（鼠标、键盘等）** - 选择后，将允许访问连接到 USB 端口的人机接口设备（鼠标、键盘等等），即使 USB 端口被拒绝。默认情况下会选择此项，这样拒绝访问 USB 端口不会禁用键盘或鼠标。
  在 Windows 和 macOS 上受支持。
- **USB 和 FireWire 网卡** - 选择后，将允许访问连接到 USB 或 FireWire (IEEE 1394) 端口的网卡，即使 USB 端口和/或 FireWire 端口被拒绝。
  在 Windows 和 macOS 上受支持。
- **USB 扫描仪和静态图像设备** - 选择后，将允许访问连接到 USB 端口的扫描仪和静态图像设备，即使 USB 端口被拒绝。
  仅在 Windows 上受支持。
- **USB 音频设备** - 选择后，将允许访问连接到 USB 端口的音频设备（例如耳机和麦克风），即使 USB 端口被拒绝。
  仅在 Windows 上受支持。
- **USB 相机** - 选择后，将允许访问连接到 USB 端口的 Web 相机，即使 USB 端口被拒绝。
  仅在 Windows 上受支持。
- **蓝牙 HID（鼠标、键盘等）** - 选择后，将允许访问通过蓝牙连接的人机接口设备（鼠标、键盘等等），即使蓝牙被拒绝。
  仅在 Windows 上受支持。
- **应用程序内的剪贴板复制/粘贴** - 选择后，允许在相同的应用程序内通过剪贴板复制/粘贴数据，即使剪贴板被拒绝。
  仅在 Windows 上受支持。

注意
如果在适用的保护计划中配置了不受支持的设备子类的设置，则这些设置会被忽略。

当使用允许列表允许设备类型时，考虑以下事项：

- 使用设备类型允许列表时，仅可以允许设备的完整子类。不能允许特定设备型号，同时拒绝相同子类的所有其他设备。例如，通过从设备访问控制中排除 USB 相机，可以允许使用任何 USB 相机，不管其型号和供应商如何。有关如何允许单个设备/型号的信息，请参阅 USB 设备允许列表。
- 设备类型仅可从已关闭的设备子类列表中选择。如果要允许的设备属于不同的子类，那么不能通过使用设备类型允许列表而得到允许。例如，诸如 USB 智能卡读取器这样的子类不能添加到允许列表。若要在拒绝 USB 端口时允许 USB 智能卡读取器，请遵循 USB 设备允许列表中的说明。
- 该设备类型允许列表仅适用于使用标准 Windows 驱动程序的设备。设备控制可能不会识别某些具有专利驱动程序的 USB 设备。结果是，不能通过使用设备类型允许列表访问此类 USB 设备。在此情况下，可以按设备/型号为基础允许访问（请参阅 USB 设备允许列表）。

USB 设备允许列表

该允许列表旨在允许使用特定 USB 设备，而不管任何其他设备控制设置。可以将单个设备或设备型号添加到允许列表，以禁用对这些设备的访问控制。例如，如果使用唯一 ID 将移动设备添加到允许列表，则允许使用该特定设备，即使任何其他 USB 设备都被拒绝。

在 **USB 设备允许列表**页面上，可以指定要从设备访问控制中排除的单个 USB 设备或 USB 设备型号。结果是，将允许对这些设备的访问，而不管设备控制模块中的访问设置如何。

有两种方法来识别允许列表中的设备：

- 设备型号 - 共同识别特定型号的所有设备。每种设备型号由供应商 ID (VID) 和产品 ID (PID) 进行识别，例如 USB\VID_0FCE&PID_E19E。

  此 VID 和 PID 组合不会识别特定设备，而是整个设备型号。通过将设备型号添加到允许列表，即允许对该型号任何设备的访问。例如，通过此方法，可以允许使用特定型号的 USB 打印机。
- 唯一设备 - 识别特定设备。每种唯一设备由供应商 ID (VID)、产品 ID (PID) 和序列号进行识别，例如 USB\VID_0FCE&PID_E19E\D55E7FCA。

  并非所有的 USB 设备都指派了序列号。仅当在生产期间为设备指派了序列号时，才可以将设备作为唯一设备添加到允许列表。例如，具有唯一序列号的记忆棒。

要将设备添加到允许列表，首先需要将其添加到 USB 设备数据库。然后，通过从该数据库中选择，可以将设备添加到允许列表。

在单独的配置页上管理的允许列表称为 **USB 设备允许列表**。列表中的每一项都代表一个设备或设备型号，并具有以下字段：

- **描述** - 当连接到 USB 设备时，操作系统指派特定的描述。可以修改 USB 设备数据库中设备的描述(请参阅 USB 数据库管理页)。
- **设备类型** - 如果列表项表示唯一设备，则显示“唯一”，或者如果它表示设备型号，则显示“型号”。
- **只读** - 选择后，仅允许接收来自该设备的数据。如果设备不支持只读访问，将阻止对设备的访问。清除此复选框以允许对设备的完全访问。
- **重新初始化** - 如果选中该选项，则会导致设备在新用户登录时模拟断开连接/重新连接。某些 USB 设备需要重新初始化才能正常工作，因此建议您为此类设备(鼠标、键盘等)选中此复选框。还建议您为数据存储设备(U 盘、光盘驱动器、外部硬盘驱动器等)清除此复选框。
  设备控制可能无法重新初始化某些具有专利驱动程序的 USB 设备。如果无法访问此类设备，则必须从 USB 端口移除该 USB 设备，然后将其重新插入。

注意
默认情况下，**重新初始化**字段处于隐藏状态。要在表中显示它，请单击表格右上角的齿轮图标，然后选中**重新初始化**复选框。

注意
只读和**重新初始化**字段在 macOS 不受支持。如果在适用的保护计划中配置了这些设置，它们会被忽略。

可以按以下步骤向允许列表添加设备/型号或从中删除：

- 单击列表上方的**从数据库添加**，然后从在 USB 设备数据库中注册的设备中选择所需的设备。选择的设备将添加到列表，可在其中配置其设置并确认更改。
- 单击警报中的**允许此 USB 设备**，该警报通知对 USB 设备的访问被拒绝(请参阅设备控制警报)。这会将设备添加到允许列表和 USB 设备数据库。
- 单击列表项末尾的删除图标。这将从允许列表中删除相应的设备/型号。

USB 设备数据库

设备控制模块维护一个 USB 设备数据库，可以从中将设备添加到排除列表(请参阅 USB 设备允许列表)。可以通过以下任一方式在数据库中注册 USB 设备：

- 将设备添加到排除列表时，在显示的页面上添加设备(请参阅 USB 设备数据库管理页)。
- 在 Cyber Protect 中控台中，从计算机的“清查”窗格的“USB 设备”选项卡添加设备(请参阅计算机上的 USB 设备列表)。
- 从拒绝访问 USB 设备的警报中允许设备(请参阅设备控制警报)。

另请参阅从数据库添加或删除 USB 设备的步骤。

USB 设备数据库管理页

当配置 USB 设备的允许列表时，可以选择从数据库中添加设备。如果选择此选项，将显示一个带有设备列表的管理页面。在可以查看数据库中注册的所有设备列表的此页面上，可以选择要添加到允许列表的设备，然后执行以下操作：

在数据库中注册设备

1. 单击页面顶部的**添加到数据库**。
2. 在出现的**添加 USB 设备**对话框中，选择要连接 USB 设备的计算机。
   仅联机的计算机会显示在计算机列表中。
   USB 设备列表仅会针对已安装适用于数据丢失预防的代理程序的计算机显示。
   USB 设备会以树状视图列出。树的第一层表示设备模型。第二层表示该模型的特定设备。
   设备描述旁边的蓝色图标表示该设备当前已连接到计算机。如果设备未连接到计算机，该图标将灰显。
3. 选中要注册的 USB 设备的复选框，然后单击**添加到数据库**。

更改设备的描述

1. 在 **USB 设备数据库**页面上，单击表示设备的列表项末尾的省略号 (...)，然后单击**编辑**。
2. 在显示的对话框中，对描述进行更改。

从数据库中删除设备

1. 单击表示设备的列表项末尾的省略号 (...)。
2. 单击**删除**，然后确认该删除。

对于每个设备，页面上的列表提供了以下信息：

- **描述** - 设备的可读标识符。可以根据需要更改描述。
- **设备类型** - 如果列表项表示唯一设备，则显示“唯一”，或者如果它表示设备型号，则显示“型号”。唯一设备必须具有序列号以及供应商 ID (VID) 和产品 ID (PID)，其中设备型号由 VID 和 PID 的组合进行标识。
- **供应商 ID**、**产品 ID**、**序列号** - 这些值一起组成了设备 ID，形式为 USB\VID_<供应商 ID>&PID_<产品 ID>\<序列号>。
- **帐户** - 表示此设备所属的租户。这是包含用于在数据库中注册设备的用户帐户的租户。

注意
默认情况下，此列是隐藏的。要在表中显示它，请单击表格右上角的齿轮图标，然后选择**帐户**。

最左侧的列用于选择要添加到允许列表的设备：选中每个要添加的设备的复选框，然后单击**添加到允许列表**按钮。要选择或清除所有复选框，请单击列标题中的复选框。

可以搜索或过滤设备列表：

- 单击页面顶部的**搜索**，并输入搜索字符串。该列表显示其描述匹配您键入的字符串的设备。
- 单击**过滤器**，然后在显示的对话框中应用过滤器。该列表限于具有在配置过滤器时选择的类型、供应商 ID、产品 ID 以及帐户的设备。要取消过滤器并列出所有设备，请单击**重置为默认值**。

导出数据库中的 USB 设备列表

可以导出已添加到数据库中的 USB 设备列表。

1. 打开设备的保护计划以进行编辑。
2. 单击**设备控制**开关旁边的箭头图标以展开设置，然后单击 **USB 设备允许列表**行。
3. 在 USB 设备允许列表页面上，单击**从数据库添加**。
4. 在显示的 USB 设备数据库管理页面上，单击**导出**。
   标准的“浏览”对话框将打开。
5. 选择要保存文件到的位置、根据需要输入新的文件名，然后单击**保存**。

USB 设备列表会导出为一个 JSON 文件。

可以编辑生成的 JSON 文件，以在其中添加或删除设备，并对设备描述进行批量更改。

将 USB 设备列表导入到数据库

可以导入 USB 设备列表，而不是在 Cyber Protect 中控台中添加 USB 设备。该列表是一个 JSON 格式的文件。

注意
可以将 JSON 文件导入到不包含文件中所描述设备的数据库。要将修改的文件导入到从中导出该文件的数据库，必须先清空数据库，因为不能导入重复的条目。如果导出 USB 设备列表、进行修改，然后尝试在不清除同一数据库的情况下导入到该数据库，则导入会失败。

1. 打开设备的保护计划以进行编辑。
2. 单击**设备控制**开关旁边的箭头图标以展开设置，然后单击 **USB 设备允许列表**行。

3. 在 USB 设备允许列表页面上，单击**从数据库添加**。
4. 对要导入的文件使用拖放(或浏览)操作。

   Cyber Protect 中控台会检查列表中是否包含数据库中已存在的重复条目，并跳过它们。在数据库中找不到的 USB 设备会附加到该数据库中。

计算机上的 USB 设备列表

在 Cyber Protect 中控台中，计算机的"清查"面板包含 **USB 设备**选项卡。如果计算机处于联机状态且已安装适用于数据丢失预防的代理程序，则 **USB 设备**选项卡会显示曾连接到该计算机的所有 USB 设备列表。

USB 设备会以树状视图列出。树的第一层表示设备模型。第二层表示该模型的特定设备。

对于每个设备，该列表提供了以下信息：

- **描述** - 当连接 USB 设备时，操作系统会指派描述。此描述可以当作设备的可读标识符。
  设备描述旁边的蓝色图标表示该设备当前已连接到计算机。如果设备未连接到计算机，该图标将灰显。
- **设备 ID** - 操作系统指派给设备的标识符。此标识符的格式如下：USB\VID_<供应商 ID>&PID_<产品 ID>\<序列号> 其中 <序列号> 是可选的。示例：USB\VID_0FCE&PID_ADDE\D55E7FCA(具有序列号的设备)；USB\VID_0FCE&PID_ADDE(无序列号的设备)。

要将设备添加到 USB 设备数据库，请选中所需设备的复选框，然后单击**添加到数据库**按钮。

从访问控制中排除进程

对 Windows 剪贴板、屏幕截图捕获、打印机和移动设备的访问是通过注入到进程中的钩子控制的。如果未钩住进程，将无法控制对这些设备的访问。

注意
从访问控制中排除进程在 macOS 不受支持。如果在适用的保护计划中配置了排除的进程列表，它会被忽略。

在**排除**页面中，可以指定将不会钩住的进程列表。这意味着剪贴板(本地和重定向)、屏幕截图捕获、打印机和移动设备访问控制将不会应用于此类进程。

例如，已应用了拒绝访问打印机的保护计划，然后启动了 Microsoft Word 应用程序。从该应用程序进行打印的尝试将被阻止。但若将 Microsoft Word 进程添加到排除列表中，则该应用程序将不会被钩住。因此，从 Microsoft Word 进行打印将不会被阻止，而从其他应用程序进行打印仍将被阻止。

将进程添加到排除

1. 打开设备的保护计划以进行编辑：
   单击保护计划名称旁边的省略号 (...)，然后选择**编辑**。

   注意
   必须在计划中启用设备控制，以便可以访问设备控制设置。

2. 单击**设备控制**开关旁边的箭头以展开设置，然后单击**排除**行。
3. 在**排除**页面上的**进程和文件夹**行中，单击 **+添加**。
4. 添加要从访问控制中排除的进程。
   例如，`C:\Folder\subfolder\process.exe`。
   可以使用通配符：
   - * 替换任意数量的字符。
   - ? 替换一个字符。

   例如：

   ```
   C:\Folder\*
   *\Folder\SubFolder?\*
   *\process.exe
   ```
5. 单击复选标记，然后单击**完成**。
6. 在保护计划中，单击**保存**。
7. 重新启动已排除的进程，以确保已正确删除了钩子。

排除的进程将有权访问剪贴板、屏幕截图捕获、打印机和移动设备，而与这些设备的访问设置无关。

从排除中删除进程

打开设备的保护计划以进行编辑：

单击保护计划名称旁边的省略号 (...)，然后选择**编辑**。

注意
必须在计划中启用设备控制，以便可以访问设备控制设置。

1. 单击**设备控制**开关旁边的箭头以展开设置，然后单击**排除**行。
2. 在**排除**页面上，单击要从排除中删除的进程旁边的垃圾箱图标。
3. 单击**完成**。
4. 在保护计划中，单击**保存**。
5. 重新启动该进程，以确保已正确注入了钩子。

保护计划中的访问设置将应用于从排除中删除的进程。

在排除中编辑进程

1. 打开设备的保护计划以进行编辑：
   单击保护计划名称旁边的省略号 (...)，然后选择**编辑**。

   注意
   必须在计划中启用设备控制，以便可以访问设备控制设置。

2. 单击**设备控制**开关旁边的箭头以展开设置，然后单击**排除**行。
3. 在**排除**页面上，单击要编辑的进程旁边的**编辑**图标。
4. 应用更改，并单击复选标记以确认。

5. 单击**完成**。
6. 在保护计划中，单击**保存**。
7. 重新启动受影响的进程，以确保所做的更改已正确应用。

设备控制警报

通过跟踪用户访问受控类型、端口或接口的尝试，设备控制维护一个事件日志。特定事件可能会引发记录在 Cyber Protect 中控台中的警报。例如，设备控制模块可以配置为防止使用可移动设备，当用户试图与此类设备传输数据时，会记录一条警报。

当配置设备控制模块时，可以为设备类型（屏幕截图捕获除外）或端口下列出的大多数项目启用警报。如果警报已启用，则用户每次尝试执行不允许的操作时都会生成警报。例如，如果对可移动设备的访问限制为只读，并且为该设备类型选中了**显示警报**选项，则每当受保护计算机上的用户尝试将数据复制到可移动设备时都会生成警报。

要在 Cyber Protect 中控台中查看警报，请转到**监视** > **警报**。在每个设备控制警报中，中控台提供以下有关各自事件的信息：

- **类型** - 警告。
- **状态** - 显示“外围设备访问已被阻止”。
- **消息** - 显示“访问‘<计算机名称>’上的‘<设备类型或端口>’已被阻止”。例如，“已阻止对‘<accountant-pc>’上的‘<可移动>’的访问”。
- **日期和时间** - 事件发生的日期和时间。
- **设备** - 发生事件的计算机的名称。
- **计划名称** - 引发事件的保护计划的名称。
- **源** - 事件中涉及的设备类型或端口。例如，在被拒绝的用户尝试访问可移动设备的事件中，此字段读取“可移动”设备。
- **操作** - 引发事件的操作。例如，在被拒绝的用户尝试将数据复制到设备的事件中，此字段读取“写入”。有关详细信息，请参阅操作字段值。
- **名称** - 事件目标对象的名称，例如用户尝试复制的文件，或用户尝试使用的设备。如果不能识别目标对象，则不会显示。
- **信息** - 有关事件目标设备的其他信息，例如 USB 设备的设备 ID。如果没有有关目标设备的其他可用信息，则不会显示。
- **用户** - 引发事件的用户名。
- **进程** - 引发事件的应用程序的可执行文件的完全限定路径。在某些情况下，可能会显示进程名称而不是路径。如果进程信息不可用，则不显示。

如果警报应用于 USB 设备（包括可移动设备和加密的可移动设备），那么管理员可以直接从警报中将设备添加到允许列表，这可防止设备控制模块限制对特定设备的访问。单击**允许此 USB 设备**会在设备控制模块的配置中将其添加到 USB 设备允许列表，还会将其添加到 USB 设备数据库供将来参考。

另请参见查看设备控制警报的步骤。

操作字段值

警报**操作**字段可以包含以下值：

- **读取** - 从设备或端口获取数据。
- **写入** - 将数据发送到设备或端口。
- **格式** - 直接访问(格式化、检查磁盘等)设备。在端口情况下，适用于连接到该端口的设备。
- **弹出** - 从系统中删除设备，或从设备中弹出媒体。在端口情况下，适用于连接到该端口的设备。
- **打印** - 将文档发送到打印机。
- **复制音频** - 通过本地剪贴板复制/粘贴音频数据。
- **复制文件** - 通过本地剪贴板复制/粘贴文件。
- **复制图像** - 通过本地剪贴板复制/粘贴图像。
- **复制文本** - 通过本地剪贴板复制/粘贴文本。
- **复制未识别的内容** - 通过本地剪贴板复制/粘贴其他数据。
- **复制 RTF 数据(图像)** - 使用 RTF 格式通过本地剪贴板复制/粘贴图像。
- **复制 RTF 数据(文件)** - 使用 RTF 格式通过本地剪贴板复制/粘贴文件。
- **复制 RTF 数据(文本、图像)** - 使用 RTF 格式通过本地剪贴板复制/粘贴文本和图像。
- **复制 RTF 数据(文本、文件)** - 使用 RTF 格式通过本地剪贴板复制/粘贴文本和文件。
- **复制 RTF 数据(图像、文件)** - 使用 RTF 格式通过本地剪贴板复制/粘贴图像和文件。
- **复制 RTF 数据(文本、图像、文件)** - 使用 RTF 格式通过本地剪贴板复制/粘贴文本以及图像和文件。
- **删除** - 从设备中删除数据(例如，可移动设备、移动设备等等)。
- **设备访问** - 访问某些设备或端口(例如，蓝牙设备、USB 端口等等)。
- **传入音频** - 通过重定向的剪贴板将音频数据从客户端计算机复制/粘贴到受托管的会话。
- **传入文件** - 通过重定向的剪贴板将文件从客户端计算机复制/粘贴到受托管的会话。
- **传入图像** - 通过重定向的剪贴板将图像从客户端计算机复制/粘贴到受托管的会话。
- **传入文本** - 通过重定向的剪贴板将文本从客户端计算机复制/粘贴到受托管的会话。
- **传入未识别的内容** - 通过重定向的剪贴板将其他数据从客户端计算机复制/粘贴到受托管的会话。
- **传入 RTF 数据(图像)** - 使用 RTF 格式并通过重定向的剪贴板将图像从客户端计算机复制/粘贴到受托管的会话。
- **传入 RTF 数据(文件)** - 使用 RTF 格式并通过重定向的剪贴板将文件从客户端计算机复制/粘贴到受托管的会话。
- **传入 RTF 数据(文本、图像)** - 使用 RTF 格式并通过重定向的剪贴板将文本和图像从客户端计算机复制/粘贴到受托管的会话。
- **传入 RTF 数据(文本、文件)** - 使用 RTF 格式并通过重定向的剪贴板将文本和文件从客户端计算机复制/粘贴到受托管的会话。
- **传入 RTF 数据(图像、文件)** - 使用 RTF 格式并通过重定向的剪贴板将图像和文件从客户端计算机复制/粘贴到受托管的会话。

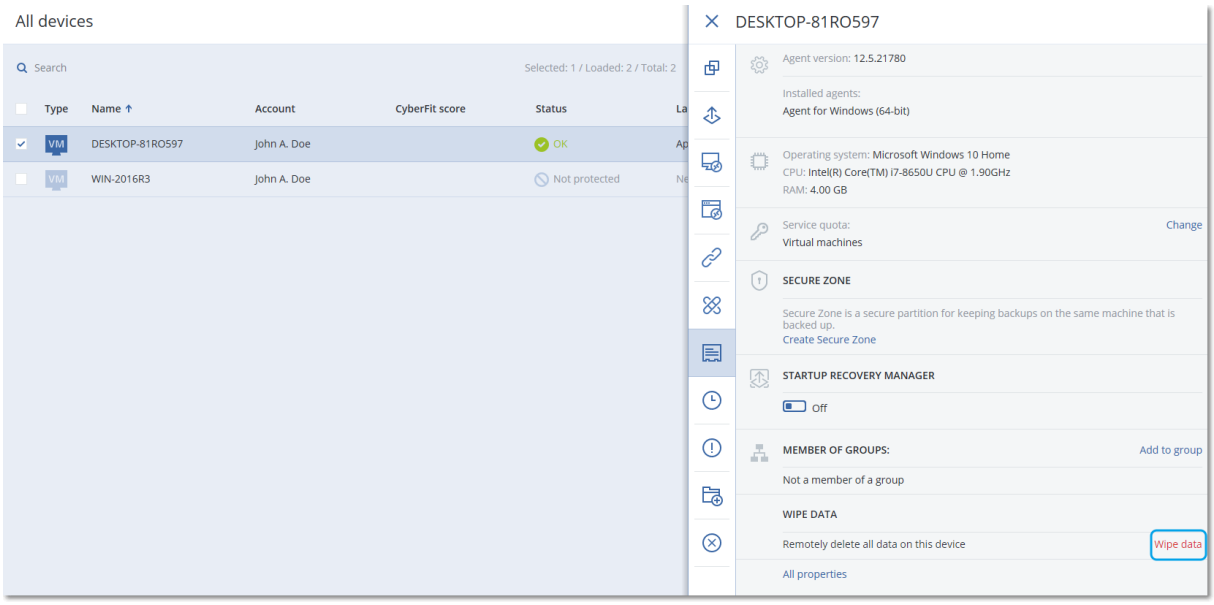
- **传入 RTF 数据(文本、图像、文件)** - 使用 RTF 格式并通过重定向的剪贴板将文本以及图像和文件从客户端计算机复制/粘贴到受托管的会话。
- **插入** -连接 USB 设备或 FireWire 设备。
- **传出音频** - 通过重定向的剪贴板将音频数据从受托管的会话复制/粘贴到客户端计算机。
- **传出文件** - 通过重定向的剪贴板将文件从受托管的会话复制/粘贴到客户端计算机。
- **传出图像** - 通过重定向的剪贴板将图像从受托管的会话复制/粘贴到客户端计算机。
- **传出文本** - 通过重定向的剪贴板将文本从受托管的会话复制/粘贴到客户端计算机。
- **传出未识别的内容** - 通过重定向的剪贴板将其他数据从受托管的会话复制/粘贴到客户端计算机。
- **传出 RTF 数据(图像)** - 使用 RTF 格式并通过重定向的剪贴板将图像从受托管的会话复制/粘贴到客户端计算机。
- **传出 RTF 数据(文件)** - 使用 RTF 格式并通过重定向的剪贴板将文件从受托管的会话复制/粘贴到客户端计算机。
- **传出 RTF 数据(文本、图像)** - 使用 RTF 格式并通过重定向的剪贴板将文本和图像从受托管的会话复制/粘贴到客户端计算机。
- **传出 RTF 数据(文本、文件)** - 使用 RTF 格式并通过重定向的剪贴板将文本和文件从受托管的会话复制/粘贴到客户端计算机。
- **传出 RTF 数据(图像、文件)** - 使用 RTF 格式并通过重定向的剪贴板将图像和文件从受托管的会话复制/粘贴到客户端计算机。
- **传出 RTF 数据(文本、图像、文件)** - 使用 RTF 格式并通过重定向的剪贴板将文本以及图像和文件从受托管的会话复制/粘贴到客户端计算机。
- **重命名** - 在设备上重命名文件(例如,在可移动设备、移动设备及其他设备上)。

从托管工作负载中擦除数据

注意
Advanced Security 包提供远程擦除。

远程擦除允许 Cyber Protection 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 及更高版本的计算机。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 Cyber Protect 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**擦除数据**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
   可以在**监控** > **活动**中，查看有关擦除过程的详细信息，以及擦除操作的发起人。

CyberApp 工作负载

CyberApp 工作负载由 ISV(独立软件供应商) 创建，并会在您启用 CyberApp 集成后显示在 Cyber Protect 中控台中。必须满足以下条件：

- 必须在 CyberApp 中启用**工作负载和操作**扩展点。
- 必须在 CyberApp 中定义至少一个**工作负载类型**。
- ISV 托管的连接器服务必须确保 CyberApp 工作负载将添加并更新到 安克诺斯 平台。

有关供应商门户和创建 CyberApp 的详细信息，请参阅《供应商门户用户指南》。

聚合的工作负载

物理工作负载可能会同时安装 Cyber Protect 代理程序以及一个或多个 CyberApp 代理程序。在这种情况下，相同的工作负载将在**所有设备**屏幕上有多个表示 - 将为 安克诺斯 工作负载和每个 CyberApp 工作负载显示一条单独的记录。如果从供应商门户或 Cyber Protect 中控台启用并配置对工作负载的自动合并，则系统将比较 安克诺斯 工作负载和 CyberApp 工作负载的主机地址和 MAC 地址，并将所有表示都合并到单个聚合工作负载中。还可以在 Cyber Protect 中控台中手动合并和取消合并工作负载。

使用 CyberApp 工作负载

除了 Cyber Protect 中控台中内置的标准操作外，还可以执行 CyberApp 工作负载出现在中控台中后可进行的操作：手动将工作负载合并到聚合工作负载中，然后执行在 CyberApp 中配置的自定义操作。

合并

先决条件

- 租户可以使用来自不同来源的工作负载。

可以手动将 安克诺斯 工作负载与一个或多个 CyberApp 工作负载合并到一个聚合工作负载中。

手动合并工作负载到聚合工作负载中

1. 在**所有设备**屏幕中，选择要合并的工作负载。

   注意
   如果选择来自不同来源的工作负载（如 Acronis 工作负载和 CyberApp 工作负载），则合并操作即会显示。

2. 单击**合并工作负载**。

执行自定义操作

先决条件

- 为租户启用已定义**工作负载操作**的 CyberApp 集成。

自定义操作是在 CyberApp 中配置并在为租户启用 CyberApp 集成时可用于相应 CyberApp 工作负载的操作。

执行自定义操作

1. 在**所有设备**屏幕中，单击相应工作负载。
2. 单击**集成的应用程序操作**。
3. 单击相应操作。

使用聚合工作负载

除了 Cyber Protect 中控台中内置的标准操作外，还可以对聚合工作负载执行以下操作：查看详细信息、取消合并源工作负载，以及执行在 CyberApp 中配置的自定义操作。

查看详细信息

先决条件

- 租户至少有一个聚合工作负载可用。

查看聚合工作负载的详细信息

1. 在**所有设备**屏幕中，单击相应聚合工作负载。
2. 单击**详细信息**。

   聚合工作负载的详细信息分为多个选项卡。每个选项卡都会显示每个工作负载表示的详细信息。

取消合并

先决条件

- 租户至少有一个聚合工作负载可用。

当取消合并聚合工作负载时，它将不再显示在设备列表中。相反，您将查看已合并到聚合工作负载的每个源工作负载的单独条目。

取消合并聚合工作负载

1. 在**所有设备**屏幕中，单击要取消合并的聚合工作负载。
2. 单击**取消合并源工作负载**。
3. 在确认窗口中，单击**取消合并**。

执行自定义操作

先决条件

- 为租户启用至少一个已定义**工作负载操作**的 CyberApp 集成。

自定义操作是在 CyberApp 中配置并在为租户启用 CyberApp 集成时可用于相应 CyberApp 工作负载的操作。

执行自定义操作

1. 在**所有设备**屏幕中，单击相应工作负载。
2. 单击**集成的应用程序操作**。
3. 根据可用的自定义操作，执行以下操作之一。
   - 如果聚合工作负载有一个 CyberApp 工作负载，则单击相应操作。
   - 如果聚合工作负载有多个 CyberApp 工作负载，则单击 CyberApp 的名称，然后单击相应操作。

查找上次登录用户

为了让管理员能够管理设备，他们必须识别现在和曾经登录到设备的用户。此信息将显示在仪表板或工作负载详细信息中。

可以启用或禁用在远程管理计划中显示上次登录信息。

在仪表板中：

1. 单击**设备**。**所有设备**窗口即会显示。
2. 在**上次登录**列中，将显示上次登录到每个设备的用户的名称。
3. 在**上次登录时间**列中，将显示用户上次登录到每个设备的时间。

在设备详细信息中：

1. 单击**设备**。**所有设备**窗口即会显示。
2. 单击要确认其详细信息的设备。
3. 单击**详细信息**图标。在**上次用户登录**部分中，将显示上次登录到选定设备的用户的名称以及日期和时间。

注意
在**上次用户登录**部分中，将显示最多 5 个登录到设备的不同用户。

在仪表板中显示或隐藏上次登录和上次登录时间列

1. 单击**设备**。**所有设备**窗口即会显示。
2. 单击右上角的齿轮图标，然后在**常规**部分中执行以下操作之一：
   - 如果要在仪表板上显示**上次登录**和**上次登录时间**列，请启用它们。
   - 如果要在仪表板中隐藏**上次登录**和**上次登录时间**列，请禁用它们。

计算机 #CyberFit 分数

#CyberFit 分数为您提供安全评估和评分机制，用于评估计算机的安全状态。它确定 IT 环境中的安全漏洞和针对端点的开放攻击载体，并以报告的形式提供建议的改进措施。此功能在全部 Cyber Protect 版本中都可用。

#CyberFit 分数功能适用于：

- Windows7(第一个版本) 及更高版本
- Windows Server 2008 R2 及更高版本

工作方式

安装在计算机上的保护代理程序将执行安全评估，并计算计算机的 #CyberFit 分数。计算机的的 #CyberFit 分数会自动定期重新计算。

#CyberFit 评分机制

计算机的 #CyberFit 分数根据以下指标进行计算：

- 反恶意软件保护 0-275
- 备份保护 0-175
- 防火墙 0-175
- 虚拟机专用网络 (VPN) 0-75
- 完整磁盘加密 0-125
- 网络安全 0-25

计算机的 #CyberFit 满分为 850 分。

公制	评估什么？	给用户的建议	评分
反恶意软件	代理程序会检查计算机上是否已安装反恶意程序软件。	查找结果： • 启用了反恶意软件保护（+275 分） • 没有反恶意软件保护，系统可能有风险（0 分） #CyberFit 分数提供的建议： 应该在计算机上安装并启用反恶意软件解决方案以得到保护，从而避免安全风险。 应该参考 AV-Test 或 AV-Comparatives 等网站，以了解推荐的反恶意软件解决方案清单。	275 - 计算机上已安装反恶意程序软件 0 - 计算机上未安装反恶意程序软件
备份	代理程序会检查计算机上是否安装了备份解决方案。	查找结果： • 您有保护数据的备份解决方案（+175 分） • 找不到备份解决方案，您的数据可能有风险（0 分） #CyberFit 分数提供的建议： 建议您定期备份数据，以防止数据丢失或勒索软件攻击。以下是您可以考虑使用的一些备份解决方案： • 安克诺斯 Cyber Protect/Cyber Backup/True Image • Windows Server 备份（Windows Server 2008 R2 及更高版本）	175 - 计算机已安装备份解决方案 0 - 计算机未安装备份解决方案
防火墙	代理程序检查您的环境中是否有可用并且已启用的防火墙。 代理程序执行以下操作： 1.检查 Windows 防火墙和网络保护是	查找结果： • 您针对公用和专用网络启用了防火墙，或者找到第三方防火墙解决方案（+175 分） • 您仅针对公用网络启用了防火墙（+100 分） • 您仅针对专用网络启用了防火墙（+75 分） • 您未启用防火墙，您的网络连接不安全（0 分） #CyberFit 分数提供的建议：	100 - Windows 公共防火墙已启用。 75 - Windows 私有防火墙已启用

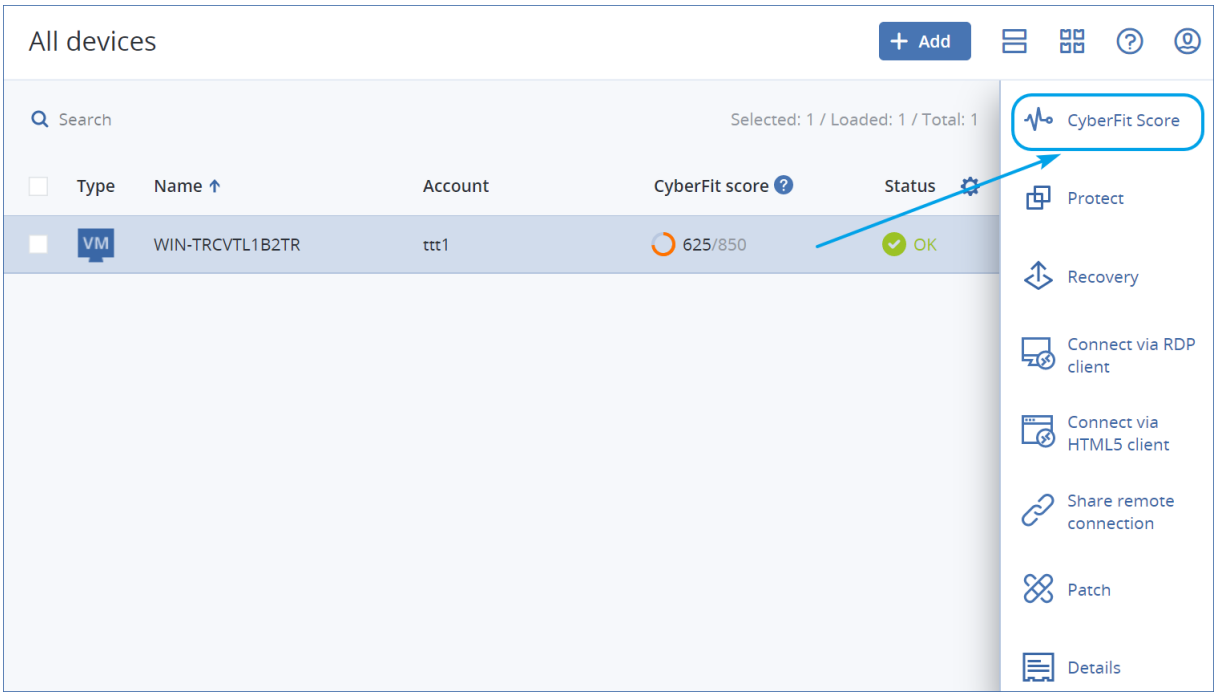
	否打开了公共防火墙。 2.检查 Windows 防火墙和网络保护是否打开了私有防火墙。 3。如果 Windows 公共和私有防火墙被禁用，则检查第三方防火墙解决方案/代理程序。	建议您为公用和专用网络启用防火墙，以加强安全保护，防止系统受到恶意攻击。下面提供了有关设置 Windows 防火墙的详细指南，具体取决于您的安全需求和网络体系结构： 针对最终用户/职员的指南： 如何在 PC 上设置 Windows Defender 防火墙 如何在 PC 上设置 Windows 防火墙 针对系统管理员和工程师的指南： 如何部署带有高级安全性的 Window Defender 防火墙 如何在 Windows 防火墙中创建高级规则	175 - Windows 公共和私有防火墙 或 已启用第三方防火墙解决方案 0 - Windows 防火墙和第三方防火墙解决方案均未启用
虚拟机专用网络 (VPN)	代理程序检查计算机上是否已安装 VPN 解决方案，以及 VPN 是否已启用并正在运行。	查找结果： • 您有 VPN 解决方案，可以安全地跨公用和共享网络接收和发送数据(+75 分) • 找不到 VPN 解决方案，与公用和共享网络的连接不安全(0 分) #CyberFit 分数提供的建议： 建议您使用 VPN 访问公司网络和机密数据。使用 VPN 来保证通信的安全性和私密性至关重要，尤其当您使用咖啡馆、图书馆、机场或其他场所提供的免费 Internet 连接时。以下是您可以考虑使用的一些 VPN 解决方案： • 安克诺斯 企业 VPN • OpenVPN • Cisco AnyConnect • NordVPN • TunnelBear • ExpressVPN • PureVPN • CyberGhost VPN • Perimeter 81 • VyprVPN • IPVanish VPN • Hotspot Shield VPN • Fortigate VPN • ZYXEL VPN • SonicWall GVPN • LANCOM VPN	75 - VPN 已经启用且正在运行 0 - VPN 未启用
磁盘加密	代理程序检查计算	查找结果：	125 - 所有磁盘均已加密

	机是否已启用磁盘加密。 代理程序检查 Windows BitLocker 是否已打开。	• 您启用了完整磁盘加密，您的计算机受到保护，不会被物理篡改(+125 分) • 仅某些硬盘驱动器已加密，您的计算机有被物理篡改的风险(+75 分) • 找不到磁盘加密，您的计算机有被物理篡改的风险(0 分) #CyberFit 分数提供的建议： 建议您打开 Windows BitLocker，以加强对数据和文件的保护。 指南：如何在 Windows 上打开设备加密	75 - 至少有一个磁盘已加密，但也有未加密的磁盘 0 - 未对任何磁盘进行加密
网络安全(发送到远程服务器的 NTLM 流量)	代理程序检查计算机是否限制了发送到远程服务器的传出 NTLM 流量。	查找结果： • 发送到远程服务器的传出 NTLM 流量被拒绝，您的凭据受保护(+25 分) • 发送到远程服务器的传出 NTLM 流量未被拒绝，您的凭据可能易遭暴露(0 分) #CyberFit 分数提供的建议： 为了加强安全保护，建议您拒绝所有传出到远程服务器的 NTLM 流量。您可以通过以下链接找到有关如何更改 NTLM 设置和添加例外的信息。 指南：限制发送到远程服务器的传出 NTLM 流量	25 - 发送的 NTLM 流量被设置为“拒绝所有” 0 - 发送的 NTLM 流量被设置为其他值

根据授予每个指标的总分，计算机的 #CyberFit 总数可能符合以下反映端点保护级别的等级之一：

- 0 - 579 - 较差
- 580 - 669 - 一般
- 670 - 739 - 较好
- 740 - 799 - 很好
- 800 - 850 - 优秀

可以在 Cyber Protect 中控台中查看您计算机的 #CyberFit 分数：转到**设备** > **所有设备**。在设备列表中，可以查看 **#CyberFit 分数**列。还可以对计算机运行 #CyberFit 分数扫描，以检查其安全状态。

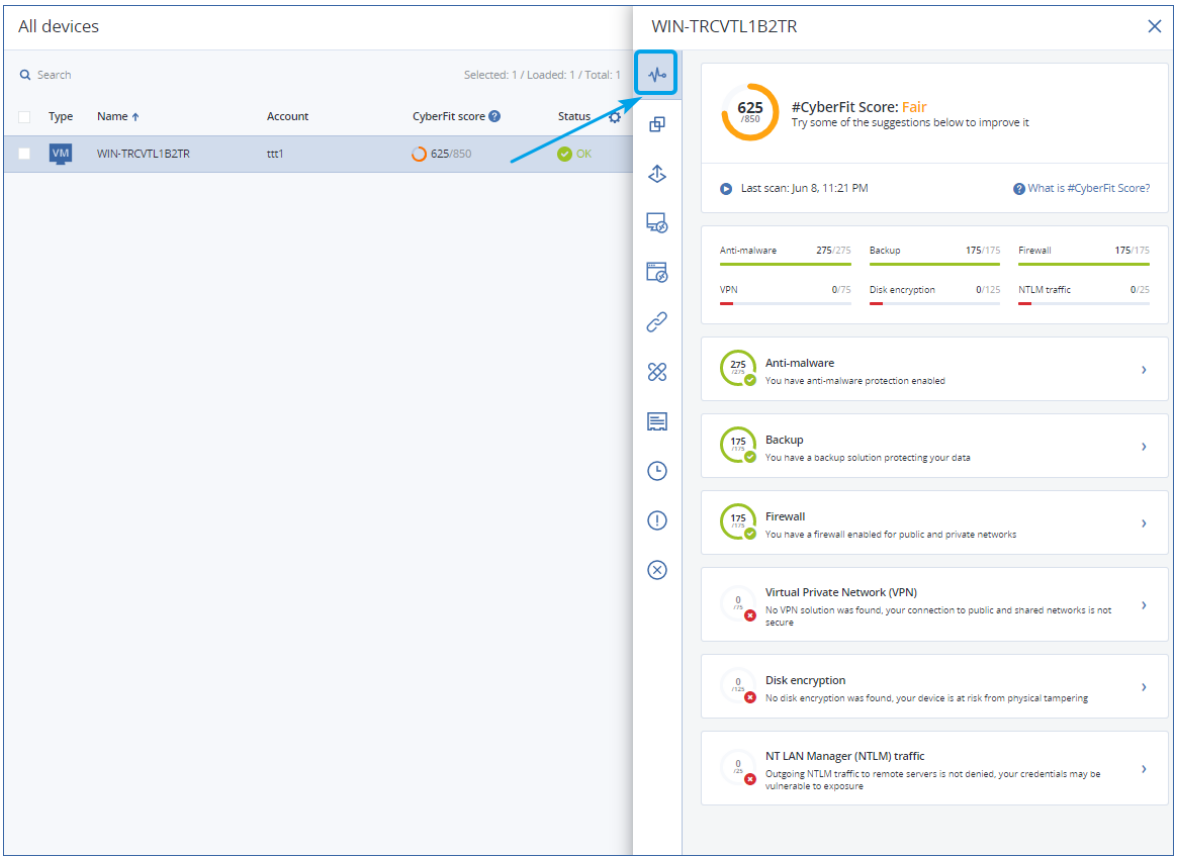


还可以在相应的小组件和报告页面中了解有关 #CyberFit 分数的信息。

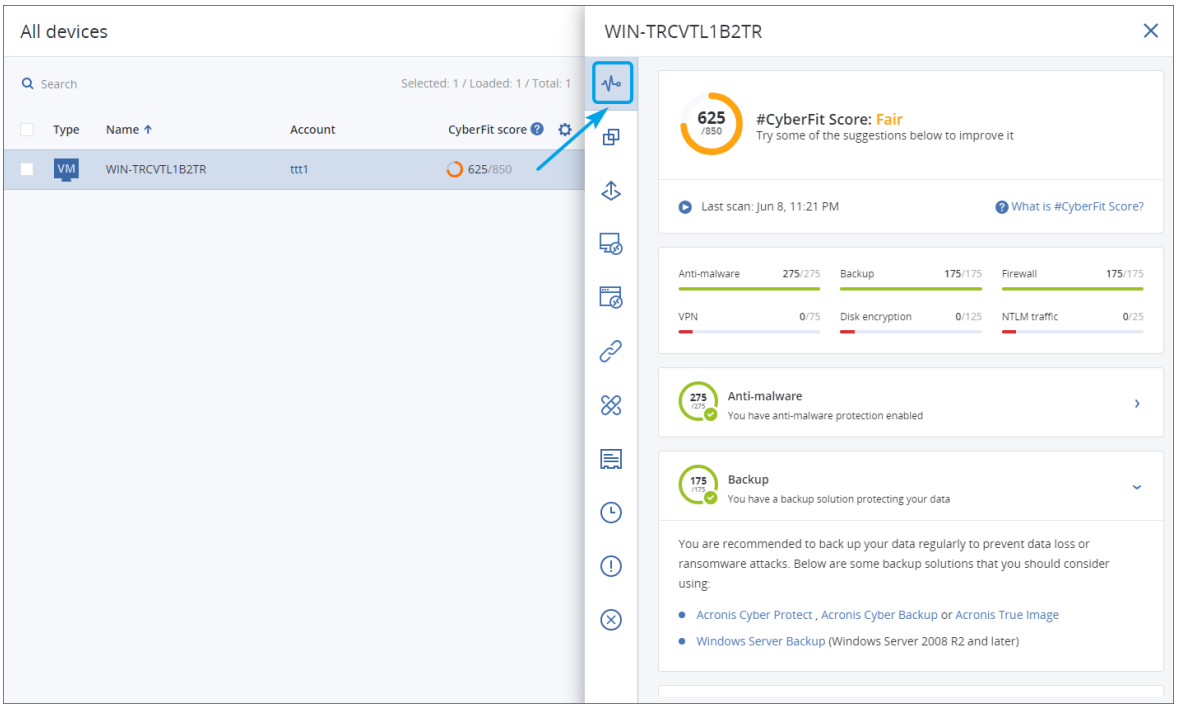
运行 #CyberFit 分数扫描

运行 #CyberFit 分数扫描

1. 在 Cyber Protect 中控台中，转到**设备**。
2. 选择计算机，然后单击 **#CyberFit 分数**。
3. 如果以前从未扫描过该计算机，则单击**运行第一次扫描**。
4. 扫描完成后，您将看到计算机的 #CyberFit 总分以及六个评估指标的分数 - 反恶意软件、备份、防火墙、虚拟专用网络 (VPN)、磁盘加密和 NT LAN Manager (NTLM) 流量。



5. 要查看如何增加可以改进安全性配置的每个指标的分数，请展开相应部分并阅读建议。



6. 解决建议后，始终可以通过单击 #CyberFit 总分下方的箭头按钮来重新计算该计算机的 #CyberFit 分数。

网络安全脚本

借助网络安全脚本，可以使用脚本对环境中的 Windows 和 macOS 计算机自动执行日常操作，例如安装软件、修改配置、启动或停止服务以及创建帐户。因此，可以减少在此类操作上所花费的时间，并降低手动执行这些操作时出现错误的风险。

网络安全脚本可供客户级别的管理员和用户以及合作伙伴管理员（服务提供商）使用。有关不同管理级别的详细信息，请参阅 "多租户支持"（第 273 页）。

可以使用的脚本必须事先获得批准。仅具有**“网络安全管理员”**角色的管理员才能批准和测试新脚本。有关更改脚本状态的详细信息，请参阅 "更改脚本状态"（第 342 页）。

根据您的用户角色，您可以使用脚本和脚本计划执行不同的操作。有关角色的更多信息，请参阅 "用户角色和网络安全脚本权限"（第 334 页）。

先决条件

- 网络安全脚本功能需要 Advanced Management 包。
- 要使用网络安全脚本的所有功能（例如脚本编辑、脚本运行、创建脚本计划等），必须为帐户启用双重身份验证。

限制

- 支持以下脚本语言：
  - PowerShell
  - Bash
- 网络安全脚本操作只能在安装有保护代理程序的目标计算机上运行。

支持的平台

网络安全脚本适用于 Windows 和 macOS 工作负载。

下表汇总了支持的版本。

操作系统	版本
Windows	Windows 7 SP1 及更高版本 - 所有版本
	Windows 8/8.1 – 除 Windows RT 版以外的所有版本(x86、x64)
	Windows 10 - 家庭版、专业版、教育版、企业版、物联网企业版
	Windows 11
	Windows Server 2008 R2 SP1 及更高版本 - 标准版、企业版、数据中心版、基础版和 Web 版
	Windows Server 2012/2012 R2 – 所有版本
	Windows Server 2016
	Windows Server 2019
	Windows Server 2022
	Windows Storage Server(2008 R2、2012、2012 R2、2016)
macOS	macOS Mojave 10.14
	macOS Catalina 10.15
	macOS Big Sur 11
	macOS Monterey 12

用户角色和网络安全脚本权限

脚本和脚本计划的可用操作取决于脚本状态和您的用户角色。

管理员可以管理他们自己的租户及其子租户中的对象。他们无法查看或访问上级管理级别的对象(如果有) 。

下级管理员对上级管理员应用于其工作负载的脚本计划仅有“只读”访问权限。

以下角色提供与网络安全脚本相关的权限:

- **公司管理员**
  此角色授予所有服务中的完全管理员权限。对于网络安全脚本, 它授予与“网络安全管理员”角色相同的权限。
- **网络管理员**
  此角色授予完全权限, 包括批准可以在租户中使用的脚本以及可以运行状态为**正在测试**的脚本。
- **管理员**
  此角色授予部分权限, 可以运行批准的脚本以及创建和运行使用批准的脚本的脚本计划。
- **只读管理员**

此角色授予有限权限，可以查看租户中使用的脚本和保护计划。

- **用户**

  此角色授予部分权限，可以运行批准的脚本以及创建和运行使用批准的脚本的脚本计划，但仅限于用户自己的计算机上。

下表汇总了所有可用操作，具体取决于脚本状态和用户角色。

角色	对象	脚本状态		
		方案	正在测试	已批准
网络管理员 **公司管理员**	脚本计划	编辑(从计划中删除草稿脚本) 删除 废除 禁用 停止	创建 编辑 应用 启用 运行 删除 废除 禁用 停止	创建 编辑 应用 启用 运行 删除 废除 禁用 停止
	脚本	创建 编辑 更改状态 克隆 删除 取消正在运行	创建 编辑 更改状态 运行 克隆 删除 取消正在运行	创建 编辑 更改状态 运行 克隆 删除 取消正在运行
管理员 **用户**(针对他们自己的工作负载)	脚本计划	查看 废除 禁用 停止	查看 取消运行	创建 编辑 应用 启用 运行 删除 废除 禁用

				停止
	脚本	创建 编辑 克隆 删除 取消正在运行	查看 克隆 取消正在运行	运行 克隆 取消正在运行
只读管理员	脚本计划	查看	查看	查看
	脚本	查看	查看	查看

脚本

脚本是一组在运行时解释并在目标计算机上执行的指令。脚本为自动化重复或复杂的任务提供了一种便捷的解决方案。

使用网络安全脚本，可以运行预定义脚本或创建自定义脚本。可以在**管理** > **脚本存储库**中查看所有可供您使用的脚本。预定义的脚本位于**库**部分中。您创建或克隆到租户的脚本位于**我的脚本**部分中。

可以通过将脚本包含在脚本计划中或执行**脚本快速运行**操作来使用脚本。

注意
只能使用在您的租户中创建或已克隆到其中的已批准脚本。如果脚本已从脚本存储库中删除或者处于**草稿**状态，则它不会运行。可以在**监控** > **活动**中检查脚本操作的详细信息或取消它。

下表提供了有关脚本可能执行的操作的更多信息，具体因脚本状态而异。

状态	可能的操作
方案	您创建的新脚本和克隆到存储库的脚本均处于**草稿**状态。无法运行这些脚本或将它们包含在脚本计划中。
正在测试	具有**网络管理员**角色的管理员可以运行这些脚本并将它们包含在脚本编写计划中。
已批准	您可以运行这些脚本并将它们包含在脚本计划中。

只有具有**网络管理员**角色的管理员才能更改脚本的状态或删除已批准的脚本。有关更多信息，请参阅 "更改脚本状态"(第 342 页)。

创建脚本

可以通过手动编写代码来创建脚本。

创建脚本

1. 在 Cyber Protect 中控台中，转到**管理** > **脚本存储库**。
2. 在**“我的脚本”**中，单击**“使用 AI 创建脚本”**。
3. 在主窗格中，编写脚本的正文。

重要事项
创建脚本时，请为每个操作包含退出代码检查。否则，失败的操作可能会被忽略，并且**监控** > **活动**中的脚本活动状态可能会错误地显示为**已成功**。

4. 指定脚本设置。

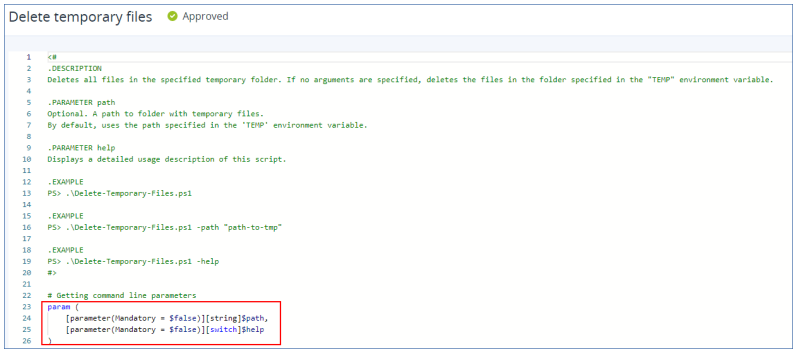
设置	描述
脚本名称	脚本名称。该字段会自动填充，但您可以更改该值。
描述	脚本描述。此设置是可选的。 [对于 AI 生成的脚本] 该字段将在脚本生成时自动填充。您可以编辑 AI 提供的描述。
语言	脚本语言。可用值为： • **PowerShell**。这是默认值。 • **Bash** [对于 AI 生成的脚本] 此设置在脚本生成之前配置。
操作系统	安装在将运行脚本的目标工作负载上的操作系统。可用值为： • **Windows**。这是默认值。 • **macOS** [对于 AI 生成的脚本] 此设置在脚本生成之前配置。
状态	脚本状态。 • **草稿**。这是默认值。您创建的新脚本和克隆到存储库的脚本均处于**草稿**状态。您无法运行**草稿**脚本或将它们包含在脚本计划中。 • **测试**。只有具有**网络管理员**角色的管理员才能将脚本的状态更改为**测试**、在**测试**状态下运行脚本以及使用此类脚本运行脚本计划。 • **已批准**。您可以运行**已批准**脚本并将它们包含在脚本计划中。 只有具有**网络管理员**角色的管理员才能更改脚本的状态或删除已批准的脚本。有关更多信息，请参阅 "更改脚本状态"(第 342 页) 。
标签	标签不区分大小写，长度最多不能超过 32 个字符。不能使用圆括号和尖括号、逗号或空格。此设置是可选的。 [对于 AI 生成的脚本] 脚本生成时会自动添加**由 AI 生成**标签。您可以手动删除此标签或添加更多标签。

5. [仅适用于需要凭据的脚本] 指定凭据。
   可以使用单个凭据(例如，令牌) ，也可以使用一对凭据(例如，用户名和密码) 。
6. [仅适用于需要参数的脚本] 指定参数及其值，如下所示：
   a. 单击**添加**。
   b. 在**“添加参数”**字段中，指定参数。

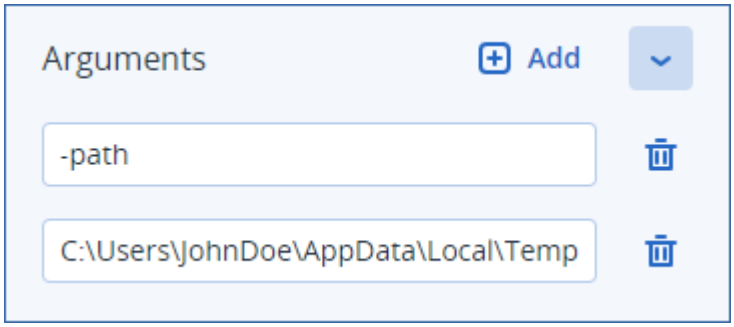
c. 单击**添加**。

d. 在出现的第二个字段中，指定参数值。

注意
您只能指定已在脚本正文中定义的参数。



例如：



e. 如果您需要添加多个参数，请重复上述步骤。

7. 单击**保存**。

该脚本以**草稿**状态保存到您的存储库中。

在具有**网络管理员**角色的管理员将其状态更改为**“已批准”**之前，您无法使用该脚本。有关更多信息，请参阅 "更改脚本状态"(第 342 页)。

若要在您管理的另一个租户中使用脚本，您必须将该脚本克隆到该租户。有关更多信息，请参阅 "克隆脚本"(第 341 页)。

使用 AI 创建脚本

注意
此功能需要 Advanced Management 包。

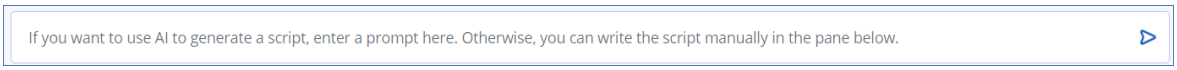
可以借助 ScriptPilot 利用 AI 将提示转换为功能强大的脚本，从而节省您的时间和精力。可以通过以下方式使用该功能：

- 输入提示，要求 AI 从头开始生成脚本。
- 输入提示，要求 AI 检查并完成您在脚本正文中输入的代码。当您在处理更复杂的代码时，可以使用此功能。

该功能使用 OpenAI 的 GPT-4 模型。您可以每个日历月使用它为组织免费创建最多 100 个脚本。

使用 AI 创建脚本

1. 在 Cyber Protect 中控台中，转到**管理** > **脚本存储库**。
2. 在**"我的脚本"**中，单击**"使用 AI 创建脚本"**。
3. 在提示中，输入脚本应执行的操作的描述。确保您输入的描述尽可能清晰和详细。

   例如：

   ```
   I need a script that deletes Temporary files for all users (including user profiles +
   Windows Temps) and disable Windows Update Service to allow the script to run
   ```

4. 在提示中，单击箭头按钮。
5. 在确认窗口中，选择语言和操作系统，然后单击**"生成"**。

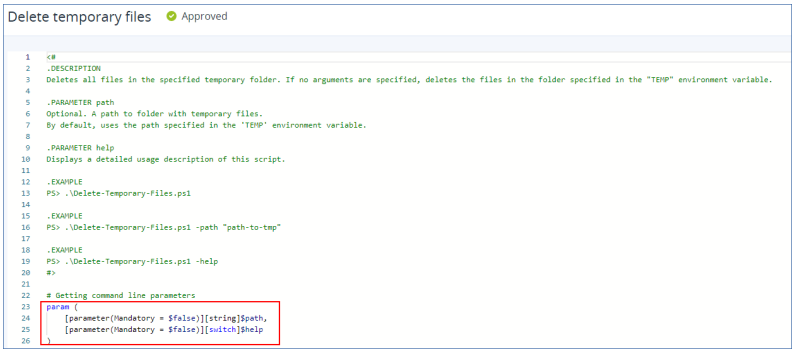
   AI 生成的脚本会显示在主窗格中。脚本的名称和描述由 AI 自动生成，以便与脚本匹配。**由 AI 生成**标签会自动指派给脚本。
6. 查看 AI 生成的脚本，如有必要，手动编辑它。
7. 如有必要，编辑脚本设置。

设置	描述
脚本名称	脚本名称。该字段会自动填充，但您可以更改该值。
描述	脚本描述。此设置是可选的。 [对于 AI 生成的脚本] 该字段将在脚本生成时自动填充。您可以编辑 AI 提供的描述。
语言	脚本语言。可用值为： • **PowerShell**。这是默认值。 • **Bash** [对于 AI 生成的脚本] 此设置在脚本生成之前配置。
操作系统	安装在将运行脚本的目标工作负载上的操作系统。可用值为： • **Windows**。这是默认值。 • **macOS** [对于 AI 生成的脚本] 此设置在脚本生成之前配置。
状态	脚本状态。 • **草稿**。这是默认值。您创建的新脚本和克隆到存储库的脚本均处于**草稿**状态。您无法运行**草稿**脚本或将它们包含在脚本计划中。 • **测试**。只有具有**网络管理员**角色的管理员才能将脚本的状态更改为**测试**、在**测试**状态下运行脚本以及使用此类脚本运行脚本计划。 • **已批准**。您可以运行**已批准**脚本并将它们包含在脚本计划中。 只有具有**网络管理员**角色的管理员才能更改脚本的状态或删除已批准的脚本。有关更多信息，请参阅 "更改脚本状态"(第 342 页) 。

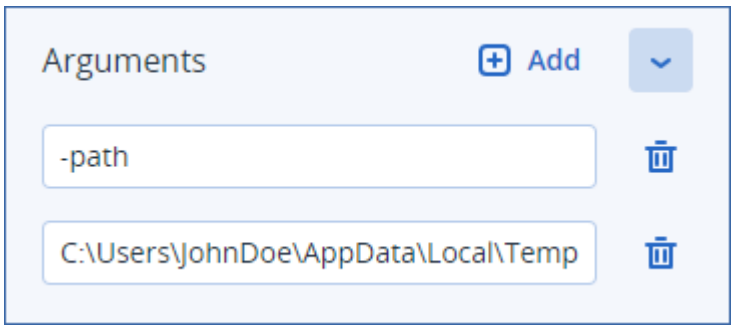
设置	描述
标签	标签不区分大小写，长度最多不能超过 32 个字符。不能使用圆括号和尖括号、逗号或空格。 此设置是可选的。 [对于 AI 生成的脚本] 脚本生成时会自动添加**由 AI 生成**标签。您可以手动删除此标签或添加更多标签。

8. [可选] [仅适用于需要凭据的脚本] 指定凭据。
   可以使用单个凭据（例如，令牌），也可以使用一对凭据（例如，用户名和密码）。
9. [仅适用于需要参数的脚本] 指定参数及其值，如下所示：
   a. 单击**添加**。
   b. 在**“添加参数”**字段中，指定参数。
   c. 单击**添加**。
   d. 在出现的第二个字段中，指定参数值。

   注意
   您只能指定已在脚本正文中定义的参数。

   例如：

   e. 如果您需要添加多个参数，请重复上述步骤。
10. 单击**保存**。
    该脚本以**草稿**状态保存到您的存储库中。
    在具有**网络管理员**角色的管理员将其状态更改为**“已批准”**之前，您无法使用该脚本。有关更多信息，请参阅 "更改脚本状态"（第 342 页）。
    若要在您管理的另一个租户中使用脚本，您必须将该脚本克隆到该租户。有关更多信息，请参阅 "克隆脚本"（第 341 页）。

克隆脚本

在以下情况下需要克隆脚本：

- 在使用**库**中的脚本之前。在这种情况下，必须先将脚本克隆到**我的脚本**部分。
- 当要将在父租户中创建的脚本克隆到其子租户或单位时。

克隆脚本

1. 在**脚本存储库**中，找到要克隆的脚本。
2. 请执行以下任一操作：
   - [如果您克隆**我的脚本**中的脚本] 单击相应脚本名称旁边的省略号 (...)，然后单击**克隆**。
   - [如果克隆**库**中的脚本] 单击已选择脚本的名称旁边的**克隆**。
3. 在**克隆脚本**弹出窗口中，从**状态**下拉列表中选择以下脚本状态之一：
   - **草稿**（默认）- 此状态不允许立即执行脚本。
   - **正在测试** - 此状态允许执行脚本。
   - **已批准** - 此状态允许执行脚本。
4. [如果您管理多个租户或单位] 选择要克隆脚本的位置。
   在**克隆脚本**对话框中，您仅会看到您可以管理并已应用 Advanced Management 包的租户。

因此，脚本会克隆到您选择的租户或单位的**我的脚本**部分。如果您仅管理一个没有单位的租户，则脚本会自动复制到**我的脚本**部分。

重要事项
将脚本克隆到非原始租户时，不会复制脚本所使用的凭据。

编辑或删除脚本

注意
根据您的用户角色，您可以使用脚本和脚本计划执行不同的操作。有关角色的更多信息，请参阅 "用户角色和网络安全脚本权限"（第 334 页）。

编辑脚本

1. 在**脚本存储库**中，转到**我的脚本**，然后找到要编辑的脚本。
2. 单击脚本名称旁边的省略号 (...)，然后单击**编辑**。
3. 编辑脚本，然后单击**保存**。
4. [如果您编辑脚本计划使用的脚本] 通过单击**保存脚本**确认您的选择。

   注意
   下次运行脚本计划时，将使用最新版本的脚本。

脚本版本

如果您编辑以下任何脚本属性，则会创建新版本的脚本：

- 脚本正文
- 脚本名称
- 描述
- 脚本语言
- 凭据
- 参数

如果更改其他属性，则编辑内容会添加到当前脚本版本。要了解有关版本以及如何比较它们的详细信息，请参阅 "比较脚本版本"(第 343 页)。

注意
仅当修改**状态**字段中的值时，脚本状态才会进行更新。仅具有“网络安全管理员”角色的管理员才能更改脚本状态。

删除脚本

1. 在**脚本存储库**中，转到**我的脚本**，然后找到要删除的脚本。
2. 单击脚本名称旁边的省略号 (...)，然后单击**删除**。
3. 单击**删除**。
4. [如果您要删除脚本计划使用的脚本] 通过单击**保存脚本**确认您的选择。

   注意
   使用已删除脚本的脚本计划将无法运行。

更改脚本状态

已创建并处于**草稿**状态的新脚本只有在其状态更改为**“已批准”**后才能使用。根据用例，脚本在获得批准之前可能会在一段时间内处于**“测试”**状态。

注意
根据您的用户角色，您可以使用脚本和脚本计划执行不同的操作。有关角色的更多信息，请参阅 "用户角色和网络安全脚本权限"(第 334 页)。

先决条件

- 您的用户是指派为**网络管理员**角色的管理员。
- 具有相应状态的脚本可用。

更改脚本状态

1. 在**“脚本存储库”**中，转到**“我的脚本“**。
2. 单击脚本名称旁边的省略号 (...)，然后单击**编辑**。
3. 在**“状态”**下拉列表中，选择状态。
4. 单击**保存**。
5. [如果更改已批准脚本的状态] 若要确认更改，请单击**“保存脚本”**。

注意

如果脚本状态降级为**草稿**，则使用它的脚本计划将无法运行。

仅具有**"网络管理员"**角色的管理员才能运行处于正在**测试**状态下的脚本和使用此类脚本的脚本计划。

比较脚本版本

可以比较脚本的两个版本并恢复到较早版本。还可以查看特定版本的创建者和创建时间。

比较脚本版本

1. 在**脚本存储库**中，转到**我的脚本**，然后找到要比较其版本的脚本。
2. 单击脚本名称旁边的省略号 (...)，然后单击**版本历史记录**。
3. 选择要比较的两个版本，然后单击**比较版本**。

   脚本正文、其参数或凭据的任何更改都会亮显。

恢复到早期版本

1. 在**比较脚本版本**窗口中，单击**恢复到此版本**。
2. 在**"恢复到先前版本"**弹出窗口的**"状态"**下拉列表中，选择脚本状态。

选定版本会恢复并另存为版本历史记录中的最新版本。

要恢复脚本，还可以从**版本历史记录**窗口中选择一个版本，然后单击**恢复**按钮。

重要事项

只能在**正在测试**或**已批准**状态下执行脚本。有关详细信息，请参阅 "更改脚本状态"(第 342 页)。

下载脚本操作的输出

可以将脚本操作的输出下载为 .zip 文件。它包含两个文本文件 - stdout 和 stderr。在 stdout 中，您可以看到成功完成脚本操作的结果。stderr 文件包含有关脚本操作期间所发生错误的信息。

下载输出文件

1. 在 Cyber Protect 中控台中，转到**监控** > **活动**。
2. 单击要下载其输出的网络安全脚本活动。
3. 在**活动详细信息**屏幕上，单击**下载输出**。

脚本存储库

可以在**管理**选项卡下找到脚本存储库。在存储库中，可以按其名称和说明搜索脚本。还可以使用过滤器，或按其名称或状态对脚本进行排序。

要管理脚本，请单击其名称旁边的省略号 (...)，然后选择所需操作。或者，单击脚本，然后使用随即打开的屏幕上的按钮。

脚本存储库包含以下部分：

- **我的脚本**

  在此处，可以找到可以直接在您的环境中使用的脚本。这些是您从头开始创建的脚本以及您在此处克隆的脚本。

  可以按以下条件过滤此部分中的脚本：

  - 标记
  - 状态
  - 语言
  - 操作系统
  - 脚本所有者
- **库**

  该库包含预定义的脚本，在将这些脚本克隆到**我的脚本**部分后即可在您的环境中使用它们。您只能检查和克隆这些脚本。

  可以按以下条件过滤此部分中的脚本：

  - 标记
  - 语言
  - 操作系统

  有关详细信息，请参阅供应商批准的脚本 (70595)。

脚本计划

脚本计划允许您在多个工作负载上运行脚本、预定脚本的运行以及配置其他设置。

可以在**管理 > 脚本计划**中找到您创建的脚本计划以及应用于工作负载的脚本计划。在此处，可以检查计划执行位置、所有者或状态。

可单击的栏会显示脚本计划的以下颜色编码状态：

- 正在运行(蓝色)
- 正在检查兼容性(深灰色)
- 已禁用(浅灰色)
- 正常(绿色)
- 严重警报(红色)
- 错误(橙色)
- 警告(黄色)

通过单击该栏，可以查看计划处于何种状态以及位于多少个工作负载上。还可以单击每个状态。

在**脚本计划**选项卡上，可以通过执行以下操作来管理计划：

- 运行
- 停止
- 编辑
- 重命名
- 禁用
- 启用

- 克隆
- 导出。计划配置将以 JSON 格式导出到本地计算机。
- 删除

脚本计划的可见性及其可用操作取决于计划所有者和您的用户角色。例如，公司管理员只能查看应用于其工作负载的合作伙伴所拥有的脚本计划，而无法对这些计划执行任何操作。

有关谁可以创建和管理脚本计划的详细信息，请参阅 "用户角色和网络安全脚本权限"(第 334 页)。

管理脚本计划

1. 在 Cyber Protect 中控台中，转到**管理** > **脚本计划**。
2. 找到要管理的计划，然后单击其旁边的省略号 (...)。
3. 选择所需操作，然后按照屏幕上的说明进行操作。

创建脚本计划

可以通过以下方式创建脚本计划：

- 在**设备**选项卡上
  选择工作负载，然后为它们创建脚本计划。
- 在**管理** > **脚本计划**选项卡上
  创建脚本计划，然后选择要应用该计划的工作负载。

在“设备”选项卡上创建脚本计划

1. 在 Cyber Protect 中控台中，转到**设备** > **装有代理程序的计算机**。
2. 选择要应用脚本计划的工作负载或设备组，然后分别单击**保护**或**保护组**。
3. [如果已有应用的计划] 单击**添加计划**。
4. 依次单击**创建计划** > **脚本计划**。
   随即打开脚本计划的模板。
5. [可选] 要修改脚本计划名称，请单击铅笔图标。
6. 单击**选择脚本**、选择要使用的脚本，然后单击**完成**。

   注意
   只能从**脚本存储库** > **我的脚本**使用您批准的脚本。仅具有**“网络安全管理员”**角色的管理员才能使用处于正在**测试**状态下的脚本。有关角色的详细信息，请参阅 "用户角色和网络安全脚本权限"(第 334 页)。

7. 配置脚本计划的预定和启动条件。
8. 选择其下的脚本将在目标工作负载上运行的帐户。可使用以下选项：
   - 系统帐户(在 macOS 中，这是 root 帐户)
   - 当前登录的帐户
9. 指定脚本可以在目标工作负载上运行的时长。
   如果脚本无法在设置的时间范围内完成运行，“网络安全脚本”操作会失败。
   可以指定的最小值为一分钟，最大值为 1440 分钟。

10. [仅适用于 PowerShell 脚本] 配置 PowerShell 执行策略。
    有关此策略的详细信息，请参阅 Microsoft 文档。
11. 单击**创建**。

在"脚本计划"选项卡上创建脚本计划

1. 在 Cyber Protect 中控台中，转到**管理** > **脚本计划**。
2. 单击**创建计划**。
   随即打开脚本计划的模板。
3. [可选] 要选择要应用新计划的工作负载或设备组，请单击**添加工作负载**。
   a. 单击**装有代理程序的计算机**以展开列表，然后选择所需的工作负载或设备组。
   b. 单击**添加**。
   有关如何在合作伙伴级别上创建设备组的详细信息，请参阅 ""设备"选项卡"(第 269 页)

   注意
   还可以在创建计划后选择工作负载或设备组。

4. [可选] 要修改脚本计划名称，请单击铅笔图标。
5. 单击**选择脚本**、选择要使用的脚本，然后单击**完成**。

   注意
   只能从**脚本存储库** > **我的脚本**使用您批准的脚本。仅具有**"网络安全管理员"**角色的管理员才能使用处于正在**测试**状态下的脚本。有关角色的详细信息，请参阅 "用户角色和网络安全脚本权限"(第 334 页)。

6. 配置脚本计划的预定和启动条件。
7. 选择其下的脚本将在目标工作负载上运行的帐户。可使用以下选项：
   - 系统帐户(在 macOS 中，这是 root 帐户)
   - 当前登录的帐户
8. 指定脚本可以在目标工作负载上运行的时长。
   如果脚本无法在设置的时间范围内完成运行，"网络安全脚本"操作会失败。
   可以指定的最小值为一分钟，最大值为 1440 分钟。
9. [仅适用于 PowerShell 脚本] 配置 PowerShell 执行策略。
   有关此策略的详细信息，请参阅 Microsoft 文档。
10. 单击**创建**。

预定和启动条件

预定

可以将脚本计划配置为运行一次或重复运行，并且可以配置为按预定启动或由特定事件触发。

可使用以下选项：

- 运行一次

  对于此选项，必须配置计划将运行的日期和时间。
- 按时间预定

  使用此选项，可以配置每小时、每天或每月运行的脚本计划。

  要使预定仅临时生效，请选中**在日期范围内运行**复选框，然后配置预定计划将运行的时间段。
- 用户登录系统时

  可以选择是特定用户还是任何登录用户触发脚本计划。
- 用户注销系统时

  可以选择是特定用户还是任何注销用户触发脚本计划。
- 系统启动时
- 系统关闭时

注意
此预定选项仅适用于在系统帐户下运行的脚本。

- 系统联机时

开始条件

启动条件会为您的预定计划增添更多灵活性。如果您配置了多个条件，则必须同时满足所有条件才能启动计划。

如果您使用**立即运行**选项手动运行计划，则启动条件无效。

条件	描述
仅当工作负载联机时运行	该条件会在目标工作负载连接到 Internet 时得到满足。
用户空闲时	当计算机正在运行屏幕保护程序或计算机已锁定时，就会满足此条件。
用户已注销	如果选择此条件，则可以推迟预定的计划，直到目标工作负载的用户注销为止。
适合时间间隔	若选择此条件，则必须定义计划可运行的时间间隔。
节省电池电量	如果选择此条件时，可以确保计划不会因电池电量不足而中断。可使用以下选项： • **不在使用电池时启动** 仅当计算机连接到电源时，该计划才会启动。 • **如果电池电量高于以下值，则在使用电池时启动** 如果计算机连接到电源或者电池电量高于指定值，则该计划会启动。
请勿在使用按流量计费的连接时启动	若选择此条件，则当目标工作负载通过按使用量计费的连接访问 Internet 时，计划将不会运行。
不在连接到以下 Wi-Fi 网络时启动	若选择此条件，如果目标工作负载已连接至任何指定的无线网络，则计划将不会运行。

条件	描述
	若要使用此条件，则必须指定禁止网络的 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，则当设备连接到以下任何网络时，计划将不会启动：John's iPhone、phone_wifi 或 my_PHONE_wifi。
检查设备 IP 地址	如果选择此条件，则目标工作负载的任何 IP 地址在指定的 IP 地址范围之内或之外，则计划将不会运行。 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** 仅支持 IPv4 地址。
如果启动条件不满足，仍运行任务	使用此选项，以设置计划将运行的时间间隔，而无需考虑任何其他条件。该计划将在其他条件满足时或这一期限结束时启动，取决于哪种情况先发生。 如果您为预定选择了**仅运行一次**选项，则无法使用此选项。

管理计划的目标工作负载

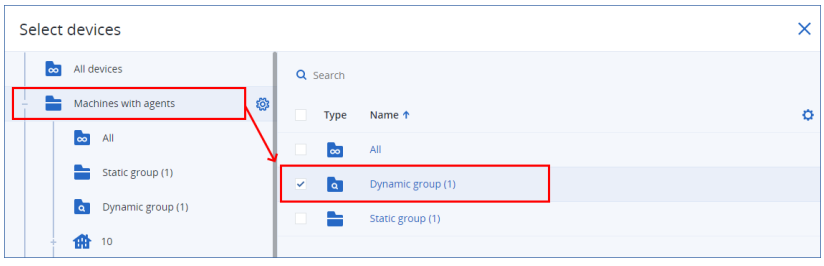
可以在创建计划时或稍后选择要应用脚本计划的工作负载或设备组。

合作伙伴管理员可以将同一计划应用于来自不同客户的工作负载，并且可以创建包含来自不同客户的工作负载的设备组。要了解如何在合作伙伴级别上创建静态或动态设备组，请参阅 ""设备"选项卡"(第 269 页)。

将初始工作负载添加到计划

1. 在 Cyber Protect 中控台中，转到**管理** > **脚本计划**。
2. 单击要为其指定目标工作负载的计划的名称。
3. 单击**添加工作负载**。
4. 选择所需工作负载或设备组，然后单击**添加**。

注意
要选择设备组，请单击其父级，然后在主窗格中选中其名称旁边的复选框。



5. 要保存编辑的计划，请单击**保存**。

管理计划的现有工作负载

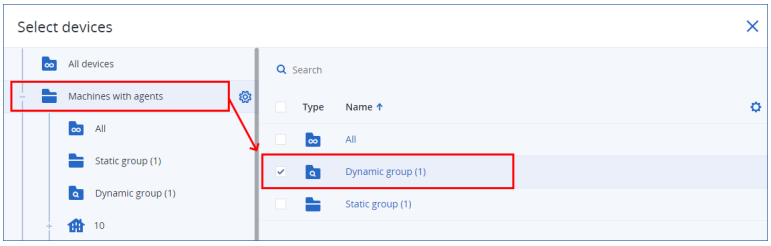
1. 在 Cyber Protect 中控台中，转到**管理** > **脚本计划**。
2. 单击要更改其目标工作负载的计划的名称。
3. 单击**管理工作负载**。

   设备屏幕会列出当前已应用脚本计划的工作负载。如果您管理多个租户，则工作负载会按租户排序。

   - 要添加新的工作负载或设备组，请单击**添加**。
     a. 选择所需工作负载或设备组。可以添加来自您管理的所有租户中的工作负载。

     注意

     要选择设备组，请单击其父级，然后在主窗格中选中其名称旁边的复选框。

     b. 单击**添加**。
   - 要删除工作负载或设备组，请选择它们，然后单击**删除**。
4. 单击**完成**。
5. 要保存编辑的计划，请单击**保存**。

不同管理级别上的计划

下表汇总了不同级别的管理员可以查看和管理的计划。

管理员	管理级别	计划	权限
合作伙伴管理员	合作伙伴级别	自己的计划	完整访问
		客户计划(包括单位中的计划)	完整访问
		单位计划	完整访问
	客户级别 (适用于由服务提供商管理的客户)	应用于此客户的工作负载的合作伙伴计划	只读
		客户计划(包括单位中的计划)	完整访问
		单位计划	完整访问

管理员	管理级别	计划	权限
	单位级别 (适用于由服务提供商管理的客户)	应用于此单位的工作负载的合作伙伴计划	只读
		应用于此单位的工作负载的客户计划	只读
		单位计划	完整访问
公司管理员	客户级别	应用于此客户或单位的工作负载的合作伙伴计划	只读
		客户计划(包括单位中的计划)	完整访问
		单位计划	完整访问
	单位级别	应用于此单位的工作负载的合作伙伴计划	只读
		应用于此单位的工作负载的客户计划	只读
		单位计划	完整访问
单位管理员	单位级别	应用于此单位的工作负载的合作伙伴计划	只读
		应用于此单位的工作负载的客户计划	只读
		单位计划	完整访问

重要事项
计划的所有者是在其中创建计划的租户。因此，如果合作伙伴管理员在客户租户级别上创建了计划，则客户租户就是该计划的所有者。

脚本计划的兼容性问题

在某些情况下，对工作负载应用脚本计划可能会导致出现兼容性问题。您可能会发现以下兼容性问题：

- 操作系统不兼容 - 当工作负载的操作系统不受支持时，会出现此问题。
- 代理程序不受支持 - 当工作负载上的保护代理程序版本已过时且不支持网络安全脚本功能时，会出现此问题。
- 配额不足 - 当租户中的服务配额不足以指派给选定工作负载时，会出现此问题。

如果脚本计划应用于多达 150 个单独选定的工作负载，则系统会提示您先解决现有冲突，然后再保存计划。要解决冲突，请消除冲突的根本原因或从计划中删除受影响的工作负载。有关详细信息，请参阅 "解决脚本计划的兼容性问题"(第 351 页)。如果在未解决冲突的情况下保存计划，则会为不兼容的工作负载自动禁用该计划，并显示警报。

如果脚本计划应用于 150 多个工作负载或设备组，则会保存它，然后检查兼容性。将针对不兼容的工作负载自动禁用该计划，并显示警报。

解决脚本计划的兼容性问题

根据兼容性问题的原因，可以在创建新脚本计划的过程中执行不同的操作来解决兼容性问题。

注意
通过从计划中删除工作负载来解决兼容性问题时，无法删除属于设备组的工作负载。

解决兼容性问题

1. 单击**查看问题**。
2. [解决操作系统不兼容的兼容性问题]
   a. 在**不兼容操作系统**选项卡上，选择要删除的工作负载。
   b. 单击**从计划中删除工作负载**。
   c. 单击**删除**，然后单击**关闭**。
3. [通过从计划中删除工作负载来解决代理程序不受支持的兼容性问题]
   a. 在**不支持的代理程序**选项卡上，选择要删除的工作负载。
   b. 单击**从计划中删除工作负载**。
   c. 单击**删除**，然后单击**关闭**。
4. [通过更新代理程序版本来解决代理程序不受支持的兼容性问题] 单击**转到代理程序列表**。

   注意
   此选项仅适用于客户管理员。

5. [通过从计划中删除工作负载来解决配额不足的兼容性问题]
   a. 在**配额不足**选项卡上，选择要删除的工作负载。
   b. 单击**从计划中删除工作负载**。
   c. 单击**删除**，然后单击**关闭**。
6. [通过增加租户的配额来解决配额不足的兼容性问题]

   注意
   此选项仅适用于合作伙伴管理员。

   a. 在**配额不足**选项卡上，单击**转到管理门户**。
   b. 增加客户的服务配额。

脚本快速运行

可以立即运行脚本，而无需将其包含在脚本计划中。无法对超过 150 个工作负载、离线工作负载或设备组使用此操作。

必须为目标工作负载指派支持“脚本快速运行”功能的服务配额，并且必须为其租户启用 Advanced Management 包。如果它在租户中可用，将自动指派合适的服务配额。

注意
只能从**脚本存储库** > **我的脚本**使用您批准的脚本。仅具有**"网络安全管理员"**角色的管理员才能使用处于正在**测试**状态下的脚本。有关角色的详细信息，请参阅 "用户角色和网络安全脚本权限"(第 334 页)。

可以通过以下方式启动"快速运行":

- 从**设备**选项卡
  选择一个或多个工作负载，然后选择要在其上运行的脚本。
- 从**管理** > **脚本存储库**选项卡
  选择一个脚本，然后选择一个或多个目标工作负载。

从"设备"选项卡运行脚本

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 选择要在其上运行脚本的工作负载，然后单击**保护**。
3. 单击**脚本快速运行**。
4. 单击**选择脚本**、选择要使用的脚本，然后单击**完成**。
5. 选择其下的脚本将在目标工作负载上运行的帐户。可使用以下选项:
   - 系统帐户(在 macOS 中，这是 root 帐户)
   - 当前登录的帐户
6. 指定脚本可以在目标工作负载上运行的时长。
   如果脚本无法在设置的时间范围内完成运行，"网络安全脚本"操作会失败。
   可以使用 1 到 1440 分钟之间的值。
7. [仅适用于 PowerShell 脚本] 配置 PowerShell 执行策略。
   有关此策略的更多信息，请参阅 Microsoft 文档。
8. 单击**立即运行**。

从"脚本存储库"选项卡运行脚本

1. 在 Cyber Protect 中控台中，转到**管理** > **脚本存储库**。
2. 选择要运行的脚本，然后单击**脚本快速运行**。
3. 单击**添加工作负载**以选择目标工作负载，然后单击**添加**。
4. 单击**选择脚本**、选择要使用的脚本，然后单击**完成**。
5. 选择其下的脚本将在目标工作负载上运行的帐户。可使用以下选项:
   - 系统帐户(在 macOS 中，这是 root 帐户)
   - 当前登录的帐户
6. 指定脚本可以在目标工作负载上运行的时长。
   如果脚本无法在设置的时间范围内完成运行，"网络安全脚本"操作会失败。
   可以使用 1 到 1440 分钟之间的值。
7. [仅适用于 PowerShell 脚本] 配置 PowerShell 执行策略。
   有关此策略的更多信息，请参阅 Microsoft 文档。
8. 单击**立即运行**。

管理工作负载和文件的备份和恢复

备份模块允许将物理机、虚拟机、文件和数据库备份和恢复至本地或云存储。

备份

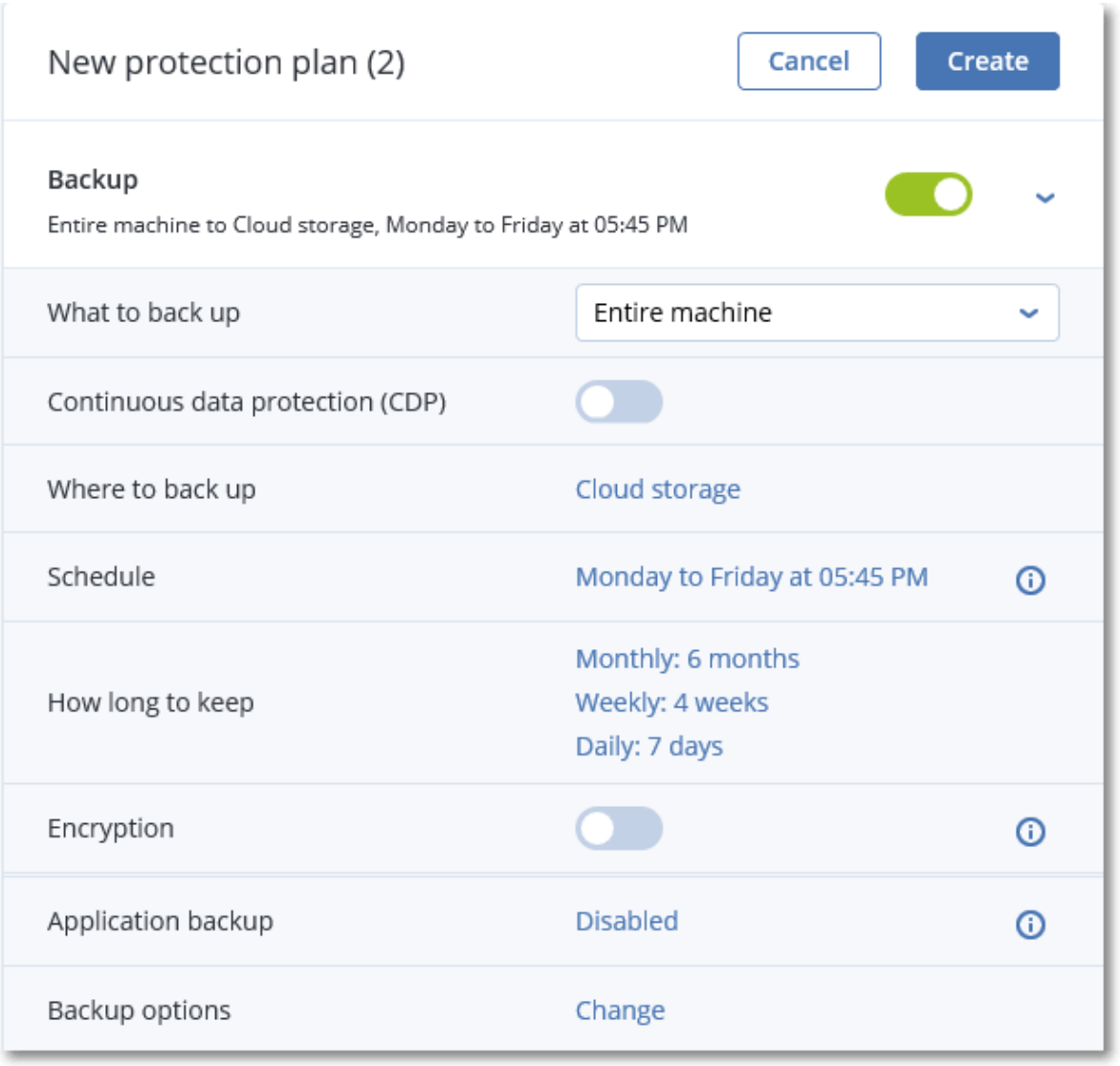
启用了备份模块的保护计划是一组规则，这些规则指定如何在给定计算机上保护给定数据。

保护计划可在其创建时或之后应用于多台计算机。

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**。

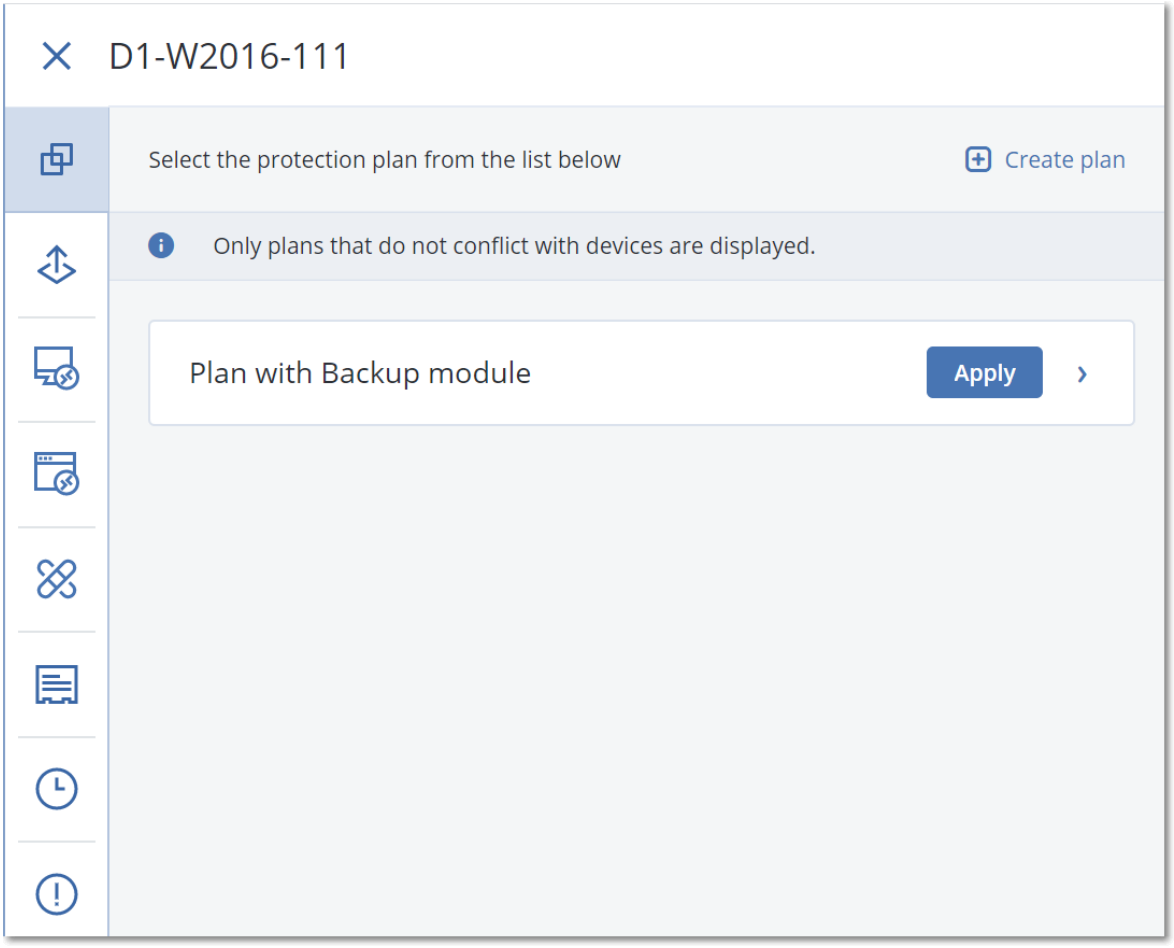
   将显示应用于计算机的保护计划。如果计算机尚未指派有任何计划，将看到可以应用的默认保护计划。可以根据需要调整设置并应用此计划，也可以创建新计划。
3. 要创建新计划，请单击**创建计划**。启用**备份**模块，然后展开设置。



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设置。
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**。

备份速查表

下表总结了最常见的备份参数。

备份内容	备份项目选择方法	备份位置	预定备份方案	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 NFS* 安全区**	始终增量备份(单个文件) 始终完整 每周完整，每日增量 每月完整备份，每周差异备份，每天增量备份(GFS) 自定义 (F-D-I)	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*** 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 NFS*		
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 NFS* 安全区**	始终增量备份(单个文件) 始终完整 每周完整，每日增量 每月完整备份，每周差异备份，每天增量备份(GFS) 自定义 (F-D-I)	
ESXi 配置	直接选择	本地文件夹 网络文件夹 NFS*		
网站(文件和 MySQL 数据库)	直接选择	云	—	
系统状态	直接选择	云 本地文件夹	始终完整 每周完整，每日增量	

备份内容	备份项目选择方法	备份位置	预定备份方案	保留时间
		网络文件夹	自定义 (F-I) 始终增量备份(单个文件) - 仅适用于 SQL 数据库	

备份内容		备份项目选择方法	备份位置	预定备份方案	保留时间
SQL 数据库		直接选择			
Exchange 数据库		直接选择			
Microsoft 365	邮箱 (适用于 Microsoft 365 的本地代理程序)	直接选择	云 本地文件夹 网络文件夹	始终增量备份(单个文件)	
	邮箱 (适用于 Microsoft 365 的云代理程序)	直接选择	云	每天最多 6 次备份	
	公用文件夹	直接选择			
	Teams	直接选择			
	OneDrive 文件	直接选择 策略规则			
	SharePoint Online 数据	直接选择 策略规则			
Google Workspace	Gmail 邮箱	直接选择	云	每天最多 6 次备份	
	Google Drive 文件	直接选择 策略规则			
	Shared Drive 文件	直接选择			

备份内容		备份项目 选择方法	备份位置	预定 备份方案	保留时间
		策略规则			

* 备份至 NFS 共享在 Windows 中不可用。

** 无法在 Mac 上创建安全区。

*** **按备份的总大小**保留规则在采用**始终增量备份(单个文件)**备份方案时或在备份到云存储时不可用。

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。有关磁盘备份的详细信息，请参阅 "选择磁盘或卷"(第 358 页)。

限制

- 对于已锁定的加密 APFS 卷，磁盘级别备份不受支持。在整个计算机的备份期间，将跳过此类卷。
- 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。在设备上不可用的文件将在备份集中有无效的内容。

选择磁盘或卷

磁盘级备份以打包形式包含磁盘或卷的副本。在磁盘级别备份中，可以恢复磁盘、卷、文件夹和文件。

可以为保护计划中的每个工作负载选择要备份的磁盘或卷(直接选择)，也可以为多个工作负载配置策略规则。此外，通过配置文件过滤器，可以从备份中排除特定文件，也可以仅将特定文件包括在备份中。有关详细信息，请参阅 "文件过滤器(包含/排除)"(第 409 页)。

选择磁盘或卷

直接选择

直接选择仅适用于物理机。

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个工作负载，请选中要备份的磁盘或卷旁边的复选框。
5. 单击**完成**。

按策略规则

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。
   有关可用策略规则的详细信息，请参阅 "磁盘和卷的策略规则"(第 360 页)。
   策略规则将应用于保护计划中包括的所有工作负载。
   如果指定的任何一个规则都无法应用于工作负载，则该工作负载的备份会失败。
5. 单击**完成**。

限制

- 对于已锁定的加密 APFS 卷，磁盘级别备份不受支持。在整个计算机的备份期间，将跳过此类卷。
- 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。在设备上不可用的文件将在备份集中有无效的内容。
- 可以将通过 iSCSI 协议连接的磁盘备份到物理机。但是，如果使用适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序备份通过 iSCSI 连接的磁盘，则会受限制。有关详细信息，请参阅 "限制"(第 32 页)。

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。其路径可在注册表值 **VSS Default Provider** 中确定，其可在注册表项 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup** 中找到。这意味着在从 Windows Vista 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。

磁盘和卷的策略规则

当选择要备份的磁盘或卷时，可以根据受保护工作负载的操作系统使用以下策略规则。

Windows

- `[All Volumes]` 选择计算机上的所有卷。
- 驱动器号(例如，`C:\`)选择带有指定驱动器号的卷。
- `[Fixed Volumes (physical machines)]` 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。
- `[BOOT+SYSTEM]` 选择系统和启动卷。这是可用于恢复操作系统的最小组合。
- `[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。

Linux

- `[All Volumes]` 选择计算机上的所有已加载卷。
- `/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，请指定以下命令：

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

macOS

- [All Volumes] 选择计算机上的所有已加载卷。
- [Disk 1] 选择计算机的第一个磁盘，包括该磁盘上的所有卷。要选择另一个磁盘，请指定相应编号。

选择文件或文件夹

使用文件级备份，只能保护特定数据（例如，当前项目中的文件）。文件级备份小于磁盘级别备份，可以节省存储空间。

重要事项
无法通过文件级备份恢复操作系统。

可以为保护计划中的每个工作负载选择要备份的文件和文件夹（直接选择），也可以为多个工作负载配置策略规则。此外，通过配置过滤器，可以从备份中排除特定文件，也可以仅将特定文件包括在备份中。有关详细信息，请参阅 "文件过滤器（包含/排除）"（第 409 页）。

选择文件或文件夹

直接选择

1. 在**备份内容**中，选择**文件/文件夹**。
2. 在**要备份的项目**中，单击**指定**。
3. 在**选择要备份的项目**中，选择**直接**。
4. 为保护计划中的每个工作负载指定要备份的文件或文件夹。
   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**。
      必须能够从选定计算机访问网络文件夹。
      当选择**网络文件夹**作为源时，可以备份来自网络连接存储 (NAS)（如 NetApp 设备）的数据。支持所有供应商的 NAS 设备。
   c. 在文件夹树中，导航到所需的文件或文件夹。
      或者，指定它们的路径，然后单击箭头按钮。
   d. [对于共享文件夹] 出现提示时，指定共享文件夹的访问凭据。
      不支持使用匿名访问来备份文件夹。
   e. 选择所需的文件和文件夹。
   f. 单击**完成**。

按策略规则

1. 在**备份内容**中，选择**文件/文件夹**。
2. 在**要备份的项目**中，单击**指定**。
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。

   有关可用策略规则的详细信息，请参阅 "文件和文件夹的策略规则"(第 362 页)。

   策略规则将应用于保护计划中包括的所有工作负载。

   如果指定的任何一个规则都无法应用于工作负载，则该工作负载的备份会失败。
5. 单击**完成**。

限制

- 当备份装有代理程序的物理机或虚拟机(基于代理程序的备份)时，可以选择文件和文件夹。文件级备份不适用于在无代理程序模式下备份的虚拟机。有关这些类型的备份之间差异的详细信息，请参阅 "基于代理程序备份和无代理程序备份"(第 56 页)。
- 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。在设备上不可用的文件将在备份集中有无效的内容。
- 可以将位于通过 iSCSI 协议连接的磁盘上的文件和文件夹备份到物理机。如果使用适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序备份通过 iSCSI 连接的磁盘上的数据，则会受一些限制。

文件和文件夹的策略规则

当选择要备份的文件或文件夹时，可以根据受保护工作负载的操作系统使用以下策略规则。

Windows

- 文件或文件夹的完整路径。例如，`D:\Work\Text.doc` 或 `C:\Windows`。
- 预定义规则：
  - `[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。例如，`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。例如，`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` 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，要选择“Program Files”文件夹中的“Java”文件夹，请指定：`%PROGRAMFILES%\Java`。

Linux

- 文件或目录的完整路径。
  例如，要备份 /home/usr/docs 中已加载卷 /dev/hda3 中的 file.txt 文件，请指定 /dev/hda3/file.txt 或 /home/usr/docs/file.txt。
- 预定义规则：
  - [All Profiles Folder] 选择 /home。默认情况下，所有用户配置文件都存储在此文件夹中。
  - /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。

macOS

- 文件或目录的完整路径。
  例如：
  - 要在用户桌面上备份 file.txt，请指定 /Users/<用户名>/Desktop/file.txt。
  - 要备份用户的 Desktop、Documents 和 Downloads 文件夹，请指定 /Users/<用户名>/Desktop、/Users/<用户名>/Documents 和 /Users/<用户名>/Downloads。
  - 要备份在此计算机上拥有帐户的所有用户的主文件夹，请指定 /Users。
  - 要备份安装有应用程序的文件夹，请指定 /Applications。
- 预定义规则
  - [All Profiles Folder] 选择 /Users。默认情况下，所有用户配置文件都存储在此文件夹中。

选择系统状态

注意
系统状态备份适用于运行 Windows 7 或更高版本并安装有适用于 Windows 的代理程序的计算机。系统状态备份不适用于以虚拟机监控程序级别备份的虚拟机(无代理程序备份)。

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。
- 您必须知道 ESXi 主机上的"根"帐户的密码。

限制

- 运行 VMware ESXi 7.0 及更高版本的主机不支持 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**保护**。
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)

持续数据保护 (CDP) 是 Advanced Backup 包的一部分。它会在该数据发生更改后立即备份关键数据，从而确保在两个预定备份之间系统出现故障时不会丢失任何所做更改。可以为以下数据配置连续数据保护：

- 特定位置的文件或文件夹
- 特定应用程序修改的文件

仅 NTFS 文件系统和以下操作系统支持连续数据保护：

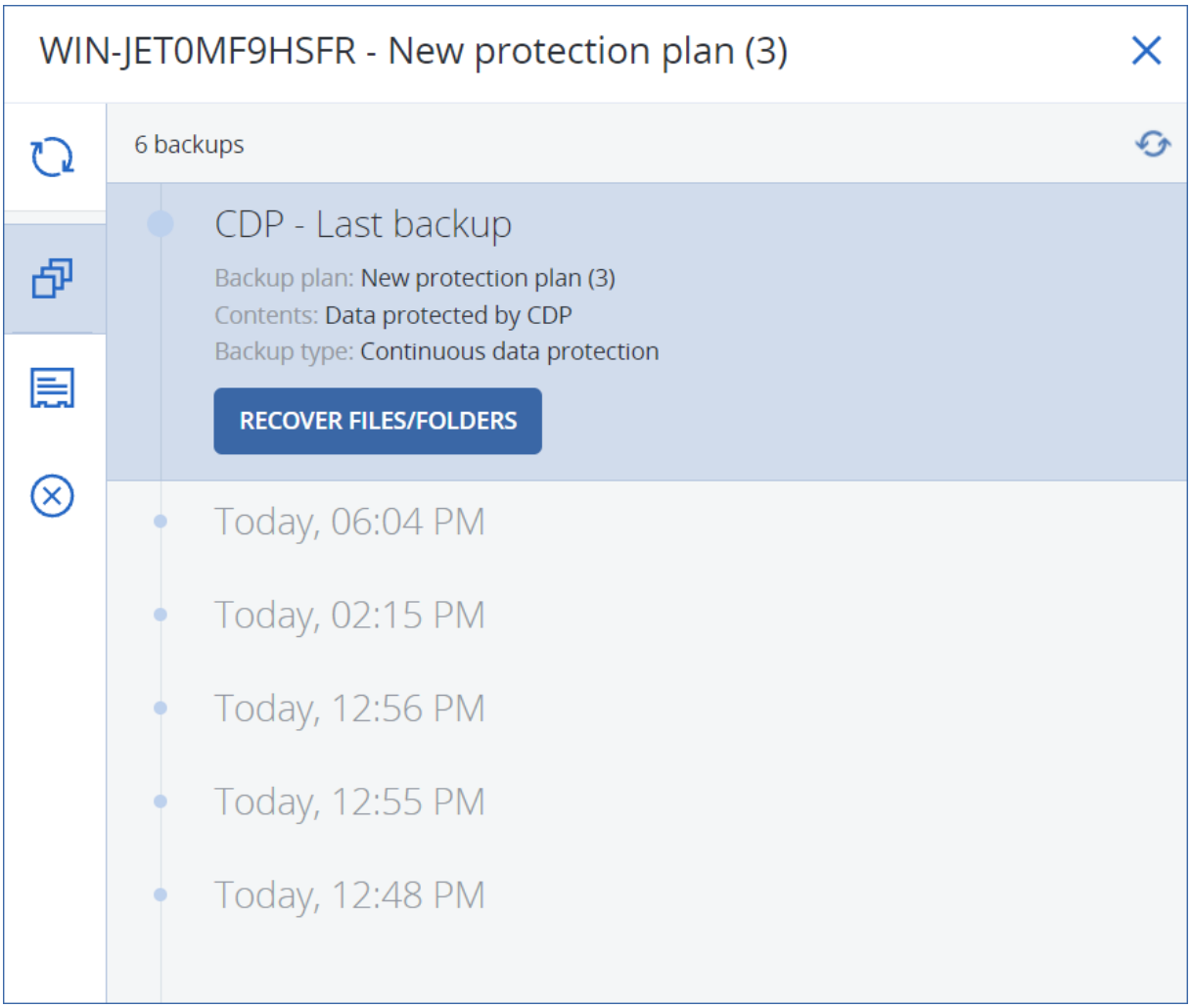
- 桌面：Windows 7 及更高版本
- 服务器：Windows Server 2008 R2 及更高版本

仅支持本地文件夹。无法为连续数据保护选择网络文件夹。

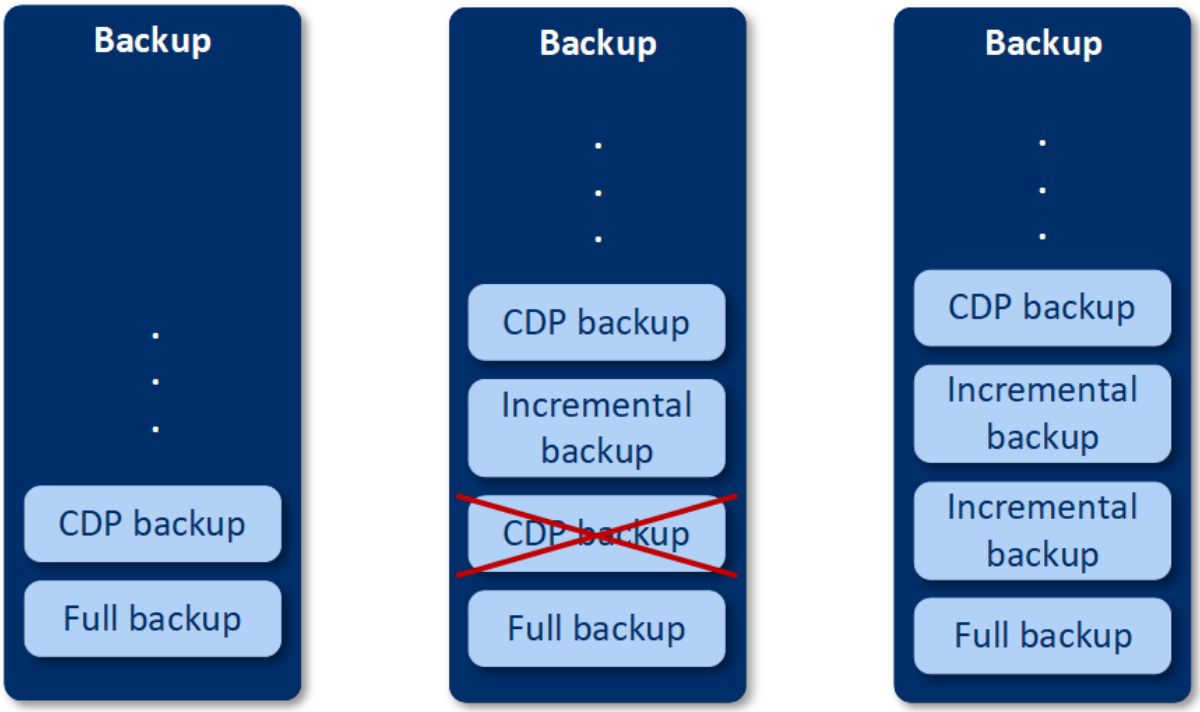
连续数据保护与**应用程序备份**选项不兼容。

工作方式

连续数据保护跟踪的文件和文件夹中发生的更改会立即保存到特殊的 CDP 备份中。一个备份集中只有一个 CDP 备份，并且该 CDP 备份始终是最新备份。



当预定的定期备份开始时，连续数据保护将暂停，因为最新数据将包含在该预定的备份中。在预定备份完成后，将恢复持续数据保护、删除旧的 CDP 备份，并创建一个新的 CDP 备份。因此，CDP 备份始终在备份集中保留最新备份，并仅存储被跟踪文件或文件夹的最新状态。



如果您的计算机在定期备份期间发生崩溃，则连续数据保护会在计算机重新启动后自动恢复，并在上次成功的预定备份基础上创建一个 CDP 备份。

连续数据保护要求在 CDP 备份之前至少创建一个定期备份。这就是出现以下情况的原因：当首次使用连续数据保护运行保护计划时，将创建一个完整备份，并在其基础上立即添加一个 CDP 备份。如果为现有保护计划启用**连续数据保护**选项，则 CDP 备份将添加到现有备份集中。

注意
如果为您启用了 Advanced Backup 功能并且您没有为选定的计算机使用其他 Advanced Backup 功能，则默认情况下会为从**设备**选项卡创建的保护计划启用持续数据保护。如果已为选定计算机制定了使用持续数据保护的计划，则默认情况下不会在新创建的计划中为该计算机启用持续数据保护。
默认情况下，不会为针对设备组创建的计划启用持续数据保护。

支持的数据源

可以使用以下数据源配置连续数据保护：

- 整台计算机
- 磁盘/卷
- 文件/文件夹

在保护计划的**备份内容**部分中选择数据源后，在**要连续保护的项目**部分中，选择连续数据保护的文件、文件夹或应用程序。有关如何配置连续数据保护的详细信息，请参阅 "配置 CDP 备份"(第 367 页)。

支持的目标

可以使用以下目标配置连续数据保护：

- 本地文件夹
- 网络文件夹
- 云存储
- 安克诺斯 Cyber Infrastructure
- 由脚本定义的位置

注意
只能通过脚本定义上面列出的位置。

配置 CDP 备份

可以在保护计划的**备份**模块中配置连续数据保护。有关如何创建保护计划的详细信息，请参阅 "创建保护计划"(第 192 页)。

配置连续数据保护设置

1. 在保护计划的**备份**模块中，启用**连续数据保护(CDP)**开关。
   该开关仅适用于以下数据源：
   - 整台计算机
   - 磁盘/卷
   - 文件/文件夹
2. 在**要连续保护的项目**中，为**应用程序**或**文件/文件夹**(或两者) 配置连续数据保护。
   - 单击**应用程序**，可为特定应用程序修改的文件配置 CDP 备份。
     可以从预定义的类别中选择应用程序，也可以通过指定应用程序可执行文件的路径来添加其他应用程序，例如：
     - `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`
     - `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`
   - 单击**文件/文件夹**，可为特定位置中的文件配置 CDP 备份。
     可以使用选择规则或直接选择文件和文件夹，来定义这些位置。
     - [对于所有计算机] 要创建选择规则，请使用文本框。
       可以使用文件的完整路径，也可以使用带有通配符(* 和 ?) 的路径。星号匹配零个或多个字符。问号匹配单个字符。

       重要事项
       要为文件夹创建 CDP 备份，必须使用星号通配符指定其内容：
       正确路径：`D:\Data\*`
       不正确的路径：`D:\Data\`

- [对于联机计算机]直接选择文件和文件夹:
  - 在**要浏览的计算机**中,选择文件或文件夹所在的计算机。
  - 单击**选择文件和文件夹**,以浏览选定的计算机。

    直接选择会创建一个选择规则。如果将保护计划应用于多台计算机,而某一选择规则对某台计算机无效,将会在这一台计算机上跳过该选择规则。

3. 在保护计划窗格中,单击**创建**。

结果,将在预定备份之间连续备份指定的数据。

选择目标

单击**备份位置**,然后选择以下各项之一:

- **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。
- **公有云**

  此选项作为 Advanced Backup 包的一部分提供。

  它使您能够配置对公有云兼容的存储的直接备份,无需部署其他组件(例如 Microsoft Azure 或其他虚拟机作为网关)。根据需要选择并连接到相关公有云。

  有关详细信息,请参阅 "将工作负载备份到公有云"(第 480 页)。
- **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安装有适用于 Linux 的代理程序的 Linux 服务器上。

  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。

  注意

  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"(第 369 页)。

高级存储选项

注意
此功能仅在 Cyber Protection 服务的高级版中提供。

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);
  ```

  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。
- 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");
  ```

  结果，本计算机的备份将保存在同一台计算机上的 C:\Backup 文件夹中。

  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 Cyber Protect 中控台中显示为不同的位置。此外，驱动器号也使用大写。

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

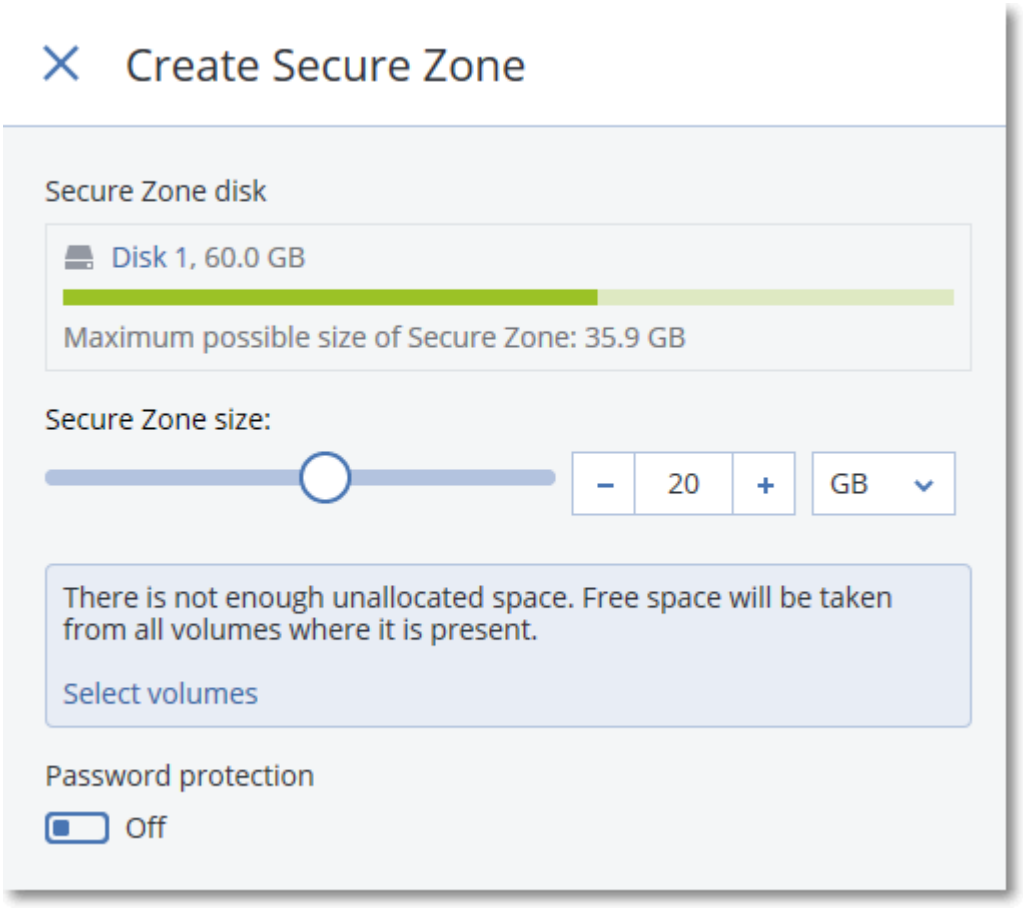
- 安全区 始终在硬盘的末尾区域进行创建。
- 如果在磁盘末尾没有未分配的空间或未分配空间不足，但是在卷之间有未分配的空间，则将会移动卷以便在磁盘的末尾区域增加更多的未分配空间。
- 当收集了所有的未分配空间，但空间仍然不足时，软件将使用您选择的卷上的可用空间，成比例降低卷的大小。
- 但是，在卷上应该有可用空间，这样操作系统和应用程序才能运行；例如创建临时文件。如果可用空间等于或低于卷总大小的 25%，软件将不会减少卷的大小。仅在磁盘上所有卷的可用空间都为 25% 或更低时，软件才会继续成比例减少卷大小。

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。

备份预定

可以将备份配置为在特定时间、以特定间隔或基于特定事件自动运行。

非云到云资源的预定备份会根据装有保护代理程序的工作负载的时区设置运行。例如，如果将相同的保护计划应用于时区设置不同的工作负载，则备份会根据每个工作负载的本地时区开始。

预定备份包括以下操作：

- 选择备份方案
- 配置时间或选择触发备份的事件
- 配置可选设置和开始条件

备份方案

备份方案是保护计划预定的一部分，该保护计划预定定义创建哪类备份（完整、差异或增量）以及何时创建。可以选择预定义的备份方案之一，也可以创建自定义方案。

可用的备份方案和类型取决于备份位置和源。例如，当备份 SQL 数据、Exchange 数据或系统状态时，差异备份不可用。磁带设备不支持**始终增量(单个文件)**方案。

备份方案	描述	可配置的元素
始终增量备份（单个文件）	第一个备份是完整备份，可能非常耗时。后续备份是增量备份，速度明显更快。 这些备份使用单文件备份格式[1]*。 默认情况下，从周一到周五每天执行备份。 由于增量备份的速度快且所需的网络流量较少，因此建议您在云存储中存储备份时使用此方案。	• 预定类型：每月、每周、每日、每小时 • 备份触发器：时间或事件 • 开始时间 • 开始条件 • 其他选项
始终完整备份	备份集中的所有备份都是完整备份。 默认情况下，从周一到周五每天执行备份。	• 预定类型：每月、每周、每日、每小时 • 备份触发器：时间或事件 • 开始时间 • 开始条件 • 其他选项
每周完整，每日增量	完整备份每周创建一次，其他备份是增量备份。 第一个备份是完整备份，该周内的其他备份是增量备份，然后循环重复。	• 备份触发器：时间或事件 • 开始时间 • 开始条件

[1]一种备份格式，初始完整和后续增量备份使用该格式保存到单个 .tibx 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时，单文件备份格式不可用。

备份方案	描述	可配置的元素
	要选择星期几创建完整备份，请在保护计划中，单击齿轮图标，然后转到**备份选项** > **每周备份**。 默认情况下，从周一到周五每天执行备份。	• 其他选项
每月完整备份，每周差异备份，每天增量备份 (GFS)	默认情况下，从星期一到星期五每日执行增量备份。每个星期六执行差异备份。每月的第一天执行完整备份。 **注意** 这是一个预定义的自定义方案。在保护计划中，它显示为**自定义**。	• 按备份类型更改现有预定： ◦ 预定类型：每月、每周、每日、每小时 ◦ 备份触发器：时间或事件 ◦ 开始时间 ◦ 开始条件 ◦ 其他选项 • 按备份类型添加新预定
自定义	必须选择备份类型（完整、差异和增量），然后为每种类型配置单独的预定*。	• 按备份类型更改现有预定： ◦ 预定类型：每月、每周、每日、每小时 ◦ 备份触发器：时间或事件 ◦ 开始时间 ◦ 开始条件 ◦ 其他选项 • 按备份类型添加新预定

* 创建保护计划后，无法在**始终增量(单个文件)**和其他备份方案之间切换，反之亦然。**始终增量(单个文件)**是单文件格式方案，其他方案是多文件格式。如果要在格式之间切换，请创建新的保护计划。

备份类型

以下备份类型可用：

- 完整 - 完整备份包含所有源数据。此备份是自给自足型备份。要恢复数据，无需访问任何其他备份。

  注意
  任何保护计划创建的第一个备份都是完整备份。

- 增量 - 增量备份存储自上次备份以来对数据所做的更改，而不管上次备份是完整备份、差异备份还是增量备份。要恢复数据，需要增量备份所依赖的整个备份链，用于恢复到初始完整备份。

- 差异 - 差异备份存储自上次完整备份以来对数据所做的更改。要恢复数据，需要差异备份和该差异备份所依赖的相应完整备份。

按预定运行备份

要在特定时间或基于特定事件自动运行备份，请在保护计划中启用预定。

启用预定

1. 在保护计划中，展开**备份**模块。
2. 单击**预定**。
3. 启用预定开关。
4. 选择备份方案。
5. 根据需要配置预定，然后单击**完成**。
   有关可用预定选项的详细信息，请参阅 "按时间预定"(第 374 页) 和 "按事件预定"(第 376 页)。
6. [可选]配置开始条件或其他预定选项。
7. 保存该保护计划。

结果，备份操作在每次满足预定条件时开始。

禁用预定

1. 在保护计划中，展开**备份**模块。
2. 单击**预定**。
3. 禁用预定开关。
4. 保存该保护计划。

因此，备份仅在手动启动时才会运行。

注意
如果预定处于禁用状态，则不会自动应用保留规则。要应用保留规则，请手动运行备份。

按时间预定

下表汇总了基于时间的预定选项。这些选项的可用性取决于备份方案。有关详细信息，请参阅 "备份方案"(第 372 页)。

选项	描述	示例
每月	选择月份、一个月几天或一周几天，然后选择备份开始时间。	在 1 月 1 日和 2 月 3 日上午 12:00 运行备份。 在每月的第一天上午 10:00 运行备份。 在 3 月 1 日、3 月 5 日、4 月 1 日和 4 月 5 日上午 09:00 运行备份。 在每月的第二个和第三个星期五上午 11:00 运行备份。

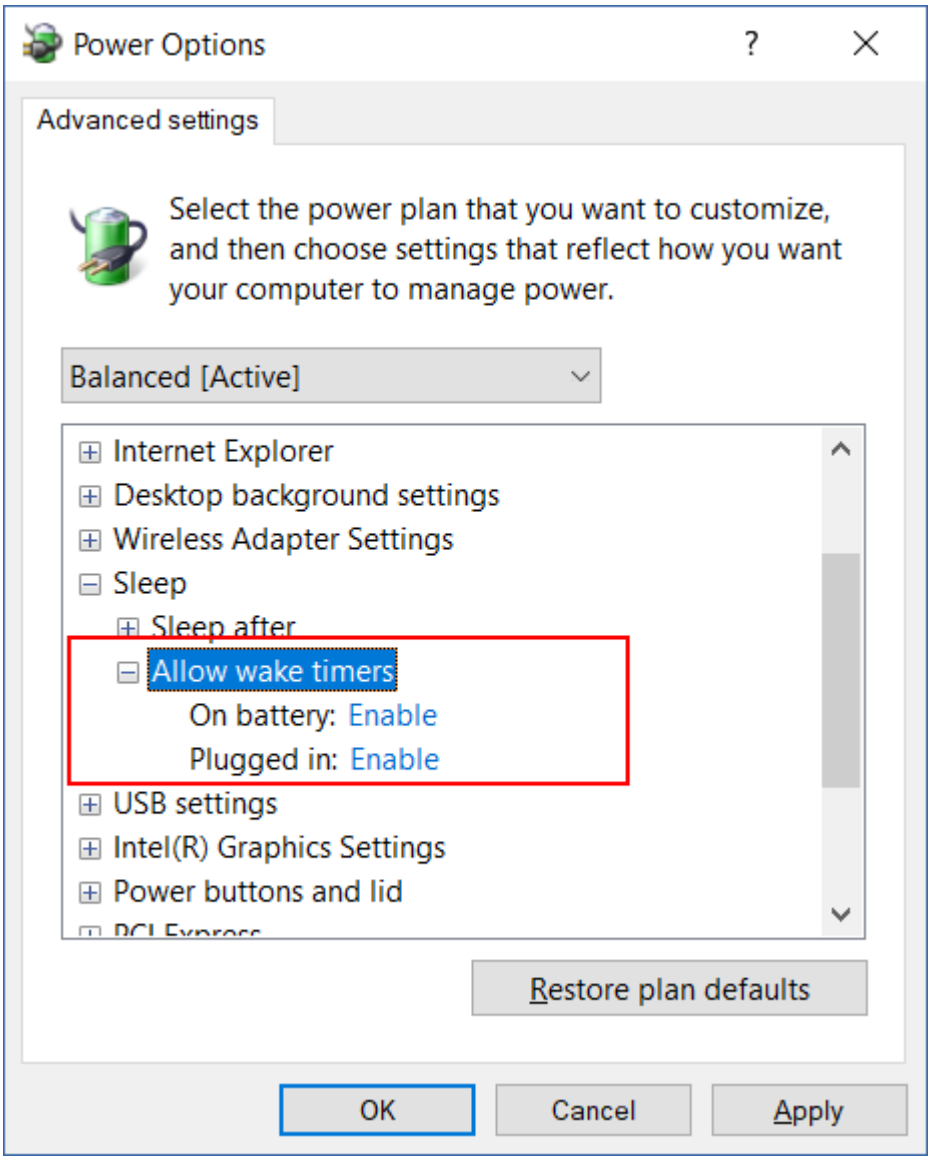
选项	描述	示例
		在当月的最后一个星期三晚上 10:30 运行备份。
每周	选择一周几天，然后选择备份开始时间。	在星期一到星期五上午 10:00 运行备份。 在星期一晚上 11:00 运行备份。 在星期二和星期六上午 08:00 运行备份。
每日	选择天数(仅限每天或工作日)，然后选择备份开始时间。	在每天上午 11:45 运行备份。 在星期一到星期五晚上 09:30 运行备份。
每小时	选择一周几天，然后选择两次连续备份之间的时间间隔以及备份运行的时间范围。 当以分钟为单位配置间隔时，可以选择 10 到 60 分钟之间的建议间隔，也可以指定自定义间隔(例如，45 或 75 分钟)。	在星期一到星期五上午 08:00 到晚上 06:00 之间，每小时运行一次备份。 在星期六和星期天凌晨 01:00 到晚上 06:00 之间，每 3 小时运行一次备份。

其他选项

当按时间预定备份时，可以使用以下其他预定选项。

要访问其他预定选项，请在**预定**窗格中，单击**显示更多**。

- **如果计算机关闭，则在计算机启动时运行遗漏的任务**
  默认设置：已禁用。
- **在备份期间防止进入睡眠或休眠模式**
  此选项仅适用于运行 Windows 的计算机。
  默认设置：已启用。
- **从睡眠或休眠模式唤醒以启动预定备份**
  此选项仅适用于运行 Windows 且在其电源计划已启用**允许唤醒计时器**选项的计算机。



此选项不使用“局域网唤醒”功能，也不适用于电源关闭的计算机。

默认设置：已禁用。

按事件预定

要配置基于特定事件运行的备份，请选择以下选项之一。

选项	描述	示例
自上次备份后的时间	备份会在上次成功备份后的指定时间段后开始。 **注意** 此选项取决于上次备份的完成情况。如果备份失败，下一次备份将不会自动开始。在这种情况下，必须手动运行备份并确保该备份成功完成，才能重置预定。	在上次成功备份一天后运行备份。 在上次成功备份四小时后运行备份。

选项	描述	示例
用户登录系统时	备份会在用户登录到计算机时开始。 可以为任何登录或特定用户的登录配置此选项。 **注意** 使用临时用户配置文件登录不会启动备份。	当用户 John Doe 登录时运行备份。
用户注销系统时	备份会在用户注销计算机时开始。 可以为任何注销或特定用户的注销配置此选项。 **注意** 使用临时用户配置文件注销将不会启动备份。 关闭计算机不会启动备份。	当每个用户注销时运行备份。
系统启动时	备份会在受保护计算机启动时运行。	当用户启动计算机时运行备份。
系统关闭时	备份会在受保护计算机关闭时运行。	当用户关闭计算机时运行备份。
发生 Windows 事件日志事件时	备份会在发生指定的 Windows 事件时运行。	当类型为错误且源为磁盘的事件 7 记录在 Windows 系统日志中时运行备份。

这些选项的可用性取决于受保护工作负载的备份源和操作系统。下表汇总了 Windows、Linux 和 macOS 的可用选项。

事件	备份源(要备份的内容)					
	整个计算机、磁盘/卷或文件/文件夹(物理机)	**整个计算机或磁盘/卷(虚拟机)**	**ESXi 配置**	**Microsoft 365 邮箱**	**Exchange 数据库和邮箱**	**SQL 数据库**
自上次备份后的时间	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
用户登录系统时	Windows	N/A	N/A	N/A	N/A	N/A
用户注销系统时	Windows	N/A	N/A	N/A	N/A	N/A
系统启动时	Windows, Linux, macOS	N/A	N/A	N/A	N/A	N/A

事件	备份源(要备份的内容)					
	整个计算机、磁盘/卷或文件/文件夹(物理机)	整个计算机或磁盘/卷(虚拟机)	ESXi 配置	Microsoft 365 邮箱	Exchange 数据库和邮箱	SQL 数据库
系统关闭时	Windows	N/A	N/A	N/A	N/A	N/A
发生 Windows 事件日志事件时	Windows	N/A	N/A	Windows	Windows	Windows

发生 Windows 事件日志事件时

当特定事件记录在 Windows 事件日志(如应用程序日志、安全日志或系统日志)中时,可以自动运行备份。

注意

可以在 Windows 的**计算机管理** > **事件查看器**中,浏览事件并查看其属性。要打开"安全日志",您需要有管理员权限。

事件参数

下表汇总了在配置**发生 Windows 事件日志事件时**选项时必须指定的参数。

参数	描述
日志名称	日志的名称。 选择标准日志的名称(应用程序、安全性、系统),或指定其他日志名称。例如,Microsoft Office 会话。
事件源	事件源指出导致发生事件的程序或系统组件。例如,磁盘。 任何包含指定文本字符串的事件源都将触发预定的备份。此选项不区分大小写。例如,如果指定 `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	事件的类型:错误、警告、信息、审核成功或审核失败。
事件 ID	事件 ID 标识事件源中特定类型的事件。 例如,当 Windows 在磁盘上发现坏块时,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:硬盘出现坏块时的紧急备份

硬盘驱动器上的一个或多个坏块可能表示即将出现故障。这就是当检测到坏块时可能要创建备份的原因。

当 Windows 在磁盘上检测到坏块时,系统会将事件源为磁盘且事件编号为 7 的错误事件记录到系统日志中。在保护计划中,配置以下预定:

- 预定:发生 Windows 事件日志事件时
- 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
为了确保备份能够在出现坏块的情况下完成,请在**备份选项**中,转到**错误处理**,然后选中**忽略坏扇区**复选框。

开始条件

要使备份仅在满足特定条件时运行,请配置一个或多个开始条件。如果配置多个条件,则必须同时满足所有这些条件才能开始备份。可以指定备份将在其后运行的时间段,无论是否满足条件都会运行备份。有关此备份选项的详细信息,请参阅 "任务开始条件"(第 439 页)。

当手动启动备份时,开始条件不适用。

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。

开始条件	备份源(要备份的内容)					
	整个计算机、磁盘/卷或文件/文件夹(物理机)	**整个计算机或磁盘/卷(虚拟机)**	**ESXi 配置**	**Microsoft 365 邮箱**	**Exchange 数据库和邮箱**	**SQL 数据库**
用户空闲时	Windows	N/A	N/A	N/A	N/A	N/A
备份位置所在的主机可用	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
用户已注销	Windows	N/A	N/A	N/A	N/A	N/A
配合时间间隔时	Windows, Linux, macOS	Windows, Linux	N/A	N/A	N/A	N/A

开始条件	备份源(要备份的内容)					
	整个计算机、磁盘/卷或文件/文件夹(物理机)	整个计算机或磁盘/卷(虚拟机)	ESXi 配置	Microsoft 365 邮箱	Exchange 数据库和邮箱	SQL 数据库
节省电池电量	Windows	N/A	N/A	N/A	N/A	N/A
不在使用按流量计费的连接时启动	Windows	N/A	N/A	N/A	N/A	N/A
不在连接到以下 Wi-Fi 网络时启动	Windows	N/A	N/A	N/A	N/A	N/A
检查设备 IP 地址	Windows	N/A	N/A	N/A	N/A	N/A

用户空闲时

“用户空闲时”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

在每天晚上 09:00 运行备份，最好是在用户空闲时。如果用户在晚上 11:00 之前仍处于活动状态，则直接运行备份。

- 预定：**每日，每天运行一次**。开始时间：**晚上 09:00**。
- 条件：**用户空闲时**。
- 备份开始条件：**等待直至满足条件，务必在 2 小时后开始任务**。

结果：

- 如果用户在晚上 09:00 前处于空闲状态，则备份会在晚上 09:00 开始。
- 如果用户在晚上 09:00 到晚上 11:00 之间处于空闲状态，则备份会立即开始。
- 如果用户在晚上 11:00 仍处于活动状态，则备份会在晚上 11:00 开始。

备份位置所在的主机可用

“备份位置所在的主机可用”意味着托管备份位置的计算机可以通过网络使用。

此条件适用于网络文件夹、云存储和存储节点管理的位置。

此条件不涉及位置本身的可用性，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

在每个工作日晚上 09:00 运行对网络文件夹的备份。如果托管文件夹的计算机此时不可用（例如，由于维护原因），您要跳过备份，并等待在下一个工作日预定开始备份。

- 预定：**每日，星期一到星期五运行**。开始时间：**晚上 09:00**。
- 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：

- 如果主机在晚上 09:00 可用，备份会立即开始。
- 如果主机在晚上 09:00 不可用，备份会在下一个工作日开始（如果主机在当天的晚上 09:00 可用）。
- 如果主机在工作日晚上 09:00 一直不可用，备份永远不会开始。

用户已注销

使用此开始条件可推迟备份，直到所有用户都从 Windows 计算机注销。

示例

在每个星期五晚上 08:00 运行备份，最好是在所有用户都已注销时。如果其中一个用户在晚上 11:00 仍处于登录状态，则会直接运行备份。

- 预定：**每周**，星期五。开始时间：**晚上 08:00**。
- 条件：**用户已注销**。
- 备份开始条件：**等待直至满足条件，务必在 3 小时后开始备份**。

结果：

- 如果所有用户在晚上 08:00 都处于注销状态，则备份会在晚上 08:00 开始。
- 如果最后一位用户在晚上 08:00 到晚上 11:00 之间注销，则备份会立即开始。
- 如果仍有用户在晚上 11:00 处于登录状态，则备份会在晚上 11:00 开始。

配合时间间隔时

使用此开始条件，将备份开始限制为指定的时间间隔。

示例

一家公司将用户数据和服务器备份到同一网络附加存储上的不同位置。

工作日的工作时间为上午 08:00 到下午 05:00。用户数据应该在用户注销后就进行备份，但备份开始不应早于下午 04:30。

该公司的服务器每天晚上 11:00 进行备份。用户数据最好在晚上 11:00 之前进行备份，以便为服务器备份释放网络带宽。

备份用户数据所需的时间不超过一个小时，因此最新备份开始时间是晚上 10:00。如果用户在指定的时间间隔内仍处于登录状态，或在任何其他时间注销，则应该跳过备份用户数据。

- 事件：**用户注销系统时**。指定用户帐户：**任何用户**。
- 条件：**配合时间间隔时**，从**下午 04:30** 到**晚上 10:00**。
- 备份开始条件：**跳过预定备份**。

结果：

- 如果用户在下午 04:30 到晚上 10:00 之间注销，备份会立即开始。
- 如果用户在任何其他时间注销，则会跳过备份。

节省电池电量

如果计算机（例如，笔记本电脑或平板电脑）未连接到电源，使用此开始条件可防止备份。根据备份开始条件选项的值，跳过的备份也许会在计算机连接到电源后开始。

可使用以下选项：

- **不在使用电池时启动**
  仅当计算机连接到电源时，备份才会开始。
- **如果电池电量高于以下值，则在使用电池时启动**
  如果计算机连接到电源或者电池电量高于指定值，备份会开始。

示例

在每个工作日晚上 09:00 备份数据。如果计算机未连接到电源，则要跳过备份以节省电池电量，等待直至将计算机连接到电源。

- 预定：**每日，星期一到星期五运行**。开始时间：**晚上 09:00**。
- 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：

- 如果计算机在晚上 09:00 连接到电源，备份会立即开始。
- 如果计算机在晚上 09:00 通过电池供电运行，备份会在将计算机连接到电源后才开始。

不在使用按流量计费的连接时启动

如果计算机通过在 Windows 中设置为按流量计费的连接方式连接到 Internet，则使用此开始条件来阻止备份（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。

当启用**不在使用按流量计费的连接时启动**条件时，其他开始条件**不在连接到以下 Wi-Fi 网络时开始**会自动启用。这是用于阻止通过移动热点进行备份的额外措施。默认指定以下网络名称：android、phone、mobile 和 modem。

要从列表中删除这些名称，请单击 X 符号。要添加新名称，请在空字段中键入。

示例

在每个工作日晚上 09:00 备份数据。如果计算机通过使用按流量计费的连接方式连接到 Internet，您要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：**每日，星期一到星期五运行**。开始时间：**晚上 09:00**。
- 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：

- 晚上 09:00，如果计算机未通过按流量计费的连接方式连接到 Internet，备份会立即开始。
- 晚上 09:00，如果计算机通过按流量计费的连接方式连接到 Internet，备份会在下一个工作日开始。
- 如果计算机始终在工作日晚上 09:00 通过按流量计费的连接方式连接到 Internet，备份永远不会开始。

不在连接到以下 Wi-Fi 网络时启动

如果计算机连接到任何指定的无线网络（例如，如果要限制通过移动手机热点进行备份），请使用此开始条件来阻止备份（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)。限制会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，则当计算机连接到以下任何网络时，备份将不会开始：John's iPhone、phone_wifi 或 my_PHONE_wifi。

当启用**不在使用按流量计费的连接时启动**条件时，开始条件**不在连接到以下 Wi-Fi 时开始**会自动启用。默认指定以下网络名称：android、phone、mobile 和 modem。

要从列表中删除这些名称，请单击 X 符号。要添加新名称，请在空字段中键入。

示例

在每个工作日晚上 09:00 备份数据。如果计算机通过移动热点连接到 Internet，您要跳过备份，并等待在下一个工作日预定开始备份。

- 预定：**每日，星期一到星期五运行**。开始时间：**晚上 09:00**。
- 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：

- 如果计算机在晚上 09:00 未连接到指定网络，备份会立即开始。
- 如果计算机在晚上 09:00 连接到指定网络，备份会在下一个工作日开始。
- 如果计算机始终在工作日晚上 09:00 连接到指定网络，备份永远不会开始。

检查设备 IP 地址

如果任何计算机 IP 地址都在指定的 IP 地址范围之内或之外，则使用此开始条件来阻止备份（包括备份到本地磁盘）。因此，例如，在备份海外用户的计算机时，可以避免支付大额数据传输费用，也可以防止通过虚拟专用网络 (VPN) 连接进行备份。

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。

示例

在每个工作日晚上 09:00 备份数据。如果计算机通过使用 VPN 隧道连接到公司网络，您要跳过备份。

- 预定：**每日，星期一到星期五运行**。在**晚上 09:00** 开始。
- 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：

- 如果计算机 IP 地址在晚上 09:00 不在指定范围内，备份会立即开始。
- 如果计算机 IP 地址在晚上 09:00 在指定范围内，备份会在计算机获得非 VPN IP 地址时开始。
- 如果计算机 IP 地址始终在工作日晚上 09:00 在指定范围内，备份永远不会开始。

其他预定选项

可以将备份配置为仅在满足特定条件时运行、仅在指定时间段内运行或相较于预定延迟运行。

配置开始条件

1. 在保护计划中，展开**备份**模块。
2. 单击**预定**。
3. 在**预定**窗格中，单击**显示更多**。
4. 选中要包括的开始条件旁边的复选框，然后单击**完成**。

   有关可用开始条件及其配置方法的详细信息，请参阅 "开始条件"（第 379 页）。
5. 保存该保护计划。

配置时间范围

1. 在保护计划中，展开**备份**模块。
2. 单击**预定**。
3. 选中**在日期范围内运行计划**复选框。

4. 根据您的需要指定时间段，然后单击**完成**。
5. 保存该保护计划。

结果，备份将仅在指定的时间段内运行。

配置延迟

为了避免在将多个工作负载备份到网络位置时导致网络负载过重，请将略微随机延迟配置为备份选项。可以禁用延迟，也可以更改其设置。

1. 在保护计划中，展开**备份**模块。
2. 单击**备份选项**，然后选择**预定**。
   每个工作负载的延迟值是在零和指定的最大值之间随机选择的。默认情况下，最大值为 30 分钟。
   有关此备份选项的详细信息，请参阅 "预定"(第 438 页)
   每个工作负载的延迟值是在将保护计划应用于该工作负载时计算的，并在编辑最大延迟值之前保持不变。
3. 根据您的需要指定时间段，然后单击**完成**。
4. 保存该保护计划。

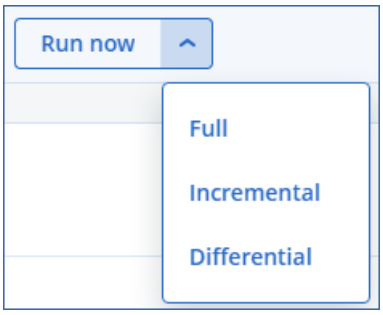
手动运行备份

可以手动运行预定备份和非预定备份。

手动运行备份

1. 在 Cyber Protect 中控台中，转到**设备**。
2. 选择要运行备份的工作负载，然后单击**保护**。
3. 选择要创建备份的保护计划。
   如果没有将保护计划应用于工作负载，请应用现有计划或创建一个新计划。
   有关如何创建保护计划的详细信息，请参阅 "创建保护计划"(第 192 页)。
4. [创建默认类型的备份] 在保护计划中，单击**立即运行**图标。

   或者，在保护计划中，展开**备份**模块，然后单击**立即运行**按钮。
5. [创建特定类型的备份] 在保护计划中，展开**备份**模块、单击**立即运行**按钮旁边的箭头，然后选择备份类型。



注意
对于仅使用一种备份方法(例如,**始终增量(单个文件)**或**始终完整**)的备份方案,无法选择类型。

结果,备份操作开始。可以在**设备**选项卡的**状态**列中,检查其进度和结果。

保留规则

要自动删除较旧备份,请在保护计划中配置备份保留规则。

可以根据以下任何备份属性制定保留规则:

- 编号(N)
- 时间
- 大小

可用保留规则及其选项取决于备份方案。这些规则还与代理程序、工作负载和云到云备份有关。有关详细信息,请参阅 "根据备份方案制定的保留规则"(第 387 页)。

根据保护计划的配置,保留规则将在备份之前或之后应用于档案。

通过在配置保留规则时选择**无限保留备份**选项,可以禁用对较旧备份的自动清理。这可能会导致存储使用量增加,必须手动删除不需要的旧备份。

重要提示

- 保留规则是保护计划的一部分。如果撤消或删除某个计划,则该计划中的保留规则将不再应用。有关如何删除不再需要的备份的详细信息,请参阅 "删除备份"(第 475 页)。
- 根据备份方案和备份格式,如果每个备份都存储为单独的文件,则无法删除其他增量备份或差异备份所依赖的备份。将根据应用于从属备份的保留规则删除此备份。此配置可能会导致存储使用量增加,因为推迟了某些备份的删除。此外,备份的备份期限、数量或大小可能会超出指定的值。有关如何更改此行为的详细信息,请参阅 "备份合并"(第 400 页)。
- 默认情况下,永远不会删除保护计划创建的最新备份。但是,如果将保留规则配置为在开始新的备份操作之前清除备份,并将要保留的备份数设置为零,则也会删除最新备份。

警告!
由于在创建新备份之前会删除现有备份,因此,如果将此保留规则应用于具有单个备份的备份集,且备份操作失败,则会无法恢复数据。

根据备份方案制定的保留规则

可用保留规则及其设置取决于在保护计划中使用的备份方案。有关备份方案的详细信息，请参阅 "备份方案"(第 372 页)。

下表汇总了可用保留规则及其设置。

备份方案	预定	可用保留规则和设置
始终增量备份(单个文件)	每月 每周 每日 每小时 事件触发的备份	按备份数量 按备份存留时间(每月、每周、每日和每小时备份的单独设置) 无限期地保留备份
始终完整备份	每月 每周 每日 每小时 事件触发的备份	按备份数量 按备份存留时间(每月、每周、每日和每小时备份的单独设置) 按备份的总大小 无限期地保留备份
每周完整，每日增量	每日 事件触发的备份	按备份数量 按备份存留时间(每周和每日备份的单独设置) 按备份的总大小 无限期地保留备份
每月完整备份，每周差异备份，每日增量备份	每月 每周 每日 每小时 事件触发的备份	按备份数量 按备份存留时间(完整备份、差异备份和增量备份的单独设置) 按备份的总大小 无限期地保留备份
自定义	每月 每周 每日 每小时 事件触发的备份	按备份数量 按备份存留时间(完整备份、差异备份和增量备份的单独设置) 按备份的总大小 无限期地保留备份

为什么有使用每小时方案的每月备份?

根据备份方案,可以为以下备份之一配置**按备份存留时间**选项:

- 每月、每周、每日和每小时备份。

  这些设置可用于所有非自定义备份方案,基于时间。所有这些备份(每月、每周、每日和每小时)都可用,即使将备份配置为每小时运行也是如此。查看下面的示例。

备份	描述
每月	每月备份是每个月的第一个备份。
每周	每周备份是在每周备份选项中指定的星期几的第一个备份。就保留规则而言,这一天被视为一周的开始。 如果每周备份也是本月的第一个备份,则每周备份视为每月备份。在这种情况下,会在下周的选定日期创建每周备份。
每日	除非每日备份符合每月备份或每周备份的定义,否则每日备份是当天的第一个备份。在这种情况下,会在第二天创建每日备份。
每小时	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,否则每小时备份是该小时的第一个备份。在这种情况下,会在下一小时创建每小时备份。

- 完整备份、差异备份和增量备份。

  这些设置可用于**自定义**备份方案,基于备份方法。**每月完整备份,每周差异备份,每天增量备份**是预配置的自定义方案。

示例

将采用默认设置的**始终增量(单个文件)**备份方案用于每小时备份:

- 已按时间预定。
- 备份每小时运行一次:星期一到星期五,每 1 小时一次,从上午 08:00 到晚上 06:00。
- **每周备份**选项设置为"星期一"。

在保护计划的**保留时间**部分中,可以将保留规则应用于每月备份、每周备份、每日备份和每小时备份。

下表汇总了在 8 天内创建的备份类型。

日期	星期几	描述
7 月 1 日	星期一	每个月的第一个备份是每月一次,因此今天的第一个备份是每月备份。当天的其他备份是每小时一次。 本周的第一个备份被视为每月备份。这就是没有每周备份的原因。下周的第一个备份将是每周备份。
7 月 2 日	星期二	第一个备份是每天一次,当天的其他备份是每小时一次。

日期	星期几	描述
7 月 3 日	星期三	第一个备份是每天一次，当天的其他备份是每小时一次。
7 月 4 日	星期四	第一个备份是每天一次，当天的其他备份是每小时一次。
7 月 5 日	星期五(F)	第一个备份是每天一次，当天的其他备份是每小时一次。
7 月 6 日	星期六	第一个备份是每天一次，当天的其他备份是每小时一次。
7 月 7 日	星期日	第一个备份是每天一次，当天的其他备份是每小时一次。
7 月 8 日	星期一	第一个备份是每周一次，当天的其他备份是每小时一次。

配置保留规则

保留规则是保护计划的一部分，其可用性和选项取决于备份方案。有关详细信息，请参阅 "根据备份方案制定的保留规则"(第 387 页)。

配置保留规则

1. 在保护计划中，展开**备份**模块。
2. 单击**保留的数目**。
3. 选择下列选项之一：
   - **按备份数量**
   - **按备份时间**

     每月、每周、每日和每小时备份的单独设置可用。所有类型的最大值都为 9999。

     还可以对所有备份使用单一设置。
   - **按备份的总大小**

     此设置不适用于**始终增量(单个文件)**备份方案。
   - **无限期地保留备份**
4. [如果未选择**无限期地保留备份**]配置选定选项的值。
5. [如果未选择**无限期地保留备份**]选择应用保留规则的时间：
   - 备份后
   - 备份前

     此选项在备份 Microsoft SQL Server 群集或 Microsoft Exchange Server 群集时不可用。
6. 单击**完成**。
7. 保存该保护计划。

复制

使用复制时，每个新备份都会自动复制到一个复制位置。复制位置中的备份不依赖于源位置中的备份，反之亦然。

仅复制源位置中的上次备份。但是，如果未复制早前备份(例如，由于网络连接问题)，则复制操作将包括上次成功复制后创建的所有备份。

如果复制操作中断，则处理的数据将由下一个复制操作使用。

注意
本主题将复制描述为保护计划的一部分。还可以创建单独的备份复制计划。有关详细信息，请参阅 "备份复制"(第 199 页)。

用法示例

- 确保可靠的恢复
  就地存储备份(用于即时恢复)和异地存储备份(以确保备份在发生存储故障或影响主要位置的自然灾害时保持安全)。
- 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
  配置用于从快速存储中删除旧备份的保留规则，以便节省存储成本。

支持的位置

位置	作为源位置	作为复制位置
本地文件夹	+	+
网络文件夹	+	+
云存储	-	+
安全区	+	+
公有云	- *	+

*从公共云进行复制仅在脱离主机数据处理计划中可用。请参阅 "用于主机外数据处理的受支持位置"(第 201 页)。

启用复制

1. 在保护计划中，展开**备份**模块，然后单击**添加位置**。

   注意
   当在**备份位置**中选择云存储时，**添加位置**选项不可用。

2. 从可用位置列表中，选择复制位置。
   保护计划中显示的位置作为**第二个位置**、**第三个位置**、**第四个位置**或**第五个位置**，具体取决于您为复制添加的位置数。
3. [可选] 单击齿轮图标以配置复制位置的选项。
   - **性能和备份窗口** - 为选定位置设置备份窗口，如 "性能和备份窗口"(第 429 页) 中所述。这些设置定义复制性能。
   - **删除位置** - 删除当前选择的复制位置。

- [仅对于云存储] **物理数据装运** - 在可移动存储设备上保存初始备份，然后装运它以上传到云存储，而不是通过 Internet 复制它。

  此选项适用于具有较慢网络连接的位置，或者在通过网络进行大文件传输时想要节省带宽的时候。启用该选项不要求高级 Cyber Protect 服务配额，但将需要物理数据装运服务配额，以创建装运订单并跟踪它。请参阅 "物理数据装运"(第 433 页)。

  注意
  此选项受版本 C21.06 或更高版本的保护代理程序版本支持。

4. [可选] 在复制位置下的**保留数量**行中，配置该位置的保留规则，如 "保留规则"(第 386 页) 中所述。
5. [可选] 重复步骤 1 - 4，以添加更多复制位置。

   可以配置最多四个复制位置(**第二个位置**、**第三个位置**、**第四个位置**和**第五个位置**)。如果选择**云存储**，则无法添加更多复制位置。

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 199 页)。

加密

高级加密标准 (AES) 加密算法以伽罗瓦/计数器模式 (GCM) 运行，并使用随机生成的 256 位密钥。然后，使用 SHA-2(256 位) 哈希的密码作为密钥对加密密钥进行 AES-256 算法加密。密码本身不会存储在磁盘或备份中，而是使用密码哈希用于验证。

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。

注意
使用 AES-256 算法和强密码可以提供抗量子性加密。它对依赖量子计算的密码分析攻击是安全的。

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。

您可以通过以下方式配置加密：

- 在保护计划中
- 作为计算机属性，通过使用 Cyber Protect Monitor或命令行接口

在保护计划中配置加密

在保护计划中，默认启用加密。使用的是 AES-256 算法。

凭借强密码，AES-256 算法可提供抗量子加密。

对于处于合规模式的账户，不能在保护计划中配置加密。有关如何在受保护设备上配置加密的详细信息，请参阅 "将加密配置为计算机属性"(第 392 页) 。

若要配置加密

1. 在保护计划中，展开**备份**模块。
2. 在**加密**中，点击**指定密码**。
3. 指定并确认加密密码。
4. 单击**确定**。

警告！
如果您丢失或忘记密码，则无法恢复加密备份。

在应用保护计划后，您不能更改加密设置。若要使用不同的加密设置，请创建一个新的计划。

将加密配置为计算机属性

您可以将备份加密配置为计算机属性。在这种情况下，备份加密不是在保护计划中配置的，而是在受保护的工作负载上配置的。作为计算机属性的加密使用 AES 算法和 256 位密钥 (AES-256)。

注意
使用 AES-256 算法和强密码可以提供抗量子性加密。它对依赖量子计算的密码分析攻击是安全的。

将加密配置为计算机属性会以通过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。将加密任何备份，即使在备份模块设置中禁用加密也是如此。

对于处于合规模式的帐户，只有作为计算机属性的加密是可用的。

如果您有多个适用于 VMware 的代理程序连接到同一个 vCenter 服务器，并且将加密配置为计算机属性，那么您必须在所有带有适用于 VMware 的代理程序的计算机上使用相同的加密密码，因为代理程序之间会进行负载均衡。

您可以通过以下方式将加密配置为计算机属性：

- 在命令行上
- 在 Cyber Protect Monitor中(适用于 Windows 和 macOS)

配置加密

在命令行上

1. 以管理员(在 Windows 中) 或 root 用户(在 Linux 中) 的身份登录。
2. 在命令行上，运行以下命令：
   - 适用 Windows：

```
<installation_path>\PyShell\bin\acropsh.exe -m manage_creds --set-password
<encryption_password>
```

默认情况下，安装路径为%ProgramFiles%\BackupClient。

- 适用 Linux：

```
/usr/sbin/acropsh -m manage_creds --set-password <encryption_password>
```

- 对于虚拟设备：

```
 /./sbin/acropsh -m manage_creds --set-password <encryption_password>
```

警告！
如果您丢失或忘记密码，则无法恢复加密备份。

在 Cyber Protect Monitor中

1. 以管理员身份登录。
2. 在通知区域 (Windows) 或菜单栏 (macOS) 中，单击 Cyber Protect Monitor图标。
3. 单击齿轮图标，然后单击**设置**> **加密**。
4. 选择**为此计算机设置密码**。指定并确认加密密码。
5. 单击**保存**。

警告！
如果您丢失或忘记密码，则无法恢复加密备份。

若要重置加密设置

1. 以管理员（在 Windows 中）或 root 用户（在 Linux 中）的身份登录。
2. 在命令行上，运行以下命令：
   - 适用 Windows：

```
<installation_path>\PyShell\bin\acropsh.exe -m manage_creds --reset
```

默认情况下，安装路径为%ProgramFiles%\BackupClient。

- 适用 Linux：

```
/usr/sbin/acropsh -m manage_creds --reset
```

- 对于虚拟设备：

```
/./sbin/acropsh -m manage_creds --reset
```

重要事项
如果您在保护计划创建备份后重置计算机属性的加密或更改加密密码，那么下一次备份操作将失败。若要继续备份工作负载，您需要创建一个新的保护计划。

公证

注意
该功能随 Advanced Backup 包提供。

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。

默认备份选项

备份选项的默认值基于公司、单位和用户级别存在。在公司内或单位内创建单位或用户帐户时，它会继承为公司或单位设置的默认值。

公司管理员、单位管理员和没有管理员权限的每个用户都可以对预定义的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基于相应级别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. 请执行以下任一操作：
   - 要更改公司的默认值，请以公司管理员身份登录到 Cyber Protect 中控台。
   - 要更改单位的默认值，请以单位的管理员身份登录到 Cyber Protect 中控台。
   - 要更改自己的默认值，请使用不具有管理员权限的帐户登录到 Cyber Protect 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**。

备份选项

要修改保护计划的备份选项，请在**备份**模块的**备份选项**字段中，单击**更改**。

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	Virtuozzo	Azure	Windows
警告	+	+	+	+	+	+	+	+	+	-	+
Azure 还原点：保留	-	-	-	-	-	-	-	-	-	+	-
Azure 还原点：一致性级别	-	-	-	-	-	-	-	-	-	+	-
Azure 还原点：处理不受支持的	-	-	-	-	-	-	-	-	-	+	-

磁盘											
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	+	+	+	+	+	+	+	+	+	+	+
错误处理											
如果发生错误，则重新尝试	+	+	+	+	+	+	+	+	+	+	+
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	+	+	+	-	-	-	-	-	-	-	-
文件级备份快照	-	-	-	+	+	+	-	-	-	-	-
文件过滤器	+	+	+	+	+	+	+	+	+	+	-
取证数据	+	-	-	-	-	-	-	-	-	-	-
日志截断	-	-	-	-	-	-	+	+	-	-	仅 SQL
LVM 快照	-	+	-	-	-	-	-	-	-	-	-
加载点	-	-	-	+	-	-	-	-	-	-	-
多卷快照	+	+	-	+	+	-	-	-	-	-	-
一键恢复	+	+	-	-	-	-	-	-	-	-	-
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	+	+	+	+	+	+	-	-	-	-	+
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	+	+	+	+	+	+	+	+	+	-	+
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。

Azure 还原点

配置无代理程序备份 Microsoft Azure 虚拟机时,有三种 Microsoft Azure 备份选项可用:

- Azure 还原点:保留
- Azure 还原点:一致性级别

- Azure 还原点：处理不受支持的磁盘

Azure 还原点：保留

此选项可让您定义在备份后保留多少个 Microsoft Azure 还原点（默认值为 3）。这些还原点可改善使用块更改跟踪 (CBT) 功能的增量备份性能。

您可保留的 Azure 还原点的最大数量为 200（Microsoft 建议的数量），每台虚拟机只能创建一个还原点集合。

若要从仍在 Microsoft Azure 中可用的具有对应 Azure 还原点的备份执行恢复，将恢复至原始 Microsoft Azure 虚拟机，则恢复进程将使用此还原点自动还原虚拟机状态，而不是从备份文件中检索数据。这有助于优化恢复的流量和性能。

请注意，还原点轮换逻辑由保护计划管理。如果有两个计划应用于同一台虚拟机，则每个计划将把集合中的所有还原点视为自己的还原点，并根据定义的**还原点**值轮换备份。

Azure 还原点：一致性级别

这样，您就可以选择还原点的一致性级别，如应用程序一致性还原点或文件系统一致性还原点。

注意
此选项仅适用于已启动的虚拟机。

可选择以下其中一个选项：

- **要求应用程序一致的还原点**：如果还原点不是应用程序一致的，则备份将失败。
  请注意，虚拟机还原点支持运行 Windows 操作系统的虚拟机的应用程序一致性，并支持运行 Linux 操作系统的虚拟机的文件系统一致性。应用程序一致性还原点使用 VSS 编写器（或 Linux 的预设/后设脚本）来确保创建还原点之前的应用程序数据一致性。
- **在文件系统或崩溃一致的还原点上发出警告**：如果还原点是文件系统一致或崩溃一致的，则备份完成时会发出警告。
  如果快照一致性级别为文件系统一致和以下（崩溃一致），则此选项将向日志添加警告，并使用警告标记活动。
- **崩溃一致还原点时发出警告**：如果还原点是崩溃一致的，则备份完成时会发出警告。文件系统一致和应用程序一致的还原点不会触发警告。此选项默认已选中。
  此选项将警告添加到日志中，并使用警告标记活动。
- **忽略一致性级别**：无论还原点的一致性级别如何，备份都将成功完成。
  此选项会将信息消息添加到日志中，并成功运行保护计划。

Azure 还原点：处理不受支持的磁盘

此选项可让您确定在备份具有未受管理、共享或临时磁盘的虚拟机时要执行的操作。请注意，Microsoft Azure 还原点不支持这些类型的磁盘，并且无法在无代理程序模式下备份这些磁盘。如果需要备份这些磁盘上的数据，请在虚拟机的来宾操作系统中安装保护代理程序。

可选择以下其中一个选项：

- **忽略不支持的磁盘**：备份成功完成，不支持的磁盘将被跳过。
- **不支持的磁盘时发出警告**：备份完成时，会发出有关不支持的磁盘的警告。此选项默认已选中。
- **不支持的磁盘上失败**：如果正在备份具有不支持的磁盘的虚拟机，则备份将失败。

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*：

- 备份目标为云存储。
- 备份方案设置为**始终增量备份（单个文件）**。
- 备份格式设置为**版本 12**。

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。

备份文件名

此选项定义由保护计划或云应用程序备份计划创建的备份文件的名称。

对于由保护计划创建的备份文件，可以在文件管理器中浏览备份位置时看到这些名称。

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。

	始终增量备份(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
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)。如果存储在本地或网络 (SMB) 文件夹中的文件大小超过 200 GB,默认情况下系统会将该文件拆分为多个 200 GB 文件。	

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或云应用程序备份计划时定义此名称(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。

如果更改保护计划或云应用程序备份计划中的备份文件名,则下一次备份将是完整备份。

如果指定同一台计算机的现有备份的文件名,将根据计划预定创建完整备份、增量备份或差异备份。

注意
如果移动原始存储中的备份文件 (.tibx),请勿重命名它们。重命名的文件会显示为已损坏,将无法从中恢复数据。

可以为文件管理器无法浏览的位置设置备份文件名(如云存储)。在这种情况下,您将在**备份存储**选项卡上看到自定义名称。

可以在哪里查看备份文件名?

对于保护计划,在**备份存储**选项卡上,选择位置,然后选择备份存档。

- 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。

对于云应用程序备份计划,在**备份存储**选项卡上,选择位置、选择备份存档,然后单击齿轮图标。

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**)。

注意

选择用户友好的备份文件名。这将帮助您在使用文件管理器浏览备份位置时轻松区分备份。

默认备份文件名

整个物理机和虚拟机、磁盘/卷、文件/文件夹、Microsoft SQL Server 数据库、Microsoft Exchange Server 数据库和 ESXi 配置的备份的默认备份文件名为 `[Machine Name]-[Plan ID]-[Unique ID]A`。

由适用于 Microsoft 365 的本地代理程序创建的 Exchange 邮箱备份和 Microsoft 365 邮箱备份的默认名称为 `[Mailbox ID]_mailbox_[Plan ID]A`。

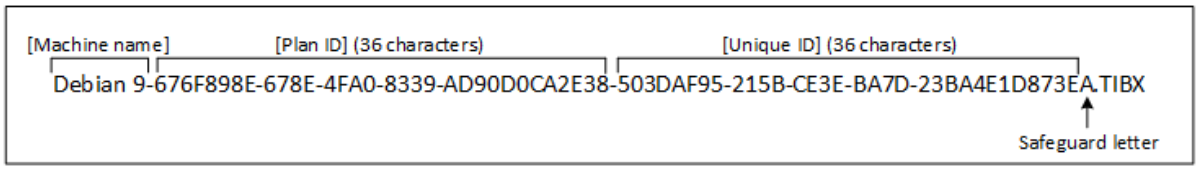
Microsoft Azure 备份的默认名称带有前缀 `[Mailbox ID]_`。无法删除此前缀。

由云代理程序创建的云应用程序备份的默认名称为 `[Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A`。

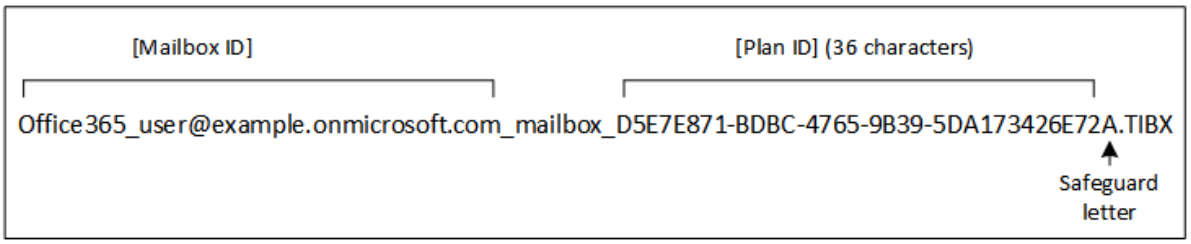
默认名称包含以下变量：

- `[Machine Name]` 该变量将替换为计算机的名称(与 Cyber Protect 中控台中显示的名称相同)。
- `[Plan ID]`, `[Plan Id]` 这些变量将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]` 此变量将替换为选定计算机的唯一标识符。重命名计算机时，此值不变。
- `[Mailbox ID]` 此变量将替换为邮箱用户的主体名称 (UPN)。
- `[Resource Name]` 此变量将替换为云数据源名称，例如用户的主体名称 (UPN)、SharePoint 站点 URL 或 Shared Drive 名称。
- `[Resource Type]` 此变量将替换为云数据源类型，例如 `mailbox`、`O365Mailbox`、`O365PublicFolder`、`OneDrive`、`SharePoint`、`GDrive`。
- `[Resource ID]` 此变量将替换为云数据源的唯一标识符。重命名云数据源时，此值不变。
- `"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。



下图显示由本地代理程序执行的 Microsoft 365 邮箱备份的默认备份文件名。



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
...
```

使用变量

除了默认使用的变量之外，还可以使用以下变量：

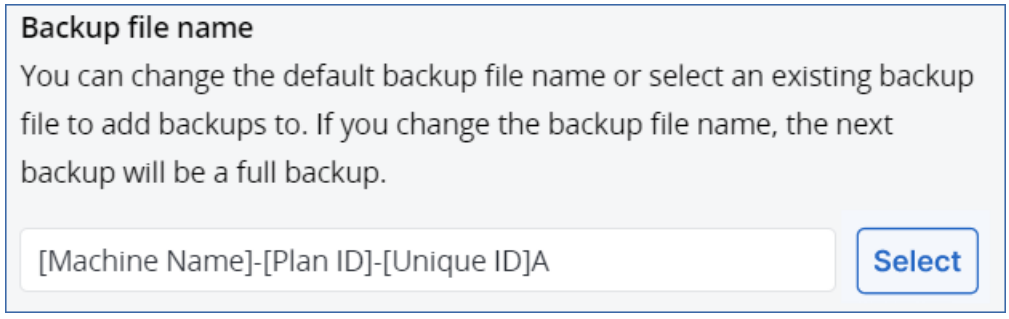
- [Plan name] 变量，该变量将替换为保护计划的名称。
- [Virtualization Server Type] 变量，该变量将替换为“vmwesx”(如果虚拟机由适用于 VMware 的代理程序备份)或“mshyperv”(如果虚拟机由适用于 Hyper-V 的代理程序备份)。

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]、[Unique ID]、[Mailbox ID]、[Resource Name] 或 [Resource Id] 变量。

在现有备份存档中创建备份

您可以配置要添加到现有备份存档的工作负载的备份。

此选项可能很有用，例如，当保护计划应用于单台计算机时，您必须从 Cyber Protect 中控台保护计划中删除该计算机，或卸载代理程序及其配置设置。再次添加计算机或重新安装代理程序后，您可以强制保护计划继续备份到原始存档。



配置要添加到现有备份存档的工作负载的备份

非云到云工作负载

1. 在**"所有设备"**屏幕上，单击工作负载，然后单击**"保护"**。
2. 在保护计划设置中，扩展**备份**模块。
3. 单击**"备份选项"**，然后单击**"更改"**。
4. 在**"备份文件名"**选项卡上，单击**"选择"**。
   "选择"按钮显示在保护计划的**"备份位置"**部分中选择的位置中的备份。

   注意
   选择按钮仅适用于为单个工作负载创建并已应用的保护计划。

5. 选择一个存档，然后单击**"完成"**。
6. 单击**"完成"**，然后单击**"应用"**。

云到云工作负载

1. 在**管理>云应用程序备份选项**卡上，选择计划。
2. 单击**编辑**，然后单击计划名称旁边的齿轮图标。
3. 在**文件备份名称**选项卡中，单击**选择**。

   注意
   "选择"按钮仅适用于为单个工作负载创建并应用到的备份计划。

4. 选择备份存档，然后单击**"完成"**。
5. 单击**"完成"**，然后单击**"保存更改"**。

备份格式

备份格式选项定义由保护计划创建的备份的格式。此选项仅适用于已使用版本 11 备份格式的保护计划。如果是这种情况，可以将备份格式更改为版本 12。在将备份格式切换为版本 12 后，该选项将不可用。

- **版本 11**
  为向后兼容保留的旧格式。

  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。

- **版本 12**
  安克诺斯 Backup 12 中引入的备份格式可用于快速备份和恢复。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。

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。下表列出了每个计算机或邮箱可以创建的文件。

	始终增量备份(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
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)。如果存储在本地或网络 (SMB) 文件夹中的文件大小超过 200 GB，默认情况下系统会将该文件拆分为多个 200 GB 文件。	

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。

存档内重复数据删除

版本 12 的 TIBX 备份格式支持存档内重复数据删除，具有以下优点：

- 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。

不同产品版本之间的备份格式兼容性

有关备份格式兼容性的信息，请参阅不同产品版本之间的备份存档兼容性 (1689)。

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。在此选项启用后，保护计划创建的每个备份都会在创建后立即使用校验和验证方法进行验证。该操作由保护代理程序执行。

预设为：**已禁用**。

有关通过校验和验证进行验证的详细信息，请参阅 "校验和验证"(第 203 页)。

注意
根据服务提供商所选择的设置，备份到云存储时可能无法使用进行验证。验证也不适用于公共云上的备份位置。

块更改跟踪 (CBT)

此选项对以下备份有效：

- 虚拟机的磁盘级别备份
- 运行 Windows 的物理机的磁盘级别备份
- Microsoft SQL Server 数据库的备份
- Microsoft Exchange Server 数据库的备份

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

注意
该功能随 Advanced Backup 包提供。

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 **已同步** 或 **正在同步** 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 **运行正常** 或 **激活** 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

注意
此选项不适用于云到云备份。这些备份的压缩默认以对应于下面**正常**级别的固定级别进行启用。

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的时间较多，但所生成的备份占用的空间较少。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。

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。**

发生可恢复的错误时，Cyber Protect 会再次尝试执行未成功的操作。您可以设置再次尝试的最大次数和再次尝试之间的间隔。如果在再次尝试的最大次数之后，操作仍无法成功完成，则操作将失败。

对于备份到网络位置或云存储(Acronis Cloud 存储或公共云存储，如 Amazon、Azure、Wasabi、S3 兼容或 Impossible Cloud)的情况，错误处理取决于错误发生的时刻。

备份启动时发生错误	正在进行备份时发生错误
重试次数取决于存储 API 的响应。如果 API 返回可重试的响应(例如，错误“503 服务不可用”)，则操作可能会在两小时内失败。 通常，此方案对于云存储而言比对于网络位置更可能。	重试次数取决于在保护计划中配置的**错误处理**设置。 例如，每次重试间隔 30 秒，重试 30 次。

对于备份到本地文件夹的情况，**错误处理**设置仅适用于正在进行备份时发生的错误。如果在备份开始时发生错误，则备份操作将立即失败。

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。

注意
Linux 不支持跳过坏扇区。可以使用本地版本的 Cyber Protect 中的可启动媒体生成器，在脱机模式下备份含有坏扇区的 Linux 系统。使用本地可启动媒体生成器需要单独的许可证。联系支持人员以寻求帮助。

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（包含/排除）

可以使用文件过滤器，可在备份中仅包含特定文件和文件夹，也可将特定文件和文件夹排除备份。

除非另有说明，否则文件过滤器可用于整机备份、磁盘级别备份和文件级备份。

文件过滤器在 XFS, JFS, exFAT 和 ReiserFS4 文件系统中不可用。有关更多信息，请参见"支持的文件系统"（第 50 页）。

文件过滤器不适用于在无代理程序模式（例如，通过适用于 VMware 的代理程序、适用于 Hyper-V 的代理程序或适用于 Scale Computing 的代理程序）下备份的虚拟机的动态磁盘（LVM 或 LDM 卷）。

文件筛选器类型

文件过滤器有以下类型：

- 包括筛选器（**仅包括符合以下条件的文件**）
  如果在包含过滤器中指定 `C:\File.exe`，则仅会备份此文件，即使选择了**整台计算机**也是如此。有关详细信息，请参阅 "筛选器示例"（第 411 页）。

  注意
  不支持不存储在云存储中的 **Version 11** 文件级备份的此筛选器。

- 排除筛选器（**排除符合以下条件的文件**）

如果在排除过滤器中指定 C:\File.exe，则在备份过程中会跳过此文件，即使选择了**整机**备份也是如此。

文件筛选器值

在文件筛选器中，您可以使用以下值：

- 文件或文件夹名称

  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。
- 文件或文件夹的完整路径

  指定文件或文件夹的完整路径，以驱动器号（备份 Windows 数据时）或根目录（备份 Linux 或 macOS 数据时）开头。在 Windows、Linux 和 macOS 中，可以使用正斜杠（C:/Temp/File.tmp）。在 Windows 中，还可以使用传统的反斜杠（C:\Temp\File.tmp）。

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，则具有完整路径文件筛选器将不起作用。对于排除筛选器，将显示一条警告。对于包含筛选器，备份将失败。

例如，一个文件的完整路径为 C:\Temp\File.tmp。如果操作系统检测不正确，则包含驱动器号或根目录的完整路径过滤器（如 C:\Temp\File.tmp 或 C:\Temp*）将导致出现警告或失败。

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，如果未正确检测到的操作系统，则这些过滤器不会起作用。

通配符

无论是文件或文件夹名称，还是文件或文件夹路径，您都可以使用以下通配符：

- 星号 (*)

  星号可替代零个或多个字符。

  例如，Doc*.txt 与文件 Doc.txt 和 Document.txt 相匹配。
- 双星号 (**)

  双星号可替代零个或多个字符，包括斜杠字符。

  例如，**/Docs/**.txt 匹配名为 Docs 的所有文件夹的所有子文件夹中的所有 TXT 文件。

  只能将双星号通配符用于“版本 12”格式的备份。
- 问号 (?)

  问号仅可替代一个字符。

  例如，Doc?.txt 匹配文件 Doc1.txt 和 Docs.txt，但不会匹配文件 Doc.txt 或 Doc11.txt。

注意

如果文件或文件夹名称中包含逗号或分号，请使用问号通配符。逗号和分号将被解释为分隔符，并将筛选器分割为两部分。例如，如果要在筛选器中使用文件夹 MyCompany,Inc，请在指定筛选器值时使用 MyCompany?Inc。否则，将创建两个单独的筛选器，如下所示：

- MyCompany
- Inc

配置文件筛选器

可以在保护计划中配置文件筛选器。

若要配置文件筛选器

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(包含/排除)**。
4. 配置文件筛选器。

   您可以配置一个或两个筛选器(包括或排除)。排除筛选器优先于包括筛选器。例如，如果在两个筛选器中都指定 C:\File.exe，则备份时将跳过 C:\File.exe。

   使用筛选器不会影响备份范围(**备份哪些内容**)中特定文件的选择。有关详细信息，请参阅 "筛选器示例"(第 411 页)。

   注意

   如果名称或路径包含逗号或分号，请将其替换为问号 (?) 通配符。逗号和分号将被解释为分隔符，并将筛选器分割为两部分。有关详细信息，请参阅 " 通配符"(第 410 页)。

5. 单击**完成**。
6. 保存该保护计划。

结果，文件筛选器将应用于保护计划的**备份哪些内容**部分中配置的范围。

筛选器示例

下表会显示文件筛选器配置的示例。

包含筛选器			
备份内容	**筛选器值**	**备份存档包含**	**描述**
C:\Folder1(包含 MyFile.txt 和其他文件) C:\Folder2(包含 MyDocument.txt 和其他文件)	MyFile.txt C:\Folder2\MyDocument.txt	C:\Folder1\MyFile.txt C:\Folder2\MyDocument.txt	包含筛选器与备份范围(**备份哪些内容**)匹配。 仅存在备份文件夹中指定的包含筛选器中的文件。 可以使用文件或文件夹名称，或使用文件或文

包含筛选器			
备份内容	**筛选器值**	**备份存档包含**	**描述**
			件夹路径来配置文件筛选器。
C:\Folder1(包含多个文件)	C:\Folder2\MyDocument.txt	C:\Folder1(作为空文件夹)	包含筛选器与备份范围(**备份哪些内容**)不匹配。 Folder1 已备份,但为空,因为它不包含包含筛选器中的文件。 未备份包含筛选器中的文件,因为它不是备份范围的一部分。
C:\Folder1(包含 MyFile.txt 和其他文件) C:\Folder2(包含 MyDocument.txt 和其他文件)	MyFile.txt	C:\Folder1\MyFile.txt C:\Folder2(作为空文件夹)	包含筛选器与备份范围(**备份哪些内容**)部分匹配。 Folder1 已备份,但它仅包含在包含筛选器中指定的文件。 Folder2 已备份,但为空,因为它不包含包含筛选器中的文件。
C:\Folder1(包含 MyFile.txt 和其他文件)	MyFile.txt	C:\Folder1\MyFile.txt C:\Folder2\MyDocument.txt	Folder1 已备份,但它仅包含在包

包含筛选器			
备份内容	**筛选器值**	**备份存档包含**	**描述**
C:\Folder2\MyDocument.txt			含筛选器中指定的文件。 还会备份第二个所选文件。使用筛选器不会影响备份范围(**备份哪些内容**)中特定文件的选择。

排除筛选器			
备份内容	**筛选器值**	**备份存档包含**	**描述**
C:\Folder1(包含 MyFile.txt 和其他文件) C:\Folder2(包含 MyDocument.txt 和其他文件)	MyFile.txt C:\Folder2\MyDocument.txt	C:\Folder1 – 所有文件,除了 MyFile.txt C:\Folder2 – 所有文件,除了 MyDocument.txt	排除筛选器与备份范围(**备份哪些内容**)匹配。 备份文件夹中缺少排除筛选器中指定的文件。 可以使用文件或文件夹名称,或使用文件或文件夹路径来配置文件筛选器。
C:\Folder1(包含多个文件)	C:\Folder2\MyDocument.txt	C:\Folder1 – 所有文件	排除筛选器与备份范围(**备份哪些内容**)不匹配。 Folder1 的全部内容均

排除筛选器			
备份内容	**筛选器值**	**备份存档包含**	**描述**
			已备份。
C:\Folder1(包含 MyFile.txt 和其他文件) C:\Folder2(包含 MyDocument.txt 和其他文件)	MyFile.txt	C:\Folder1 – 所有文件，除了 MyFile.txt C:\Folder2 – 所有文件	包含筛选器与备份范围(**备份哪些内容**)部分匹配。 Folder1 已备份，但在排除筛选器中指定的文件已丢失。 Folder2 的全部内容均已备份。
C:\Folder1(包含 MyFile.txt 和其他文件) C:\Folder2\MyDocument.txt	MyFile.txt	C:\Folder1 – 所有文件，除了 MyFile.txt C:\Folder2\MyDocument.txt	Folder1 已备份，但在排除筛选器中指定的文件已丢失。 第二个选定的文件将被备份，因为它不符合排除筛选器。

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

病毒、恶意软件和勒索软件可以实施恶意活动，例如盗窃或更改数据。这些活动可能需要进行调查，仅当提供了数字证据时才有可能。但是，部分数字证据(例如文件或活动痕迹)可能被删除，或者发生恶意活动的计算机可能不可用。

具有取证数据的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。**取证数据**备份选项让您可以收集可用于取证调查的以下部分的数字证据：未使用的磁盘空间快照、内存转储以及运行的进程的快照。

带有取证数据的备份会自动进行公证。

取证数据选项仅适用于运行以下操作系统的 Windows 计算机的完整计算机备份：

- Windows 8.1，Windows 10
- Windows Server 2012 R2 – Windows Server 2019

具有取证数据的备份不可用于以下计算机：

- 通过 VPN 连接到您网络并且无法直接访问 Internet 的计算机
- 其磁盘由 BitLocker 加密的计算机

注意
将启用了**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。要使用不同的取证数据设置，请创建新的保护计划。

可以在以下位置存储具有取证数据的备份：

- 云存储
- 本地文件夹

  注意
  仅支持通过 USB 连接的外部硬盘上的本地文件夹位置。
  本地动态磁盘不支持用作具有取证数据的备份的位置。

- 网络文件夹

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 Cyber Protect 中控台中，转到**设备** > **所有设备**。或者，可以从**管理**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。

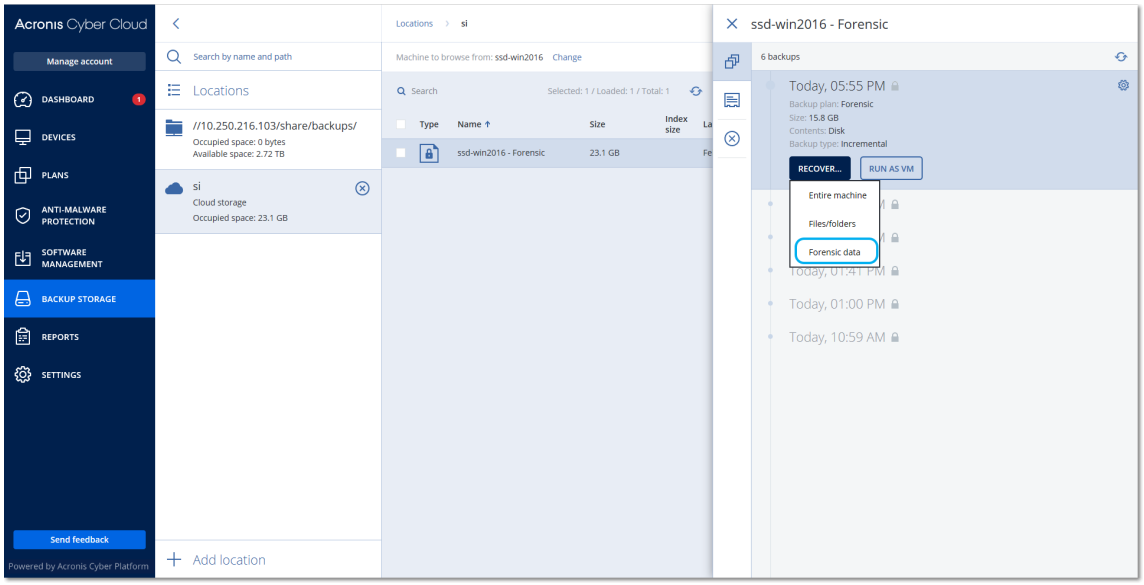
8. 指定位置。
9. 单击**立即运行**以立即执行带有取证数据的备份，或者等到根据预定创建备份。
10. 转到**监控** > **活动**，验证是否已成功创建带有取证数据的备份。

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。

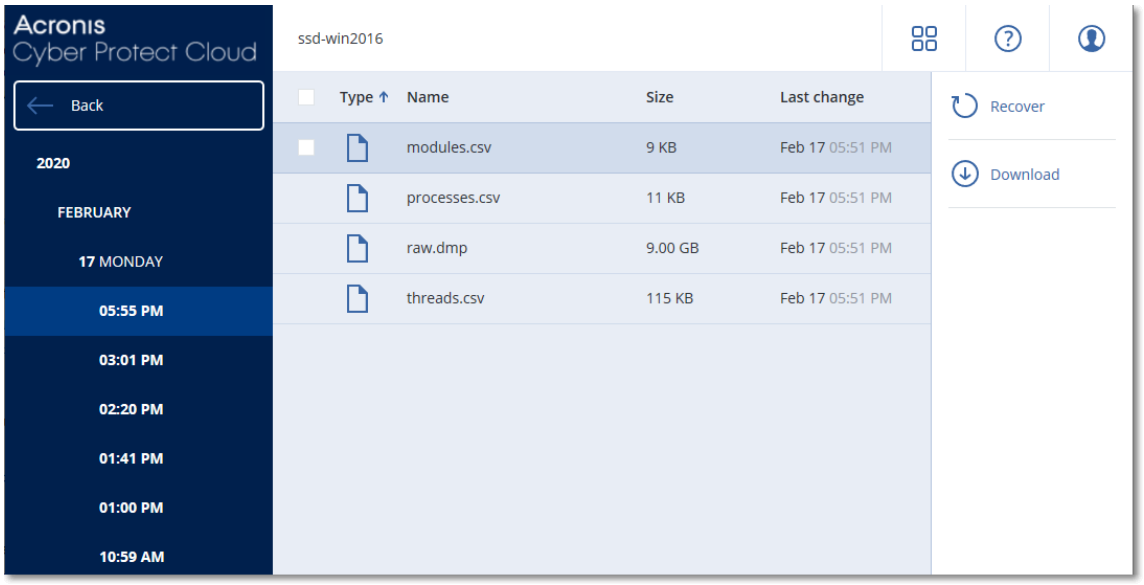
如何从备份中获取取证数据？

1. 在 Cyber Protect 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

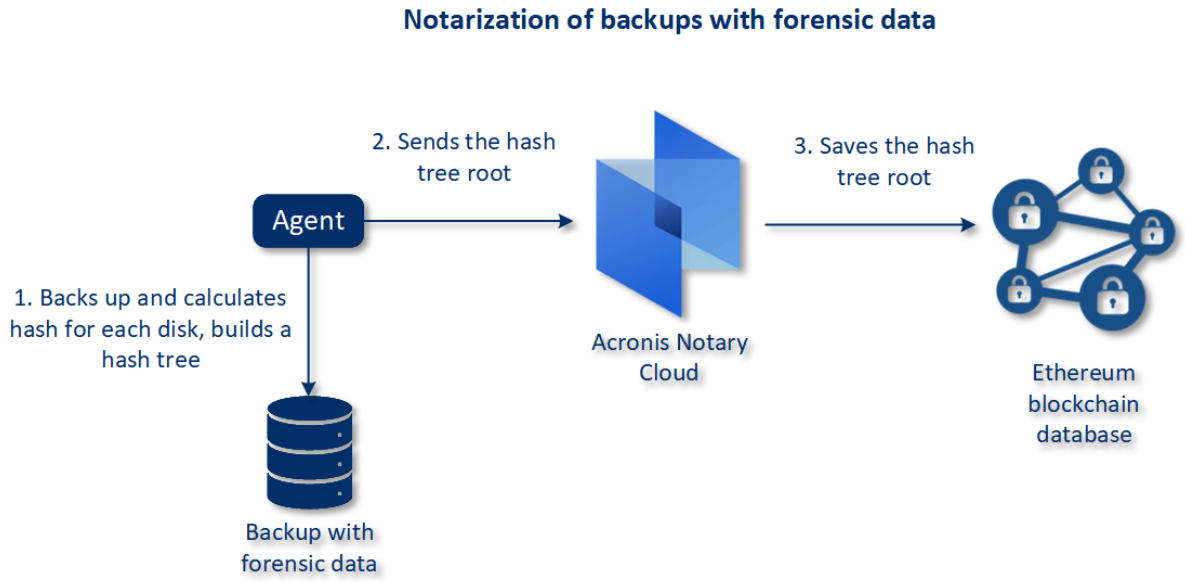
公证让您能够证明带有取证数据的磁盘在备份后仍是可信的且未经更改。

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”

Cyber Protection 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。

安装路径：该文件夹与代理程序所在的文件夹相同（例如，C:\Program Files\BackupClient\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
```

输出模板：

```
GUID Date Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> - 备份的 GUID。

<date> - 备份的创建日期。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-2(256 位) 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	描述
--arc=BACKUP_NAME	可以从 Cyber Protect 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 Protect 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 Protect 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”。
--	备份的加密密码。如果不加密备份,请将该值保留为空。

password=PASSWORD	

--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。备份速度更快，不需要卷组上的未分配空间。因此，建议您仅当在备份逻辑卷时遇到问题的情况下才更改预设。
- **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。

快照仅在备份操作期间进行使用，并在备份操作完成后自动删除。不会保留任何临时文件。

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。

注意
对于 Linux 和 macOS，将忽略 **备份挂载点** 选项，行为将如下所示：
- "本地" 挂载点（如本地磁盘、USB 驱动器等）中的数据将始终备份。
- "远程"挂载点中的数据（如 CIFS/NFS 共享等）将永远不会备份。

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**。
- 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

注意
该功能随 Advanced Backup 包提供。

通过一键恢复,您可以自动恢复 Windows 或 Linux 计算机的磁盘备份。此备份可以是整个计算机的备份,也可以是该计算机上特定磁盘或卷的备份。

一键恢复支持以下操作:

- 从最新备份自动恢复
- 从备份存档中的特定备份(也称为恢复点)恢复

一键恢复支持以下备份存储:

- 安全区
- 网络文件夹
- 云存储

重要事项
当执行以下任一操作时,请暂停 BitLocker 加密,直到下次重新启动计算机:

- 创建、修改或删除安全区。
- 启用或禁用“启动恢复管理器”。
- [仅当“启动恢复管理器”尚未启用时]在保护计划中启用一键恢复后运行第一个备份。此操作会自动启用“启动恢复管理器”。
- 更新“启动恢复管理器”,例如通过更新保护。

如果在这些操作期间 BitLocker 加密未暂停,则需要在重新启动计算机后指定 BitLocker PIN。

启用一键恢复

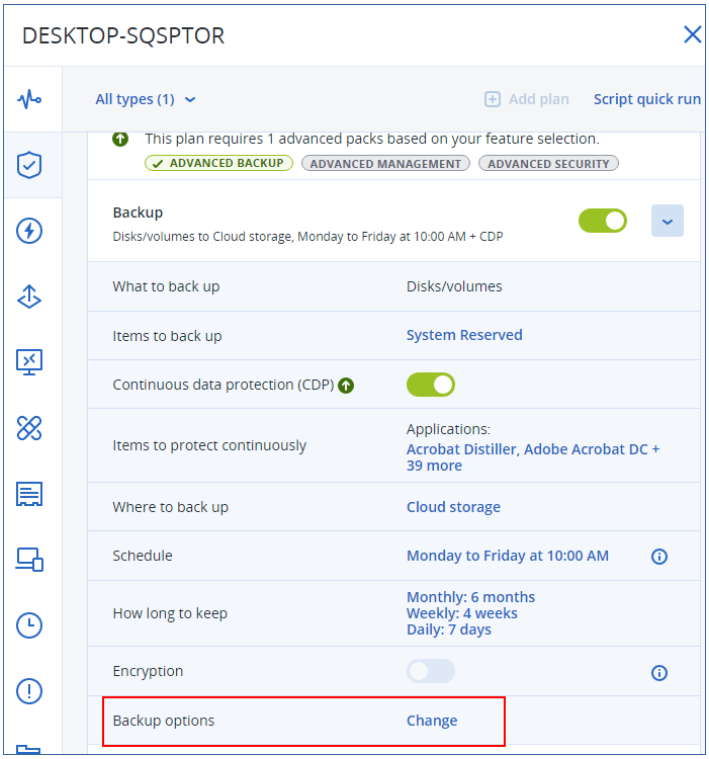
一键恢复是保护计划中的备份选项。有关如何创建计划的更多信息,请参阅 "创建保护计划"(第 192 页)。

注意

启用一键恢复还会在目标机器上启用 启动恢复管理器。如果无法启用 启动恢复管理器，创建一键恢复备份的备份操作将失败。欲了解更多 启动恢复管理器 信息，请参阅 "启动恢复管理器"(第 652 页)。

若要启用一键恢复

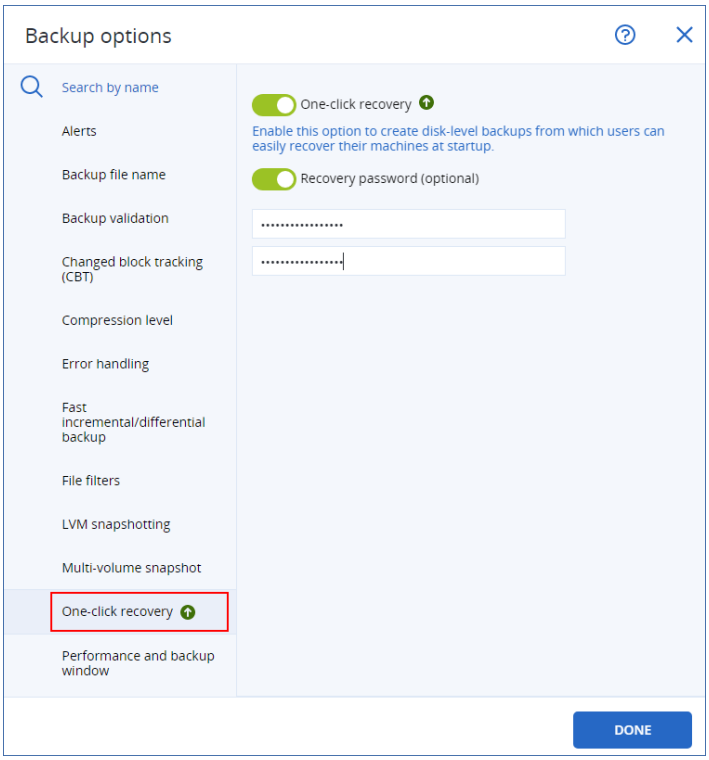
1. 在保护计划中，展开**备份**模块。
2. 在**要备份的内容**中，选择**整个计算机**或**磁盘/卷**。
3. [如果已选择**磁盘/卷**]。在**要备份的项目**中，指定要备份的磁盘或卷。
4. 在**备份选项**中，单击**更改**，然后选择**一键恢复**。



5. 启用**一键恢复**开关。
6. [可选] 启用**恢复密码**开关，然后指定密码。

重要事项

强烈建议您指定恢复密码。确保在目标计算机上执行一键恢复的用户知道这个密码。



7. 单击**完成**。
8. 根据您的需求配置保护计划的其他元素，然后保存计划。

结果，在保护计划运行并创建备份后，一键恢复即会可供受保护计算机的用户使用。

禁用一键恢复

您可以通过以下方式禁用特定工作负载的一键恢复：

- 在应用于工作负载的保护计划中禁用**一键恢复**选项。
- 撤销启用**一键恢复**选项的保护计划。
- 删除启用**一键恢复**选项的保护计划。

通过“一键恢复”恢复计算机

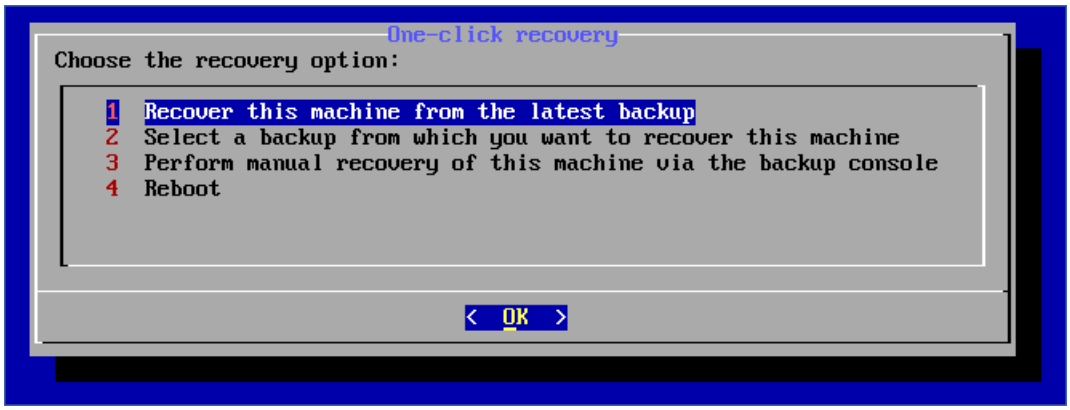
先决条件

- 已启用**一键恢复**备份选项的保护计划将应用于计算机。
- 计算机至少有一个磁盘备份。

恢复计算机

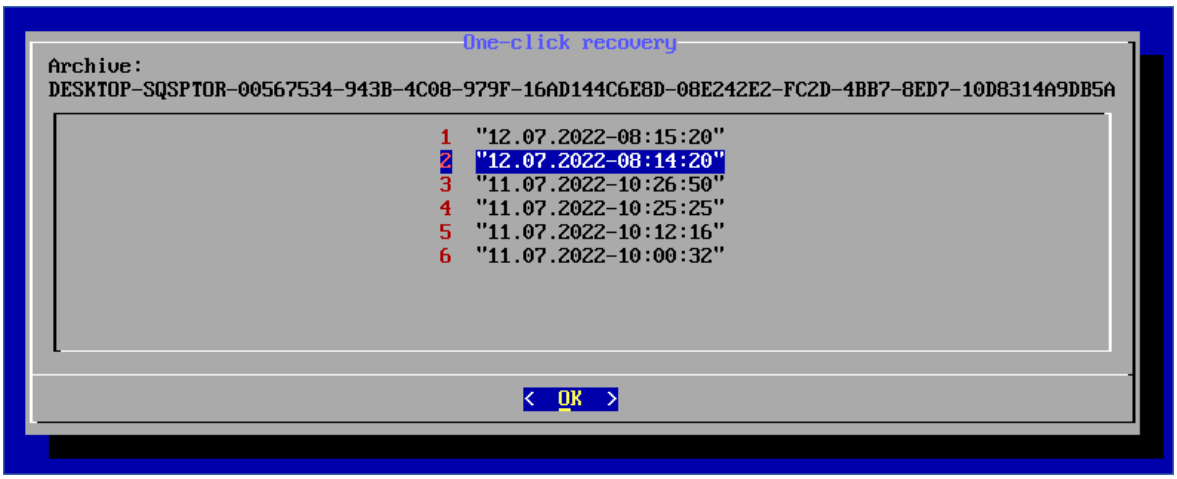
1. 重新启动要恢复的计算机。
2. 在重新启动期间，按 F11 键以进入 启动恢复管理器。
   应急媒体窗口即会打开。
3. 选择 **安克诺斯 Cyber Protect**。
4. [如果在保护计划中指定了恢复密码] 输入恢复密码，然后单击**确定**。

5. 选择一键恢复选项。
   - 要自动恢复最新备份，请选择第一个选项，然后单击**确定**。
   - 若要恢复备份存档中的另一个备份，请选择第二个选项，然后单击**“确定”**。

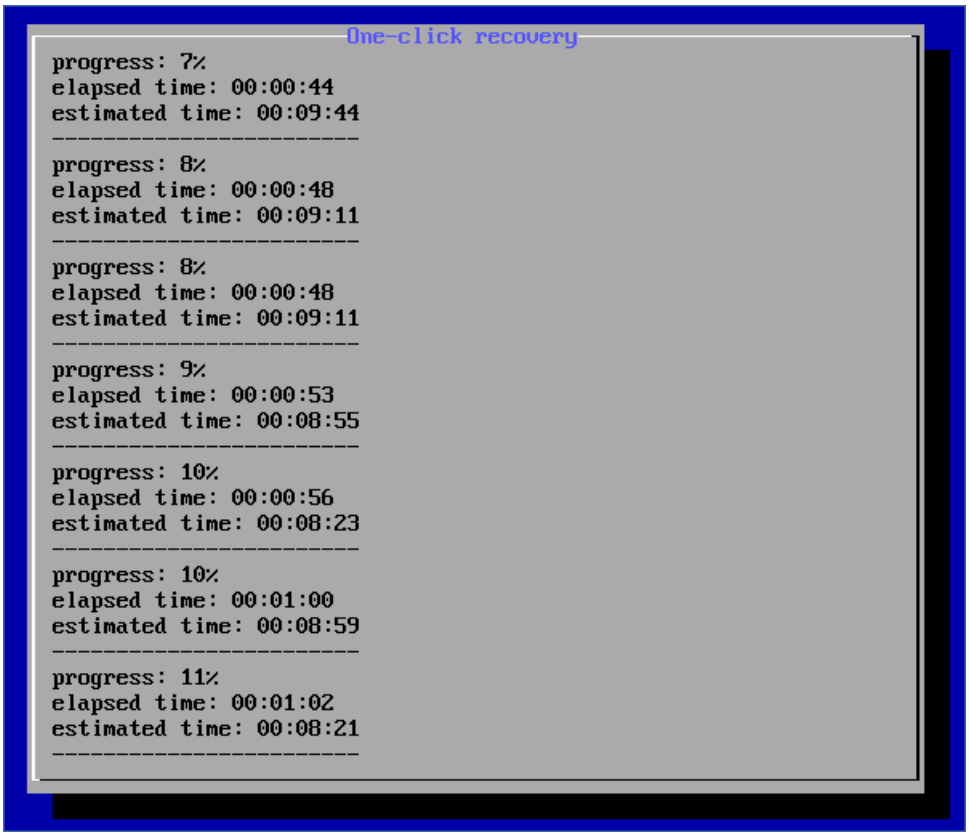


6. 单击**是**来确认选择。

   应急媒体窗口即会打开，然后消失。在没有它的情况下，恢复过程会继续。
7. [如果选择恢复特定备份]选择要恢复的备份，然后单击**确定**。



一段时间后，恢复开始并显示其进度。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。

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(例如,验证)都将运行,而不管此选项如何。

预设为:**已禁用**。

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**低于正常水平**)
- 输出速度:**无限制**

启用此选项后,将根据当前小时指定的性能参数允许或阻止计划备份。在备份被阻止的一小时之初,备份进程会自动停止并生成警报。即使计划的备份被阻止,也可以手动启动备份。它将使用允许备份的最近一小时的性能参数。

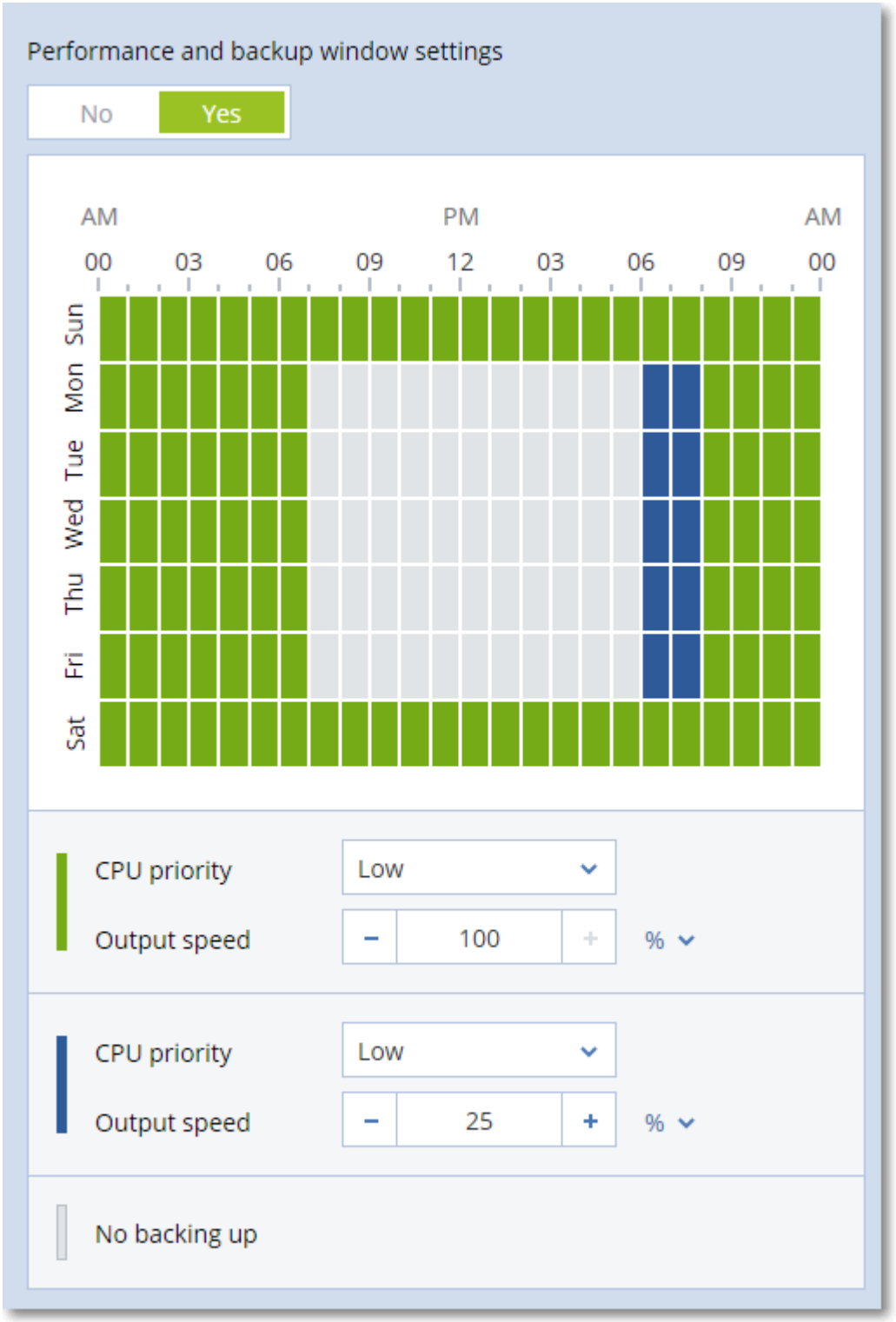
注意
您可以为每个复制位置单独配置性能和备份窗口。要访问复制位置的设置,请在保护计划中单击位置名称旁边的齿轮图标,然后单击**性能和备份窗口**。

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。



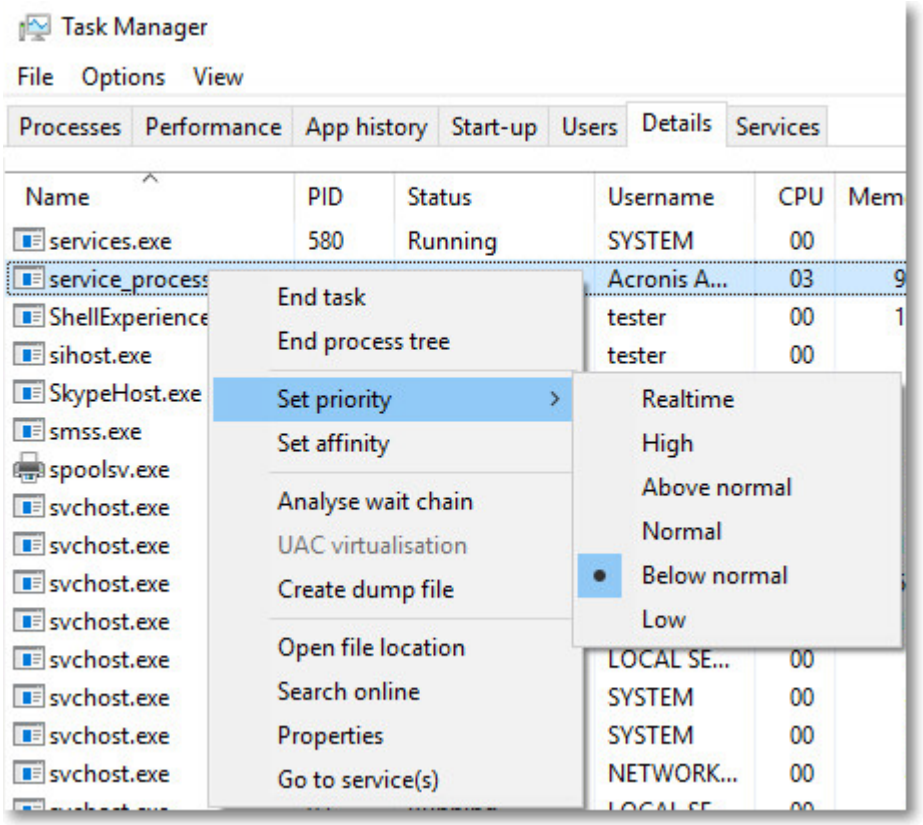
CPU 优先级

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**、**正常**、**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，而在 Linux 和 macOS 中设置备份进程 (**service_process**) 的良好度。



下表汇总了 Windows、Linux 和 macOS 中此设置的映射。

Cyber Protection 优先级	Windows 优先权	Linux 和 macOS 优先级
低	低于正常	10
正常	正常	0
高	高	-10

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

如果备份或复制目标是云存储并且备份格式设置为**版本 12**,则此选项可用。

此选项对适用于 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、适用于 Hyper-V 的代理程序和适用于 Virtuozzo 的代理程序创建的磁盘级别备份和文件备份有效。

使用此选项将通过使用"物理数据装运"服务将保护计划创建的第一个完整备份装运到硬盘驱动器上的云存储。后续增量备份通过网络执行。

对于复制到云的本地备份,增量备份继续并本地保存,直到在云存储中上传了初始备份。然后所有增量更改都复制到云,并且复制按照备份预定继续。

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. [装运将云存储作为主备份位置的备份的步骤]
   a. 通过备份到云创建新的保护计划。
   b. 在**备份选项**行中,单击**更改**。
   c. 在可用选项列表中,单击**物理数据装运**。

   可以直接备份到可移动驱动器,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。
2. [装运复制到云的本地备份的步骤]

   注意
   此选项受版本 C21.06 或更高版本的保护代理程序版本支持。

   a. 通过备份到本地或网络存储创建新的保护计划。
   b. 单击**添加位置**,并选择**云存储**。
   c. 在**云存储**位置行,单击齿轮图标并选择**物理数据装运**。
3. 在**使用物理数据装运**下,单击**是**和**完成**。

   在保护计划中自动启用"加密"选项,因为所有装运的所有备份必须已加密。
4. 在**加密**行中,单击**指定密码**并为加密输入密码。

5. 在**物理数据装运**行中，选择将保存初始备份的可移动驱动器。
6. 单击**创建**以保存该保护计划。
7. 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。
   若要访问该 Web 界面，请登录到管理门户，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**。

   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。

8. 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。

9. 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。

代理程序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。

注意
如果脚本由于出现与 Linux 中所需库版本相关的冲突而无法运行，请通过在脚本中添加以下各行来取消包括 LD_LIBRARY_PATH 和 LD_PRELOAD 环境变量：

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

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

此选项让您可以定义在数据捕获(即创建数据快照)之前和之后要自动运行的命令。数据捕获将在备份过程开始时执行数据捕获。

以下方案说明了何时运行数据捕获前/后命令。

	<---------- 备份 ---------->				
备份前命令	数据捕获前命令	数据捕获	数据捕获后命令	将数据写入备份集	备份后命令

与其他备份选项的交互

其他备份选项可以修改数据捕获前/后命令的运行。

如果**多卷快照**选项处于启用状态,则数据捕获前/后命令将只运行一次,因为所有卷的快照是同时创建的。如果**多卷快照**选项处于禁用状态,则数据捕获前/后命令将针对每个正在备份的卷运行,因为快照是按一个卷接一个卷的顺序创建的。

如果**卷影复制服务(VSS)**选项处于启用状态,则数据捕获前/后命令和 Microsoft VSS 操作将按如下所示运行:

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。

注意
如果脚本由于出现与 Linux 中所需库版本相关的冲突而无法运行，请通过在脚本中添加以下各行来取消包括 LD_LIBRARY_PATH 和 LD_PRELOAD 环境变量：

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

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。

预定

此选项定义备份是完全按预定开始还是延迟开始，以及同时备份的虚拟机数量。

有关如何配置备份预定的详细信息，请参阅 "按预定运行备份"(第 374 页)。

预设为：**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**

  使用此选项，可管理在虚拟机监控程序级别上备份的虚拟机的并行备份(无代理程序备份)。

  此选项处于选中状态的保护计划可以与同一代理程序同时操作的其他保护计划一起运行。当选择此选项时，必须指定每个计划中的并行备份数。所有计划同时备份的计算机总数限制为每个代理程序 10 台。要了解如何更改默认限制，请参阅 "限制同时备份虚拟机的总数"(第 629 页)。

  此选项未处于选中状态的保护计划会依次运行备份操作，一个接一个地运行虚拟机。

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

此选项可使您选择将大型备份分割为较小文件的方法。

注意

分割在使用云存储作为备份位置的保护计划中不可用。

预设为：

- 如果备份位置为本地文件夹或网络 (SMB) 文件夹，并且备份格式为版本 12：**固定大小 - 200 GB**
  此设置允许备份软件在 NTFS 文件系统上处理大量数据，而不会因文件碎片而产生不良影响。
- 否则：**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。

任务失败处理

此选项确定在以下情况下的程序行为：保护计划的预定执行失败，或在备份运行时计算机重新启动。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。在尝试成功完成或已执行指定尝试次数（具体取决于哪个操作先完成）后，程序将停止尝试。

如果此选项已启用并且计算机在备份运行时重新启动，则备份操作不会失败。重新启动几分钟后，备份操作将自动继续，并使用丢失的数据完成备份文件。在此用例中，与**尝试间隔**选项无关。

预设为：**已启用**。

注意
此选项在取证备份中无效。

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。有关条件的详细信息，请参阅 "开始条件"（第 379 页）。

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)

此选项仅适用于 Windows 操作系统。

它定义备份在一个或多个卷影复制服务 (VSS) 写入程序失败的情况下是否可以成功，以及哪个提供程序必须通知 VSS 感知应用程序备份将开始。

使用卷影复制服务，可确保应用程序使用的所有数据的一致状态；尤其是在备份软件创建数据快照时，可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。

快照仅在备份操作期间进行使用，并在备份操作完成后自动删除。不会保留任何临时文件。

还可以使用数据捕获前/后命令，来确保数据在一致状态下进行备份。例如，指定将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，然后指定将在创建快照后恢复数据库运行的数据捕获后命令。

注意
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。

忽略失败的 VSS Writer

可选择以下其中一个选项：

- **忽略失败的 VSS Writer**
  使用此选项时，即使一个或多个 VSS 写入程序失败，也可以成功备份。

  重要事项
  如果特定于应用程序的写入程序失败，则应用程序感知备份会始终失败。例如，如果正在对 SQL Server 数据进行应用程序感知备份，但 **SqlServerWriter** 失败，则备份操作也会失败。

  启用此选项后，将对 VSS 快照连续进行最多三次尝试。
  在第一次尝试时，需要使用所有 VSS 写入程序。如果此尝试失败，将重复进行该尝试。如果第二次尝试也失败，则失败的 VSS 写入程序会被排除在备份操作的范围之外，然后进行第三次尝试。如果第三次尝试成功，则备份将完成，并显示有关失败的 VSS 写入程序的警告。如果第三次尝试不成功，则备份将失败。

- **要求成功处理所有 VSS 写入程序**
  如果任何 VSS 写入程序失败，则备份操作也会失败。

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**
  自动选择硬件快照供应商、软件快照供应商或 Microsoft Software Shadow Copy 供应商。

  注意
  我们建议尽可能使用快照提供程序的自动选择。

- **使用 Microsoft Software Shadow Copy Provider**
  如果有其他不想使用的第三方 VSS 提供程序，并且受保护的工作负载不包含集群共享卷，我们建议强制使用 Microsoft 软件卷影副本提供程序。

  警告！
  仅当需要明确使用时才强制使用 Microsoft 软件卷影副本提供程序，因为它可能会导致在具有集群共享卷和 Microsoft 软件卷影副本提供程序不支持的其他卷的环境中备份失败。

启用 VSS 完整备份

如果此选项已启用，则 Microsoft Exchange Server 和其他 VSS 感知应用程序（Microsoft SQL Server 除外）的日志会在每次成功执行完整、增量或差异磁盘级别备份后截断。

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。

重要事项
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。

预设为：**已启用**。

当此选项处于禁用状态时，将创建非静态快照。将在故障一致状态下备份虚拟机。

当此选项处于启用状态时，将结束在虚拟机中运行的所有 VSS 感知应用程序的事务，然后拍摄静态快照。

如果在“错误处理”选项中指定的重试次数之后无法拍摄静态快照，并且应用程序备份处于启用状态，则备份将失败。

如果在“错误处理”选项中指定的重试次数之后无法拍摄静态快照，并且应用程序备份处于禁用状态，则将创建崩溃一致性备份。要使备份失败而不是创建崩溃一致性备份，请选中**如果无法拍摄静态快照，则备份失败”**复选框。

下表汇总了可用设置及其结果。

设置	静态快照已成功拍摄		静态快照未拍摄	
	应用程序备份已启用	应用程序备份已禁用	应用程序备份已启用	应用程序备份已禁用
适用于虚拟机的卷影复制服务 (VSS) 已启用 **如果无法拍摄静态快照，则备份失败** 未选中	将拍摄静态快照。将创建应用程序一致性备份。	将拍摄静态快照。将创建应用程序一致性备份。	备份将失败。	将拍摄非静态快照。将创建崩溃一致性备份。
适用于虚拟机的卷影复制服务 (VSS) 已启用 **如果无法拍摄静态快照，则备份失败** 已选中	将拍摄静态快照。将创建应用程序一致性备份。	将拍摄静态快照。将创建应用程序一致性备份。	备份将失败。	备份将失败。
适用于虚拟机的卷影复制服务 (VSS) 已禁用	将拍摄非静态快照。将创建崩溃一致性备份。	将拍摄非静态快照。将创建崩溃一致性备份。	将拍摄非静态快照。将创建崩溃一致性备份。	将拍摄非静态快照。将创建崩溃一致性备份。

启用**适用于虚拟机的卷影复制服务 (VSS)** 还会触发可能在备份的虚拟机上所具有的冻结前和解冻后脚本。有关这些脚本的详细信息，请参阅 "自动运行冻结前和解冻后脚本"(第 622 页) 。

要创建静默快照，备份软件将通过使用 VMware Tools、Hyper-V 集成服务、Virtuozzo 来宾工具、Red Hat Virtualization 来宾工具或 QEMU 来宾工具在虚拟机内分别应用 VSS。

注意
对于 Red Hat Virtualization (oVirt) 虚拟机，建议您安装 QEMU 来宾工具而不是 Red Hat Virtualization 来宾工具。某些版本的 Red Hat Virtualization 来宾工具不支持应用程序一致的快照。

该选项不会影响 Scale Computing HC3 虚拟机。对于这些脚本，静默取决于虚拟机上是否已安装 Scale Tools。

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。

注意
在 Cyber Protect 中控台中，无法为处于合规模式下的租户恢复备份。有关如何恢复此类备份的详细信息，请参阅 "在合规模式下恢复租户的备份"(第 996 页)。

恢复内容	恢复方法
物理机 (Windows 或 Linux)	使用 Cyber Protect 中控台 使用可启动媒体
物理机 (Mac)	使用可启动媒体
虚拟机 (VMware、Hyper-V、Red Hat Virtualization (oVirt) 或 Scale Computing HC3)	使用 Cyber Protect 中控台 使用可启动媒体
虚拟机或容器 (Virtuozzo、Virtuozzo Hybrid Server 或 Virtuozzo Hybrid Infrastructure)	使用 Cyber Protect 中控台
ESXi 配置	使用可启动媒体
文件/文件夹	使用 Cyber Protect 中控台 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 Cyber Protect 中控台

SQL 数据库	使用 Cyber Protect 中控台
Exchange 数据库	使用 Cyber Protect 中控台
Exchange 邮箱	使用 Cyber Protect 中控台
网站	使用 Cyber Protect 中控台
Microsoft 365	
邮箱 (适用于 Microsoft 365 的本地代理程序)	使用 Cyber Protect 中控台
邮箱 (适用于 Microsoft 365 的云代理程序)	使用 Cyber Protect 中控台
公用文件夹	使用 Cyber Protect 中控台
OneDrive 文件	使用 Cyber Protect 中控台
SharePoint Online 数据	使用 Cyber Protect 中控台
Google Workspace	
邮箱	使用 Cyber Protect 中控台
Google Drive 文件	使用 Cyber Protect 中控台
Shared Drive 文件	使用 Cyber Protect 中控台

跨平台恢复

跨平台恢复可用于整个计算机的备份，以及包含操作系统的磁盘的备份。

在以下情况下可以进行跨平台恢复：

- 备份由一种类型的代理程序创建，但由另一种类型的代理程序恢复。
- 基于代理程序的备份在虚拟机监控程序级别恢复(无代理程序恢复)，或者由代理程序恢复无代理程序备份(基于代理程序的恢复)。
- 备份恢复到不同硬件(包括虚拟硬件)。

注意
在进行跨平台恢复时，一些外围设备(例如打印机)可能无法正确恢复。

下表显示了一些跨平台恢复示例。

跨平台恢复	
无代理程序备份	基于代理程序的恢复
基于代理程序的备份	无代理程序恢复
由适用于 Windows 的代理程序备份	由适用于 VMware 的代理程序恢复
由适用于 VMware 的代理程序备份	由适用于 Hyper-V 的代理程序恢复
由安装在 VMware ESXi 虚拟机上的适用于 Windows 的代理程序备份(基于代理程序)	由相同 VMware ESXi 主机上的适用于 VMware 的代理程序(无代理程序)恢复
由适用于 Windows 的代理程序备份	由安装在具有不同硬件的虚拟机上的适用于 Windows 的代理程序恢复
物理机的备份	作为虚拟机恢复

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

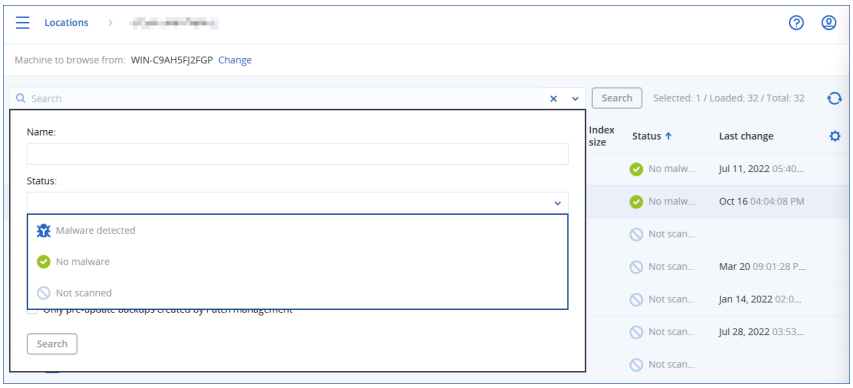
将安全恢复与对 Windows 工作负载的**整台计算机**或**磁盘/卷**备份一起使用，以确保仅恢复无恶意软件的数据，即使备份包含被感染文件。

在安全恢复操作期间，会自动扫描备份以查找恶意软件。然后，保护代理程序恢复目标工作负载上的备份，并删除任何被感染文件。结果，一个无恶意软件的备份即会恢复。

此外，以下状态之一会指派给备份：

- 检测到恶意软件
- 无恶意软件
- 未扫描

可以使用状态来过滤备份存档。



限制

- 装有保护代理程序的物理和虚拟 Windows 计算机支持安全恢复。
- **整台计算机**和**磁盘/卷**备份支持安全恢复。
- 仅会扫描 NTFS 卷以查找恶意软件。非 NTFS 卷会在不执行防恶意软件扫描的情况下进行恢复。
- 存档中的持续数据保护 (CDP) 备份不支持安全恢复。要从 CDP 备份中恢复数据，请另外运行**文件/文件夹**恢复操作。有关 CDP 备份的更多操作，请参阅 "连续数据保护 (CDP)"(第 364 页)。

恢复计算机

恢复物理机

本部分介绍使用 Web 界面恢复物理机。

如果要恢复以下内容，请使用可启动媒体，而不是 Web 界面：

- 运行 macOS 的计算机
- 租户中的计算机处于“合规模式”下
- 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。

注意
您不能恢复基于 Intel 的 Mac 对使用 Apple Silicon 处理器的 Mac 的磁盘级别备份，反之亦然。您可以恢复文件和文件夹。

恢复至物理机

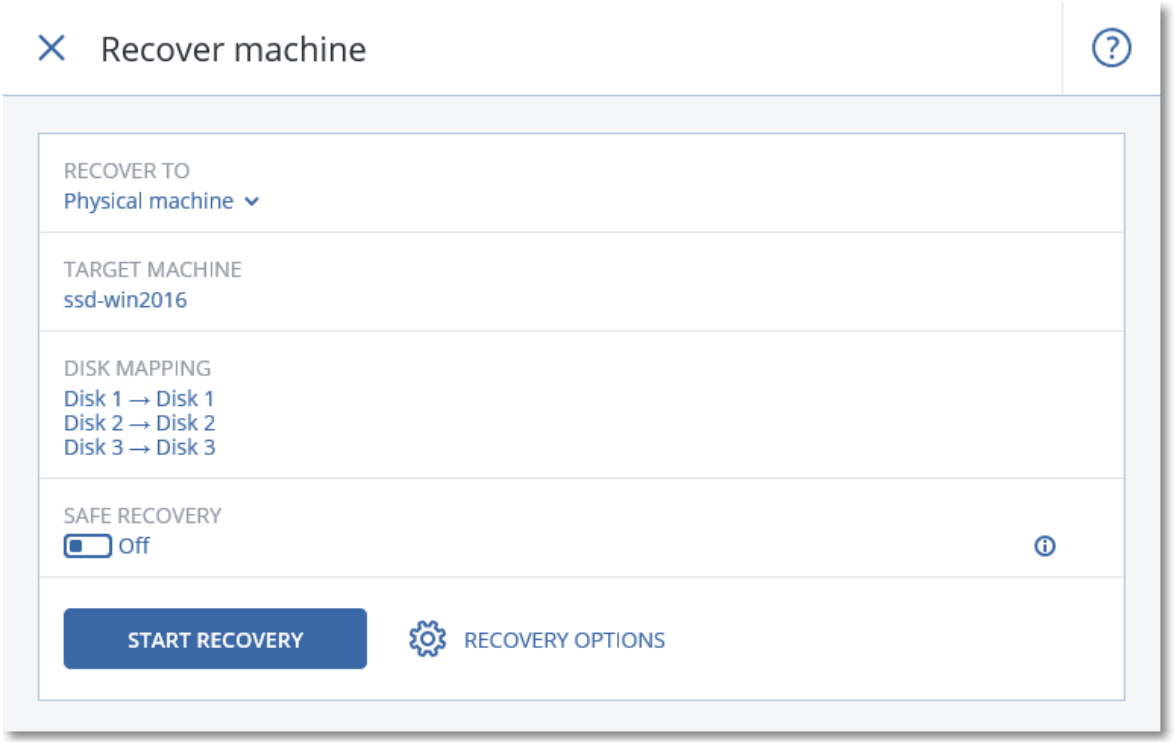
1. 选择已备份的计算机。
2. 单击**恢复**。
3. 选择恢复点。请注意，恢复点按位置过滤。
   如果计算机处于脱机状态，将不显示恢复点。请执行以下任一操作：
   - 如果备份位置是云或共享存储(即其他代理程序可以访问它)，单击**选择计算机**，选择处于联机状态的目标计算机，然后选择恢复点。

- 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**。

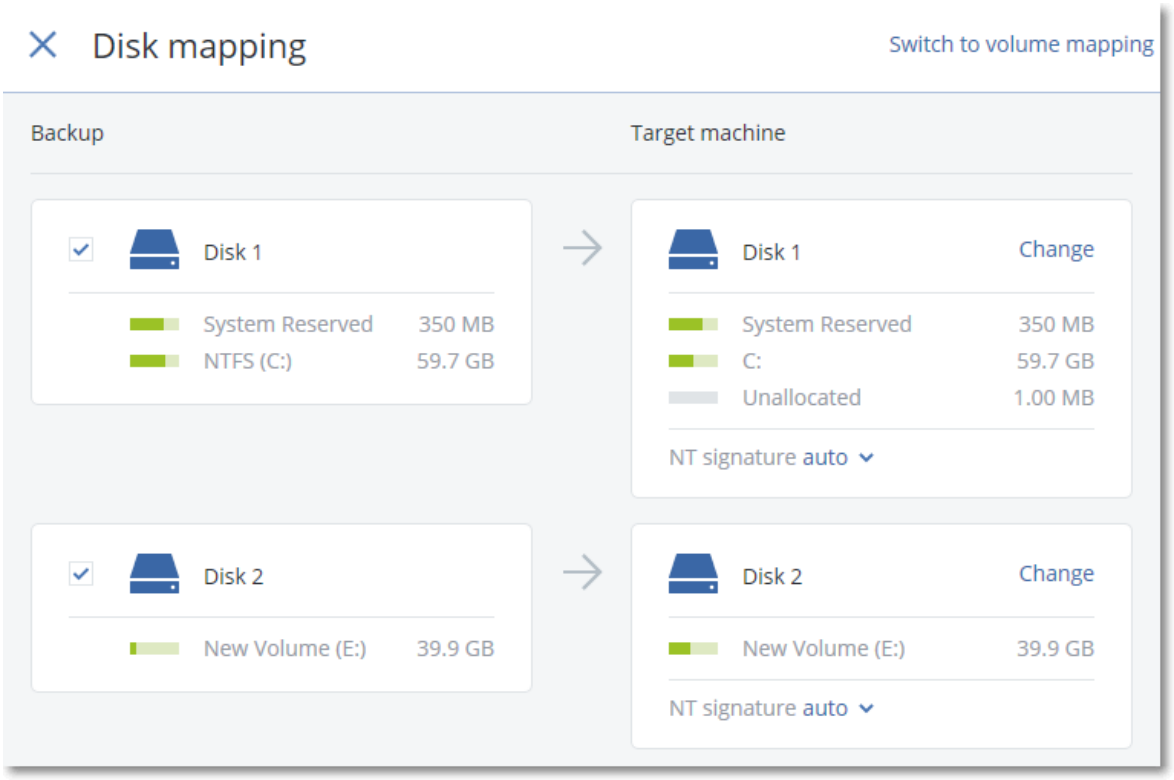
   软件会将磁盘从备份自动映射到目标计算机的磁盘。

   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**卷映射**以手动重新映射磁盘。

   该映射部分也可让您选择个别磁盘或卷进行恢复。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. [仅适用于装有保护代理程序的 Windows 计算机] 启用**安全恢复**开关，以确保恢复后的数据无恶意软件。有关安全恢复如何工作的详细信息，请参阅 "安全恢复"(第 445 页)。
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。

物理机到虚拟机

可以在支持的虚拟机监控程序之一上将物理机恢复至虚拟机。这也是一种将物理机迁移至虚拟机的机制。有关受支持 P2V 迁移路径的详细信息，请参阅“计算机迁移”。

本部分介绍如何使用 Web 界面将物理机恢复为虚拟机。如果在 安克诺斯 管理服务器中安装并注册了至少一个适用于相关虚拟机监控程序的代理程序，则可以执行此操作。例如，恢复至 VMware ESXi 需要至少一个适用于 VMware 的代理程序，恢复至 Hyper-V 需要至少一个适用于 Hyper-V 的代理程序在环境中安装并注册。

对于处于“合规模式”下的租户，无法通过 Web 界面进行恢复。

注意

无法将 macOS 虚拟机恢复为 Hyper-V 主机，因为 Hyper-V 不支持 macOS。可以将 macOS 虚拟机恢复为在 Mac 硬件上安装的 VMware 主机。

此外，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)，单击**选择计算机**，选择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。
   - 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**。
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。

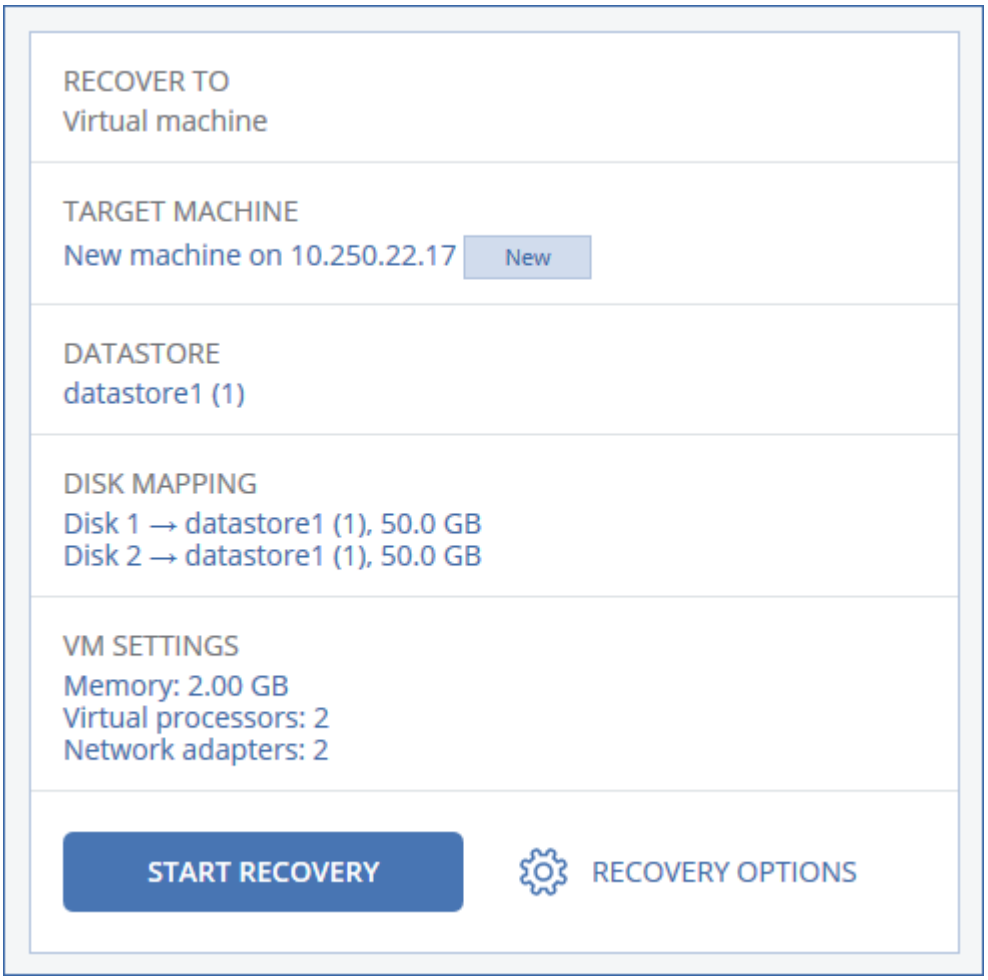
      注意
      必须在 安克诺斯 管理服务器中安装并注册至少一个适用于该虚拟机监控程序的代理程序。

   b. 选择恢复至新计算机还是现有计算机。新计算机选项优先，因为它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。
   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**，以选择**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。

   注意
   对于 Virtuozzo Hybrid Infrastructure，选择规格是必要步骤。

8. [可选] 配置其他恢复选项：
   - [不适用于 Virtuozzo Hybrid Infrastructure] 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(存储)。
   - 单击**磁盘映射**，以为每个虚拟磁盘选择数据存储(存储)、界面和调配模式。该映射部分也可让您选择个别磁盘进行恢复。

     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。
   - [对于 VMware ESXi、Hyper-V 和 Red Hat Virtualization/oVirt] 单击 **VM 设置**以更改虚拟机的内存大小、处理器数量和网络连接。



9. [仅适用于装有保护代理程序的 Windows 计算机] 启用**安全恢复**开关，以确保恢复后的数据无恶意软件。有关安全恢复如何工作的详细信息，请参阅 "安全恢复"(第 445 页)。
10. 单击**开始恢复**。
11. 当恢复至现有虚拟机时，请确认您希望覆盖磁盘。

恢复进度显示在**活动**选项卡上。

恢复虚拟机

可以从虚拟机的备份中恢复它们。

注意
在 Cyber Protect 中控台中，无法为处于合规模式下的租户恢复备份。有关如何恢复此类备份的详细信息，请参阅 "在合规模式下恢复租户的备份"(第 996 页)。

先决条件

- 在恢复至此计算机时，该虚拟机必须处于停止状态。默认情况下，该软件会在无提示的情况下停止计算机运行。当完成恢复时，您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。

步骤

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. 如果您希望恢复至物理机，请在**恢复至**中选择**物理机**。否则，请跳过此步骤。

   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，可以恢复至物理机。

   如果是这种情况，请继续执行“物理机”中的第 4 步。否则，我们建议使用可启动媒体执行 V2P 迁移。
4. [可选] 默认情况下，该软件会自动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（**VMware ESXi**、**Hyper-V**、**Virtuozzo**、**Virtuozzo Hybrid Infrastructure**、**Scale Computing HC3** 或 **oVirt**）。

      仅 Virtuozzo 虚拟机可恢复至 Virtuozzo。有关 V2V 迁移的详细信息，请参阅“计算机迁移”。

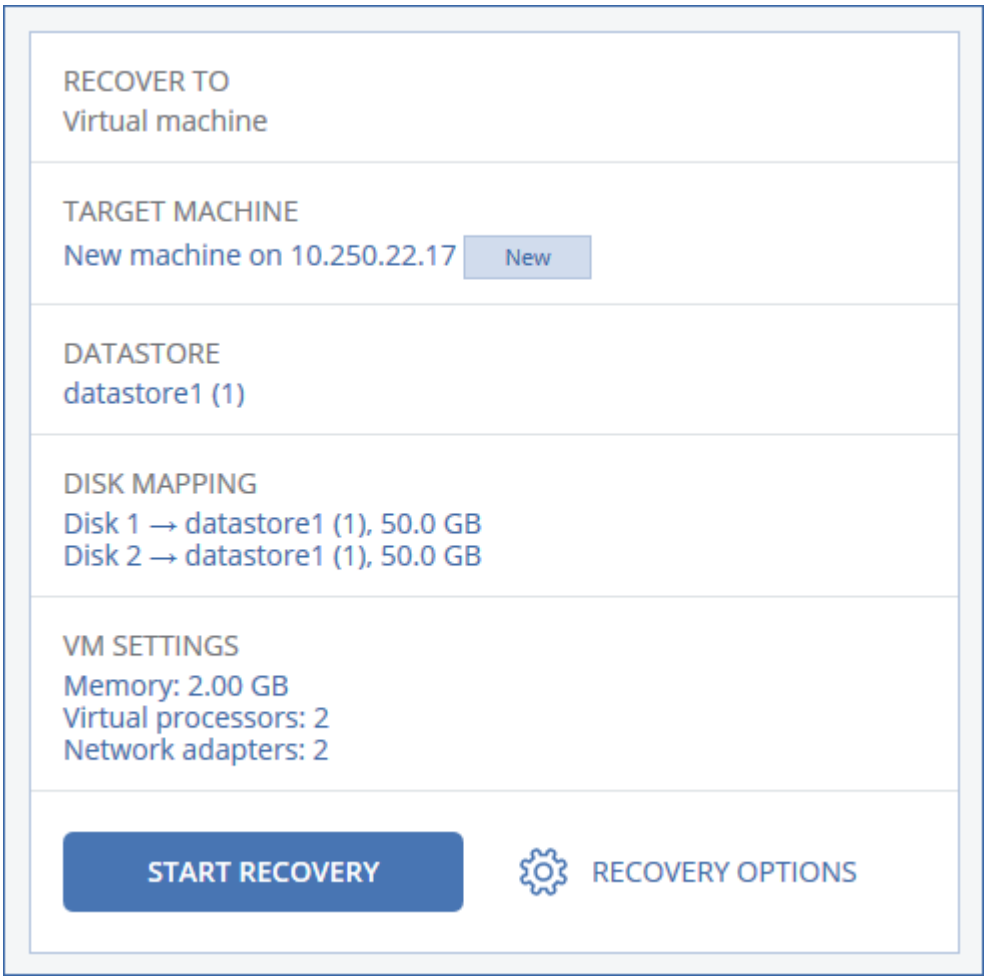
      请注意，当选择 **Microsoft Azure** 作为目标时，可以选择相关的 Azure 订购许可、区域和资源组。
   b. 选择恢复至新计算机还是现有计算机。
   c. 选择主机并指定新计算机名称，或选择现有目标计算机。
   d. 单击**确定**。
5. 设置所需的其他恢复选项。
   - [可选] [不适用于 Virtuozzo Hybrid Infrastructure 和 Scale Computing HC3] 要为虚拟机选择数据存储，请针对 ESXi 单击**数据存储**、针对 Hyper-V 和 Virtuozzo 单击**路径**或针对 Red Hat Virtualization (oVirt) 单击**存储域**，然后为虚拟机选择数据存储（存储）。
   - [可选] 要查看每个虚拟磁盘的数据存储（存储）、接口和调配模式，请单击**磁盘映射**。可以更改这些设置，除非您要恢复 Virtuozzo 容器或 Virtuozzo Hybrid Infrastructure 虚拟机。

     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**。

     该映射部分也可让您选择个别磁盘进行恢复。

     对于 Microsoft Azure，可以通过选择相关存储类型（本地冗余存储 (LRS) 或区域冗余存储 (ZRS)）来更改每个目标磁盘的存储类型。
   - [可选] [可用于 VMware ESXi、Hyper-V 和 Virtuozzo] 要更改虚拟机的内存大小、处理器数量和网络连接，请单击 **VM 设置**。

     [适用于 Microsoft Azure] 若要更改虚拟机的可用性类型和区域、内存大小以及网络连接（包括子网和安全组），请单击 **VM 设置**。
   - [对于 Virtuozzo Hybrid Infrastructure] 要更改虚拟机的内存大小和处理器数量，请选择**规格**。



6. [仅适用于装有保护代理程序的 Windows 计算机] 启用**安全恢复**开关，以确保恢复后的数据无恶意软件。有关安全恢复如何工作的详细信息，请参阅 "安全恢复"(第 445 页)。
7. 单击**开始恢复**。
8. 当恢复至现有虚拟机时，请确认您希望覆盖磁盘。

恢复进度显示在**活动**选项卡上。

重新启动时恢复

Windows 和 Linux 计算机支持重启恢复。

可以选择是否自动重启计算机或将其指定为**需要互动**状态。恢复的操作系统将自动上线。

恢复以下内容时需要重新启动：

- 操作系统

  例如，当恢复整台计算机或计算机的系统卷时。
- 加密卷

  例如，当恢复 BitLocker 加密或 CheckPoint 加密的卷时。

重要事项
已备份的加密卷会恢复为未加密卷。

恢复的计算机会自动准备恢复环境。环境准备就绪后，计算机将重新启动，然后打开恢复环境。恢复完成后，操作系统将启动。

恢复环境

重启恢复使用 Linux 恢复环境。

注意
在具有加密系统卷的计算机上恢复 需要至少一个非加密卷。

磁盘空间要求

恢复环境需要磁盘空间来存放临时文件。具体要求取决于要恢复的计算机。

下表总结了可用的选项。

启动模式	具有非加密系统卷的计算机	具有加密系统卷的计算机
BIOS	系统卷上有 200 MB	未加密卷上有 400 MB
UEFI	EFI 系统分区 (ESP) 上有 200 MB	以下之一： • EFI 系统分区 (ESP) 上有 400 MB • 启动过程中 EFI 系统分区 (ESP) 上有 200 MB，可访问的未加密分区上有 200 MB

限制

- 恢复之前，必须锁定所有加密的非系统卷。可以通过打开位于卷上的文件来锁定卷。如果卷未锁定，则恢复将继续进行而无需重新启动，并且操作系统可能无法识别该卷。
  不需要锁定加密的系统卷。

疑难解答

如果恢复失败，并且重启后显示“无法从分区获取文件”错误，请禁用安全启动。有关更多信息，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

有关如何创建可启动媒体的信息，请参阅 "创建物理可启动媒体"(第 635 页)。

注意
您不能恢复基于 Intel 的 Mac 对使用 Apple Silicon 处理器的 Mac 的磁盘级别备份，反之亦然。您可以恢复文件和文件夹。

使用可启动媒体恢复磁盘

1. 通过使用可启动媒体启动目标计算机。
2. [仅在恢复 Mac 时] 如果您要将 APFS 格式的磁盘/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. 擦除目标磁盘并将其格式化为 APFS。有关说明，请参阅 https://support.apple.com/en-us/HT208496#erasedisk。
   c. 重新创建原始磁盘配置。有关说明，请参阅 https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15。
   d. 依次单击**磁盘实用工具 > 退出磁盘实用工具**。
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. 如果在网络中启用了代理服务器，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、端口和凭据。否则，请跳过此步骤。
5. [可选] 当恢复 Windows 或 Linux 时，请依次单击**工具 > 在 Cyber Protection 服务中注册媒体**，然后指定在下载该媒体时获得的注册标记。如果这样做，将无需按照步骤 8 中所述输入凭据或注册码来访问云存储。
6. 在欢迎屏幕上，单击**恢复**。
7. 单击**选择数据**，然后单击**浏览**。
8. 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。
     在恢复 Windows 或 Linux 时，可以选择请求注册码，用它来代替凭据。依次单击**使用注册码 > 请求代码**。软件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。注册码在一个小时内有效。
   - 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。
   - 要从公共云存储（例如 Microsoft Azure、Amazon S3、Wasabi 或 S3 兼容）上的备份位置进行恢复，请首先单击**“注册媒体”Cyber Protection 服务**，然后使用 Web 界面配置恢复。有关通过 Web 界面远程管理媒体的更多信息，请参阅 "通过可启动媒体进行的远程操作"（第 650 页）。

   单击**确定**确认您的选择。
9. 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。
10. 在**备份内容**中，选择要恢复的磁盘。单击**确定**确认您的选择。
11. 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。

12. [当恢复 Linux 时] 如果备份计算机具有逻辑卷 (LVM) 并且您希望重新生成原始 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。

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 Universal Restore

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 Universal Restore 工具更新对于操作系统启动至关重要的驱动程序和模块。

Universal Restore 适用于 Windows 和 Linux。

应用 Universal Restore

1. 从可启动媒体启动计算机。
2. 单击**应用 Universal Restore**。
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 Universal Restore 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 Universal Restore

准备

准备驱动程序

在将 Universal Restore 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 Universal Restore 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。

Universal Restore 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，Universal Restore 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。

Universal Restore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。Universal Restore 还会搜索网络适配器驱动程序；然后 Universal Restore 会将所发现驱动程序的路径传输给操作系统。如果硬件具有多个网络接口卡，Universal Restore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。

Universal Restore 流程

在指定所需的设置后，单击**确定**。

如果 Universal Restore 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 Universal Restore。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 Universal Restore

Universal Restore 可应用到内核版本为 2.6.8 或更高版本的 Linux 操作系统。

当 Universal Restore 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。

Universal Restore 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 Universal Restore 未能找到所需的模块,它会将模块的文件名记录到日志中。

Universal Restore 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。

Universal Restore 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 Universal Restore 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

在 Cyber Protect 中控台中恢复文件

注意
在 Cyber Protect 中控台中,无法为处于合规模式下的租户恢复备份。有关如何恢复此类备份的详细信息,请参阅 "在合规模式下恢复租户的备份"(第 996 页)。

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. 浏览到所需文件夹,或使用搜索栏获取所需文件和文件夹的列表。
   搜索与语言无关。
   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 掩码。

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。
   您的选择包含了文件夹或所选文件的总大小超过了 100 MB，则下载不可用。要从云中检索大量数据，请使用步骤 "从云存储下载文件"(第 458 页)。
8. 单击**恢复**。
   在**恢复到**中，单击以选择恢复操作的目标，或保留默认目标。默认目标会因备份源而异。
   以下目标可用：
   - 源计算机(如果保护代理程序已在其上安装)。
     这是最初包含要恢复的文件的计算机。
   - 已安装保护代理程序的其他计算机 - 已安装保护代理程序的物理机、虚拟机和虚拟化主机，或虚拟设备。
     可以将文件恢复到已安装保护代理程序的物理机、虚拟机和虚拟化主机。无法将文件恢复到未安装保护代理程序的虚拟机(Virtuozzo 虚拟机除外)。
   - Virtuozzo 容器或虚拟机。
     可以将文件恢复到 Virtuozzo 容器和虚拟机，但有一些限制。有关它们的详细信息，请参阅 "在 Cyber Protect 中控台中恢复文件的限制"(第 462 页)。
9. 在**路径**中，选择恢复目标位置。可选择以下其中一个选项：
   - [恢复到原始计算机时] 原始位置。
   - 目标计算机上的本地文件夹或本地连接的存储。

     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。
     例如，从 Microsoft Azure 虚拟机恢复文件时，虚拟机上部署的 Agent for Azure 必须可以访问网络文件夹。
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

在 Web 中控台中，您可以浏览云存储，查看备份的内容，并下载备份的文件和文件夹。

注意
仅当您是客户 Cyber Protection 管理员或客户租户用户时才可以访问 Web Restore 中控台。不允许使用合作伙伴级别的用户角色。

限制

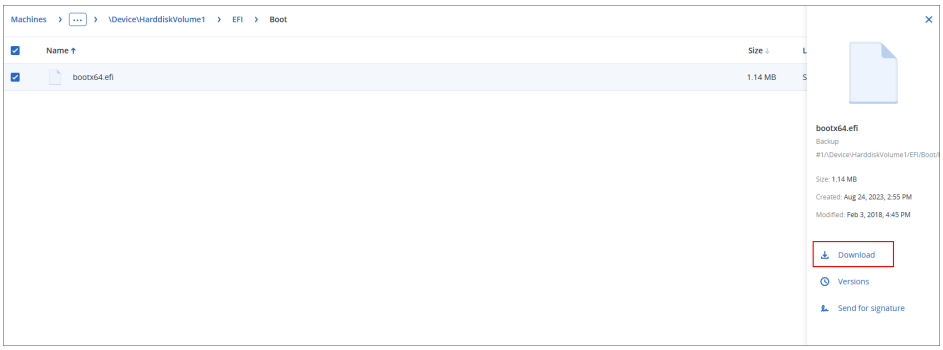
- 您无法下载备份的磁盘、卷或整个恢复点。
- 当您浏览磁盘级别备份时，不会显示逻辑卷(例如 LVM 和 LDM)。
- 您无法浏览系统状态、SQL 数据库和 Exchange 数据库的备份。

从云存储下载文件和文件夹

1. 在 Cyber Protection 中控台中，选择所需的工作负载，然后点击**恢复**。
2. [如果有多个备份位置可用]选择备份位置，然后点击**更多恢复方式**。
3. 点击**下载文件**。
4. 在**计算机**下，点击工作负载名称，然后点击备份存档。
   备份存档包含一个或多个备份(恢复点)。
5. 点击您想要下载文件或文件夹的备份号码(恢复点)，然后导航到所需的项目。
6. 选中您要下载的项目旁边的复选框。

   注意
   如果您选择多个项目，它们将作为 ZIP 文件下载。

7. 单击**下载**。



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

注意
该功能随 Advanced Backup 包提供。

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. 如果在网络中启用了代理服务器，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、端口和凭据。否则，请跳过此步骤。
4. [可选] 当恢复 Windows 或 Linux 时，请依次单击**工具** > **在 Cyber Protection 服务中注册媒体**，然后指定在下载该媒体时获得的注册标记。如果这样做，将无需按照步骤 7 中所述输入凭据或注册码来访问云存储。
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。

     在恢复 Windows 或 Linux 时，可以选择请求注册码，用它来代替凭据。依次单击**使用注册码** > **请求代码**。软件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。注册码在一个小时内有效。
   - 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。
   - 要从公共云存储（例如 Microsoft Azure、Amazon S3、Wasabi 或 S3 兼容）上的备份位置进行恢复，请首先单击**“注册媒体”Cyber Protection 服务**，然后使用 Web 界面配置恢复。有关通过 Web 界面远程管理媒体的更多信息，请参阅 "通过可启动媒体进行的远程操作"（第 650 页）。

   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**文件夹/文件**。
10. 选择要恢复的数据。单击**确定**确认您的选择。
11. 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。

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。

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。
- 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+。

先决条件

- 保护代理程序必须安装在浏览备份的计算机上。
- 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。

在 Cyber Protect 中控台中恢复文件的限制

合规模式下的租户

在 Cyber Protect 中控台中，无法为处于合规模式下的租户恢复备份。有关如何恢复此类备份的详细信息，请参阅 "在合规模式下恢复租户的备份"(第 996 页)。

恢复到 Virtuozzo 容器或 Virtuozzo 虚拟机

- QEMU 来宾代理程序必须安装在目标虚拟机上。
- [仅适用于恢复到容器] 容器内的加载点不能用作恢复的目标。例如，无法将文件恢复到第二个硬盘或加载到容器的 NFS 共享。
- 将文件恢复到 Windows 虚拟机时，如果 "文件级安全性"(第 467 页) 恢复选项已启用，则存档位属性会设置为恢复的文件。
- 在运行 Windows Server 2012 或更旧版本的计算机上和运行 Windows 7 或更旧版本的计算机上，名称中带有非 ANSI 字符的文件恢复后的名称不正确。

- 要将文件恢复到在 Virtuozzo Hybrid Server 上运行的 CentOS 或 Red Hat Enterprise Linux 虚拟机，必须编辑 qemu-ga 文件，如下所示：
  - 在目标虚拟机上，导航到 /etc/sysconfig/，然后打开 qemu-ga 文件以进行编辑。
  - 导航到以下行，然后删除等号 (=) 之后的所有内容：

    ```
    BLACKLIST_RPC=
    ```

  - 通过运行以下命令来重新启动 QEMU 来宾代理程序：

    ```
    systemctl restart qemu-guest-agent
    ```

恢复系统状态

注意
在 Cyber Protect 中控台中，无法为处于合规模式下的租户恢复备份。有关如何恢复此类备份的详细信息，请参阅 "在合规模式下恢复租户的备份"(第 996 页)。

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，请参阅 "创建物理可启动媒体"(第 635 页)。

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、oVirt 和 Virtuozzo**	**Azure**	**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	-	-	-	+	+	+	+	-	-	-
文件级安	-	-	-	+	-	-	-	-	-	-

全性										
Flashback	+	+	+	-	-	-	-	+	-	-
完整路径恢复	-	-	-	+	+	+	+	-	-	-
加载点	-	-	-	+	-	-	-	-	-	-
性能	+	+	-	+	+	+	-	+	-	+
预/后命令	+	+	-	+	+	+	-	+	-	+
SID 更改	+	-	-	-	-	-	-	-	-	-
VM 电源管理	-	-	-	-	-	-	-	+	+	-
Windows 事件日志	+	-	-	+	-	-	-	仅 Hyper-V	-	+

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**。

有关通过校验和验证进行验证的详细信息，请参阅 "校验和验证"(第 203 页) 。

注意
根据服务提供商所选择的设置，备份到云存储时可能无法使用进行验证。

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)。

忽略错误

此选项对文件级恢复有效。

预设为：**已启用**。

当此选项启用且文件恢复失败时，将继续为其余文件执行恢复操作。在**活动**屏幕上显示警告。不会触发选项**如果发生错误，则重新尝试**，因为未记录错误。

当禁用此选项且文件恢复失败时，恢复操作将失败。在**活动**屏幕上将显示错误。

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。

仅当正在恢复的磁盘的卷布局与目标磁盘的卷布局完全匹配时，此选项才有效。

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。这将加速恢复物理机和虚拟机。数据在块级别上进行比较。

恢复物理机时，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。

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、适用于 Scale Computing HC3 的代理程序或适用于 oVirt 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、Agent for Azure、适用于 Hyper-V 的代理程序、适用于 Virtuozzo 的代理程序、适用于 Scale Computing HC3 的代理程序或适用于 oVirt 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**。

与备份有关的操作

备份存储选项卡

备份存储选项卡提供对所有备份(包括脱机计算机的备份、不再注册在 Cyber Protection 服务中计算机的备份、到 Microsoft Azure 等公共云的备份和孤立的备份[1])的访问权限。

通过acrocmd创建的备份被标记为无主备份。在产品的 12.5 版本中创建的备份也标识为无主备份。

注意
请注意,无主备份也会被收费。

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。

管理员可以通过选择属于给定单位或公司及其子组的任何帐户的云存储,来代表该帐户查看云备份。要选择要用于从云中获取数据的设备,请在**要浏览的计算机**行中单击**更改**。**备份存储**选项卡会显示曾注册在选定帐户下的所有计算机的备份。

由适用于 Microsoft 365 的云代理程序创建的备份和 Google Workspace 数据的备份不显示在**云存储**位置,而是显示在名为**云应用程序备份**的单独部分中。

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。

如果您已使用文件管理器添加或删除某些备份,单击位置名称旁边的齿轮图标,然后单击**刷新**。

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,建议您使用备份复制,而不是手动移动备份文件。

如果从服务中删除所有曾备份到相应位置的计算机,则备份位置(云存储除外)将从**备份存储**选项卡中消失。这可确保您无需为存储在此位置的备份支付费用。只要发生到此位置的备份,就会重新添加该位置以及存储在其中的所有备份。

在**备份存储**选项卡上,可以使用以下条件过滤列表中的备份:

- **仅限取证数据** - 将仅显示具有取证数据的备份。
- **仅修补程序管理创建的更新前备份** - 将仅显示在修补程序安装之前运行的修补程序管理过程中创建的备份。

使用"备份存储"选项卡选择恢复点

[1]孤立的备份是一个不再与保护计划关联的备份。

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。

添加备份位置

注意
仅当代理程序处于联机状态时，才可执行此操作。

在**备份存储**选项卡上，单击**添加位置**。

从以下其中一个位置类型中选择一个位置，然后单击**完成**：

- 本地文件夹
- 网络文件夹
- 安全区
- NFS 文件夹
- 公有云

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。这将允许访问数据库，直到出现故障的计算机恢复。此方法还可用于使用 SharePoint 资源管理器粒度恢复 Microsoft SharePoint 数据。
- 脱机病毒删除

  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，请通过此备份恢复系统。

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。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，然后选择以下选项之一：
   a. **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。

   b. **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. [可选] 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。

正在验证备份

可以验证备份以确认是否可以恢复数据。有关此操作的详细信息，请参阅 "验证"(第 201 页)。

注意
此功能适用于将**Advanced Backup – 服务器**或**Advanced Backup – NAS** 配额作为 Advanced Backup 包的一部分启用的客户租户。

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 471 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

导出操作会在指定的位置创建一个备份的自足副本。原始备份保持原样不变。借助导出操作，可以将特定备份与增量备份和差异备份链分离，以便实现快速恢复、写入到可移动媒体或可卸除媒体或者用于其他用途。

注意
此功能适用于将**Advanced Backup – 服务器**或**Advanced Backup – NAS** 配额作为 Advanced Backup 包的一部分启用的客户租户。

导出操作的结果始终是完整备份。如果要将整个备份链复制到其他位置并保留多个恢复点，请使用备份复制计划。有关此计划的详细信息，请参阅 "备份复制"(第 199 页)。

导出的备份的备份文件名与原始备份的备份文件名相同，只是序号不同。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。

导出的备份继承原始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 471 页)。
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

备份存档包含一个或多个备份。您可以删除整个存档或存档中的特定备份(恢复点)。

删除备份存档会删除其中的所有备份。删除工作负载的所有备份也会删除包含这些备份的备份存档。

您可以使用 Cyber Protect 中控台在**"设备"**选项卡和**"备份存储"**选项卡上删除备份。此外，还可以使用 Web Restore 中控台从云存储中删除备份。

警告！
如果禁用不可变存储，备份的数据将被永久删除且无法恢复。

删除备份或备份存档

在设备选项卡上

此过程仅适用于在线工作负载。

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 选择要删除的工作负载备份。
3. 单击**恢复**。
4. [如果有多个备份位置可用]选择备份位置。
5. [删除工作负载的所有备份]单击**全部删除**。

   删除所有备份也会删除包含这些备份的备份存档。
6. [删除特定备份]选择要删除的备份(恢复点)，然后单击**操作**>**删除**。
7. [删除所有备份时]选中该复选框，然后单击**删除**以确认您的决定。
8. [删除特定备份时]单击**删除**以确认您的决定。

在备份存储选项卡上

此过程适用于在线和离线工作负载。

1. 在 Cyber Protect 中控台中，转到**备份存储**。
2. 选择要从中删除备份的位置。
3. 选择要从中删除备份的备份存档。

   存档名称使用以下模板：
   - 非云到云备份档案：<工作负载名称> - <保护计划名称>
   - 云到云备份存档：<用户名>或<驱动器名称>或<团队名称> - <云服务> - <保护计划名称>
4. [删除整个备份存档] 单击**删除**。

   删除备份存档会删除该存档中的所有备份。
5. [删除备份存档中的特定备份] 单击**显示备份**。

   a. 选择要删除的备份（恢复点）。

   b. 单击**操作**>**删除**。
6. [删除备份存档时] 选中该复选框，然后单击**删除**以确认您的决定。
7. [删除特定备份时] 单击**删除**以确认您的决定。

在 Web 恢复中控台中

此过程仅适用于云存储中的备份存档。

1. 在 Cyber Protection 中控台中，转到**设备** > **所有设备**。
2. 选择要删除的工作负载备份，然后单击**"恢复"**。
3. [如果有多个备份位置可用] 选择备份位置，然后点击**更多恢复方式**。
4. 点击**下载文件**。

   您将重定向到 Web Restore 中控台。
5. 在 Web Restore 中控台的**"计算机"**下，单击工作负载名称。
6. 在**"上一个版本"**下，单击日期，然后单击**删除**。

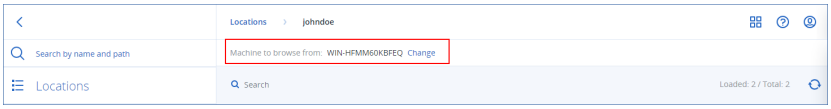
   此操作仅在备份存档级别可用。您将无法深入查看存档并从中删除特定备份。
7. 单击**删除**以确认您的决定。

删除 Cyber Protect 中控台外部的备份

我们建议您使用 Cyber Protect 中控台删除备份。如果您使用 Web Restore 中控台从云存储中删除备份或使用文件管理器删除本地备份，则必须刷新备份位置以将更改同步到 Cyber Protect 中控台。

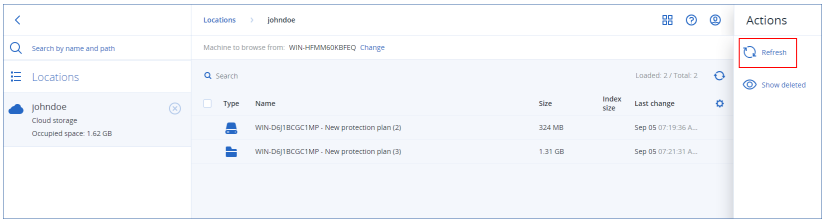
先决条件

- 必须选择可以访问备份位置的在线代理程序作为要从 中控台中**浏览的计算机**。



若要刷新备份位置

1. 在 Cyber Protect 中控台中，转到**备份存储**。
2. 选择存储已删除备份的备份位置。
3. 在**"操作"**窗格中，单击**"刷新"**。



了解瓶颈检测

瓶颈检测功能通过亮显系统中哪个组件在备份或恢复过程中速度最慢，来帮助您了解可以在哪些方面提高性能。

由于瓶颈总是发生在任何传输事件中，因此这并不一定意味着需要解决它们。您的备份可能已经足够快并完全满足备份窗口要求，也满足 SLA 要求，因此通常没有任何需要实际解决的问题。

可以在**活动详细信息**选项卡中，轻松查看和跟踪瓶颈。为此，请在 Cyber Protect 中控台中，转到**监视 > 活动**，然后单击相关活动。有关查看瓶颈的详细信息，请参阅 "查看瓶颈详细信息"(第 478 页)和 "显示有关哪些工作负载、代理程序和备份位置的瓶颈？"(第 480 页)。

什么是瓶颈？

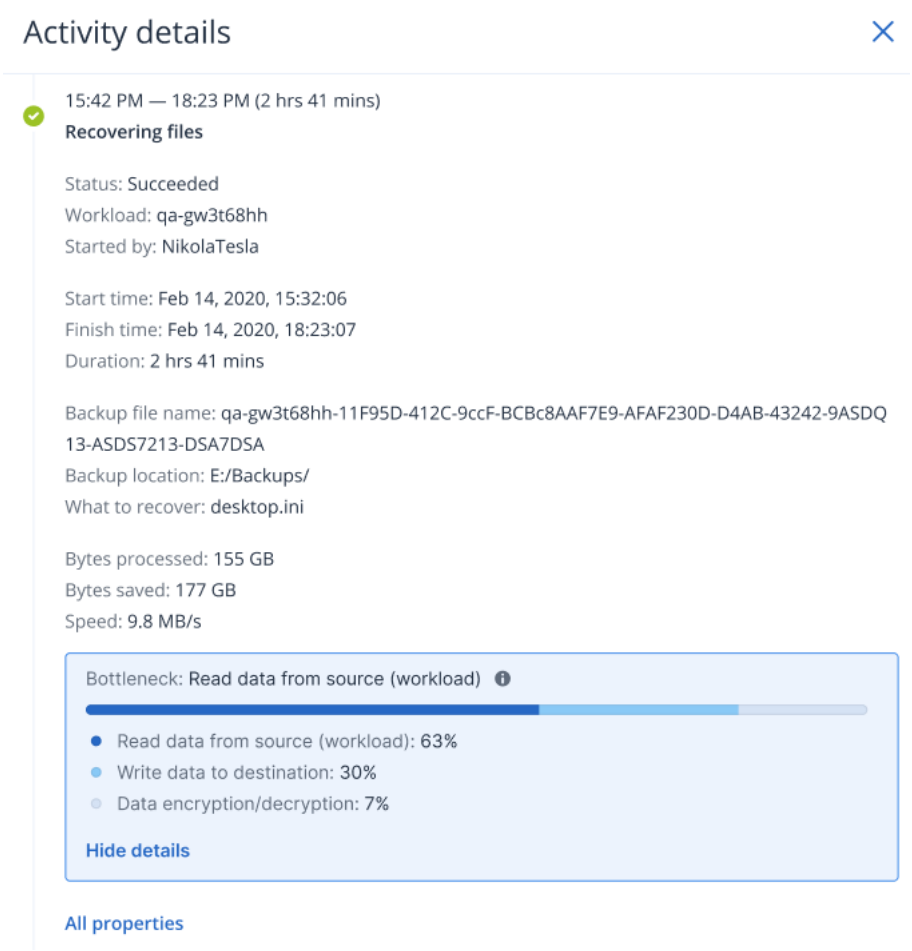
瓶颈通常是因处理链中慢速组件引起的，换句话说，通常是因其他组件等待的组件引起的。

瓶颈检测功能使您能够跟踪备份和恢复过程中的这些慢速组件，从而帮助您了解以下哪种组件类型的速度最慢：

- **源**：可以一目了然地确定备份/恢复源的读取速度是否会导致出现瓶颈。
- **目标**：了解备份/恢复目标的写入速度是否会影响性能。
- **代理程序**：了解代理程序处理数据的速度是否足够快。

瓶颈类型(无论是来自源、目标还是代理程序)可能会在备份/恢复活动的不同时间发生变化。下面**活动详细信息**选项卡的**瓶颈**部分中显示的百分比(例如，**从源(工作负载)读取数据：63%**)，表示遇到此类瓶颈时的时间百分比。在这种情况下，对于 63% 的恢复活动时间，瓶颈类型是读取数据，换句话说，代理程序从备份存档中读取数据的速度较慢。

同样，对于 30% 的时间，瓶颈出现的原因是将数据写入恢复目标的速度较慢(**将数据写入目标：30%**)。



注意

在**活动详细信息**选项卡中查看瓶颈统计信息是正常行为。这些统计信息仅获取自时长超过一分钟的任务。

如何减少瓶颈

如上所述，瓶颈检测功能会亮显备份组件之间的*读取*和*写入*数据流。*读取*统计信息是指从数据源到执行备份/恢复操作的代理程序的数据流，*写入*统计信息是指代理程序和备份存档(目标)之间的数据流。

为了减少瓶颈并提高读/写数据流性能，您应该分析代理程序和数据源/备份存档之间的通道。例如，如果代理程序正在备份一些本地文件，可以尝试对硬盘进行基准测试。

查看瓶颈详细信息

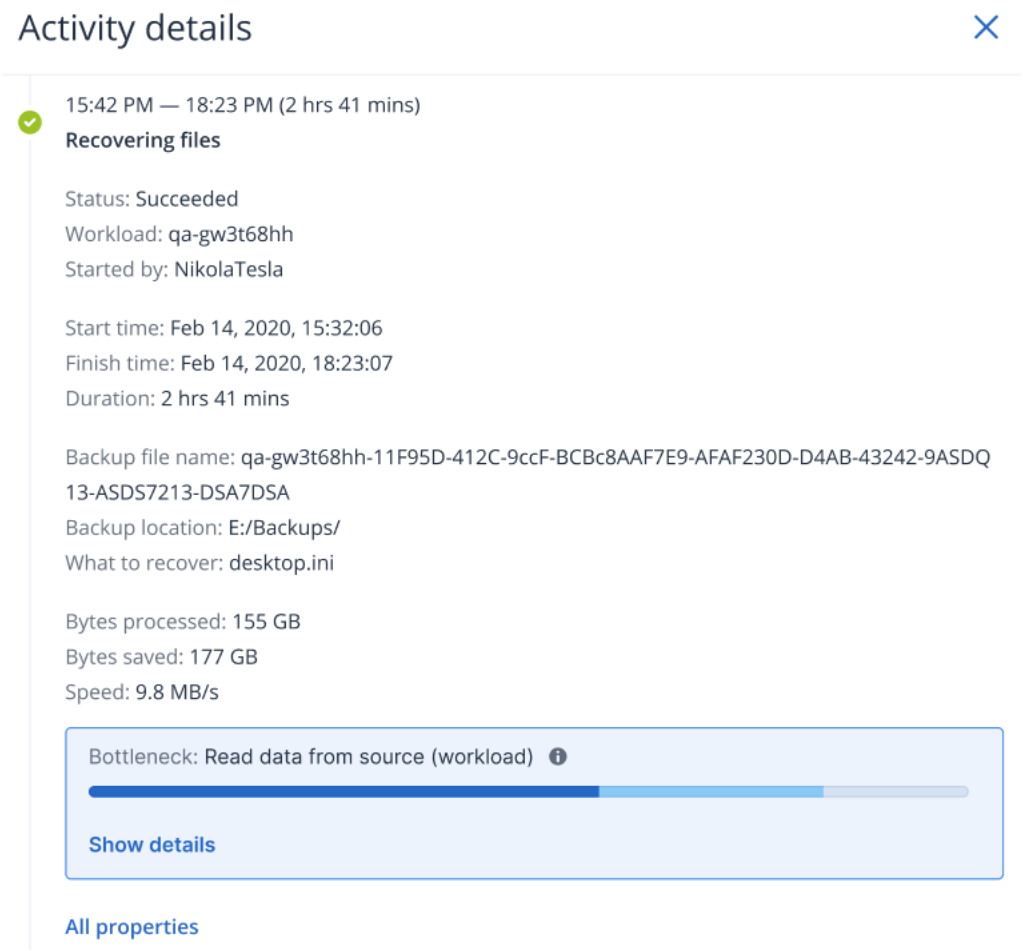
可以查看检测到的任何类型的备份、备份复制或恢复过程(到任何类型的目标文件夹或位置)的瓶颈，包括虚拟机备份、计算机备份和文件/文件夹备份。还可以查看虚拟机复制和故障恢复活动的瓶颈。

有关瓶颈类型的定义和核心概念的详细信息，请参阅 "了解瓶颈检测"(第 477 页)。

查看瓶颈详细信息

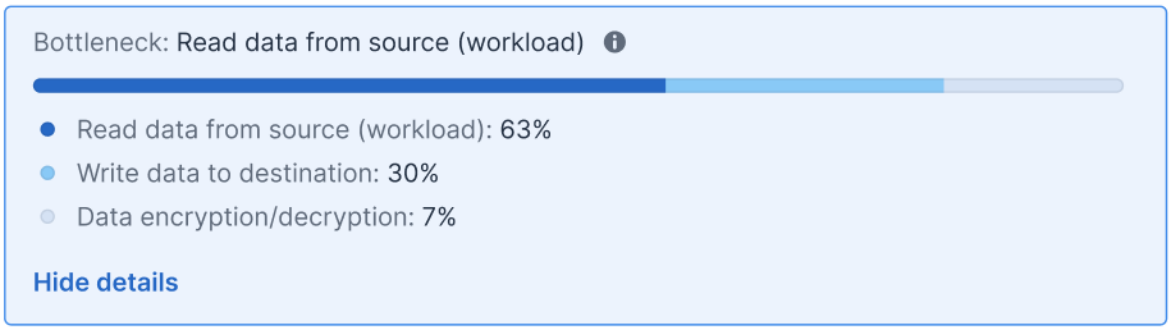
1. 在 Cyber Protect 中控台中，转到**监视 > 活动**。
2. 单击相关活动。

   在**活动详细信息**选项卡中，**瓶颈**部分以蓝色显示。



3. 单击**显示详细信息**，以查看备份/恢复操作过程中最常见的瓶颈。

   瓶颈部分展开以显示相关瓶颈类型的摘要。



   在上面的示例中，占整个操作时间 63% 的瓶颈是由*读取*操作（由代理程序执行）引起的。

注意

当相应活动正在运行时，瓶颈值每分钟动态更新一次。

显示有关哪些工作负载、代理程序和备份位置的瓶颈?

瓶颈检测可用于以下类型的工作负载、代理程序和备份位置:

- 磁盘/映像级备份的执行者:
  - 适用于 Azure 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 VMware 的代理程序(虚拟设备和 Windows, 包括 VM 复制和从副本故障恢复(从副本恢复)活动)
  - 适用于 Hyper-V 的代理程序
  - 适用于 Scale Computing 的代理程序
  - 适用于 oVirt 的代理程序 (KVM)
  - 适用于 Virtuozzo 基础架构平台的代理程序
  - 适用于 Virtuozzo 的代理程序
  - 适用于 VMware Cloud Director 的代理程序 (vCD-BA)
- 文件级备份
  - 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
- 应用程序级备份
  - 适用于 SQL 的代理程序
  - 适用于 Exchange 的代理程序
  - 适用于 MySQL/MariaDB 的代理程序
  - 适用于 Oracle 的代理程序
  - 适用于 SAP HANA 的代理程序
- 备份位置
  - Acronis Cloud 存储(包括合作伙伴托管的存储)
  - 公共云存储
  - 网络共享 (SMB + NFS)
  - 本地文件夹
  - 脚本定义的位置
  - Acronis 安全区

将工作负载备份到公有云

注意

此功能是 “Advanced Backup” 包的一部分, 而该包又是网络安全保护服务的一部分。请注意, 当您将此功能添加到保护计划中时, 可能会收取额外费用。

重要事项
仅在 Windows 7 或更高版本以及 Windows Server 2008 R2 或更高版本上运行的保护代理才可以将工作负载备份到任何受支持的公共云服务。此外，在过时的操作系统（例如 Windows Vista 或 Windows Server 2008 或更低版本）上运行时执行脱离主机数据保护计划的代理程序无法与公共云上的位置配合使用。

您可以选择公有云服务，比如 Microsoft Azure、Amazon S3（简单存储服务）和 Wasabi 作为 Cyber Protect 中控台中的备份目标位置。

要在公共云上配置备份位置，您必须是公司管理员或单位管理员，或者具有在网络安全保护服务中定义的以下角色之一：网络管理员、管理员，或用户。

在 Microsoft Azure 中定义备份位置

注意
若要在 Microsoft Azure 中配置备份位置，您必须具有在网络安全保护服务中定义的以下角色之一：公司管理员、用户、网络安全管理员。

可以在 Microsoft Azure Blob 存储服务上的以下 Microsoft Azure 存储帐户类型之一下定义备份位置：

- 标准通用用途 v2 (StorageV2)
- 高级块 Blob

有关 Microsoft Azure 存储帐户类型的详细信息，请参阅 Microsoft 文档。

要将工作负载备份到 Microsoft Azure，需要在 Cyber Protect 中控台中定义 Microsoft Azure 备份位置，并连接到相关 Microsoft Azure 订购许可。此操作可以通过以下方法完成：

- 当创建或编辑保护计划时。
- 当定义和管理备份存储位置时。

重要事项
管理员和非管理员用户都可以将工作负载备份到 Microsoft Azure。

非管理员用户可以添加对 Microsoft Azure 订购许可的访问权限（请参阅 "管理对 Microsoft Azure 订购许可的访问权限"（第 493 页）），但仅可在备份位置连接到他们添加自身的 Microsoft Azure 订购许可的位置应用保护计划，以及用于在 Cyber Protect 中控台其名称下注册的工作负载。

管理员可以在备份位置连接到他们添加自身的 Microsoft Azure 订购许可的位置应用保护计划，或者应用于由任何其他管理员添加的订购许可，以及用于在 Cyber Protect 中控台任何用户下注册的工作负载。

在 Microsoft Azure 中定义备份位置

1. 在 Cyber Protect 中控台中，请执行以下任一操作：
   - 如果正在创建或编辑保护计划，则转至**设备**并选择想要备份到 Microsoft Azure 的相关工作负载。在选定工作负载的保护计划的**备份**部分中，单击**备份位置**行中的链接。

     有关使用保护计划的更多信息，请参阅 "保护计划和模块"(第 192 页)。
   - 如果您正在管理您的备份存储位置并且想要添加 Microsoft Azure 作为一个新位置，则转至**备份存储**。

     有关管理备份存储位置的详细信息，请参阅 "备份存储选项卡"(第 471 页)。
2. 单击**添加位置**。
3. 从**公共云**下拉列表中，选择 **Microsoft Azure**。
4. 如果相关 Microsoft Azure 订购许可已注册在 Cyber Protect 中控台，则从订购许可列表中选择它。

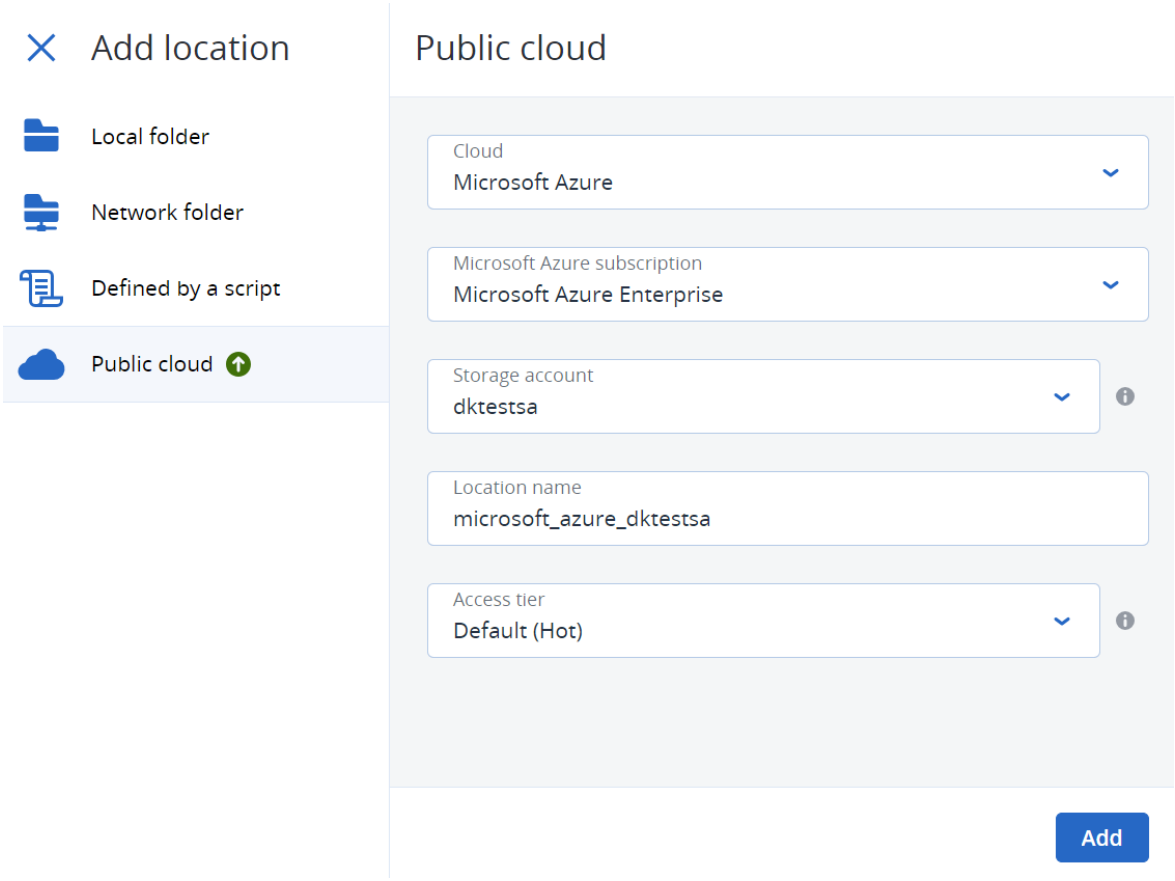
   如果相关订购许可未注册在 Cyber Protect 中控台中，请单击**添加**，然后在显示的对话框中，单击**登录**。系统即会将您重定向到 Microsoft 登录页面。有关添加和定义对 Microsoft Azure 订购许可的访问权限的详细信息，请参阅 "添加对 Microsoft Azure 订购许可的访问权限"(第 493 页)。
5. 在**存储帐户**字段中，选择相关帐户。

   注意
   当前仅支持具有包含 `core.windows.net` 的常规终端后缀的 Microsoft Azure 存储帐户。

   在默认情况下，**位置名称**和**访问层**字段会根据选定的存储帐户自动填充。显示的位置名称是 `microsoft_azure_[storage account]`，选定的访问层是**默认(热)**。这两个字段都可以根据需要进行修改。

   注意
   目前仅支持热和冷访问层(有关访问层的更多信息，请参阅Microsoft 文档)。

   注意
   在更改位置名时，请输入唯一位置名称(该名称必须对客户租户唯一)。如果添加的名称已存在于存储帐户中，则 安克诺斯 会为名称添加后缀数字。例如，如果 **Microsoft Azure Storage** 已存在，则该名称将自动更新为 **Microsoft Azure Storage_01**。



6. 单击**添加**。

   如果正在创建或编辑保护计划，则 Microsoft Azure 备份位置设置为**备份位置**行中的位置。当备份运行时(手动或者预定时)，备份将保存在定义的位置。

   如果您正在管理您的备份存储位置，则可以根据需要查看和更新位置详细信息。当为工作负载定义备份位置时，Microsoft Azure 位置也可用。有关详细信息，请参阅 "查看和更新公共云备份位置"(第 488 页)。

在 Amazon S3 中定义备份位置

注意

若要在 Amazon S3 上配置备份位置，您必须具有在 Cyber Protection 服务中定义的以下角色之一：公司管理员、用户、网络安全管理员。

若要将工作负载备份到 Amazon S3，您必须在 Cyber Protect 中控台定义 Amazon S3 备份位置，然后连接到相关的 Amazon S3 连接。可以通过以下方式执行此操作：

- 当创建或编辑保护计划时。
- 当定义和管理备份存储位置时。

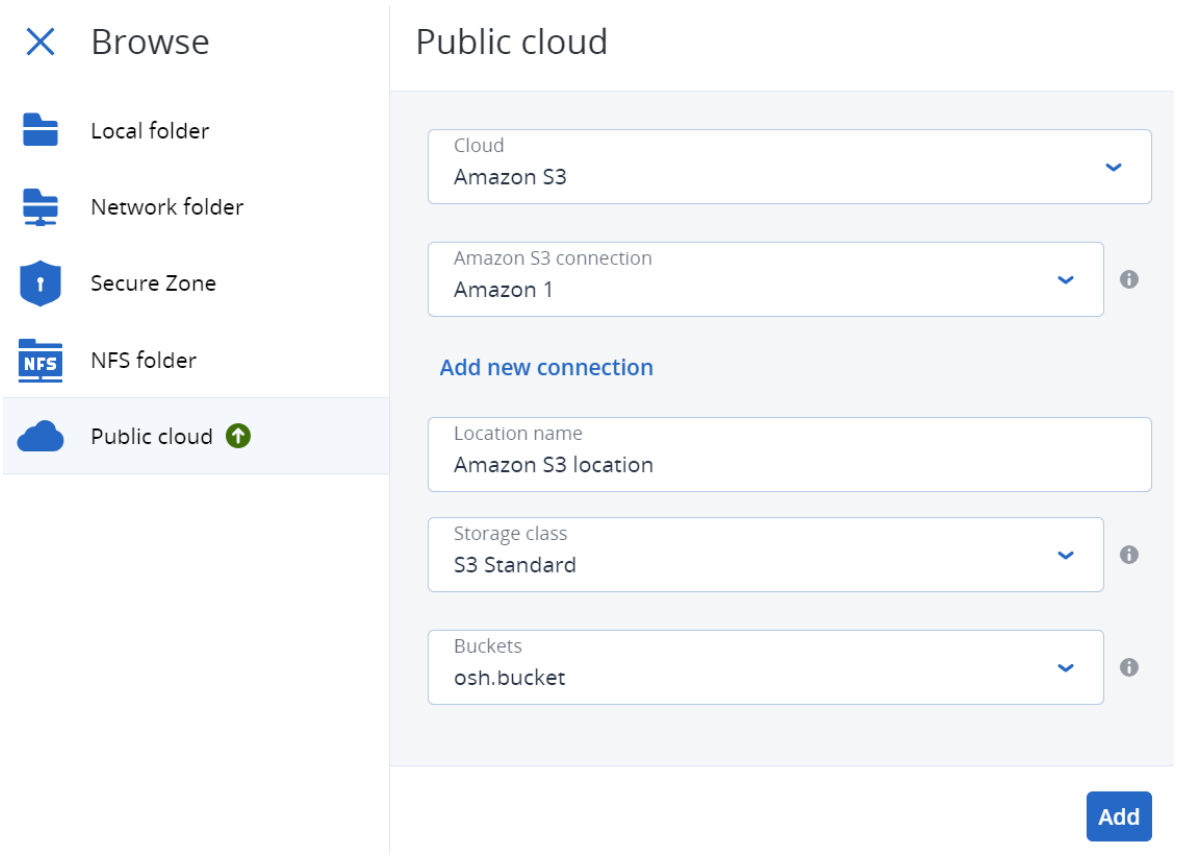
重要事项
管理员和非管理员用户都可以将工作负载备份到 Amazon S3。

非管理员用户可以添加对 Amazon S3 连接的访问权限(请参阅 "管理对其他公共云存储服务的访问"(第 496 页)),但仅可在备份位置连接到他们添加自身的 Amazon S3 连接的位置应用保护计划,以及用于在 Cyber Protect 中控台其名称下注册的工作负载。

管理员可以在备份位置连接到他们添加自身的 Amazon S3 连接的位置应用保护计划,或者应用于由任何其他管理员添加的订购许可,以及用于在 Cyber Protect 中控台任何用户下注册的工作负载。

在 Amazon S3 中定义备份位置

1. 在 Cyber Protect 中控台中,请执行以下任一操作:
   - 如果正在创建或编辑保护计划,则转至**设备**并选择想要备份到 Amazon S3 的工作负载。在选定工作负载的保护计划的**备份**部分中,单击**备份位置**行中的链接。
     有关使用保护计划的更多信息,请参阅 "保护计划和模块"(第 192 页)。
   - 如果您正在管理您的备份存储位置并且想要添加 Amazon S3 作为一个新位置,则转至**备份存储**。
     有关管理备份存储位置的详细信息,请参阅 "备份存储选项卡"(第 471 页)。
2. 单击**添加位置**。
3. 从**公共云**下拉列表中,选择 **Amazon S3**。
4. 如果相关 Amazon S3 连接已注册到 Cyber Protect 中控台,从列表中选择它。
   如果相关连接没有注册到 Cyber Protect 中控台,单击 **添加新连接**。有关添加和定义对 Amazon S3 连接的访问的更多信息,请参阅"添加对公共云连接的访问"(第 496 页)。添加连接后,继续下一步。



5. 定义以下内容：
   - 在**"位置名称"**字段中，输入备份位置的名称。

     注意
     位置名称对于客户租户必须是唯一的。如果添加的名称已存在于连接中，安克诺斯 会为名称添加后缀数字。例如，如果 **Amazon S3 存储**已存在，则名称将自动更新为**Amazon S3 存储 1**。

   - 在**存储类别**字段中，从以下受支持的存储类别之一中进行选择：
     - S3 标准
     - 标准 - 不频繁访问（S3 标准-IA）
     - 一区 - 不频繁访问（S3 一区-IA）
     - S3 智能分层
   - 在**存储桶**字段中，选择相关的 Amazon S3 存储桶。
     如果所选存储桶已启用对象锁定和对象版本控制功能（在 AWS 管理中控台中启用），则会启用 **备份不变性期限（天）**复选框。您可以定义不变性期限的天数，以确保在此期间不会删除备份的数据，并将其应用于 Acronis 创建的所有备份对象。
     请注意，当您将不可变性期限设置为备份位置属性时，将忽略在 AWS 管理中控台中为存储桶定义的默认保留期限。有关"对象锁定"功能和保留期限的详细信息，请参阅 Amazon S3 文档。

注意
版本 24.05 之前的代理程序可以执行备份到 Amazon S3，但只有版本 24.05 或更高版本的代理程序才会将“对象锁定”应用于在 Amazon S3 存储中创建的对象。这意味着只有较新的代理程序才能确认备份位置属性中设置的不可变性期限，并将为所有创建的备份管理此期限。版本 24.05 之前的代理程序将忽略此设置，而默认存储桶“对象锁定”属性（在 AWS 管理中控台或通过 API 中定义）将应用于在 Amazon S3 中创建的对象。

6. 单击**添加**。
   如果正在创建或编辑保护计划，则 Amazon S3 备份位置设置为**备份位置**行中的位置。当备份运行时（手动或者预定时），备份将保存在定义的位置。
   如果您正在管理您的备份存储位置，则可以根据需要查看和更新位置详细信息。当为工作负载定义备份位置时，Amazon S3 位置也可用。有关详细信息，请参阅 "查看和更新公共云备份位置"（第 488 页）。

在 Wasabi、Impossible Cloud 或 S3 兼容存储中定义备份位置

注意
若要在 Wasabi、Impossible Cloud 或 S3 兼容存储中配置备份位置，您必须在 Cyber Protection 服务中定义以下角色之一：公司管理员、用户、网络安全管理员。

若要将工作负载备份到 Wasabi、Impossible Cloud 或 S3 兼容存储，必须在 Cyber Protect 中控台中定义备份位置，并连接到相关的 Wasabi、Impossible Cloud 或 S3 兼容存储连接。可使用以下方法执行此操作：

- 当创建或编辑保护计划时。
- 当定义和管理备份存储位置时。

重要事项
管理员和非管理员用户都可以将工作负载备份到 Wasabi、Impossible Cloud 或 S3 兼容存储。

非管理员用户可以添加对 Wasabi、Impossible Cloud 或 S3 兼容存储连接的访问权限（请参阅 "管理对其他公共云存储服务的访问"（第 496 页）），但仅可在备份位置连接到他们添加自身的 Wasabi、Impossible Cloud 或 S3 兼容存储连接的位置应用保护计划，以及用于在 Cyber Protect 中控台其名称下注册的工作负载。

管理员可以在备份位置连接到他们添加自身的 Wasabi、Impossible Cloud 或 S3 兼容存储连接的位置应用保护计划，或者应用于由任何其他管理员添加的订购许可，以及用于在 Cyber Protect 中控台任何用户下注册的工作负载。

若要在 Wasabi、Impossible Cloud 或 S3 兼容存储中定义备份位置

1. 在 Cyber Protect 中控台中，请执行以下任一操作：
   - 如果正在创建或编辑保护计划，则转至**设备**并选择想要备份到 Wasabi、Impossible Cloud 或 S3 兼容存储的工作负载。在选定工作负载的保护计划的**备份**部分中，单击**备份位置**行中的链

接。

有关使用保护计划的更多信息，请参阅 "保护计划和模块"(第 192 页)。

- 如果您正在管理您的备份存储位置并且想要添加 Wasabi、Impossible Cloud 或 S3 兼容存储作为一个新位置，则转至**备份存储**。

  有关管理备份存储位置的详细信息，请参阅 "备份存储选项卡"(第 471 页)。

2. 单击**添加位置**。
3. 从**公共云**下拉列表中，选择以下条件之一：
   - **Wasabi**
   - **S3 兼容**
   - **Impossible Cloud**
4. 如果相关连接已注册到 Cyber Protect 中控台，从连接列表中选择它。

   如果相关连接没有注册到 Cyber Protect 中控台，单击 **添加新连接**。有关添加和定义对 Wasabi、Impossible Cloud 或 S3 兼容存储连接的访问的更多信息，请参阅 "添加对公共云连接的访问"(第 496 页)。添加连接后，继续下一步。

   重要事项

   Wasabi 上的根用户帐户的访问密钥无法使用，因为根用户无法调用 AssumeRole。应该创建一个单独的非根用户并为该用户生成访问密钥。

5. 定义以下内容：
   - 在**"位置名称"**字段中，输入备份位置的名称。

     注意

     位置名称对于客户租户必须是唯一的。如果添加的名称已存在于连接中，安克诺斯 会为名称添加后缀数字。例如，如果 **Wasabi 存储**已存在，则名称将自动更新为**Wasabi 存储 1**。

   - (仅限 Impossible Cloud) 在**区域**字段中，选择相关区域。
   - 在 **Bucket** 字段中，选择相关的 Wasabi、Impossible Cloud 或 S3 兼容存储桶。

     如果所选存储桶已启用对象锁定和版本控制功能，则会启用 **备份不变性期限(天)** 复选框。您可以定义不变性期限的天数，以确保在此期间不会删除备份的数据，并将其应用于 Acronis 创建的所有备份对象。

     注意

     无法在 Wasabi 上为备份位置设置不可变期。目前仅支持 S3 兼容、Impossible Cloud 和 Amazon S3(请参阅 "在 Amazon S3 中定义备份位置"(第 483 页))类型。

     请注意，当您将不可变性期限设置为备份位置属性时，将忽略为存储桶定义的默认保留期限。有关"对象锁定"功能和保留期限的详细信息，请参阅相关文档。例如，请参阅 Impossible Cloud 文档。

注意
版本 24.06 之前的代理程序可执行备份至 Wasabi、Impossible Cloud 或 S3 兼容存储，但只有版本 24.06 或更高版本的代理程序才会将“对象锁定”应用于在 Wasabi、Impossible Cloud 或 S3 兼容存储中创建的对象。这意味着只有更新的代理程序才能确认备份位置属性中设置的不可变性期限，并将为所有创建的备份管理此期限。版本 24.06 之前的代理程序将忽略此设置，并将默认存储桶“对象锁定”属性应用于在 Wasabi、Impossible Cloud 或 S3 兼容存储中创建的对象。

- (仅适用于 S3 兼容存储) 选择 **允许使用终端的自签名证书 (易受 MITM 攻击，不建议使用)** 复选框，以跳过对证书链的验证，并接受 S3 终端 URL 的自签名证书。
  请注意，此选项仅在创建与 S3 兼容的备份位置时可用，且无法在编辑备份位置时更改。

6. 单击**添加**。
   如果正在创建或编辑保护计划，则 Wasabi、Impossible Cloud 或 S3 兼容存储备份位置设置为**备份位置**行中的位置。当备份运行时(手动或者预定时)，备份将保存在定义的位置。
   如果您正在管理您的备份存储位置，则可以根据需要查看和更新位置详细信息。当为工作负载定义备份位置时，Wasabi、Impossible Cloud 或 S3 兼容存储位置也可用。有关详细信息，请参阅 "查看和更新公共云备份位置"(第 488 页)。

查看和更新公共云备份位置

可以查看和更新在**备份存储**模块中定义的 Microsoft Azure、Amazon S3, 和 Wasabi 备份位置，也可以在创建或编辑保护计划时查看和更新 Microsoft Azure 备份位置。

有关从以下位置删除对 Microsoft Azure 订购许可的访问权限的信息：Cyber Protect 主控台，请参阅 "删除对 Microsoft Azure 订购许可的访问权限"(第 495 页)。有关删除对其他公共云连接的访问的信息，请参阅 "管理对其他公共云存储服务的访问"(第 496 页)。

注意
您无法手动刷新或删除**备份存储**模块中的公共云备份位置。每次备份或恢复操作后，备份位置的内容都会自动更新。

若要查看公共云备份位置

1. 在 Cyber Protect 中控台中，转到**备份存储**。
   备份位置的列表，以及存储容量的详细信息和指派给每个位置的备份数量会一起显示
   有关使用列出的备份位置的详细信息，请参阅 "备份存储选项卡"(第 471 页)。
2. 选择相关位置。
   选定位置的任何当前备份即会列出。
3. (可选) 单击一个备份，可查看该备份的更多详细信息。

更新保护计划中的公共云备份位置

1. 转到相关保护计划，然后选择**编辑**。
2. 单击**备份位置**行中的链接。
3. 从现有备份位置列表中选择，或单击**添加位置**以添加新位置。

如果相关的 Microsoft Azure 订购许可或公共云连接已在 Cyber Protect 中控台中，从显示的列表中选择它。

如果正在添加新的 Microsoft Azure 订购许可，系统会提示您验证 Microsoft 帐户详细信息（请参阅 "添加对 Microsoft Azure 订购许可的访问权限"（第 493 页））。有关连接到 Microsoft Azure 时所需权限的详细信息，请参阅文章 Microsoft Azure 连接安全和审核 (72684)。

管理公共云帐户访问

要在公共云平台中启用 安克诺斯 Cyber Protection 服务，需要配置对相关公共云帐户的访问权限。

例如，使用 Microsoft Azure 时，需要访问 Microsoft Azure 订购许可。一旦添加到 Cyber Protect 中控台，在配置直接备份到 Microsoft Azure 时可以选择订购许可。同样，在使用 Amazon S3 和 Wasabi 时，需要与特定备份相关策略关联的相关访问密钥。

通过 中控台中的**基础架构**菜单，管理对公共云的访问权限。

重要事项

对公共云存储上的备份禁用备份验证，以避免过多的出口流量成本。此外，如果之前删除了公共云上的备份位置，则当前无法将其“重新附加”到相同或不同的客户租户。欲了解更多信息，请联系支持团队。

备份到公共云存储所需的访问要求

直接备份到公共云存储服务时，每个平台都需要考虑许多访问要求：

- Microsoft Azure
- Amazon S3
- S3 兼容存储（包括 Wasabi 和 Impossible Cloud）

备份到 Microsoft Azure

若要连接到 Microsoft Azure 订购许可，必须拥有多项权限。有关它们的详细信息，请参阅文章 Microsoft Azure 连接安全性和审核 (72684)。

注意

必须在 Microsoft Azure AD 中为您指派以下角色之一，才能完成与订购许可的连接：云应用程序管理员、应用程序管理员或全局管理员。还必须为您指派每个选定订购许可的“所有者”角色。

备份到 Amazon S3

当您备份到 Amazon S3 时，定义 Amazon S3 备份位置有几个要求：

- 支持的存储类别
- 策略权限
- 访问密钥
- 存储桶设置

支持的存储类别

目前支持以下 Amazon S3 存储类:

- S3 标准
- 标准 - 不频繁访问(S3 标准-IA)
- 一区 - 不频繁访问(S3 一区-IA)
- S3 智能分层

策略权限

当备份到 Amazon S3 时, 您的 Amazon 账户必须应用最低权限, 以确保 Acronis 可以将相关工作负载备份到 Amazon S3。这意味着相关用户应该有权访问 AWS 管理中控台, 并将相关策略应用于他们指派到的组。

注意
Amazon S3 指定的策略权限可由其他 S3 兼容的存储服务重复使用。有关详细信息, 请参阅 "备份至 S3 兼容存储(包括 Wasabi 和 Impossible Cloud) "(第 491 页) 。

示例

以下示例策略显示了备份和恢复至/自特定存储桶(由 [BUCKETNAME] 指示) 的大范围资源的最小权限集。请注意, * 表示所有资源。

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource":
"arn:aws:s3:::*" }, { "Effect": "Allow", "Action": [ "s3:ListBucket",
"s3:ListBucketVersions" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": "sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject",
"s3:GetObjectVersion", "s3:GetObjectRetention", "s3:PutObjectRetention" ],
"Resource": "arn:aws:s3:::[BUCKETNAME]/*" } ] }
```

以下示例策略显示了帐户中任何存储桶的最低权限。请注意, [BUCKETNAME] 应替换为存储桶的名称。

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource":
"arn:aws:s3:::*" }, { "Effect": "Allow", "Action": [ "s3:ListBucket",
"s3:ListBucketVersions" ], "Resource": "arn:aws:s3:::*" }, { "Effect": "Allow",
"Action": "sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject",
"s3:GetObjectVersion", "s3:GetObjectRetention", "s3:PutObjectRetention" ],
"Resource": "arn:aws:s3:::*" } ] }
```

访问密钥

需要每个 Amazon S3 连接的访问密钥，并在定义 Amazon S3 连接时使用。有关生成访问密钥和访问密钥 ID 的更多信息，请参阅 Amazon S3 文档。

存储桶设置

使用 Amazon S3 存储桶作为备份位置时，请确保存储桶配置为默认设置，包括阻止所有公共访问（默认情况下设置为**On**）。有关使用存储桶的更多信息，请参阅 Amazon S3 文档。

注意

策略权限中的示例包括完整的权限集。如果不需要在存储桶上使用不可变性，可以排除相关权限，例如 `s3:GetBucketObjectLockConfiguration`（用于创建和编辑备份位置）和 `s3:GetObjectRetention`（用于检测减少期间需要更新对象锁）权限。

备份至 S3 兼容存储（包括 Wasabi 和 Impossible Cloud）

当您备份到 S3 兼容存储时，定义备份位置时需要考虑许多要求：

- 策略权限
- 访问密钥
- 存储桶设置

策略权限

当您在 S3 兼容存储中定义备份位置时，请确保相关策略应用于相关组和用户。

注意

Amazon S3 指定的策略权限（请参阅上文）可被其他 S3 兼容的存储服务重用。请注意，`sts:GetFederationToken` 权限仅适用于 Wasabi，不适用于其他 S3 兼容的存储服务。

示例

以下示例策略仅适用于 Wasabi，并显示了在备份和恢复到/从特定存储桶（由 [BUCKETNAME] 指示）时，用于广泛范围资源的最小权限集。请注意，* 表示任何资源。此外，请使用 Wasabi 帐户的 ID 替换 `[ACCOUNTID]`。

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource":
"arn:aws:s3:::*" }, { "Effect": "Allow", "Action": [ "s3:ListBucket",
"s3:ListBucketVersions" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": [ "iam:CreateRole", "iam:AttachRolePolicy",
"sts:GetCallerIdentity", "sts:AssumeRole" ], "Resource": "arn:aws:iam::
[ACCOUNTID]:*" }, { "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject",
"s3:DeleteObject", "s3:GetObjectVersion", "s3:GetObjectRetention",
"s3:PutObjectRetention" ], "Resource": "arn:aws:s3:::[BUCKETNAME]/*" } ] }
```

以下示例策略仅适用于 Wasabi，显示了帐户中任何存储桶的最低权限。

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource": "*"
}, { "Effect": "Allow", "Action": [ "s3:ListBucket", "s3:ListBucketVersions" ],
"Resource": "*" }, { "Effect": "Allow", "Action": [ "iam:CreateRole",
"iam:AttachRolePolicy", "sts:GetCallerIdentity", "sts:AssumeRole" ], "Resource": "*"
}, { "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject",
"s3:DeleteObject", "s3:GetObjectVersion", "s3:GetObjectRetention",
"s3:PutObjectRetention" ], "Resource": "*" } ] }
```

以下示例策略适用于 S3 兼容和 Impossible Cloud 存储，显示了受限权限和受限资源范围。请注意，[BUCKETNAME] 应替换为存储桶的名称。

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource":
"arn:aws:s3:::*" }, { "Effect": "Allow", "Action": [ "s3:ListBucket",
"s3:ListBucketVersions" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject",
"s3:GetObjectVersion", "s3:GetObjectRetention", "s3:PutObjectRetention" ],
"Resource": "arn:aws:s3:::[BUCKETNAME]/*" } ] }
```

以下示例策略适用于 S3 兼容和 Impossible Cloud 存储，显示了帐户中任何存储桶的最低权限。

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [
"s3:ListAllMyBuckets", "s3:GetBucketLocation",
"s3:GetBucketObjectLockConfiguration", "s3:GetBucketVersioning" ], "Resource":
"arn:aws:s3:::*" }, { "Effect": "Allow", "Action": [ "s3:ListBucket",
"s3:ListBucketVersions" ], "Resource": "arn:aws:s3:::*" }, { "Effect": "Allow",
"Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject",
"s3:GetObjectVersion", "s3:GetObjectRetention", "s3:PutObjectRetention" ],
"Resource": "arn:aws:s3:::*" } ] }
```

访问密钥

要求每个 S3 兼容连接都具有访问密钥，并在定义连接时使用。

请注意，Wasabi 上的根用户帐户的访问密钥无法使用，因为根用户无法调用 AssumeRole。应该创建一个单独的非根用户并为该用户生成访问密钥。

有关生成访问密钥和访问密钥 ID 的详细信息，请参阅相关文档。例如，请参阅 Wasabi 文档和 Impossible Cloud 文档。

存储桶设置

使用存储桶作为备份位置时，请确保已使用默认设置配置存善桶。有关使用存储桶的更多信息，请参阅相关文档。例如，请参阅 Wasabi 文档和 Impossible Cloud 文档。

管理对 Microsoft Azure 订购许可的访问权限

通过在 Cyber Protect 中控台中连接到相关 Microsoft Azure 订购许可，可以直接将相关工作负载备份到 Microsoft Azure。

在通过**设备**或**备份存储**菜单创建备份位置时，可以配置与订购许可的连接，如 "在 Microsoft Azure 中定义备份位置"(第 481 页) 中所述。

或者，可以在**公共云**屏幕(转到**基础架构 > 公共云**) 中配置这些 Microsoft Azure 订购许可。在此处，还可以管理您的订购许可，包括续订对订购许可的访问、查看订购许可属性和活动，或删除订购许可。请注意，如果正在部署用于在 Microsoft Azure 虚拟机上运行无代理程序备份的 Agent for Azure，则会显示一个额外的选项卡，可以在其中查看和更新您的部署。有关详细信息，请参阅 "查看和更新已部署的 Agent for Azure"(第 146 页) 。

根据您的已指派用户角色，您可能能够管理组织内其他用户添加的 Microsoft Azure 订购许可。例如，如果您是公司管理员或单位管理员，或者您在网络安全保护服务中已指派有网络安全管理员或管理员角色，则您可以查看和管理其他管理员添加的 Microsoft Azure 订购许可，以及非管理员用户添加的订购许可。非管理员用户只能查看和访问他们添加到 Cyber Protect 中控台中的 Microsoft Azure 订购许可。

注意
合作伙伴可以管理层次结构中低于其级别的客户的 Microsoft Azure 订购许可。但是，当合作伙伴选择**所有客户**时，中控台中的**基础架构**菜单不可用。

重要事项
当连接到 Microsoft Azure 订购许可时，安克诺斯 需要最低权限才能连接到该订购许可。有关所需权限的详细信息，请参阅文章 Microsoft Azure 连接安全和审核 (72684)。

添加对 Microsoft Azure 订购许可的访问权限

通过在 Cyber Protect 中控台中添加 Microsoft Azure 订购许可，安克诺斯 可以安全地访问您的订购许可，并直接将相关工作负载备份到 Microsoft Azure。

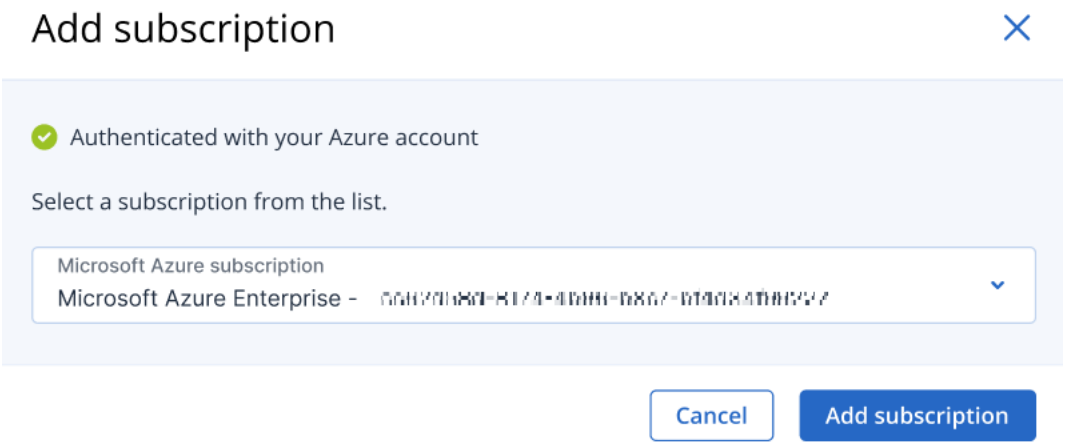
添加对 Microsoft Azure 订购许可的访问权限

1. 在 Cyber Protect 中控台中，转到**基础架构 > 公共云**。
2. 单击**“添加”**，然后从显示的选项列表中选择**“Microsoft Azure”**。
3. 在显示的对话框中，单击**登录**。系统即会将您重定向到 Microsoft 登录页面。

注意
必须在 Microsoft Azure AD 中为您指派以下角色之一，才能完成与订购许可的连接：云应用程序管理员、应用程序管理员或全局管理员。还必须为您指派每个选定订购许可的“所有者”角色。

4. 在 Microsoft 登录屏幕中，输入登录凭据并接受请求的权限。连接过程即会开始，可能需要几分钟时间。

   有关安全访问 Microsoft Azure 和订购许可的详细信息，请参阅文章 Microsoft Azure 连接安全和审核 (72684)。
5. 在连接完成后，从显示的对话框的下拉列表中选择相关订购许可，然后单击**添加订购许可**。



   订购许可即会添加到公共云的列表中。

   要续订订购许可的年度访问证书，请参阅 "续订对 Microsoft Azure 订购许可的访问权限"(第 494 页)。

   要删除对订购许可的访问权限，请参阅 "删除对 Microsoft Azure 订购许可的访问权限"(第 495 页)。

注意
如果您登录到的 Microsoft Azure 帐户包括对多个 Microsoft Azure AD 的访问权限(包括您在其中受邀作为来宾用户的 AD)，则仅默认用户目录处于选中状态。如果要使用您是来宾用户的目录，则需要在该特定 Microsoft Azure AD 中创建一个新用户。然后，可以登录到该帐户并连接到相关订购许可。

续订对 Microsoft Azure 订购许可的访问权限

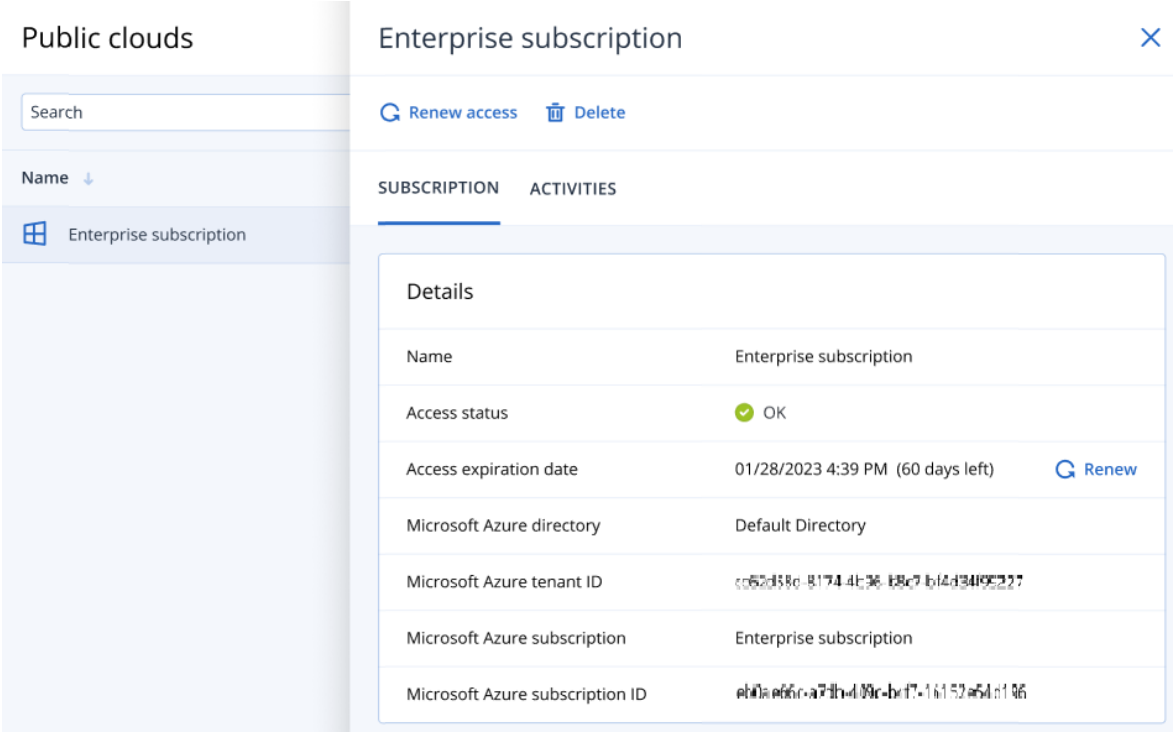
在 Cyber Protect 中控台中注册后，安克诺斯 即会使用免费的唯一访问证书自动设置对 Microsoft Azure 订购许可的一年访问。当证书即将到期时，可以快速轻松地续订该证书。

续订 Microsoft Azure 订购许可的访问凭据

1. 在 Cyber Protect 中控台中，转到**基础架构 > 公共云**。
2. 从显示的列表中选择相关订购许可。

注意
该**访问状态**列指示每个订购许可的访问证书的当前状态，并显示以下两种状态之一：**确定**或**已到期**。

3. 在右侧窗格中，单击**续订访问**。
   或者，单击**订购许可**选项卡，然后单击**访问到期日期**字段中的**续订**。



4. 在 Microsoft 登录屏幕中，输入登录凭据并接受请求的权限。连接过程即会开始，可能需要几分钟时间。
   在身份验证成功后，访问将自动续订一年。
   有关所需权限的详细信息，请参阅文章 Microsoft Azure 连接安全和审核 (72684)。

删除对 Microsoft Azure 订购许可的访问权限

如果您不在将工作负载备份到 Microsoft Azure，则应该删除对 Microsoft Azure 订购许可的访问权限。

删除对 Microsoft Azure 订购许可的访问权限

重要事项
如果订购许可当前正用于备份到 Microsoft Azure，则无法删除该订购许可。

1. 在 Cyber Protect 中控台中，转到**基础架构 > 公共云**。
2. 从显示的列表中选择相关订购许可。
3. 在右侧窗格中，单击**删除**。

注意
您只能删除您添加的订购许可。如果您是公司管理员或单位管理员，或者您在网络安全保护服务中指派有网络安全管理员或管理员角色，则您也可以删除订购许可。

4. 在显示的确认消息中，单击**删除**。

管理对其他公共云存储服务的访问

注意
本部分涉及管理对除 Microsoft Azure 之外的所有公共云存储服务的访问，如 "管理对 Microsoft Azure 订购许可的访问权限"(第 493 页) 中所述。

通过在 Cyber Protect 中控台中连接到相关公共云账号，可以直接将工作负载备份到相关公共云存储中。

通过**设备**或**备份存储**菜单创建备份位置时，可以配置与公共云存储帐户的连接。或者，可以在**公共云**屏幕中配置公共云连接(转至**基础设施 > 公共云**) 。还可以在此处管理连接，包括续订对连接的访问权限、查看连接属性和活动或删除连接。

根据您的已指派用户角色，您可能能够管理组织内其他用户添加的公共云连接。例如，如果您是公司管理员或单位管理员，或者您在网络安全保护服务中已指派有网络安全管理员或管理员角色，则您可以查看和管理其他管理员添加的公共云连接，以及非管理员用户添加的云连接。非管理员用户只能查看和访问他们添加到 Cyber Protect 中控台中的公共云连接。

注意
合作伙伴可以管理层次结构中低于其级别的客户的公共云连接。但是，当合作伙伴选择**"所有客户"**时，**"基础设施"**菜单中的Cyber Protect中控台不可用。

重要事项
连接到公共云连接时，安克诺斯 需要一些权限。有关更多信息，请参阅 "备份到公共云存储所需的访问要求"(第 489 页) 。

添加对公共云连接的访问

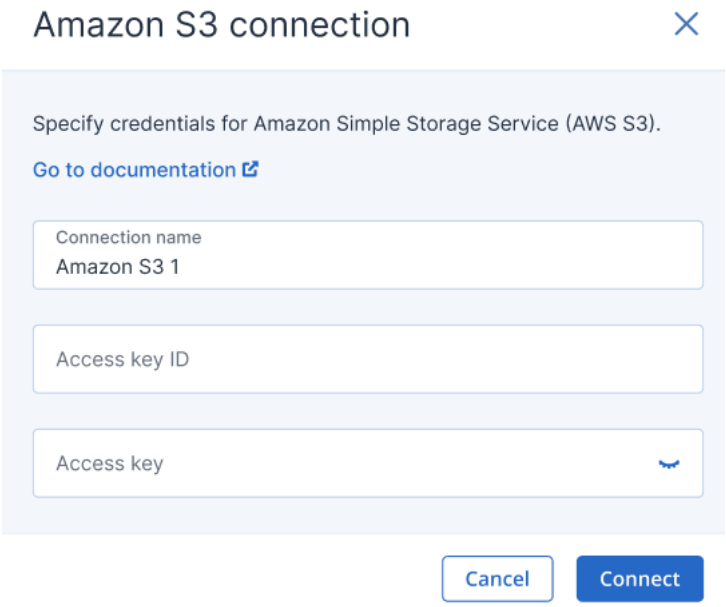
在 Cyber Protect 中控台添加公共云连接(例如 Amazon S3、S3 兼容或 Wasabi) 后，可以安全地访问您的云资源，并将工作负载直接备份到相关的公共云存储。

若要添加对公共云连接的访问

1. 在 Cyber Protect 中控台中，转到**基础架构 > 公共云**。
2. 单击**"添加"**，然后选择以下选项之一：

   Amazon S3
   在显示的对话框中，定义以下内容：
   - **连接名称**：Amazon S3 连接的名称。
   - **访问密钥 ID**：Amazon S3 服务的用户访问密钥 ID。

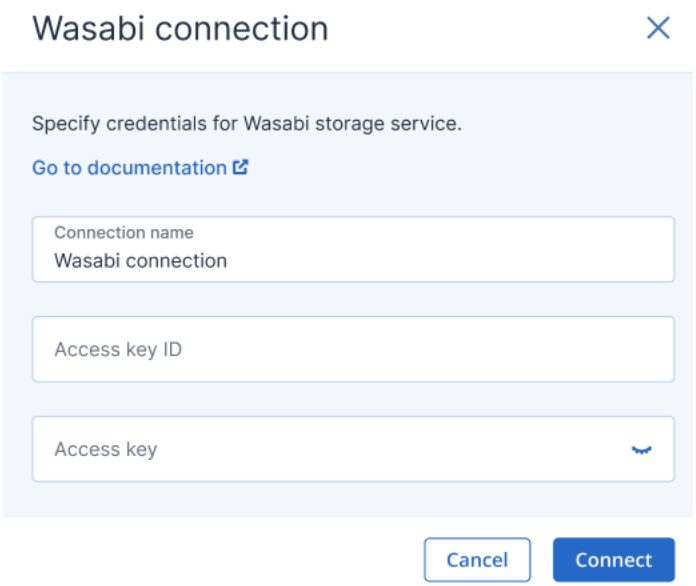
- **访问密钥**：Amazon S3 服务的用户访问密钥。
  访问密钥和访问密钥 ID 会启用对相关连接的存储类和存储桶的访问。有关访问密钥和权限的详细信息，请参阅 "备份到公共云存储所需的访问要求"(第 489 页)。



注意
若要成功访问存储，与 Amazon S3 存储一起执行备份和恢复操作的代理程序上的系统时间必须与 NTP 服务器同步。

Wasabi
在显示的对话框中，定义以下内容：

- **连接名称**：Wasabi 连接的名称。
- **访问密钥 ID**：Wasabi 服务的用户访问密钥 ID。
- **访问密钥**：Wasabi 服务的用户访问密钥。
  访问密钥和访问密钥 ID 会启用对相关连接的存储类和存储桶的访问。有关访问密钥和权限的详细信息，请参阅 "备份到公共云存储所需的访问要求"(第 489 页)。



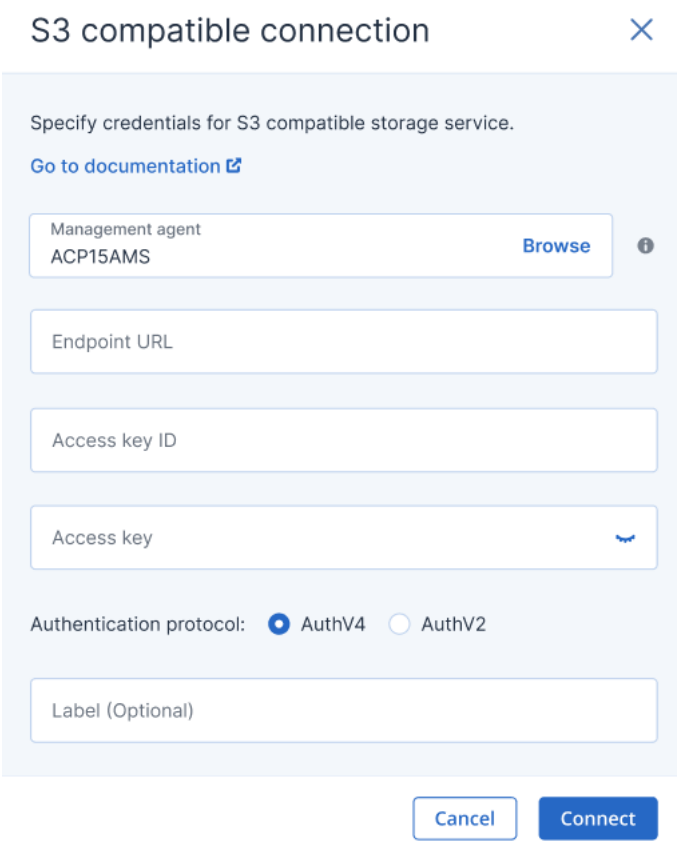
注意
若要成功访问存储，与 Wasabi 存储一起执行备份和恢复操作的代理程序上的系统时间必须与 NTP 服务器同步。

S3 兼容

注意
支持私人托管（指通过 Internet 无法访问）和公开托管的 S3 兼容存储服务。

在显示的对话框中，定义以下内容：

- **管理代理程序**：单击**浏览**以从合适的代理程序列表中选择管理代理程序。此代理程序将与 S3 兼容存储建立初始通信。如果需要，您可以稍后修改备份位置的参数。
  此管理代理程序可从任何受支持的代理程序类型（包括代理程序适用于 Windows/Linux/VMware（虚拟设备）/Hyper-V/oVirt（但不包括代理程序适用于 Azure））中选择，仅会在创建或编辑备份位置时使用。代理程序的脱机/联机状态不会影响其他常规代理程序执行的备份。
- **终端 URL**：请输入 S3 兼容存储供应商共享的终端 URL，以便使用存储执行操作。请注意，此 URL 中指定的终端必须有有效的安全证书链。不允许使用自签名证书连接到终端。
- **访问密钥 ID**：S3 兼容存储的用户访问密钥 ID。
- **访问密钥**：S3 兼容存储的用户访问密钥。
  访问密钥和访问密钥 ID 会启用对相关连接的存储类和存储桶的访问。有关访问密钥和权限的详细信息，请参阅 "备份到公共云存储所需的访问要求"（第 489 页）。
- **身份验证协议**：选择存储侧支持的身份验证协议版本。默认情况下，会选择 **AuthV4**。
- **标签**：（可选）根据需要添加标签。



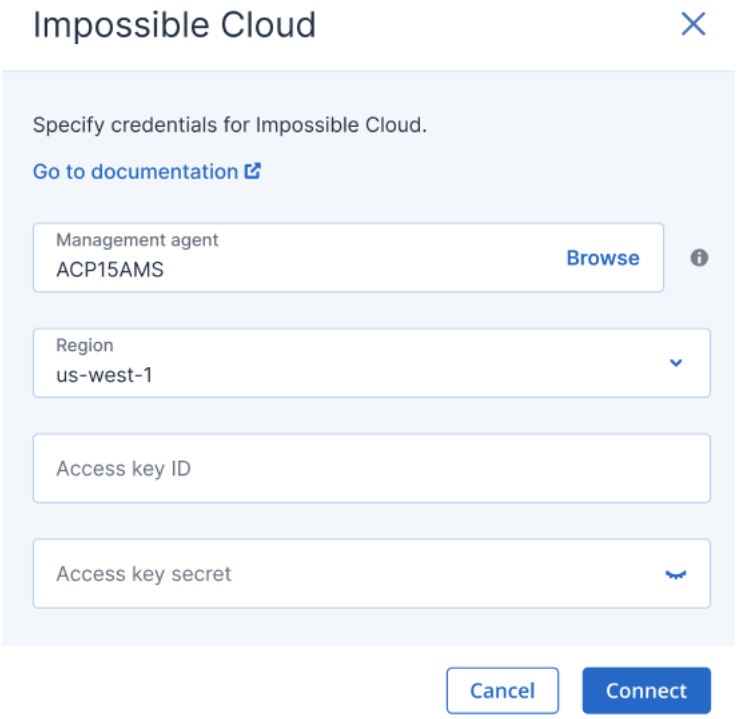
Impossible Cloud

在显示的对话框中，定义以下内容：

- **管理代理程序**：单击**浏览**以从合适的代理程序列表中选择管理代理程序。此代理程序将与 Impossible Cloud 建立初始通信。如果需要，您可以稍后修改备份位置的参数。

  此管理代理程序可从任何受支持的代理程序类型（包括代理程序适用于 Windows/Linux/VMware（虚拟设备）/Hyper-V/oVirt（但不包括代理程序适用于 Azure））中选择，仅会在创建或编辑备份位置时使用。代理程序的脱机/联机状态不会影响其他常规代理程序执行的备份。
- **区域**：选择相关区域。
- **访问密钥 ID**：Impossible Cloud 存储的用户访问密钥 ID。
- **访问密钥**：Impossible Cloud 存储的用户访问密钥。

  访问密钥和访问密钥 ID 会启用对相关连接的存储类和存储桶的访问。有关访问密钥和权限的详细信息，请参阅 "备份到公共云存储所需的访问要求"（第 489 页）。



注意
执行与 Impossible Cloud 存储相关的备份和恢复操作的代理程序上的系统时间必须与 NTP 服务器同步，以便成功访问存储。

3. 单击**连接**。
   连接过程开始，可能需要几分钟时间。完成后，该连接将添加到公共云列表中。
   要续订连接的年度访问证书，请参阅 "续订对公共云连接的访问权限"(第 500 页)。
   要删除对连接的访问，请参阅 "删除对公共云连接的访问"(第 501 页)。

续订对公共云连接的访问权限

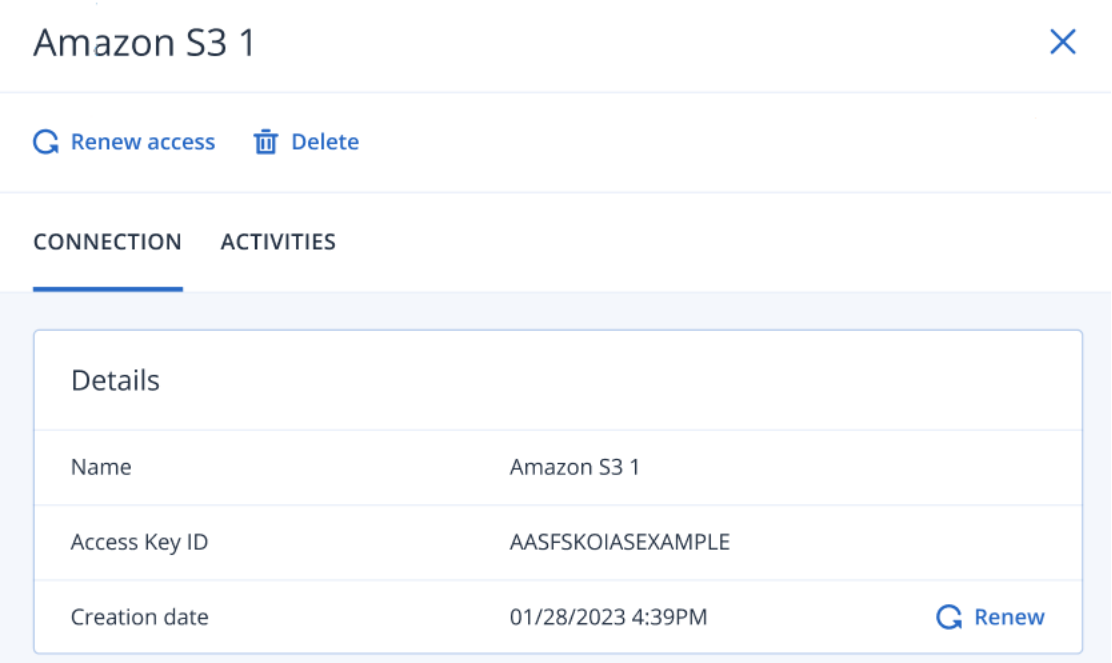
在 Cyber Protect 中控台注册公共云连接后，安克诺斯 会自动指派免费且唯一的访问证书，以允许访问公共云连接。该证书的有效期为一年。当证书接近到期日期时，您可以续订。

若要续订公共云连接的访问证书

1. 在 Cyber Protect 中控台中，转到**基础架构 > 公共云**。
2. 从列表中选择相关连接。

注意
该**访问状态**列指示每个连接的访问证书的当前状态，并显示以下两种状态之一：**确定**或**已到期**。

3. 在右侧窗格中，单击**续订访问**。
   或者，单击**"连接"**选项卡，然后单击**"创建日期"**行中的**"续订"**。



在身份验证成功后，访问将自动续订一年。

删除对公共云连接的访问

如果不将工作负载备份到公共云，则应删除对公共云连接的访问权限。

若要删除对公共云连接的访问

重要事项
如果连接当前用于备份到公共云，则无法删除该连接。

1. 在 Cyber Protect 中控台中，转到**基础架构 > 公共云**。
2. 从列表中选择连接。
3. 在右侧窗格中，单击**删除**。

注意
您只能移除由您添加的连接。如果您是公司管理员或单位管理员，或在网络安全保护服务中指派有网络安全管理员或管理员角色，则也可以移除连接。

4. 在显示的确认消息中，单击**删除**。

电子邮件存档

使用电子邮件存档，Microsoft 365 组织中的所有电子邮件将保留在云中的外部存档中，从而使您能够实现合规性并响应 eDiscovery 请求。随着电子邮件的发送或接收，新的电子邮件将不断添加到存档中，且无法修改或手动删除。

每个用户邮箱中的电子邮件显示在两个文件夹中，即 **收件箱**和**发件箱**。在每个文件夹中，电子邮件会按时间顺序排序，从最近到最旧。

存档已使用 AES-256 算法加密。只有授权的用户可以根据其访问级别访问存档，并且所有操作的审核记录可用。

除了与合规性相关的功能外，电子邮件存档还提供备份和恢复功能。

您可以执行以下操作：

- 浏览存档
- 使用即席搜索查询和已保存的搜索查询搜索特定的邮件
- 在不恢复电子邮件的情况下预览电子邮件
- 恢复特定电子邮件、**收件箱**和**发件箱**文件夹，以及整个邮箱至原始或非原始邮箱
- 下载电子邮件附件

限制

- 存档中仅包括已获许可的邮箱。未指派许可证的共享邮箱不包括在存档中。
- 由于 Microsoft 的限制，可包含在存档中的电子邮件的最大大小为 150 MB。
- 存档中不包括草稿电子邮件。
- 您可以将一个存档计划应用到一个邮件服务器。

配置电子邮件存档

添加邮件服务器

先决条件

在管理门户中，必须为租户启用以下提供项目。

- **电子邮件存档席位**
- **存档存储**

若要添加电子邮件服务器

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**设备**，然后单击 **添加** > **Microsoft 365 商业版 - 电子邮件存档**。
   系统即会将您重定向到 Microsoft 365 登录页面。
3. 在 Microsoft 登录页面上，以全局管理员身份登录。
4. 查看所需权限列表，然后单击**接受**。

结果，Microsoft 365 邮件服务器将出现在 Cyber Protect 中控台上，其位于 **设备** > **邮件服务器** 选项卡上。

然后，按 "创建存档计划"(第 502 页) 中所述配置存档计划。

创建存档计划

在存档计划中，您可以选择要导入电子邮件存档的现有电子邮件。初始导入仅会影响邮件服务器上已存在的电子邮件。

将邮件服务器添加到 Cyber Protect 中控台后，将自动将所有新的已发送或已接收的电子邮件添加到存档。这不是可配置的设置，也不依赖于初始导入的范围。

您可以将一个存档计划应用到一个邮件服务器。

新邮件服务器

若要创建存档计划

1. 如 "添加邮件服务器"(第 502 页) 中所述，将邮件服务器添加到 Cyber Protect 中控台。
   添加服务器后，将打开**创建计划**窗口。
2. [可选] 若要更改存档计划名称，请单击铅笔图标，指定新名称，然后单击**确定**。
3. 若要配置导入范围，请单击**要导入的内容**。
   可使用以下选项。

导入范围	日期范围
所有邮箱	所有可用项 依电子邮件年限 按日期
不要导入任何内容	N/A

4. [若选择了 **日期范围 > 按电子邮件年龄**] 请指定时间段，选择时间单位，然后单击**完成**。
   例如，您可以选择 1 年、2 个月或 300 天。
   只有在指定期间收到或发送的电子邮件才会导入存档。
5. [若选择**日期范围 > 按日期**] 请选择开始日期和结束日期，然后单击 **完成**。
   只有在指定期间收到或发送的电子邮件才会导入存档。
6. 单击**加密**，指定并确认加密密码，然后单击**保存**。

   警告！
   如果丢失或忘记此密码，将将无法浏览存档并从中恢复数据。

7. 单击**创建**。

现有邮件服务器

先决条件

- 已将邮件服务器添加到 Cyber Protect 中控台，但没有应用存档计划。

若要创建存档计划

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**设备**，然后选择要创建计划的邮件服务器。
3. 单击省略号图标 (...)，然后选择**保护**。
4. [可选] 若要更改存档计划名称，请单击铅笔图标，指定新名称，然后单击**确定**。
5. 若要配置导入范围，请单击**要导入的内容**。
   可使用以下选项。

导入范围	日期范围
所有邮箱	所有可用项 依电子邮件年限 按日期
不要导入任何内容	N/A

6. [若选择了 **日期范围 > 按电子邮件年龄**] 请指定时间段，选择时间单位，然后单击**完成**。
   例如，您可以选择 1 年、2 个月或 300 天。
   只有在指定期间收到或发送的电子邮件才会导入存档。
7. [若选择**日期范围 > 按日期**] 请选择开始日期和结束日期，然后单击 **完成**。
   只有在指定期间收到或发送的电子邮件才会导入存档。
8. 单击**加密**，指定并确认加密密码，然后单击**保存**。

   警告！
   如果丢失或忘记此密码，将将无法浏览存档并从中恢复数据。

9. 单击**创建**。

因此，会创建电子邮件存档计划并应用于邮件服务器，并创建电子邮件存档。

初始导入将花费一些时间，具体取决于所选的导入范围和时间段。所有新的电子邮件将都将在其被发送或接收时继续添加到存档中。

监视计划的存档操作

您可以编辑、应用和删除存档计划。

编辑

若要编辑存档计划

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**管理 > 存档计划**，然后单击**存档计划**。
3. 单击计划名称旁边的省略号图标 (...)，然后单击**编辑**。
4. 若要更改计划名称，请单击铅笔图标，指定新名称，然后单击**确定**。
5. 若要更改导入范围，请单击**要导入的内容**。
6. 编辑范围或日期范围，然后单击**完成**。
7. 单击**保存**。

因此，如果扩大了导入范围，则会将其他电子邮件消息导入存档。

如果缩小了导入范围，则不会执行任何操作，也不会删除已导入电子邮件存档的电子邮件。

应用

先决条件

- 您的租户中必须至少存在一个存档计划。

若要应用存档计划

注意
只有在尚未将存档计划应用到邮件服务器时，此操作才可用。您只能将一个存档计划应用到邮件服务器。

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**设备** > **邮件服务器**。
3. 单击邮件服务器名称旁边的省略号图标 (...)，然后选择 **保护**。
4. 选择现有存档计划，然后单击**应用**。

因此，电子邮件存档计划将应用于邮件服务器，并创建电子邮件存档。

初始导入将花费一些时间，具体取决于所选的导入范围和时间段。所有新的电子邮件将都将在其被发送或接收时继续添加到存档中。

删除

若要删除存档计划

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**管理** > **存档计划**，然后单击**存档计划**。
3. 单击计划名称旁边的省略号图标 (...)，然后单击**删除**。
4. 勾选复选框以确认您的决定，然后单击**删除**。

因此，将应用该计划的邮件服务器的存档将不再更新。已导入存档的电子邮件将不会被删除。

创建已保存的搜索查询

可以使用搜索查询在存档中查找特定的电子邮件，然后保存查询以备将来使用。

若要创建已保存的搜索查询

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**备份存储** > **云应用程序备份**，然后选择要搜索的电子邮件存档。
3. 单击**浏览存档**。
4. [若显示隐私警告] 在**隐私警告**对话框中，单击**继续**。
5. 在**加密密码**对话框中，指定密码，然后单击**继续**。
6. 选择要进行搜索的层级。
   可以选择**所有电子邮件**、用户邮箱或用户邮箱中的**收件箱**或**发件箱**文件夹。
7. 单击**搜索**，指定搜索查询，然后单击 **搜索**。
   您可以使用一个或多个字词。若要搜索特定短语，请将短语置于引号中。不支持通配符。
   将在以下字段中执行搜索：
   - 发件人
   - 收件人
   - 抄送

- 密件抄送
- 主题

8. [可选] 若要仅在特定字段(如 **发件人**、**收件人/抄送/密件抄送**、**主题包含**) 中搜索，或指定其他搜索条件，请单击**筛选器**。
   a. 配置您的搜索条件。
      例如，可以仅搜索包含附件的电子邮件，或在特定日期发送或接收的电子邮件。
   b. 单击**应用**。
9. 点击**保存为**。
10. 在**搜索查询标签**中，指定名称。
11. 单击**保存**。

因此，将列出与搜索查询匹配的电子邮件。会创建新的已保存搜索查询，并在电子邮件存档树上方的**已保存搜索查询**部分显示。

每次重新应用保存的搜索查询至存档时，搜索结果都会更新。

使用已保存的搜索查询进行其他操作

您可以编辑和删除已保存的搜索查询。

编辑

若要编辑搜索查询

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**管理** > **存档计划**，然后单击**搜索查询**。
3. 单击查询名称旁边的省略号图标 (...)，然后单击**编辑**。
4. 编辑搜索查询，然后单击**保存**。

删除

若要删除搜索查询

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**管理** > **存档计划**，然后单击**搜索查询**。
3. 单击查询名称旁边的省略号图标 (...)，然后单击**删除**。
4. 勾选复选框以确认您的决定，然后单击**删除**。

移除邮件服务器

可以删除已添加至 Cyber Protect 中控台的邮件服务器。

若要删除邮件服务器

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**设备** > **邮件服务器**。
3. 单击邮件服务器名称旁边的省略号图标 (...)，然后点击**删除**。
4. 若要确认您的选择，请单击**删除**。

因此，邮件服务器将从 Cyber Protect 中控台中删除。将保留电子邮件存档，但不会再更新。

从电子邮件存档中恢复数据

搜索电子邮件

您可以在存档中使用以下级别的搜索查询来搜索特定的电子邮件：

- 电子邮件存档(**所有电子邮件**)
- 用户邮箱
- 用户邮箱中的**收件箱**或**发件箱**文件夹

若要搜索电子邮件

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**备份存储** > **云应用程序备份**，然后选择要搜索的电子邮件存档。
3. 单击**浏览存档**。
4. [若显示隐私警告] 在**隐私警告**对话框中，单击**继续**。
5. 在**加密密码**对话框中，指定密码，然后单击**继续**。
6. 选择要进行搜索的层级。
   可以选择**所有电子邮件**、用户邮箱或用户邮箱中的**收件箱**或**发件箱**文件夹。
7. 单击**搜索**，指定搜索查询，然后单击 **搜索**。
   您可以使用一个或多个字词。若要搜索特定短语，请将短语置于引号中。不支持通配符。
   将在以下字段中执行搜索：
   - 发件人
   - 收件人
   - 抄送
   - 密件抄送
   - 主题
8. [可选] 若要仅在特定字段(如 **发件人**、**收件人/抄送/密件抄送**、**主题包含**)中搜索，或指定其他搜索条件，请单击**筛选器**。
   a. 配置您的搜索条件。
      例如，可以仅搜索包含附件的电子邮件，或在特定日期发送或接收的电子邮件。
   b. 单击**应用**。

结果是，会列出与搜索查询匹配的电子邮件。

预览电子邮件

您可以在不恢复存档电子邮件的情况下进行预览。

若要预览电子邮件

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**备份存储** > **云应用程序备份**，然后选择要搜索的电子邮件存档。

3. 单击**浏览存档**。
4. [若显示隐私警告] 在**隐私警告**对话框中，单击**继续**。
5. 在**加密密码**对话框中，指定密码，然后单击**继续**。
6. 搜索要预览的电子邮件。
   您可以使用即席搜索查询和已保存的搜索查询。有关详细信息，请参阅 "搜索电子邮件"(第 507 页)。
7. 选择要预览的电子邮件。

由此，将显示电子邮件，您可以检查其内容和元数据。

恢复电子邮件、文件夹和邮箱

您可以将电子邮件、文件夹和邮箱恢复到原始邮箱或非原始邮箱。

电子邮件

若要恢复邮箱

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**备份存储** > **云应用程序备份**，然后选择要恢复数据的电子邮件存档。
3. 单击**浏览存档**。
4. [若显示隐私警告] 在**隐私警告**对话框中，单击**继续**。
5. 在**加密密码**对话框中，指定密码，然后单击**继续**。
6. [可选] 搜索要恢复的电子邮件。
   您可以使用即席搜索查询和已保存的搜索查询。有关详细信息，请参阅 "搜索电子邮件"(第 507 页)。
7. 选择要恢复的电子邮件，然单击**恢复电子邮件**。
8. [如果向 Cyber Protect 中控台添加了多个邮件服务器] 请选择要恢复数据的组织。
   a. 在**组织**中，单击**选择**。
   b. 选择组织，然后单击**选择**。
9. 在**恢复位置**中，选择要恢复电子邮件的位置。
10. [如果选择了**新位置**] 请选择目标邮箱。
    a. 在**恢复至**中，单击**选择**。
    b. 选择目标邮箱，然后单击**选择**。
11. 单击**开始恢复**。

这样，选定邮箱的传入电子邮件将恢复到目标邮箱的**收件箱**文件夹中，选定邮箱的传出电子邮件将恢复到目标邮箱的**已发送**文件夹中。

文件夹

若要恢复文件夹

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**备份存储** > **云应用程序备份**，然后选择要恢复数据的电子邮件存档。
3. 单击**浏览存档**。

4. [若显示隐私警告] 在**隐私警告**对话框中，单击**继续**。
5. 在**加密密码**对话框中，指定密码，然后单击**继续**。
6. 选择要恢复的**收件箱**或**发件箱**文件夹，然后单击**恢复文件夹**。
7. [如果向 Cyber Protect 中控台添加了多个邮件服务器] 请选择要恢复数据的组织。
   a. 在**组织**中，单击**选择**。
   b. 选择组织，然后单击**选择**。
8. 在**恢复位置**中，选择要在其中恢复数据的位置。
9. [如果选择了**新位置**] 请选择目标邮箱。
   a. 在**恢复至**中，单击**选择**。
   b. 选择目标邮箱，然后单击**选择**。
10. 单击**开始恢复**。

这样，选定邮箱的传入电子邮件将恢复到目标邮箱的**收件箱**文件夹中，选定邮箱的传出电子邮件将恢复到目标邮箱的**已发送**文件夹中。

邮箱

恢复邮箱

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**备份存储** > **云应用程序备份**，然后选择要恢复数据的电子邮件存档。
3. 单击**浏览存档**。
4. [若显示隐私警告] 在**隐私警告**对话框中，单击**继续**。
5. 在**加密密码**对话框中，指定密码，然后单击**继续**。
6. 选择要恢复的邮箱，然单击**恢复用户电子邮件**。
7. [如果向 Cyber Protect 中控台添加了多个邮件服务器] 请选择要恢复数据的组织。
   a. 在**组织**中，单击**选择**。
   b. 选择组织，然后单击**选择**。
8. 在**恢复位置**中，选择要在其中恢复数据的位置。
9. [如果选择了**新位置**] 请选择目标邮箱。
   a. 在**恢复至**中，单击**选择**。
   b. 选择目标邮箱，然后单击**选择**。
10. 单击**开始恢复**。

这样，选定邮箱的传入电子邮件将恢复到目标邮箱的**收件箱**文件夹中，选定邮箱的传出电子邮件将恢复到目标邮箱的**已发送**文件夹中。

下载附件

可以下载存档中一封或多封电子邮件的附件。

若要下载附件

1. 以管理员身份登录 Cyber Protect 中控台。
2. 转到**备份存储** > **云应用程序备份**，然后选择电子邮件存档。

3. 单击**浏览存档**。
4. [若显示隐私警告] 在**隐私警告**对话框中，单击**继续**。
5. 在**加密密码**对话框中，指定密码，然后单击**继续**。
6. [可选] 搜索要下载的带附件的电子邮件。
   您可以使用即席搜索查询和已保存的搜索查询。有关详细信息，请参阅 "搜索电子邮件"(第 507 页)。
7. 选择要下载其附件的电子邮件，然后单击**下载附件**。

由此，选定电子邮件的附件将下载到您的计算机。

当下载多个项目时，附件将作为 ZIP 文件下载。

保护 Microsoft 应用程序

正在保护 Microsoft SQL Server 和 Microsoft Exchange Server

注意
仅在 NFTS、REFS 和 FAT32 文件系统上运行的数据库支持 Microsoft SQL 备份。不支持 ExFat。

有两种保护 Microsoft 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	-

* 还可以通过邮箱备份提供粒度恢复。在本地安装适用于 Microsoft 365 的代理程序的情况下，支持将 Exchange 数据项恢复到 Microsoft 365，反之亦然。

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大小至少是 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，如更改临时文件和文件夹位置 (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：

- 对于物理机和其中安装有代理程序的计算机，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。
  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。

  注意
  使用在创建域时配置的内置域管理员帐户。以后创建的帐户不受支持。

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。
  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。

  注意
  使用在创建域时配置的内置域管理员帐户。以后创建的帐户不受支持。

- 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"(第 520 页) 中所述配置了适用于 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。有关如何备份 DAG 的详细信息，请参阅 "保护数据库可用性组 (DAG)"(第 516 页)。
   - 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"(第 520 页) 中所述配置了适用于 Exchange 的代理程序，则可以选择要备份的邮箱。

   如果您的选择包含多个数据库，则一次处理两个数据库。当第一个组的备份完成时，下一个组将开始备份。
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)

注意
该功能随 Advanced Backup 包提供。

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。
2. 如“选择 SQL 数据库”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)

注意
该功能随 Advanced Backup 包提供。

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。

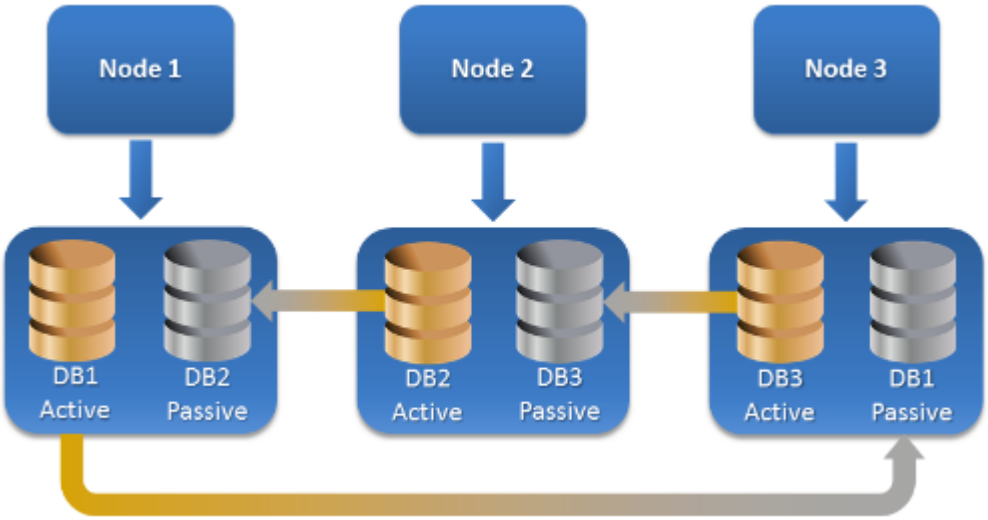
群集感知备份

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，Cyber Protect 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，选择 DAG，如 "选择 Exchange Server 数据"(第 514 页) 中所述。
2. 配置 "群集备份模式"(第 406 页) 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"(第 529 页) 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

适用于个别物理机、ESXi 虚拟机和 Hyper-V 虚拟机的应用程序感知磁盘级别备份可用。但不适用于设备组。

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：

- 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。
- 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。
- 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。
- 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
不支持运行 Windows Server 2022 的 Hyper-V 和 VMware ESXi 虚拟机的无代理程序应用程序感知备份。若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保护代理程序。有关详细信息，请参阅 "在 Windows Server 2022 虚拟机上配置应用程序感知备份"(第 519 页)。

适用于 VMware(虚拟设备)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。若要从此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**要浏览的计算机**中选择此计算机。

"先决条件"和"所需用户权限"部分中列出了其他要求。

注意
如果在高负载的主机上执行备份，则由于 Windows Management Instrumentation 不响应或延迟响应，从而导致 Hyper-V 虚拟机的应用程序感知备份可能会失败，并显示错误"WMI'ExecQuery'无法执行查询。"或"无法通过 WMI 创建新进程"。请在主机上的负载较低的时间段内重试这些备份。

在 Windows Server 2022 虚拟机上配置应用程序感知备份

若要对运行 Windows Server 2022 的 Hyper-V 和 VMware ESXi 虚拟机执行应用程序感知备份，则必须使用基于代理程序的备份。有关备份模式的详细信息，请参阅 "基于代理程序备份和无代理程序备份"(第 56 页)。

	基于代理程序的备份	无代理程序备份
应用程序感知备份	受支持	不支持
Cyber Protect 中控台中的虚拟机图标		

若要在基于代理程序的模式下配置应用程序感知备份

1. 在虚拟机的来宾操作系统中安装保护代理程序(如 Windows 代理程序、SQL 代理程序或 Exchange 代理程序)。
2. 在 Cyber Protect 中控台中，选择安装了保护代理程序的计算机。
3. 在新的保护计划中配置应用程序感知备份。
4. 将保护计划应用于虚拟机。
5. 运行保护计划。

因此，将创建包含应用程序感知备份的备份存档。

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：
  该帐户必须是计算机上**备份操作员**或**管理员**组的成员，以及要备份的每个实例上**sysadmin**角色的成员。

  注意
  仅支持 Windows 身份验证。

- 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。

注意
使用在创建域时配置的内置域管理员帐户。以后创建的帐户不受支持。

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，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。

注意
使用在创建域时配置的内置域管理员帐户。以后创建的帐户不受支持。

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。

注意
可以从数据库备份和应用程序感知备份中恢复邮箱和邮箱项目。有关详细信息，请参阅 "恢复 Exchange 邮箱和邮箱项目"(第 531 页)。在使用数据库备份和应用程序感知备份的情况下，无法为个别邮箱创建保护计划。

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**保护**。

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

可以从数据库备份和应用程序感知备份中恢复 SQL 数据库。有关这两种备份类型之间差异的详细信息，请参阅 "正在保护 Microsoft SQL Server 和 Microsoft Exchange Server"(第 510 页)。

可以将 SQL 数据库恢复为原始实例、原始计算机上的其他实例或非原始计算机上的实例。在执行恢复到非原始计算机时，必须在目标计算机上安装适用于 SQL 的代理程序

此外，还可以将数据库恢复为文件。

如果针对 SQL 实例使用 Windows 身份验证，则必须提供计算机上的**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，则必须提供目标实例上的 **sysadmin** 角色的成员帐户的凭据。

系统数据库会恢复为用户数据库，但有一些区别。要了解有关这些区别的详细信息，请参阅 "恢复系统数据库"(第 528 页)。

在恢复过程中，可以在 Cyber Protect 中控台中的**监控** > **活动**选项卡上查看操作进度。

正在将 SQL 数据库恢复到原始计算机

可以将 SQL 数据库恢复为其原始实例、原始计算机上的其他实例或非原始目标计算机上的实例。

将 SQL 数据库恢复到原始计算机

从数据库备份

1. 在 Cyber Protect 中控台中，转到**设备** > **Microsoft SQL**。
2. 选择 SQL Server 实例或单击实例名称以选择要恢复的特定数据库，然后单击**恢复**。

   如果计算机处于脱机状态，将不会显示恢复点。要将数据恢复到非原始计算机，请参阅 "正在将 SQL 数据库恢复到非原始计算机"(第 524 页)。
3. 选择恢复点。

   恢复点会按位置过滤。
4. 依次单击**恢复** > **将数据库恢复为实例**。

默认情况下，实例和数据库会恢复为原始实例和数据库。还可以将原始数据库恢复为新数据库。

5. [恢复为同一计算机上的非原始实例时] 单击**目标 SQL Server 实例**、选择目标实例，然后单击**完成**。
6. [将数据库恢复为新数据库时] 单击数据库名称，然后在**恢复到**中选择**新数据库**。
   - 指定新数据库名称。
   - 指定新数据库路径。
   - 指定日志路径。
7. [可选] [将数据库恢复为新数据库时不可用] 要在恢复后更改数据库状态，请单击数据库名称、选择以下状态之一，然后单击**完成**。
   - **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。
8. 单击**开始恢复**。

从应用程序感知备份

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 选择最初包含要恢复的数据的计算机，然后单击**恢复**。

   如果计算机处于脱机状态，将不会显示恢复点。要将数据恢复到非原始计算机，请参阅 "正在将 SQL 数据库恢复到非原始计算机"(第 524 页) 。
3. 选择恢复点。

   恢复点会按位置过滤。
4. 依次单击**恢复** > **SQL 数据库**。
5. 选择 SQL Server 实例或单击实例名称以选择要恢复的特定数据库，然后单击**恢复**。

   默认情况下，实例和数据库会恢复为原始实例和数据库。还可以将原始数据库恢复为新数据库。
6. [恢复为同一计算机上的非原始实例时] 单击**目标 SQL Server 实例**、选择目标实例，然后单击**完成**。
7. [将数据库恢复为新数据库时] 单击数据库名称，然后在**恢复到**中选择**新数据库**。
   - 指定新数据库名称。
   - 指定新数据库路径。
   - 指定日志路径。

8. [可选] [将数据库恢复为新数据库时不可用] 要在恢复后更改数据库状态，请单击数据库名称、选择以下状态之一，然后单击**完成**。
   - **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。
9. 单击**开始恢复**。

正在将 SQL 数据库恢复到非原始计算机

可以将应用程序感知备份和数据库备份恢复到非原始目标计算机（安装有适用于 SQL 的代理程序）上的 SQL Server 实例。备份必须位于云存储或目标计算机可以访问的共享存储中。

目标计算机上的 SQL Server 版本必须与源计算机上的版本相同或更新。

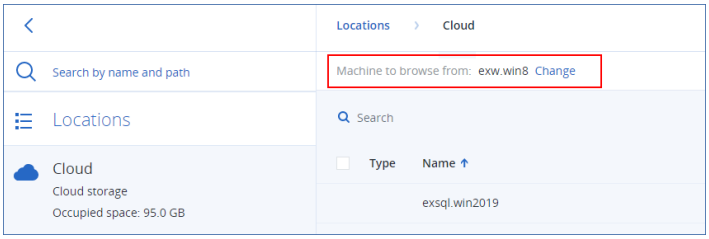
将 SQL 数据库恢复到非原始计算机

从备份存储

此过程适用于应用程序感知备份和数据库备份。

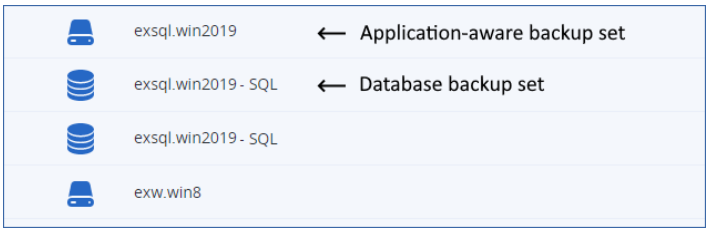
1. 在 Cyber Protect 中控台中，转到**备份存储**。
2. 选择要从中恢复数据的备份集的位置。
3. 在**要浏览的计算机**中，选择目标计算机。

   这是数据将恢复到的计算机。目标计算机必须处于联机状态。



4. 选择备份集，然后在**操作**窗格中单击**显示备份**。

   应用程序感知备份集和数据库备份集的图标不同。



5. 选择要从中恢复数据的恢复点。
6. [对于数据库备份] 单击**恢复 SQL 数据库**。
7. [对于应用程序感知备份] 依次单击**恢复** > **SQL 数据库**。
8. 选择 SQL Server 实例或单击实例名称以选择要恢复的特定数据库，然后单击**恢复**。
9. [如果目标计算机上有多个 SQL 实例] 单击**目标 SQL Server 实例**、选择目标实例，然后单击**完成**。
10. 单击数据库名称、指定新的数据库路径和日志路径，然后单击**完成**。
    可以在两个字段中指定相同的路径，例如：

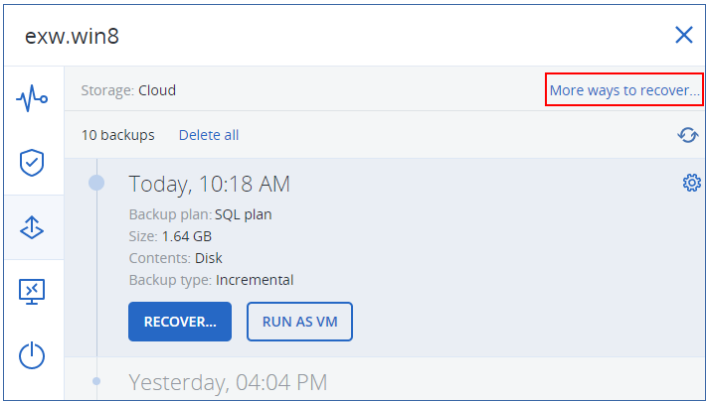
    ```
    C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
    ```

11. 单击**开始恢复**。

从设备

此过程仅适用于应用程序感知备份。

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 选择最初包含要恢复的数据的计算机，然后单击**恢复**。
3. [如果源计算机处于联机状态] 单击**更多恢复方法**。



4. 单击**选择计算机**以选择目标计算机，然后单击**确定**。
   这是数据将恢复到的计算机。目标计算机必须处于联机状态。
5. 选择恢复点。
   恢复点会按位置过滤。
6. 依次单击**恢复** > **SQL 数据库**。
7. 选择 SQL Server 实例或单击实例名称以选择要恢复的特定数据库，然后单击**恢复**。
8. [如果目标计算机上有多个 SQL 实例] 单击**目标 SQL Server 实例**、选择目标实例，然后单击**完成**。

9. 单击数据库名称、指定新的数据库路径和日志路径，然后单击**完成**。
   可以在两个字段中指定相同的路径，例如：

   ```
   C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
   ```

10. 单击**开始恢复**。

正在将 SQL 数据库恢复为文件

可以将数据库恢复为文件。如果需要提取数据以进行数据挖掘、审核或由第三方工具进行进一步处理，则此选项可能很有用。要了解如何将 SQL 数据库文件附加到 SQL Server 实例，请参阅 "连接 SQL Server 数据库"(第 528 页)。

可以将数据库作为文件恢复到原始计算机或安装有适用于 SQL 的代理程序的非原始目标计算机。将数据恢复到非原始计算机时，备份必须位于云存储或目标计算机可以访问的共享存储中。

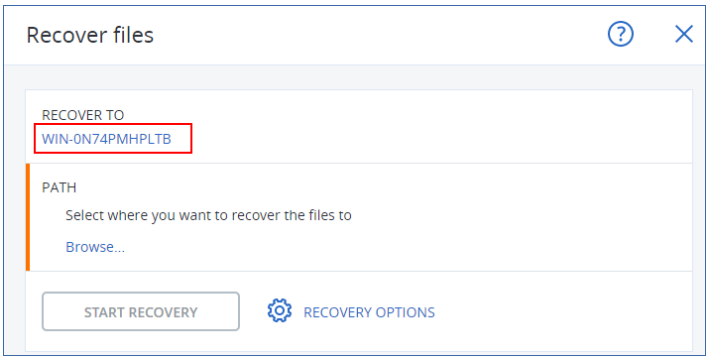
注意
如果使用适用于 VMware 的代理程序 (Windows)，则将数据库恢复为文件是唯一的恢复方法。无法使用适用于 VMware 的代理程序 (虚拟设备) 恢复数据库。

将 SQL 数据库恢复为文件

从数据库备份

此过程适用于联机源计算机。

1. 在 Cyber Protect 中控台中，转到**设备** > **Microsoft SQL**。
2. 选择要恢复的数据库，然后单击**恢复**。
3. 选择恢复点。
   恢复点会按位置过滤。
4. 依次单击**恢复** > **将数据库恢复为文件**。
5. [恢复到非原始计算机时] 在**恢复到**中，选择目标计算机。
   这是数据将恢复到的计算机。目标计算机必须处于联机状态。
   要更改选择，请单击计算机名称、选择另一台计算机，然后单击**确定**。



6. 在**路径**中，单击**浏览**、选择要将文件保存到的本地文件夹或网络文件夹，然后单击**完成**。
7. 单击**开始恢复**。

从应用程序感知备份

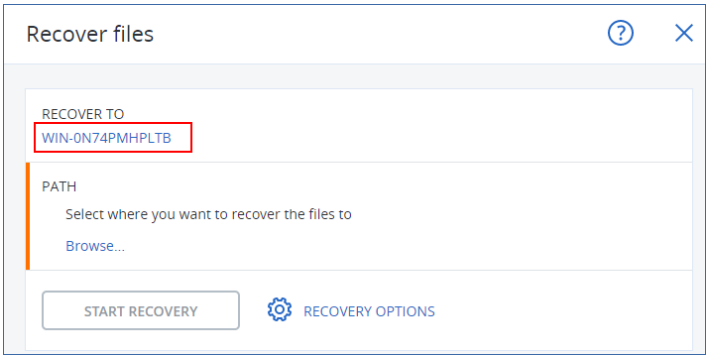
此过程适用于联机源计算机。

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 选择最初包含要恢复的数据的计算机，然后单击**恢复**。
3. 选择恢复点。

   恢复点会按位置过滤。
4. 依次单击**恢复** > **SQL 数据库**、选择要恢复的数据库，然后单击**恢复为文件**。
5. [恢复到非原始计算机时] 在**恢复到**中，选择目标计算机。

   这是数据将恢复到的计算机。目标计算机必须处于联机状态。

   要更改选择，请单击计算机名称、选择另一台计算机，然后单击**确定**。



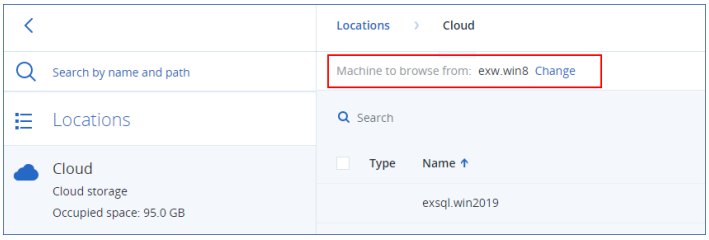
6. 在**路径**中，单击**浏览**、选择要将文件保存到的本地文件夹或网络文件夹，然后单击**完成**。
7. 单击**开始恢复**。

从脱机计算机上的备份

此过程适用于处于脱机状态的源计算机上的应用程序感知备份和数据库备份。

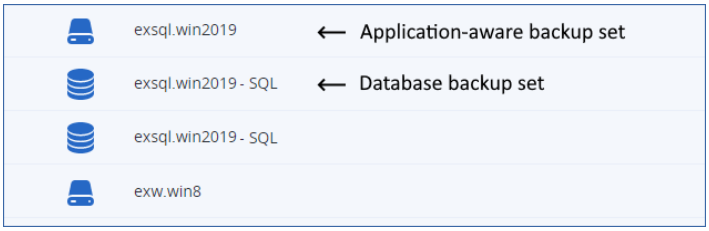
1. 在 Cyber Protect 中控台中，转到**备份存储**。
2. 选择要从中恢复数据的备份集的位置。
3. 在**要浏览的计算机**中，选择目标计算机。

   这是数据将恢复到的计算机。目标计算机必须处于联机状态。



4. 选择备份集，然后在**操作**窗格中单击**显示备份**。

   应用程序感知备份集和数据库备份集的图标不同。



5. 选择要从中恢复数据的恢复点。
6. [对于数据库备份] 单击**恢复 SQL 数据库**。
7. [对于应用程序感知备份] 依次单击**恢复** > **SQL 数据库**。
8. 选择 SQL Server 实例或单击实例名称以选择要恢复的特定数据库，然后单击**恢复为文件**。
9. 在**路径**中，单击**浏览**、选择要将文件保存到的本地文件夹或网络文件夹，然后单击**完成**。
10. 单击**开始恢复**。

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

可以从以下备份中恢复 Exchange 邮箱和邮箱项目：

- 数据库备份
- 应用程序感知备份
- 邮箱备份

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 514 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。

邮箱或邮箱项目可以恢复至活动 Exchange Server 或 Microsoft 365。

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

在本地安装适用于 Microsoft 365 的代理程序的情况下，支持将 Exchange 数据项恢复到 Microsoft 365，反之亦然。

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 数据"(第 543 页)。

恢复邮箱

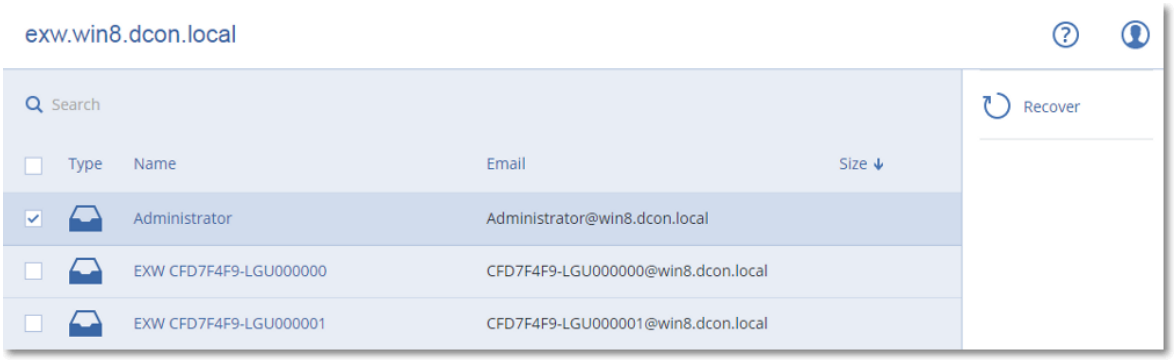
从应用程序感知备份或数据库备份恢复邮箱

1. [仅在从数据库备份恢复至 Microsoft 365 时] 如果适用于 Microsoft 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 Microsoft 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 Microsoft 365 的代理程序。
   - 如果贵组织中已有适用于 Microsoft 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 Microsoft 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 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。

   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。
9. 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"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. [仅在从数据库备份恢复至 Microsoft 365 时] 如果适用于 Microsoft 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 Microsoft 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 Microsoft 365 的代理程序。

- 如果贵组织中已有适用于 Microsoft 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 Microsoft 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。

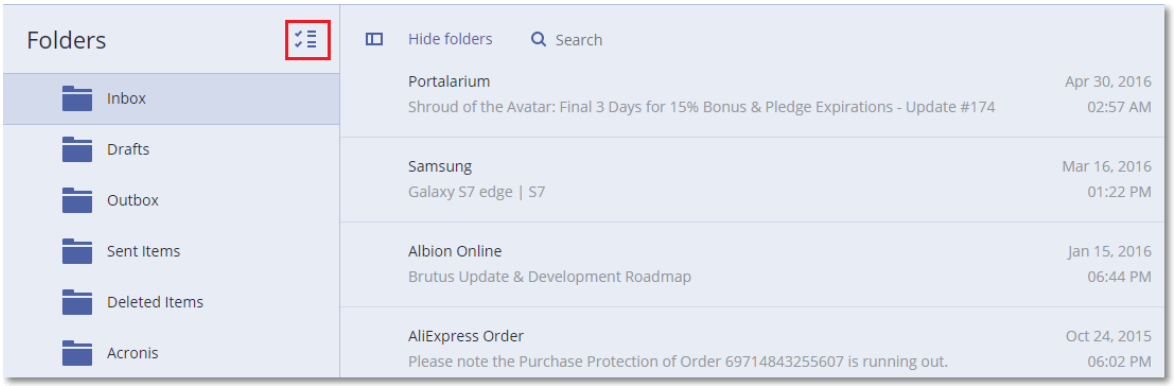
   在上述一项操作中选择用于浏览的计算机(而非处于脱机状态的初始计算机)将执行恢复。
5. 依次单击**恢复** > **Exchange 邮箱**。
6. 单击原先包含要恢复的项目的邮箱。
7. 选择要恢复的项目。

   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 365**。

   若要恢复至 Exchange Server，请保留**恢复至**中的默认 **Microsoft Exchange** 值。

[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。

10. 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"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(或装有相同版本 Microsoft Exchange Server 的其他计算机)复制到装有适用于 Microsoft 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%\安克诺斯\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**。

保护移动设备

该 Acronis Cyber Protect 应用程序让您可以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 Acronis Cyber Protect 应用程序：

- iOS 15 至 iOS 17(iPhone、iPod、iPad)
- Android 10 到 Android 14

重要事项
若要启动备份处理，您必须手动启动应用程序。

备份内容

- 通讯录(姓名、电话号码和电子邮件)
- 照片(将保留照片的原始大小和格式)
- 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。如果此设置处于启用状态，则 Acronis Cyber Protect 应用程序会自动即时检测新数据，然后将其上传到云。
- 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 安克诺斯 Cyber Protect 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。
- 设备上的电池优化可能会阻止 Acronis Cyber Protect 应用程序正常运行。要按时运行备份，应该停止针对该应用程序的电池优化。
- 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 Acronis Cyber Protect 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**。如果该设置已打开，则 Acronis Cyber Protect 应用程序会仅在设备电池电量较高时才备份数据。设备电池电量变低时，持续备份会暂停。
- 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 Cyber Protect 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 Acronis Cyber Protect 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 Cyber Protect 中控台。
- 保留规则不适用于移动设备的备份。
- [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。

在哪里可以获取 Cyber Protect 应用程序

视移动设备而定，从应用程序商店或 Google Play 安装该应用程序。

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。
3. 点击**设置**创建备份。请注意，仅当您没有移动设备的备份时，此按钮才会显示。
4. 选择要备份的数据分类。默认情况下，选定所有分类。
5. [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**。
6. 点击**备份**。
7. 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

警告！
若要恢复移动数据，必须使用最终用户帐户。

1. 打开 Acronis Cyber Protect 应用。
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。

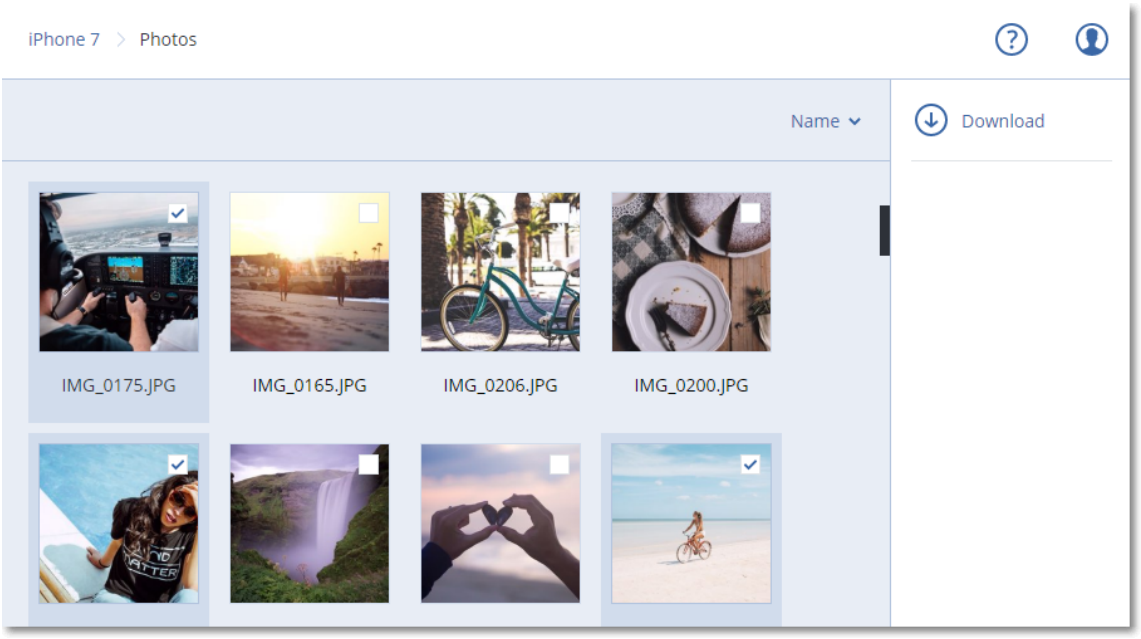
- 若要恢复属于同一数据分类的一个或多个数据项目，请点击数据分类。继续执行后续步骤。

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 Cyber Protect 中控台查看数据

1. 在计算机上，打开浏览器并键入 Cyber Protect 中控台的 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。

保护托管的 Exchange 数据

可以备份哪些项目？

您可以备份用户邮箱、共享邮箱和组邮箱。或者，您可以选择备份选定邮箱的存档邮箱(**就地存档**)。

可以恢复哪些项目？

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。

在恢复邮箱、邮箱项目、公用文件夹和公用文件夹项目时，可以选择是否覆盖目标位置的项目。

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。

选择 Exchange Online 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 Online 邮箱

1. 单击**设备 > 托管的 Exchange**。
2. 如果多个托管的 Exchange 组织已添加到 Cyber Protection 服务，则选择要备份其用户数据的组织。否则，请跳过此步骤。
3. 请执行以下任一操作：
   - 若要备份所有用户的邮箱和所有共享邮箱(包括将来要创建的邮箱)，请展开**用户**节点，选择**所有用户**，然后单击**组备份**。
   - 若要备份单个用户邮箱或共享邮箱，请展开**用户**节点，选择**所有用户**，选择要备份其邮箱的用户，然后单击**备份**。
   - 若要备份所有组邮箱(包括将来将要创建的组邮箱)，请展开**组**节点，选择**所有组**，然后单击**组备份**。
   - 若要恢复单个组邮箱，请展开**组**节点，选择**所有组**，选择您要备份其邮箱的组，然后单击**备份**。

恢复邮箱和邮箱项目

恢复邮箱

1. 单击**设备 > 托管的 Exchange**。
2. 如果多个托管的 Exchange 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 请执行以下任一操作：
   - 若要恢复用户邮箱，请展开**用户**节点，选择**所有用户**，选择您要恢复其邮箱的用户，然后单击**恢复**。
   - 若要恢复共享邮箱，请展开**用户**节点，选择**所有用户**，选择要恢复的共享邮箱，然后单击**恢复**。
   - 若要恢复组邮箱，请展开**组**节点，选择**所有组**，选择您要恢复其邮箱的组，然后单击**恢复**。
   - 如果用户、组或共享邮箱已删除，请在备份存储选项卡的**云应用程序备份**部分中将它们选中，然后单击**显示备份**。

   可以按名称搜索用户和组。不支持通配符。
4. 选择恢复点。
5. 依次单击**恢复 > 整个邮箱**。
6. 如果多个托管的 Exchange 组织添加到 Cyber Protection 服务，则单击**托管的 Exchange 组织**即可查看、更改或指定目标组织。

   默认情况下，选择原始组织。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
7. 在**恢复至邮箱**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组织，必须指定目标邮箱。

8. 单击**开始恢复**。
9. 选择任一覆盖选项：
   - **覆盖现有项目**
   - **不覆盖现有项目**
10. 单击**继续**以确认您的决定。

恢复邮箱项目

1. 单击**设备 > 托管的 Exchange**。
2. 如果多个托管的 Exchange 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 请执行以下任一操作：
   - 若要从用户邮箱中恢复项目，请展开**用户**节点，选择**所有用户**，选择其邮箱最初包含您要恢复的项目的用户，然后单击**恢复**。
   - 若要恢复共享邮箱中的项目，请展开**用户**节点，选择**所有用户**，选择最初包含要恢复的项目的共享邮箱，然后单击**恢复**。
   - 若要从组邮箱中恢复项目，请展开**组**节点，选择**所有组**，选择其邮箱最初包含您要恢复的项目的组，然后单击**恢复**。
   - 如果用户、组或共享邮箱已删除，请在备份存储选项卡的**云应用程序备份**部分中将它们选中，然后单击**显示备份**。

   可以按名称搜索用户和组。不支持通配符。
4. 选择恢复点。
5. 依次单击**恢复 > 电子邮件**。
6. 浏览到所需的文件夹或使用搜索功能获取所需项目的列表。

   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、附件名称和日期搜索。
   - 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。
7. 选择要恢复的项目。为了能够选择文件夹，请单击“恢复文件夹”图标： 

   此外，您可以执行以下任一操作：
   - 当已选择某个项目时，单击**显示内容**即可查看其内容，包括附件。单击附加文件的名称即可下载它。
   - 当选择电子邮件消息或日历项目时，单击**作为电子邮件发送**以将项目发送到指定的电子邮件地址。您可以选择发件人并编写要添加到转发项目中的文本。
   - 仅在备份未加密且您使用了搜索功能并在搜索结果中选择了单个项目时：单击**显示版本**以选择要恢复的项目版本。可以选择在选定的恢复点之前或之后的任何备份版本。
8. 单击**恢复**。

9. 如果多个托管的 Exchange 组织已添加到 Cyber Protection 服务，则单击**托管的 Exchange 组织**即可查看、更改或指定目标组织。

   默认情况下，选择原始组织。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
10. 在**恢复至邮箱**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组织，必须指定目标邮箱。
11. [仅在恢复到用户或共享邮箱时] 在**路径**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。

    组邮箱项目始终恢复至**收件箱**文件夹。
12. 单击**开始恢复**。
13. 选择任一覆盖选项：
    - **覆盖现有项目**
    - **不覆盖现有项目**
14. 单击**继续**以确认您的决定。

保护 Microsoft 365 数据

为什么备份 Microsoft 365 数据？

尽管 Microsoft 365 是一组云服务，但定期备份会提供额外的一层保护，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，出于法规遵从性需要，可以保留 Exchange Online 邮箱的本地副本。

备份数据会自动进行压缩，并且它所占用的备份位置空间少于其原始位置空间。云到云备份的压缩级别是固定的，对应于非云到云备份的**正常**级别。有关这些级别的详细信息，请参阅 "压缩级别"(第 407 页)。

云代理程序和本地代理程序

对于 Microsoft 365 作负载，有两个代理程序可用：

- 云代理程序

  云代理程序将提供可在 Cyber Protect 中控台中直接访问的扩展备份功能。无需安装。有关详细信息，请参阅 "使用适用于 Microsoft 365 的云代理程序"(第 551 页)。
- 本地代理程序

  本地代理程序仅提供对 Exchange Online 邮箱的备份。此代理程序必须安装在已连接到 Internet 的 Windows 计算机上。有关详细信息，请参阅 "使用本地安装的适用于 Office 365 的代理程序" (第 547 页)。

两类代理程序都支持 Azure 信息保护 (AIP)。

注意

对于处于合规模式下的租户，仅本地代理程序可用。这些租户只能备份 Microsoft 365 邮箱。他们无法使用云代理程序提供的扩展功能。

下表汇总了代理程序的功能。

	本地代理程序	云代理程序
可以备份的数据项目	**Exchange Online**:用户邮箱和共享邮箱(包括 Kiosk 计划中用户的邮箱和诉讼保留的邮箱)	• **Exchange Online**: ◦ 用户邮箱和共享邮箱(包括 Kiosk 计划中用户的邮箱和诉讼保留的邮箱) ◦ 组邮箱 ◦ 公用文件夹 • **OneDrive**:用户文件与文件夹 • **SharePoint Online**: ◦ 经典站点集 ◦ 组(团队)站点 ◦ 通信站点 ◦ 个别数据项 • **Microsoft 365 Teams**: ◦ 整个团队 ◦ 团队频道 ◦ 频道文件 ◦ 团队邮箱 ◦ 团队邮箱中的文件和电子邮件 ◦ 会议 ◦ 团队站点 • **OneNote 笔记本**:作为 OneDrive、SharePoint Online 和 Microsoft 365 Teams 备份的一部分
存档邮箱(**就位存档**)备份	否	是
备份预定	用户定义	每天最多六次*
备份位置	云存储、本地文件夹、网络文件夹	仅限云存储 (包括合作伙伴托管的存储)
自动保护新的 Microsoft 365 用户、组、站点和团队	否	是,方法是将保护计划应用于**所有用户**、**所有组**、**所有站点**、**所有团队**组
保护多个 Microsoft 365 组织	否	是
粒度恢复	是	是
还原至同一 Microsoft 365 组织中的另一用户	是	是

	本地代理程序	云代理程序
还原至同一租户中的另一个 Microsoft 365 组织	否	是
恢复至本地 Microsoft Exchange Server	否	否
在性能不下降的情况下可以备份的最大项目数	备份到云存储时：每个公司 5,000 个邮箱 备份到其他目标位置时：每个保护计划 2,000 个邮箱（对每个公司的邮箱数量不作限制）	每家公司最多有 50,000 个受保护的工作负载**
最大手动备份运行数	否	每小时内 10 个手动运行
最大同时恢复操作数	否	10 个操作，包括 Google Workspace 恢复操作

* 默认选项是**每天一次**。使用 Advanced Backup 包，您可以每天预定最多六个备份。备份按大概的间隔时间开始，间隔时间取决于在数据中心服务多个客户的云代理程序的当前负载。这可确保当天的负载均匀，以及对所有客户同等的服务质量。

注意
保护预定可能会受第三方服务操作的影响，例如 Microsoft 365 服务器的可访问性、Microsoft 服务器上的限制设置等。另请参见 https://docs.microsoft.com/en-us/graph/throttling。

** 工作负载的最大数量取决于工作负载类型，如下所示：50,000 个邮箱或 10,000 个团队或 10,000 个 SharePoint 站点或 5,000 个 OneDrive。

若要计算支持的组合，请使用以下公式：

```
10 mailboxes = 2 teams = 2 sites = 1 OneDrive
```

例如：

- 50,000 个邮箱
- 40,000 个邮箱和 1,000 个 OneDrive
- 40,000 个邮箱和 2,000 个站点
- 40,000 个邮箱和 2,000 个团队
- 30,000 个邮箱、1,000 个 OneDrive、1,000 个站点和 1,000 个团队
- 30,000 个邮箱、2,000 个站点和 2,000 个团队

我们建议您按照以下顺序逐步备份工作负载：

1. 邮箱。
2. 在所有邮箱都完成备份后，继续处理 OneDrive。

3. OneDrive 备份完成后，请继续处理 Teams。
4. Teams 备份完成后，请继续处理 SharePoint 站点。

第一个完整备份可能需要几天时间，具体取决于受保护项目的数量及其大小。

所需用户权限

在 Cyber Protection 中

本地代理程序必须注册在公司管理员帐户下，并在客户租户级别上使用。单位级别的公司管理员、单位管理员和用户无法备份或恢复 Microsoft 365 数据。

云代理程序可以在客户租户级别和单位级别上使用。有关这些级别及其相应管理员的详细信息，请参阅 "管理在不同级别上添加的 Microsoft 365 组织"(第 552 页)。

在 Microsoft 365 中

必须在 Microsoft 365 中向您的帐户指派全局管理员角色。

要发现、备份和恢复 Microsoft 365 公用文件夹，您的至少一个 Microsoft 365 管理员帐户必须有邮箱并对要备份的公用文件夹有读取/写入权限。

- 本地代理程序将使用此帐户登录到 Microsoft 365。若要启用代理程序来访问所有邮箱的内容，将向此帐户分配 **ApplicationImpersonation** 管理角色。如果更改帐户密码，请在 Cyber Protect 中控台中更新密码，如 "更改 Microsoft 365 访问凭据"(第 549 页) 中所述。
- 云代理程序不会登录到 Microsoft 365。您需要以全局管理员身份登录到 Microsoft 365 一次，才能授予运行云代理程序所需的权限。

  在 Microsoft 365 中，需要以下权限：
  - 登录和读取用户个人资料
  - 在所有站点集中读取和写入文件
  - 读取和写入所有用户的完整个人资料
  - 读取和写入所有组
  - 读取目录数据
  - 读取所有通道消息
  - 读取和写入托管元数据
  - 在所有站点集中读取和写入项目和列表
  - 完全控制所有站点集
  - 在所有站点集中读取和写入项目
  - 使用对所有邮箱有完全访问权限的 Exchange Web 服务
- 云代理程序不会存储您的帐户凭据，也不会使用它们来执行备份和恢复。更改凭据、禁用帐户或删除帐户不会影响云代理程序的运行。

限制

- 通过本地代理程序，最多可以保护 5,000 个工作负载。通过云代理程序，则可以保护多达 50,000 个工作负载。
- 拥有邮箱或 OneDrive 的所有用户都会显示在 Cyber Protect 中控台中，包括没有 Microsoft 365 许可证的用户和被阻止登录到 Microsoft 365 服务的用户。
- 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**、**DiscoveryHold**、**日历日志记录**)。
- 无法在恢复期间自动创建用户、公用文件夹、组或站点。例如，如果要恢复已删除的 SharePoint Online 站点，请首先手动创建一个新站点，然后在恢复期间将其指定为目标站点。
- 即使可以从搜索结果中选择此类项目，也无法同时从不同恢复点来恢复项目。
- 在备份期间，将保留应用于内容的任何敏感标签。因此，如果它恢复到非原始的位置并且其用户具有不同的访问权限，则不会显示敏感内容。
- 您只能对一个工作负载应用一个单独的备份计划。
- 当单独的备份计划和组备份计划应用于相同的工作负载时，单独计划中的设置优先。

Microsoft 365 席位许可报告

公司管理员可以下载有关受保护的 Microsoft 365 席位及其许可的报告。该报告采用 CSV 格式，包含有关席位的许可状态和许可证的使用原因的信息。该报告还包含受保护的席位名称、关联的电子邮件地址、组、Microsoft 365 组织、受保护工作负载的名称和类型。

此报告仅适用于注册有 Microsoft 365 组织的租户。

下载 Microsoft 365 席位许可报告

1. 以公司管理员身份登录到 Cyber Protect 中控台。
2. 单击右上角的帐户图标。
3. 单击 **Microsoft 365 席位许可报告**。

日志记录

使用云到云资源的操作，例如查看备份电子邮件的内容、下载附件或文件、将电子邮件恢复到非原始邮箱或将其作为电子邮件发送可能会侵犯用户隐私。这些操作记录在管理门户的**监控** > **审核日志**中。

使用本地安装的适用于 Office 365 的代理程序

添加 Microsoft 365 组织

添加 Microsoft 365 组织

1. 以公司管理员身份登录到 Cyber Protect 中控台。
2. 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**。
3. 下载该代理程序并将其安装在已连接 Internet 的 Windows 计算机上。

4. 在 Cyber Protect 中控台中，转到**设备** > **Microsoft Office 365**。
5. 在打开的窗口中，输入应用程序 ID、应用程序密钥和 Microsoft 365 租户 ID。有关如何找到这些项目的详细信息，请参阅 "获取应用程序 ID 和应用程序秘钥"(第 548 页)。
6. 单击**确定**。

这样，贵组织的数据项目会显示在 Cyber Protect 中控台中的 **Microsoft Office 365** 选项卡上。

重要事项
组织(公司组)中必须仅有一个在本地安装的适用于 Office 365 的代理程序。

获取应用程序 ID 和应用程序秘钥

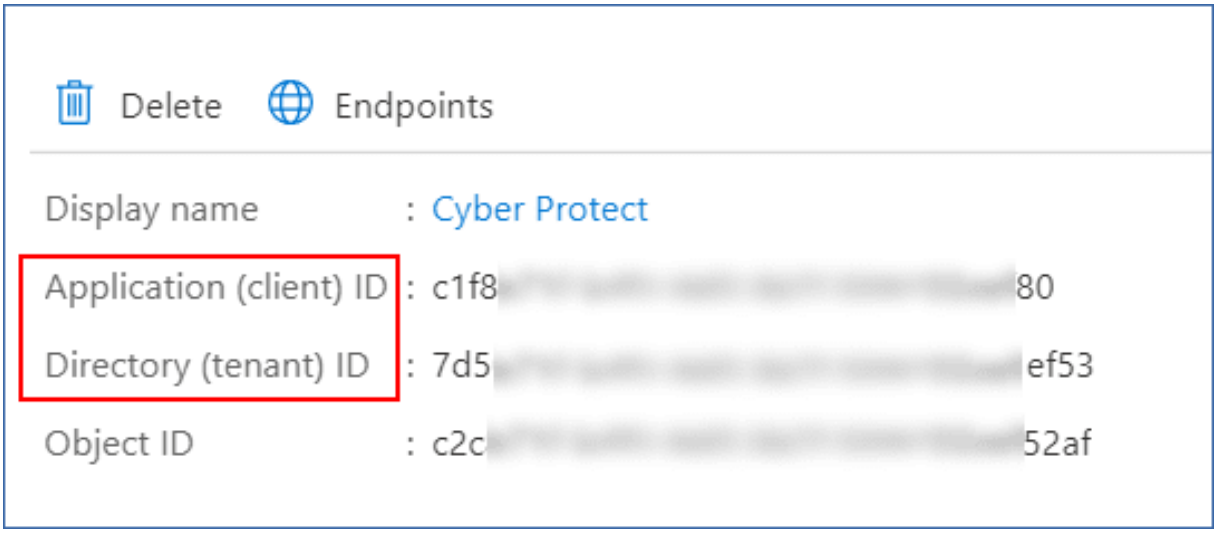
若要使用 Office 365 的新式验证，您需要在 Entra 管理中心中创建自定义应用程序并授予其特定的 API 权限。因此，您将获得在 中控台中输入所需的**应用程序 ID**、**应用程序密钥**和**目录(租户) ID**。

注意
在装有适用于 Office 365 的代理程序的计算机上，确保您允许通过端口 443 访问 graph.microsoft.com。

若要在 Entra 管理中心创建应用程序

1. 以管理员身份登录 Entra 管理中心。
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 Cyber Protection。
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 Entra 管理中心中，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。



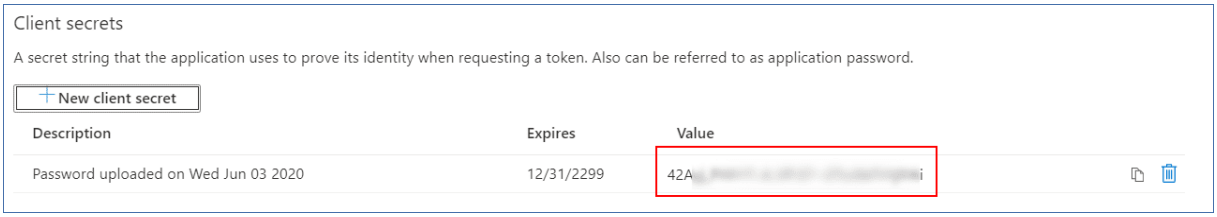
有关如何在 Entra 管理中心中创建应用程序的详细信息，请参阅 Microsoft 文档。

向应用程序授予必要的 API 权限。

1. 在 Entra 管理中心中，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 Entra 管理中心中，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. 依次单击**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。有关如何找到这些项目的详细信息，请参阅 "获取应用程序 ID 和应用程序秘钥"(第 548 页) 。
5. 单击**确定**。

保护 Exchange Online 邮箱

可以备份哪些项目？

您可以备份用户邮箱和共享邮箱。组邮箱和存档邮箱(**就位存档**) 无法备份。

可以恢复哪些项目？

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

您可以使用搜索找到项目。

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。

选择 Microsoft 365 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. 单击 **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. 单击 **Microsoft Office 365**。
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. 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。
6. 单击**开始恢复**。

恢复邮箱项目

1. 单击 **Microsoft Office 365**。
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、附件名称和日期搜索。
   - 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. 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**。
9. 确认您的决定。

邮箱项目始终恢复至目标邮箱的**恢复项目**文件夹。

使用适用于 Microsoft 365 的云代理程序

添加 Microsoft 365 组织

管理员可以将一个或多个 Microsoft 365 组织添加到客户租户或单位。

公司管理员将组织添加到客户租户。在单位级别操作的单位管理员和客户管理员将组织添加到单位。

添加 Microsoft 365 组织

1. 根据需要添加组织的位置,以公司管理员或单位管理员身份登录到 Cyber Protect 中控台。
2. [对于在单位级别操作的公司管理员]在管理门户中,导航到所需的单位。
3. 请依次单击**设备** > **添加** > **Microsoft 365 Business - 备份**。

   该软件将您重定向到 Microsoft 365 登录页面。
4. 使用 Microsoft 365 全局管理员凭据登录。

   Microsoft 365 显示备份和恢复组织数据所必需的权限列表。
5. 确认您向 Cyber Protection 服务授予这些权限。

结果,Microsoft 365 组织显示在 中控台中的**设备**选项卡下。

有用提示

- 从将组织添加到 Cyber Protection 服务的那一刻开始，云代理程序就每 24 小时与 Microsoft 365 同步一次。如果添加或删除用户、组或站点，您在 Cyber Protect 中控台中不会立即看到此更改。若要立即同步更改，请在 **Microsoft 365** 页面中选择组织，然后单击**刷新**。

  有关同步 Microsoft 365 组织和 Cyber Protect 中控台的资源的详细信息，请参阅 "发现 Microsoft 365 资源"(第 553 页)。
- 如果已将保护计划应用于**所有用户**、**所有组**或**所有站点**组，则新添加的项目将仅在进行同步后才会包含在备份中。
- 根据 Microsoft 策略，在某个用户、组或站点从 Microsoft 365 图形用户界面中删除后，它仍可通过 API 使用几天。在此期间，已删除的项目在 Cyber Protect 中控台中处于不活动状态(灰显)，不会进行备份。当无法通过 API 使用已删除的项目时，即表示该项目不存在于 Cyber Protect 中控台中。其备份(如果有)可以在**备份存储** > **云应用程序备份**中找到。

管理在不同级别上添加的 Microsoft 365 组织

公司管理员具有对添加到客户租户级别的 Microsoft 365 组织的完全访问权限。

公司管理员具有对添加到单位的组织的有限访问权限。在这些组织中，公司管理员与单位名称一起显示在括号中，可以执行以下操作：

- 通过备份进行数据恢复。

  公司管理员可以将数据恢复到租户中的所有组织，而不管添加这些组织的级别如何。
- 浏览备份和备份中的恢复点。
- 删除备份和备份中的恢复点。
- 查看警报和活动。

在客户租户级别进行操作时，公司管理员不能执行以下操作：

- 将 Microsoft 365 组织添加到单位。
- 从单位中删除 Microsoft 365 组织。
- 同步已添加到单位的 Microsoft 365 组织。
- 针对添加到单位的 Microsoft 365 组织中的数据项，查看、创建、编辑、删除、应用、运行或吊销保护计划。

对于在单位级别进行操作的单位管理员和公司管理员，具有对添加到单位的组织的完全访问权限。但是，他们没有对父客户租户的任何资源的访问权限，包括在其中创建的保护计划。

删除 Microsoft 365 组织

删除 Microsoft 365 组织不会影响该组织数据的现有备份。如果不再需要这些备份，请先删除它们，然后再删除 Microsoft 365 组织。否则，备份仍将使用可能已计费的云存储空间。

有关如何删除备份的详细信息，请参阅 "删除备份或备份存档"(第 475 页)。

删除 Microsoft 365 组织

1. 根据添加组织的位置，以公司管理员或单位管理员身份登录到 Cyber Protect 中控台。
2. [对于在单位级别操作的公司管理员] 在管理门户中，导航到所需的单位。
3. 转到**设备** > **Microsoft 365**。
4. 选择组织，然后单击**删除组**。

结果，将撤销已应用于此组的备份计划。

但是，您还应该手动撤销备份服务应用程序对 Microsoft 365 组织数据的访问权限。

撤销访问权限

1. 以全局管理员身份登录到 Microsoft 365。
2. 转到**管理中心** > **Azure Active Directory** > **企业应用程序** > **所有应用程序**。
3. 选择**备份服务**应用程序，然后对它逐层展开。
4. 转到**属性**选项卡，然后在操作面板上单击**删除**。
5. 确认删除操作。

结果，将从备份服务应用程序中撤销对 Microsoft 365 组织数据的访问权限。

发现 Microsoft 365 资源

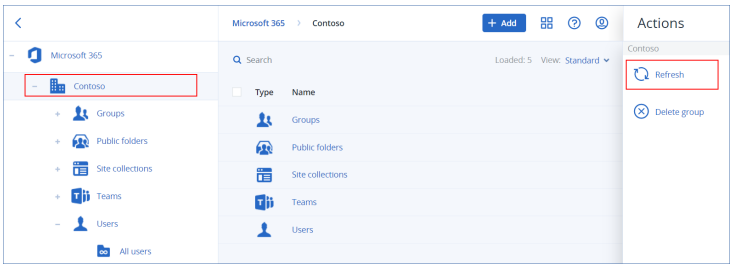
当将 Microsoft 365 组织添加到 Cyber Protection 服务中时，该组织中的资源（如邮箱、OneDrive 存储、Microsoft Teams 和 SharePoint 站点）会同步到 Cyber Protect 中控台。此操作称为“发现”，并会记录在**监控** > **活动**中。

在发现操作完成后，可以在 中控台的**设备** > **Microsoft 365** 选项卡上查看 Microsoft 365 组织的资源，并可以对这些资源应用备份计划。

自动发现操作每天运行一次，以使 Cyber Protect 中控台中的资源列表保持最新。还可以通过手动重新运行发现操作，来手动同步此列表。

手动重新运行发现操作

1. 在 Cyber Protect 中控台中，转到**设备** > **Microsoft 365**。
2. 选择 Microsoft 365 组织，然后在**操作**窗格中，单击**刷新**。



注意
每小时最多可以手动运行 10 次发现操作。达到此数量后，允许的运行数量重置为每小时一次，此后每小时再可运行一次，直到再次达到每小时总计 10 次运行。

设置 Microsoft 365 备份的频率

使用标准包含的功能，Microsoft 365 备份默认每天会运行一次，且无法使用其他预定选项。

如果在您的租户中启用了 Advanced Backup 包，则默认情况下会启用 **每天两次** 选项，并且可供您选择的频率更多。

注意
可以选择每天的备份数，但不能配置备份开始时间。备份按大概的间隔时间自动开始，间隔时间取决于在数据中心服务多个客户的云代理程序的当前负载。这可确保当天的负载均匀，以及对所有客户同等的服务质量。

可使用以下选项。

日程安排选项	每个备份之间的大概间隔
每天一次*	24 小时
每天两次(默认) **	12 小时
每天 3 次**	8 小时
每天 6 次**	4 小时

* 虽然启用 Advanced Backup 时 **每天两次**选项是默认值，但根据存储可用性，某些数据中心可能会临时启用 **每天一次** 选项。

**需要 Advanced Backup 包

注意
根据 Microsoft 365 方面的云代理程序负载和可能的限制，备份可能晚于计划的时间开始或者花费更长时间结束。如果备份花费的时间长于两次备份之间的平均间隔时间，则下次备份将重新计划，这可能导致每天的备份比选择的备份少。例如，即使您选择了每天六次备份，但可能每天只能完成两次备份。

组邮箱的备份每天只能运行一次。

保护 Exchange Online 数据

可以备份哪些项目？

您可以备份用户邮箱、共享邮箱和组邮箱。或者，可以选择备份选定邮箱的联机存档邮箱(**就地存档**)。

从 Cyber Protection 服务的 8.0 版开始，可以备份公用文件夹。如果贵组织是在 8.0 版发布之前添加到 Cyber Protection 服务中的，则需要重新添加组织才能获得此功能。请勿删除组织，只需重复执行 "添加 Microsoft 365 组织"(第 551 页) 中所述的步骤。结果是，Cyber Protection 服务获得使用相应 API 的权限。

可以恢复哪些项目?

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

可从公用文件夹备份中恢复以下项目:

- 子文件夹
- 邮寄
- 电子邮件

可以使用搜索功能查找项目。

在恢复邮箱、邮箱项目、公用文件夹和公用文件夹项目时,可以选择是否覆盖目标位置的项目。

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 Exchange Online 邮箱

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务,则选择要备份其用户数据的组织。否则,请跳过此步骤。
3. 请执行以下任一操作:
   - 若要备份所有用户的邮箱和所有共享邮箱(包括将来要创建的邮箱),请展开**用户**节点,选择**所有用户**,然后单击**组备份**。
   - 若要备份单个用户邮箱或共享邮箱,请展开**用户**节点,选择**所有用户**,选择要备份其邮箱的用户,然后单击**备份**。
   - 若要备份所有组邮箱(包括将来将要创建的组邮箱),请展开**组**节点,选择**所有组**,然后单击**组备份**。
   - 若要恢复单个组邮箱,请展开**组**节点,选择**所有组**,选择您要备份其邮箱的组,然后单击**备份**。

     注意
     适用于 Microsoft 365 的云代理程序使用具有相应权限的帐户来访问组邮箱。因此,要备份组邮箱,必须向至少一个组所有者许可具有邮箱的 Microsoft 365 用户。如果组是私有或隐藏成员资格,则所有者还必须是该组的成员。

4. 在保护计划面板上：
   - 请确保已在**备份内容**中选定 **Microsoft 365 邮箱**项目。

     如果某些单独选定的用户未将 Exchange 服务包括在其 Microsoft 365 计划中，将无法选择此选项。

     如果某些选定的组备份用户未将 Exchange 服务包括在其 Microsoft 365 计划中，将可以选择此选项，但不会将保护计划应用于这些用户。
   - 如果不想备份存档邮箱，可禁用**存档邮箱**切换。

选择公用文件夹

按如下所述方法选择公用文件夹，然后相应地指定保护计划的其他设置。

注意
公用文件夹将使用 Microsoft 365 席位的备份配额中的许可证。

选择 Exchange Online 公用文件夹

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则展开要备份其数据的组织。否则，请跳过此步骤。
3. 展开**公用文件夹**节点，然后选择**所有公用文件夹**。
4. 请执行以下任一操作：
   - 要备份所有公用文件夹(包括将来要创建的公用文件夹) ，单击**组备份**。
   - 要备份个别公用文件夹，请选择要备份的公用文件夹，然后单击**备份**。
5. 在保护计划面板中，确保已在**备份内容**中选择 **Microsoft 365 邮箱**项目。

恢复邮箱和邮箱项目

恢复邮箱

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 请执行以下任一操作：
   - 若要恢复用户邮箱，请展开**用户**节点，选择**所有用户**，选择您要恢复其邮箱的用户，然后单击**恢复**。
   - 若要恢复共享邮箱，请展开**用户**节点，选择**所有用户**，选择要恢复的共享邮箱，然后单击**恢复**。
   - 若要恢复组邮箱，请展开**组**节点，选择**所有组**，选择您要恢复其邮箱的组，然后单击**恢复**。
   - 如果用户、组或共享邮箱已删除，请在备份存储选项卡的**云应用程序备份**部分中将它们选中，然后单击**显示备份**。

   可以按名称搜索用户和组。不支持通配符。
4. 选择恢复点。

注意
若要仅查看包含邮箱的恢复点，请在**按内容过滤**中选择 **邮箱**。

5. 依次单击**恢复** > **整个邮箱**。
6. 如果多个 Microsoft 365 组织添加到 Cyber Protection 服务，则单击 **Microsoft 365 组织**即可查看、更改或指定目标组织。
   默认情况下，选择原始组织。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
7. 在**恢复至邮箱**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组织，必须指定目标邮箱。
   您无法在恢复期间创建新的目标邮箱。要将邮箱恢复为新邮箱，首先需要在所需的 Microsoft 365 组织中创建目标邮箱，然后让云代理程序同步更改。云代理程序每 24 小时自动与 Microsoft 365 同步一次。要立即同步更改，请在 Cyber Protect 中控台中的**Microsoft 365**页面上选择组织，然后单击**"刷新"**。
8. 单击**开始恢复**。
9. 选择任一覆盖选项：
   - **覆盖现有项目**
   - **不覆盖现有项目**
10. 单击**继续**以确认您的决定。

恢复邮箱项目

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 请执行以下任一操作：
   - 若要从用户邮箱中恢复项目，请展开**用户**节点，选择**所有用户**，选择其邮箱最初包含您要恢复的项目的用户，然后单击**恢复**。
   - 若要恢复共享邮箱中的项目，请展开**用户**节点，选择**所有用户**，选择最初包含要恢复的项目的共享邮箱，然后单击**恢复**。
   - 若要从组邮箱中恢复项目，请展开**组**节点，选择**所有组**，选择其邮箱最初包含您要恢复的项目的组，然后单击**恢复**。
   - 如果用户、组或共享邮箱已删除，请在备份存储选项卡的**云应用程序备份**部分中将它们选中，然后单击**显示备份**。

   可以按名称搜索用户和组。不支持通配符。
4. 选择恢复点。

注意
若要仅查看包含邮箱的恢复点，请在**按内容过滤**中选择 **邮箱**。

5. 依次单击**恢复** > **电子邮件**。
6. 浏览到所需的文件夹或使用搜索功能获取所需项目的列表。

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、附件名称和日期搜索。可以在时间范围内选择开始日期或结束日期(包括两者)，也可以同时选择两个日期进行搜索。
- 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。

7. 选择要恢复的项目。为了能够选择文件夹，请单击“恢复文件夹”图标： 

   您无法在恢复期间创建新的目标邮箱。要将新邮箱项目恢复到新邮箱，首先需要在 Microsoft 365 组织中创建目标新邮箱项目，然后让云代理程序同步更改。云代理程序每 24 小时自动与 Microsoft 365 同步一次。要立即同步更改，请在 Cyber Protect 中控台中的**Microsoft 365**页面上选择组织，然后单击**“刷新”**。

   此外，您可以执行以下任一操作：

   - 选择某个项目后，单击**“显示内容”**以查看其内容，包括附件。单击附件的名称即可下载。
   - 当选择电子邮件消息或日历项目时，单击**作为电子邮件发送**以将项目发送到指定的电子邮件地址。您可以选择发件人并编写要添加到转发项目中的文本。
   - 仅在备份未加密且您使用了搜索功能并在搜索结果中选择了单个项目时：单击**显示版本**以选择要恢复的项目版本。可以选择在选定的恢复点之前或之后的任何备份版本。
8. 单击**恢复**。
9. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则单击 **Microsoft 365 组织**即可查看、更改或指定目标组织。

   默认情况下，选择原始组织。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
10. 在**恢复至邮箱**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组织，必须指定目标邮箱。
11. [仅在恢复到用户或共享邮箱时] 在**路径**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。

    组邮箱项目始终恢复至**收件箱**文件夹。
12. 单击**开始恢复**。
13. 选择任一覆盖选项：
    - **覆盖现有项目**
    - **不覆盖现有项目**
14. 单击**继续**以确认您的决定。

恢复整个邮箱至 PST 数据文件

注意

可以使用**恢复 > 电子邮件选项**将就地存档中的电子邮件或文件夹恢复为单独的邮箱项目。有关更多信息，请参阅 "恢复邮箱项目"(第 557 页)。当使用**恢复 > 整个邮箱**或**恢复 > 作为 PST 文件**选项时，不会恢复就地存档。

恢复邮箱

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 请执行以下任一操作：
   - 要恢复用户邮箱至 PST 数据文件，请展开**用户**节点、选择**所有用户**、选择要恢复的邮箱，然后单击**恢复**。
   - 要恢复共享邮箱至 PST 数据文件，请展开**用户**节点、选择**所有用户**、选择要恢复的邮箱，然后单击**恢复**。
   - 要恢复组邮箱至 PST 数据文件，请展开**组**节点、选择**所有组**、选择要恢复其邮箱的组，然后单击**恢复**。

   可以按名称搜索用户和组。不支持通配符。

   如果用户、组或共享 Outlook 数据文件已删除，请在备份存储选项卡的**云应用程序备份**部分中选择相应项目，然后单击**显示备份**。
4. 依次单击**恢复** > **作为 PST 文件**。
5. 设置密码以加密内含 PST 文件的存档。

   密码必须至少包含一个符号。
6. 确认密码，然后单击**完成**。
7. 选定的邮箱项目将恢复为 PST 数据文件并以 ZIP 格式存档。一个 PST 文件的最大大小限制为 2 GB；因此，如果要恢复的数据超过 2 GB，它会被拆分为多个 PST 文件。ZIP 存档将受您设置的密码保护。
8. 您将收到一封电子邮件，内含指向包含已创建 PST 文件的 ZIP 存档的链接。
9. 管理员将收到您已执行恢复过程的电子邮件通知。

注意

邮箱恢复到 PST 文件可能非常耗时，原因是它不仅涉及数据传输，还涉及使用复杂算法的数据转换。

下载包含 PST 文件的存档并完成恢复

1. 请执行以下任一操作：
   - 若要从电子邮件中下载档案，请点击**下载文件**链接。

     该档案的可用时长为 96 小时。若要在 96 小时后下载档案，请重复该恢复过程。
   - 从 Cyber Protect 中控台下载存档：
     a. 转到**备份存储** > **PST 文件**。
     b. 选择亮显的最新存档。
     c. 在右侧窗格中，单击**下载**。

   存档将下载到您计算机上的默认下载目录。
2. 使用您设置用于加密存档的密码从存档中提取 PST 文件。
3. 使用 Microsoft Outlook 打开 PST 文件。

   生成的 PST 文件的大小可能比原始邮箱小得多。这是正常的。

重要事项

请勿使用**导入和导出向导**将这些文件导入到 Microsoft Outlook。

通过双击文件或右键单击文件并在上下文菜单中选择**打开方式...** > **Microsoft Outlook** 来打开文件。

恢复邮箱项目至 PST 文件

注意

可以使用**恢复 > 电子邮件选项**将就地存档中的电子邮件或文件夹恢复为单独的邮箱项目。有关更多信息，请参阅 "恢复邮箱项目"(第 557 页)。当使用**恢复 > 整个邮箱**或**恢复 > 作为 PST 文件**选项时，不会恢复就地存档。

恢复邮箱项目

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 请执行以下任一操作：
   - 若要从用户邮箱中恢复项目，请展开**用户**节点，选择**所有用户**，选择其邮箱最初包含您要恢复的项目的用户，然后单击**恢复**。
   - 若要恢复共享邮箱中的项目，请展开**用户**节点，选择**所有用户**，选择最初包含要恢复的项目的共享邮箱，然后单击**恢复**。
   - 若要从组邮箱中恢复项目，请展开**组**节点，选择**所有组**，选择其邮箱最初包含您要恢复的项目的组，然后单击**恢复**。
   - 如果用户、组或共享邮箱已删除，请在备份存储选项卡的**云应用程序备份**部分中将它们选中，然后单击**显示备份**。

   可以按名称搜索用户和组。不支持通配符。
4. 依次单击**恢复** > **电子邮件**。
5. 浏览到所需的文件夹或使用搜索功能获取所需项目的列表。

   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、附件名称和日期搜索。
   - 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。
6. 选择要恢复的项目。为了能够选择文件夹，请单击“恢复文件夹”图标： 

   此外，您可以执行以下任一操作：
   - 当已选择某个项目时，单击**显示内容**即可查看其内容，包括附件。单击附加文件的名称即可下载它。
   - 当选择电子邮件消息或日历项目时，单击**作为电子邮件发送**以将项目发送到指定的电子邮件地址。您可以选择发件人并编写要添加到转发项目中的文本。

- 仅在备份未加密且您使用了搜索功能并在搜索结果中选择了单个项目时：单击**显示版本**以选择要恢复的项目版本。可以选择在选定的恢复点之前或之后的任何备份版本。

7. 单击**恢复为 PST 文件**。
8. 设置密码以加密内含 PST 文件的存档。
   密码应至少包含一个符号。
9. 确认密码，然后单击**完成**。

选定的邮箱项目将恢复为 PST 数据文件并以 ZIP 格式存档。一个 PST 文件的最大大小限制为 2 GB；因此，如果要恢复的数据超过 2 GB，它会被拆分为多个 PST 文件。ZIP 存档将受您设置的密码保护。

您将收到一封电子邮件，内含指向包含已创建 PST 文件的 ZIP 存档的链接。

管理员将收到您已执行恢复过程的电子邮件通知。

下载包含 PST 文件的存档并完成恢复

1. 请执行以下任一操作：
   - 若要从电子邮件中下载档案，请点击**下载文件**链接。
     该档案的可用时长为 96 小时。若要在 96 小时后下载档案，请重复该恢复过程。
   - 从 Cyber Protect 中控台下载存档：
     a. 转到**备份存储** > **PST 文件**。
     b. 选择亮显的最新存档。
     c. 在右侧窗格中，单击**下载**。

   存档将下载到您计算机上的默认下载目录。
2. 使用您设置用于加密存档的密码从存档中提取 PST 文件。
3. 使用 Microsoft Outlook 打开 PST 文件。
   生成的 PST 文件的大小可能比原始邮箱小得多。这是正常的。

重要事项
请勿使用**导入和导出向导**将这些文件导入到 Microsoft Outlook。
通过双击文件或右键单击文件并在上下文菜单中选择**打开方式...** > **Microsoft Outlook** 来打开文件。

恢复公用文件夹和文件夹项目

为了恢复公用文件夹或公用文件夹项目，目标 Microsoft 365 组织的至少一个管理员必须拥有目标公用文件夹的**所有者**权限。如果恢复失败并显示拒绝访问错误，请在目标文件夹属性中指派这些权限、在 Cyber Protect 中控台中选择目标组织、单击**刷新**，然后重复执行恢复。

恢复公用文件夹或文件夹项目

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织添加到 Cyber Protection 服务，则展开要恢复其已备份数据的组织。否则，请跳过此步骤。
3. 请执行以下任一操作：

- 展开**公共文件夹**节点，选择**所有公用文件夹**，选择要恢复或最初包含要恢复项目的公用文件夹，然后单击**恢复**。
- 如果公用文件夹已删除，请在"备份存储"选项卡的**云应用程序备份**部分中选择它，然后单击**显示备份**。

可以按名称搜索公用文件夹。不支持通配符。

4. 选择恢复点。
5. 单击**恢复数据**。
6. 浏览到所需的文件夹或使用搜索功能获取所需项目的列表。

   可以按主题、发件人、收件人和日期搜索电子邮件和帖子。不支持通配符。
7. 选择要恢复的项目。为了能够选择文件夹，请单击"恢复文件夹"图标： 

   此外，您可以执行以下任一操作：
   - 当已选择电子邮件或帖子时，单击**显示内容**即可查看其内容，包括附件。单击附加文件的名称即可下载它。
   - 当电子邮件或帖子已选择时，单击**作为电子邮件发送**可将项目发送到指定的电子邮件地址。您可以选择发件人并编写要添加到转发项目中的文本。
   - 仅在备份未加密且您使用了搜索功能并在搜索结果中选择了单个项目时：单击**显示版本**以选择要恢复的项目版本。可以选择在选定的恢复点之前或之后的任何备份版本。
8. 单击**恢复**。
9. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则单击 **Microsoft 365 组织**即可查看、更改或指定目标组织。

   默认情况下，选择原始组织。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
10. 在**恢复至公用文件夹**中，查看、更改或指定目标公用文件夹。

    默认情况下，选择原始文件夹。如果此文件夹不存在或者选择了非原始组织，必须指定目标文件夹。

    您无法在恢复期间创建新的公用文件夹。要将公用文件夹恢复为新文件夹，首先需要在所需的 Microsoft 365 组织中创建目标公用文件夹，然后让云代理程序同步更改。云代理程序每 24 小时自动与 Microsoft 365 同步一次。要立即同步更改，请在 Cyber Protect 中控台中的**Microsoft 365**页面上选择组织，然后单击**"刷新"**。
11. 在**路径**中，查看或更改目标公用文件夹中的目标子文件夹。默认情况下，将重新创建原始路径。
12. 单击**开始恢复**。
13. 选择任一覆盖选项：

选项	描述
覆盖现有项目	目标位置中的所有现有文件都将被覆盖。
不覆盖现有项目	如果目标位置包含同名的文件，则不会覆盖该文件，也不会将源文件保存到目标位置。

14. 单击**继续**以确认您的决定。

保护 OneDrive 文件

可以备份哪些项目?

您可以备份整个 OneDrive 或单个文件和文件夹。

备份计划中的一个单独选项可启用对 OneNote 笔记本的备份。

文件连同它们的共享权限一起备份。不备份高级权限级别(**设计**、**完整**、**贡献**)。

某些文件中可能包含敏感信息,而 Microsoft 365 中的数据丢失防护 (DLP) 规则可能会阻止对它们的访问。将不会备份这些文件,并且在备份操作完成后也不会显示任何警告。

限制

共享邮箱不支持备份 OneDrive 内容。要备份此内容,请将共享邮箱转换为常规用户帐户,并确保已为该帐户启用 OneDrive。

可以恢复哪些项目?

您可以恢复整个 OneDrive 或备份的任何文件或文件夹。

可以使用搜索功能查找项目。

您可以选择是恢复共享权限,还是让文件从其恢复到的文件夹继承权限。

不恢复文件和文件夹的共享链接。

选择 OneDrive 文件

按如下所述选择文件,然后相应地指定保护计划的其他设置。

选择 OneDrive 文件

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务,则选择要备份其用户数据的组织。否则,请跳过此步骤。
3. 请执行以下任一操作:
   - 若要备份所有用户(包括将来将要创建的用户)的文件,请展开**用户**节点,选择**所有用户**,然后单击**组备份**。
   - 若要备份单个用户的文件,请展开**用户**节点,选择**所有用户**,选择您要备份其文件的用户,然后单击**备份**。
4. 在保护计划面板上:
   - 请确保已在**备份内容**中选定 **OneDrive** 项目。

     如果某些单独选定的用户未将 OneDrive 服务包括在其 Microsoft 365 计划中,将无法选择此选项。

     如果某些选择的组备份用户未将 OneDrive 服务包括在其 Microsoft 365 计划中,则将可以选择此选项,但不会将保护计划应用于这些用户。

- 在**要备份的项目**中，执行以下任一操作：
  - 保留默认设置 **[全部]**（所有文件）。
  - 通过添加名称或路径指定要备份的文件和文件夹。
    可以使用通配符（*、** 和 ?）。有关指定路径和使用通配符的更多详细信息，请参阅“文件过滤器”。
  - 通过浏览指定要备份的文件和文件夹。
    浏览链接仅在为单个用户创建保护计划时才可用。
- [可选] 在**要备份的项目**中，单击**显示排除**，指定要在备份期间跳过的文件和文件夹。
  文件排除优先于文件选择；即，如果在这两个字段中指定相同的文件，将在备份期间跳过此文件。
- [可选] 要备份 OneNote 笔记本，请启用**包括 OneNote** 开关。

恢复 OneDrive 和 OneDrive 文件

恢复整个 OneDrive

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 展开**用户**节点，选择**所有用户**，选择您要恢复其 OneDrive 的用户，然后单击**恢复**。
   如果用户已删除，请在备份存储选项卡的**云应用程序备份**部分中将该用户选中，然后单击**显示备份**。
   可以按名称搜索用户。不支持通配符。
4. 选择恢复点。

   注意
   若要仅查看包含 OneDrive 文件的恢复点，请在**按内容过滤**中选择 **OneDrive**。

5. 依次单击**恢复** > **整个 OneDrive**。
6. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则单击 **Microsoft 365 组织**即可查看、更改或指定目标组织。
   默认情况下，选择原始组织。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
   您无法在恢复期间创建新的 OneDrive 目标。要将 OneDrive 恢复为新的，首先需要在 Microsoft 365 组织中创建目标 OneDrive，然后让云代理程序同步更改。云代理程序每 24 小时自动与 Microsoft 365 同步一次。要立即同步更改，请在 Cyber Protect 中控台中的**Microsoft 365**页面上选择组织，然后单击**“刷新”**。
7. 在**恢复至驱动器**中，查看、更改或指定目标用户。
   默认情况下，选择原始用户。如果此用户不存在或者选择了非原始组织，必须指定目标用户。
8. 选择是否恢复文件的共享权限。
9. 单击**开始恢复**。
10. 选择任一覆盖选项：

选项	描述
覆盖现有文件(如果较旧)	如果目标位置中的同名文件比源文件旧，则源文件将保存到目标位置，以替换旧版本。
覆盖现有文件	目标位置中的所有现有文件都将被覆盖，无论其上次修改日期如何。
不覆盖现有文件	如果目标位置中有同名文件，则不会对其应用任何更改，也不会将源文件保存到目标位置。

注意
当恢复 OneNote 笔记本时，**覆盖现有文件(如果较旧)**和**覆盖现有文件**都会导致覆盖现有 OneNote 笔记本。

11. 单击**继续**以确认您的决定。

恢复 OneDrive 文件

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 展开**用户**节点，选择**所有用户**，选择您要恢复其 OneDrive 文件的用户，然后单击**恢复**。
   如果用户已删除，请在备份存储选项卡的**云应用程序备份**部分中将该用户选中，然后单击**显示备份**。
   可以按名称搜索用户。不支持通配符。
4. 选择恢复点。

注意
若要仅查看包含 OneDrive 文件的恢复点，请在**按内容过滤**中选择 **OneDrive**。

5. 依次单击**恢复** > **文件/文件夹**。
6. 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。
7. 选择要恢复的文件。
   如果备份未加密且您选择了单个文件，则可以单击**显示版本**以选择要恢复的文件版本。可以选择在选定的恢复点之前或之后的任何备份版本。
8. 如果要下载某个文件，请选择该文件，单击**下载**，选择要将文件保存到的位置，然后单击**保存**。否则，请跳过此步骤。
9. 单击**恢复**。
10. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则单击 **Microsoft 365 组织**即可查看、更改或指定目标组织。
    默认情况下，选择原始组织。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
    您无法在恢复期间创建新的 OneDrive。要将文件恢复到新的 OneDrive，首先需要在所需的 Microsoft 365 组织中创建目标 OneDrive，然后让云代理程序同步更改。云代理程序每 24 小时

自动与 Microsoft 365 同步一次。要立即同步更改，请在 Cyber Protect 中控台中的**Microsoft 365**页面上选择组织，然后单击**"刷新"**。

11. 在**恢复至驱动器**中，查看、更改或指定目标用户。
    默认情况下，选择原始用户。如果此用户不存在或者选择了非原始组织，必须指定目标用户。
12. 在**路径**中，查看或更改目标用户的 OneDrive 中的目标文件夹。默认情况下，选择原始位置。
13. 选择是否恢复文件的共享权限。
14. 单击**开始恢复**。
15. 选择文件覆盖选项之一：

选项	描述
覆盖现有文件(如果较旧)	如果目标位置中的同名文件比源文件旧，则源文件将保存到目标位置，以替换旧版本。
覆盖现有文件	目标位置中的所有现有文件都将被覆盖，无论其上次修改日期如何。
不覆盖现有文件	如果目标位置中有同名文件，则不会对其应用任何更改，也不会将源文件保存到目标位置。

注意
当恢复 OneNote 笔记本时，**覆盖现有文件(如果较旧)**和**覆盖现有文件**都会导致覆盖现有 OneNote 笔记本。

16. 单击**继续**以确认您的决定。

保护 SharePoint Online 站点

可以备份哪些项目？

可以备份 SharePoint 经典站点集合、组(现代团队)站点和通信站点。此外，还可以选择单个子站点、列表和库进行备份。

备份计划中的一个单独选项可启用对 OneNote 笔记本的备份。

在备份期间*跳过*下列项目：

- **外观和感觉**站点设置(**标题、描述和徽标**除外)。
- 站点页面注释和页面注释设置(注释**打开/关闭**)。
- **站点功能**站点设置。
- Web 部件页面和 wiki 页面中嵌入的Web 部件(由于 SharePoint Online API 限制)。
- 检出的文件 - 手动检出要编辑的文件和在库中创建或上传的所有文件(已为其启用选项**需要检出**)。要备份这些文件，请先将它们检入。
- 外部数据和受控元数据类型的列。
- 默认站点集合"domain-my.sharepoint.com"。此集合驻留所有组织用户的 OneDrive 文件。
- 回收站的内容。

限制

- 如果标题/说明大小大于 10,000 个字节，则在备份期间将截断站点/子站点/列表/列的标题和说明。
- 无法备份在 SharePoint Online 中创建的文件的早期版本。仅保护最新版本的文件。
- 无法备份演示文稿保留库。
- 无法备份在 Business Productivity Online Suite (BPOS)(即 Microsoft 365 的前身) 中创建的站点。
- 无法备份使用托管路径 `/portals`(例如，`https://<tenant>.sharepoint.com/portals/...`) 的站点的设置。
- 仅当在目标 Microsoft 365 组织中启用信息权限管理 (IRM) 时，才能恢复列表或库的 IRM 设置。

可以恢复哪些项目？

可从站点备份中恢复以下项目：

- 整个站点
- 子站点
- 列表
- 列表项目
- 文档库
- 文档
- 列表项目附件
- 站点页面和 wiki 页面

可以使用搜索功能查找项目。

项目可以恢复至原始或非原始站点。已恢复项目的路径与原始项目相同。如果此路径不存在，请进行创建。

您可以选择是恢复共享权限，还是在恢复后让项目从父对象继承权限。

无法恢复哪些项目？

- 子站点基于 **Visio 进程存储库**模板。
- 以下类型的列表：**调查列表**、**任务列表**、**图片库**、**链接**、**日历**、**讨论板**、**外部**和**导入电子表格**。
- 启用多种内容类型的列表。

选择 SharePoint Online 数据

按如下所述选择数据，然后相应地指定保护计划的其他设置。

选择 SharePoint Online 数据

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要备份其用户数据的组织。否则，请跳过此步骤。
3. 请执行以下任一操作：

- 要备份组织中所有经典 SharePoint 站点(包括将来要创建的站点),请展开**站点集合**节点、选择**所有站点集合**,然后单击**组备份**。
- 若要备份单个经典站点,请展开**站点集合**节点,选择**所有站点集合**,选择您要备份的站点,然后单击**备份**。
- 要备份所有组(现代团队)站点(包括将来要创建的站点),请展开**组**节点、选择**所有组**,然后单击**组备份**。
- 要备份单个组(现代团队)站点,请展开**组**节点、选择**所有组**、选择要备份其站点的组,然后单击**备份**。

4. 在保护计划面板上:
   - 请确保已在**备份内容**中选定 **SharePoint 站点**项目。
   - 在**要备份的项目**中,执行以下任一操作:
     - 保留默认设置**[全部]**(已选定站点的所有项目)。
     - 通过添加名称或路径指定要备份的子站点、列表和库。

       若要备份子站点或顶级站点列表/库,请按以下格式指定其显示名称:`/display name/**`

       若要备份子站点列表/库,请按以下格式指定其显示名称:`/subsite display name/list display name/**`

       子站点、列表和库的显示名称显示在 SharePoint 站点或子站点的**站点内容**页面上。
     - 通过浏览指定要备份的子站点。

       浏览链接仅在为单个站点创建保护计划时才可用。
   - [可选]在**要备份的项目**中,单击**显示排除**,指定备份期间要跳过的子站点、列表和列表。

     文件排除优先于文件选择,即,如果您在这两个字段中指定 相同的子站点,将在备份期间跳过此子站点。
   - [可选]要备份 OneNote 笔记本,请启用**包括 OneNote** 开关。

恢复 SharePoint Online 数据

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务,则选择要恢复其备份数据的组织。否则,请跳过此步骤。
3. 请执行以下任一操作:
   - 要从组(现代团队)站点中恢复数据,请展开**组**节点、选择**所有组**、选择其站点最初包含要恢复的项目的组,然后单击**恢复**。
   - 若要从经典站点中恢复数据,请展开**站点集合**节点,选择**所有站点集合**,选择最初包含您要恢复的项目的站点,然后单击**恢复**。
   - 如果站点已删除,请在备份存储选项卡的**云应用程序备份**部分中将它选中,然后单击**显示备份**。

   您可以按名称搜索组和站点。不支持通配符。
4. 选择恢复点。

注意

若要仅查看包含 SharePoint 站点的恢复点,请在**按内容过滤**中选择 **SharePoint 站点**。

5. 单击**恢复 SharePoint 文件**。
6. 浏览到所需的文件夹或使用搜索功能获取所需数据项目的列表。
7. 选择要恢复的项目。

   如果备份未加密且您使用了搜索功能并在搜索结果中选择了单个项目，则可以单击**显示版本**以选择要恢复的项目版本。可以选择在选定的恢复点之前或之后的任何备份版本。
8. [可选] 要下载某个项目，请选择该项目、单击**下载**、选择要保存项目的位置，然后单击**保存**。
9. 单击**恢复**。
10. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则单击 **Microsoft 365 组织**即可查看、更改或指定目标组织。

    默认情况下，选择原始组织。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
11. 在**恢复至站点**中，查看、更改或指定目标站点。

    您无法在恢复期间创建新的 SharePoint 网站。要将 SharePoint 网站恢复为新网站，首先需要在所需的 Microsoft 365 组织中创建目标网站，然后让云代理程序同步更改。云代理程序每 24 小时自动与 Microsoft 365 同步一次。要立即同步更改，请在 Cyber Protect 中控台中的**Microsoft 365**页面上选择组织，然后单击**“刷新”**。
12. 选择是否恢复已恢复的项目的共享权限。
13. 单击**开始恢复**。
14. 选择任一覆盖选项：

选项	描述
覆盖现有文件(如果较旧)	如果目标位置中的同名文件比源文件旧，则源文件将保存到目标位置，以替换旧版本。
覆盖现有文件	目标位置中的所有现有文件都将被覆盖，无论其上次修改日期如何。
不覆盖现有文件	如果目标位置中有同名文件，则不会对其应用任何更改，也不会将源文件保存到目标位置。

注意
当恢复 OneNote 笔记本时，**覆盖现有文件(如果较旧)**和**覆盖现有文件**都会导致覆盖现有 OneNote 笔记本。

15. 单击**继续**以确认您的决定。

保护 Microsoft 365 Teams

可以备份哪些项目？

可以备份整个团队。这包括团队名称、团队成员列表、团队频道及其内容、团队邮箱和会议以及团队站点。

备份计划中的一个单独选项可启用对 OneNote 笔记本的备份。

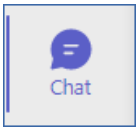
可以恢复哪些项目?

- 整个团队
- 团队频道
- 频道文件
- 团队邮箱
- 团队邮箱中的电子邮件文件夹
- 团队邮箱中的电子邮件
- 会议
- 团队站点

无法恢复团队频道中的会话,但可以将它们下载为单个 html 文件。

限制

不备份以下项目:

- 常规频道的设置(适度首选项) - 由于 Microsoft Teams beta API 限制。
- 自定义频道的设置(适度首选项) - 由于 Microsoft Teams beta API 限制。
- 会议记录。
- 聊天会话 

中的消息。此会话包含私人一对一聊天和群聊。
- 贴纸和好评。

以下频道选项卡支持备份和恢复:

- Word
- Excel
- PowerPoint
- PDF
- 文档库

选择团队

按如下所述选择团队,然后相应地指定保护计划的其他设置。

选择团队

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务,则选择要备份其团队的组织。否则,请跳过此步骤。
3. 请执行以下任一操作:
   - 要备份组织中的所有团队(包括将来要创建的团队),请展开**团队**节点、选择**所有团队**,然后单击**组备份**。

- 要备份个别团队，请展开**团队**节点、选择**所有团队**、选择要备份的团队，然后单击**备份**。

  可以按名称搜索团队。不支持通配符。

4. 在保护计划面板上：
   - 确保已在**备份内容**中选择 **Microsoft Teams** 项目。
   - [可选] 在**保留时间**中，设置清理选项。
   - [可选] 如果要加密备份，请启用**加密**开关，然后设置密码并选择加密算法。
   - [可选] 要备份 OneNote 笔记本，请启用**包括 OneNote** 开关。

恢复整个团队

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要恢复其备份团队的组织。否则，请跳过此步骤。
3. 展开**团队**节点、选择**所有团队**、选择要恢复的团队，然后单击**恢复**。

   可以按名称搜索团队。不支持通配符。
4. 选择恢复点。
5. 依次单击**恢复** > **整个团队**。

   如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则单击 **Microsoft 365 组织**即可查看、更改或指定目标组织。

   默认情况下，选择原始组织。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
6. 在**恢复至团队**中，查看目标团队或选择另一个团队。

   默认情况下，原始团队处于选中状态。如果此团队不存在(例如，它已删除)或选择的组织不包含原始团队，则必须从下拉列表中选择目标团队。

   只能将团队恢复到现有团队。无法在恢复操作期间创建团队。
7. 单击**开始恢复**。
8. 选择任一覆盖选项：
   - **覆盖现有内容(如果较旧)**
   - **覆盖现有内容**
   - **不覆盖现有内容**

   注意

   当恢复 OneNote 笔记本时，**覆盖现有内容(如果较旧)**和**覆盖现有内容**选项都会导致覆盖现有 OneNote 笔记本。
9. 单击**继续**以确认您的决定。

当删除 Microsoft Teams 图形界面中的频道时，不会立即将其从系统中删除。因此，当恢复整个团队时，将无法使用该频道的名称，并且将向其添加一个后缀。

在频道的**文件**选项卡中，会话恢复为单个 html 文件。可以在根据以下模式命名的文件夹中找到此文件：<团队名称>_<频道名称>_conversations_backup_<恢复日期>T<恢复时间>Z。

注意
恢复团队或团队频道后，请转到 Microsoft Teams、选择已恢复的频道，然后单击其**文件**选项卡。否则，这些频道的后续备份将不包括此选项卡的内容 - 由于 Microsoft Teams beta API 限制。

恢复团队频道或团队频道中的文件

恢复团队频道

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要恢复其备份团队的组织。否则，请跳过此步骤。
3. 展开 **Teams**节点、选择**所有团队**、选择要恢复其频道的团队，然后单击**恢复**。
4. 选择恢复点。
5. 依次单击**恢复** > **频道**。
6. 选择要恢复的频道，然单击**恢复**。要选择主页中的频道，请选中其名称前面的复选框。
   提供以下搜索选项：
   - 对于**会话**：发件人、主题、内容、语言、附件名称、日期或日期范围。
   - 对于**文件**：文件名或文件夹名称、文件类型、大小、上次更改的日期或日期范围。

   注意
   还可以在本地下载文件，而不是恢复它们。
7. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则单击 **Microsoft 365 组织**即可查看、更改或指定目标组织。
   默认情况下，选择原始组织。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
8. 在**恢复至团队**中，查看、更改或指定目标团队。
   默认情况下，原始团队处于选中状态。如果此团队不存在或者选择了非原始组织，则必须指定目标团队。
9. 在**恢复至频道**中，查看、更改或指定目标频道。
10. 单击**开始恢复**。
11. 选择任一覆盖选项：
    - **覆盖现有内容(如果较旧)**
    - **覆盖现有内容**
    - **不覆盖现有内容**

    注意
    当恢复 OneNote 笔记本时，**覆盖现有内容(如果较旧)**和**覆盖现有内容**选项都会导致覆盖现有 OneNote 笔记本。
12. 单击**继续**以确认您的决定。

在频道的**文件**选项卡中，会话恢复为单个 html 文件。可以在根据以下模式命名的文件夹中找到此文件：<团队名称>_<频道名称>_conversations_backup_<恢复日期>T<恢复时间>Z。

注意
恢复团队或团队频道后，请转到 Microsoft Teams、选择已恢复的频道，然后单击其**文件**选项卡。否则，这些频道的后续备份将不包括此选项卡的内容 - 由于 Microsoft Teams beta API 限制。

恢复团队频道中的文件

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要恢复其备份团队的组织。否则，请跳过此步骤。
3. 展开 **Teams**节点、选择**所有团队**、选择要恢复其频道的团队，然后单击**恢复**。
4. 选择恢复点。
5. 依次单击**恢复** > **频道**。
6. 选择所需频道，然后打开**文件**文件夹。
   浏览并找到所需项目，或者使用搜索功能获取所需项目的列表。以下搜索选项可用：文件名或文件夹名称、文件类型、大小、上次更改的日期或日期范围。
7. [可选] 要下载某个项目，请选择该项目、单击**下载**、选择要保存项目的位置，然后单击**保存**。
8. 选择要恢复的项目，然单击**恢复**
9. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则单击 Microsoft 365 组织即可查看、更改或指定目标组织。
   默认情况下，选择原始组织。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
10. 在**恢复至团队**中，查看、更改或指定目标团队。
    默认情况下，原始团队处于选中状态。如果此团队不存在或者选择了非原始组织，则必须指定目标团队。
11. 在**恢复至频道**中，查看、更改或指定目标频道。
12. 选择是否恢复已恢复的项目的共享权限。
13. 单击**开始恢复**。
14. 选择任一覆盖选项：
    - **覆盖现有内容(如果较旧)**
    - **覆盖现有内容**
    - **不覆盖现有内容**

    注意
    当恢复 OneNote 笔记本时，**覆盖现有内容(如果较旧)**和**覆盖现有内容**选项都会导致覆盖现有 OneNote 笔记本。
15. 单击**继续**以确认您的决定。

无法恢复个别会话。在主窗格中，只能浏览**会话**文件夹或将其内容下载为单个 html 文件。为此，请单击“恢复文件夹”图标  、选择所需的**会话**文件夹，然后单击**下载**。

可以在**会话**文件夹中按以下内容搜索邮件：

- 发件人
- 内容
- 附件名称
- 日期

恢复团队邮箱

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要恢复其备份团队的组织。否则，请跳过此步骤。
3. 展开**团队**节点、选择**所有团队**、选择要恢复其邮箱的团队，然后单击**恢复**。
   可以按名称搜索团队。不支持通配符。
4. 选择恢复点。
5. 依次单击**恢复** > **电子邮件**。
6. 单击“恢复文件夹”图标  、选择根邮箱文件夹，然后单击**恢复**。

   注意
   还可以恢复选定邮箱中的个别文件夹。

7. 单击**恢复**。
8. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则单击 **Microsoft 365 组织**即可查看、更改或指定目标组织。
   默认情况下，选择原始组织。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
9. 在**恢复至邮箱**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组织，必须指定目标邮箱。
10. 单击**开始恢复**。
11. 选择任一覆盖选项：
    - **覆盖现有项目**
    - **不覆盖现有项目**
12. 单击**继续**以确认您的决定。

恢复团队邮箱项目至 PST 文件

恢复团队邮箱项目

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 可以按名称搜索用户和组。不支持通配符。
4. 展开**团队**节点、选择**所有团队**、选择要恢复其邮箱(最初包含相应项目)的团队，然后单击**恢复**。

5. 依次单击**恢复** > **电子邮件**。
6. 浏览到所需的文件夹或使用搜索功能获取所需项目的列表。
   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、附件名称和日期搜索。
   - 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。
7. 选择要恢复的项目。为了能够选择文件夹，请单击“恢复文件夹”图标： 
   此外，您可以执行以下任一操作：
   - 当已选择某个项目时，单击**显示内容**即可查看其内容，包括附件。单击附加文件的名称即可下载它。
   - 当选择电子邮件消息或日历项目时，单击**作为电子邮件发送**以将项目发送到指定的电子邮件地址。您可以选择发件人并编写要添加到转发项目中的文本。
   - 当备份未加密时，您使用了搜索，并从搜索结果中选择了一个项目：单击**显示版本**以查看项目版本。可以选择任何备份的版本，无论它早于还是晚于选定恢复点。
8. 单击**恢复为 PST 文件**。
9. 设置密码以加密内含 PST 文件的存档。
   密码应至少包含一个符号。
10. 确认密码，然后单击**完成**。

选定的邮箱项目将恢复为 PST 数据文件并以 ZIP 格式存档。一个 PST 文件的最大大小限制为 2 GB；因此，如果要恢复的数据超过 2 GB，它会被拆分为多个 PST 文件。ZIP 存档将受您设置的密码保护。

您将收到一封电子邮件，内含指向包含已创建 PST 文件的 ZIP 存档的链接。

管理员将收到您已执行恢复过程的电子邮件通知。

下载包含 PST 文件的存档并完成恢复

1. 请执行以下任一操作：
   - 要从电子邮件中下载存档，请点击**下载文件**链接。
     存档可在 24 小时内下载。如果链接过期，请重复恢复过程。
   - 从 Cyber Protect 中控台下载存档：
     a. 转到**备份存储** > **PST 文件**。
     b. 选择亮显的最新存档。
     c. 在右侧窗格中，单击**下载**。

   存档将下载到您计算机上的默认下载目录。
2. 使用您设置用于加密存档的密码从存档中提取 PST 文件。
3. 在 Microsoft Outlook 中，打开或导入 PST 文件。要了解如何操作，请参阅 Microsoft 文档。

恢复电子邮件和会议

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要恢复其备份团队的组织。否则，请跳过此步骤。
3. 展开**团队**节点、选择**所有团队**、选择要恢复其电子邮件或会议的团队，然后单击**恢复**。
   可以按名称搜索团队。不支持通配符。
4. 选择恢复点。
5. 依次单击**恢复** > **电子邮件**。
6. 浏览并找到所需项目，或者使用搜索功能获取所需项目的列表。
   提供以下搜索选项：
   - 对于电子邮件：按主题、发件人、收件人和日期搜索。
   - 对于会议：按事件名称和日期搜索。
7. 选择要恢复的项目，然单击**恢复**。

   注意
   可以在**日历**文件夹中找到会议。

   此外，您可以执行以下任一操作：
   - 当已选择某个项目时，单击**显示内容**即可查看其内容，包括附件。单击附加的文件的名称可下载它。
   - 当已选择电子邮件或会议时，单击**作为电子邮件发送**即可将项目发送到指定的电子邮件地址。您可以选择发件人并编写要添加到转发项目中的文本。
8. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则单击 **Microsoft 365 组织**即可查看、更改或指定目标组织。
   默认情况下，选择原始组织。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
9. 在**恢复至邮箱**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组织，必须指定目标邮箱。
10. 单击**开始恢复**。
11. 选择任一覆盖选项：
    - **覆盖现有项目**
    - **不覆盖现有项目**
12. 单击**继续**以确认您的决定。

恢复团队站点或站点的特定项目

1. 单击 **Microsoft 365**。
2. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则选择要恢复其备份团队的组织。否则，请跳过此步骤。
3. 展开**团队**节点、选择**所有团队**、选择要恢复其站点的团队，然后单击**恢复**。

可以按名称搜索团队。不支持通配符。

4. 选择恢复点。
5. 依次单击**恢复** > **团队站点**。
6. 浏览并找到所需项目，或者使用搜索功能获取所需项目的列表。
7. [可选] 要下载某个项目，请选择该项目、单击**下载**、选择要保存项目的位置，然后单击**保存**。
8. 选择要恢复的项目，然单击**恢复**。
9. 如果多个 Microsoft 365 组织已添加到 Cyber Protection 服务，则单击 **Microsoft 365 组织**即可查看、更改或指定目标组织。

   默认情况下，原始组织和团队处于选中状态。如果该组织不再注册在 Cyber Protection 服务中，则必须指定目标组织。
10. 在**恢复至团队**中，查看、更改或指定目标团队。

    默认情况下，原始团队处于选中状态。如果此团队不存在或者选择了非原始组织，则必须指定目标站点。
11. 选择是否恢复已恢复的项目的共享权限。
12. 单击**开始恢复**。
13. 选择任一覆盖选项：
    - **覆盖现有内容(如果较旧)**
    - **覆盖现有内容**
    - **不覆盖现有内容**

    注意
    当恢复 OneNote 笔记本时，**覆盖现有内容(如果较旧)** 和**覆盖现有内容**选项都会导致覆盖现有 OneNote 笔记本。
14. 单击**继续**以确认您的决定。

保护 OneNote 笔记本

默认情况下，OneNote 笔记本包含在 OneDrive 文件、Microsoft Teams 和 SharePoint 站点的备份中。

要从这些备份中排除 OneNote 笔记本，请在相应备份计划中禁用**包括 OneNote** 开关。

恢复备份的 OneNote 笔记本

要了解如何恢复备份的 OneNote 笔记本，请参阅相应主题：

- 对于 OneDrive 备份，请参阅 "恢复整个 OneDrive"(第 564 页) 或 "恢复 OneDrive 文件"(第 565 页)。
- 对于 Teams 备份，请参阅 "恢复整个团队"(第 571 页)、"恢复团队频道或团队频道中的文件"(第 572 页) 或 "恢复团队站点或站点的特定项目"(第 576 页)。
- 对于 SharePoint 站点备份，请参阅 "恢复 SharePoint Online 数据"(第 568 页)。

支持的版本

- OneNote(OneNote 2016 及更高版本)
- 适用于 Windows 10 的 OneNote

限制和已知问题

- 保存在 OneDrive 或 SharePoint 中的 OneNote 笔记本限制为 2 GB。无法将较大的 OneNote 笔记本恢复到 OneDrive 或 SharePoint 目标。
- 不支持带有分区组的 OneNote 笔记本。
- 在包含带有非默认名称的分区的备份 OneNote 笔记本中，第一个分区以默认名称显示(例如新分区或未命名分区) 。这可能会影响具有多个分区的笔记本中的分区顺序。
- 当恢复 OneNote 笔记本时，**覆盖现有内容(如果较旧)** 和**覆盖现有内容**选项都会导致覆盖现有 OneNote 笔记本。
- 当恢复整个团队、团队站点或团队站点的站点资产文件夹，并已选择**覆盖现有内容(如果较旧)** 或**覆盖现有内容**选项时，将不会覆盖该团队的默认 OneNote 笔记本。恢复成功，并显示警告*无法更新文件"/sites/<团队名称>/SiteAssets/<OneNote 笔记本名称>"的属性*。

保护 Microsoft 365 协作应用程序席位

可以使用 "Advanced Email Security" 包，它会为您的 Microsoft 365、Google Workspace 或 Open-Xchange 邮箱提供实时保护：

- 防恶意软件和防垃圾邮件
- 电子邮件中 URL 扫描
- DMARC 分析
- 防网络钓鱼
- 假冒保护
- 附件扫描
- 内容拆解与重建
- 信任图

还可以启用 Microsoft 365 协作应用程序席位，从而保护 Microsoft 365 云协作应用程序免受内容传播安全威胁。这些应用程序包括 OneDrive、SharePoint 和 Teams。

Advanced Email Security 可以按工作负载或按 GB 启用，这将影响您的许可模式。

从 Cyber Protect Cloud 中控台进行 Advanced Email Security 数据录入

1. 单击**设备** > **Microsoft 365**。
2. 单击**"用户"**节点，然后单击右上角的**"转至电子邮件安全"**链接。

在Advanced Email Security 产品彩页中，了解有关 Advanced Email Security 的详细信息。

有关配置说明，请参阅Advanced Email Security with Perception Point。

保护 Google Workspace 数据

注意
在合规模式下，此功能不适用于租户。有关详细信息，请参阅 "合规模式"(第 995 页) 。

Google Workspace 保护是什么意思？

- Google Workspace 用户数据(Gmail 邮箱、日历、联系人、Google Drive) 和 Google Workspace Shared Drive 的云到云备份和恢复。
- 电子邮件、文件、联系人和其他项目的粒度恢复。
- 支持多个 Google Workspace 组织和跨组织恢复。
- 已备份文件的可选公证(通过 Ethereum 块链数据库方式) 。如果启用，则可以证明文件在备份后是可信的且未经更改。
- 可选全文本搜索。如果启用，则可以按其内容搜索电子邮件。
- 在性能不下降的情况下，每个公司最多 5,000 个项目(邮箱、Google Drive 和 Shared Drive) 可以得到保护。
- 备份数据会自动进行压缩，并且它所占用的备份位置空间少于其原始位置空间。云到云备份的压缩级别是固定的，对应于非云到云备份的**正常**级别。有关这些级别的详细信息，请参阅 "压缩级别"(第 407 页) 。

所需用户权限

在 Cyber Protection 中

在 Cyber Protection 中，您需要成为客户租户级别的公司管理员。单位级别的公司管理员、单位管理员和用户无法备份或恢复 Google Workspace 数据。

在 Google Workspace 中

要将 Google Workspace 组织添加到 Cyber Protection 服务，您必须以已启用 API 访问权限的超级管理员身份登录(在 Google 管理中控台中，**安全** > **API 参考** > **启用 API 访问权限**) 。

超级管理员密码不会存储在任何位置，也不会用于执行备份和恢复。在 Google Workspace 中更改此密码并不会影响 Cyber Protection 服务操作。

如果从 Google Workspace 中删除已添加 Google Workspace 组织的超级管理员或已指派权限较少的角色，则备份会失败并显示诸如“访问被拒绝”之类的错误。在这种情况下，请重复 "添加 Google Workspace 组织"(第 580 页) 中所述的步骤，然后指定有效的超级管理员凭据。为了避免出现这种情况，建议您创建一个专用超级管理员用户来执行备份和恢复。

关于备份预定

由于云代理程序为多个客户提供服务，因此它会自行确定每个保护计划的开始时间，以确保一天中的负载均匀，并为所有客户提供同等的服务质量。

每个保护计划每天都在当天的同一时间运行。

默认选项是**每天一次**。使用 Advanced Backup 包，您可以每天预定最多六个备份。备份按大概的间隔时间开始，间隔时间取决于在数据中心服务多个客户的云代理程序的当前负载。这可确保当天的负载均匀，以及对所有客户同等的服务质量。

限制

- Cyber Protect 中控台仅会显示指派有 Google Workspace 许可证和邮箱或 Google Drive 的用户。
- 归档或暂停的 Google Workspace 用户在发现操作更改其状态后，将在 Cyber Protect 中控台中显示为非活动状态(已灰显) 。您无法将新备份计划应用于非活动用户。现有备份计划将保持 72 小时。

  在 72 小时后的发现操作后，已存档或暂停的用户将从 Cyber Protect 中控台中删除，其数据将不再备份。现有备份仍然可用。
- 已删除的 Google Workspace 用户帐户的备份不会自动从云存储中删除。这些备份会按其使用的存储空间进行计费。
- 原生 Google 格式的文档作为一般办公文档进行备份，在 Cyber Protect 中控台中用不同的扩展名显示(例如 .docx 或 .pptx) 。在恢复期间，文档会转换回其原始格式。
- 可每小时手动运行多达 10 个备份。有关详细信息，请参阅 "手动运行云到云备份"(第 212 页) 。
- 可以同时运行多达 10 个云到云恢复操作。此数量包括 Microsoft 365 和 Google Workspace 恢复操作。
- 即使可以从搜索结果中选择此类项目，也无法同时从不同恢复点来恢复项目。
- 您只能对一个工作负载应用一个单独的备份计划。
- 当单独的备份计划和组备份计划应用于相同的工作负载时，单独计划中的设置优先。

日志记录

使用云到云资源的操作，例如查看备份电子邮件的内容、下载附件或文件、将电子邮件恢复到非原始邮箱或将其作为电子邮件发送可能会侵犯用户隐私。这些操作记录在管理门户的**监控** > **审核日志**中。

添加 Google Workspace 组织

要将 Google Workspace 组织添加到 Cyber Protection 服务，需要一个个人专用的 Google Cloud 项目。有关如何创建和配置此类项目的更多信息，请参阅 "创建个人版 Google Cloud 项目"(第 581 页) 。

通过使用专用的个人版 Google Cloud 项目添加 Google Workspace 组织

1. 以公司管理员身份登录到 Cyber Protect 中控台。
2. 依次单击**设备** > **添加** > **Google Workspace**。
3. 输入 Google Workspace 帐户的超级管理员的电子邮件地址。
   对于此过程，是否已为超级管理员电子邮件帐户启用了两步验证无关紧要。
4. 浏览到 JSON 文件，它包含在 Google Cloud 项目中创建的服务帐户的私钥。
   还可以将文件内容粘贴为文本。

5. 单击**确认**。

结果，Google Workspace 组织显示在 中控台中的**设备**选项卡下。

有用提示

- 在添加 Google Workspace 组织之后，系统将备份主域和所有辅助域(如果有)中的用户数据和 Shared Drive。备份的资源将显示在一个列表中，并且不会按其域分组。
- 从将组织添加到 Cyber Protection 服务的那一刻开始，云代理程序就会每 24 小时与 Google Workspace 同步一次。如果添加或删除用户或 Shared Drive，您在 Cyber Protect 中控台中不会立即看到此更改。要立即同步更改，请在 **Google Workspace** 页面上选择相应组织，然后单击**刷新**。

  有关同步 Google Workspace 组织和 Cyber Protect 中控台的资源的详细信息，请参阅 "发现 Google Workspace 资源"(第 584 页)。
- 如果已将保护计划应用于**所有用户**或**所有 Shared Drive** 组，则新添加的项目将仅在进行同步后才会包含在备份中。
- 根据 Google 策略，当某个用户或 Shared Drive 从 Google Workspace 图形用户界面中删除时，它仍可在几天内通过 API 进行使用。在此期间，已删除的项目在 Cyber Protect 中控台中处于不活动状态(灰显)，不会进行备份。当无法通过 API 使用已删除的项目时，即表示该项目不存在于 Cyber Protect 中控台中。其备份(如果有)可以在**备份存储** > **云应用程序备份**中找到。

创建个人版 Google Cloud 项目

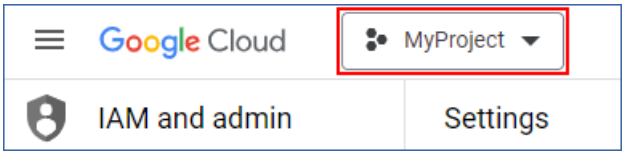
若要通过使用专用的 Google Cloud 项目将 Google Workspace 组织添加到 Cyber Protection 服务，需要执行以下操作：

1. 创建新 Google Cloud 项目。
2. 为此项目启用所需的 API。
3. 为此项目配置凭据。
   a. 配置 OAuth 同意屏幕。
   b. 为 Cyber Protection 服务创建和配置服务帐户。
4. 将新项目访问权限授予 Google Workspace 帐户。

注意
本主题包含第三方用户界面的描述，该用户界面可能在不提前通知的情况下进行更改。

创建新 Google Cloud 项目

1. 作为超级管理员登录到 Google Cloud Platform (console.cloud.google.com)。
2. 在 Google Cloud Platform 中控台中，单击左上角的项目选择器。



3. 在打开的屏幕中，选择一个组织，然后单击**新建项目**。

4. 为新项目指定一个名称。
5. 单击**创建**。

结果将创建新的 Google Cloud 项目。

为此项目启用所需的 API

1. 在 Google Cloud Platform 中控台中，选择新项目。
2. 从导航菜单，选择 **API 和服务** > **启用的 API 和服务**。
3. 在此项目中依次禁用默认启用的 API。
   a. 向下滚动**启用的 API 和服务**页面，然后单击启用的 API 的名称。
      将打开选定 API 的 **API/服务详细信息**页面。
   b. 单击**禁用 API**，然后通过单击**禁用**来确认选择。
   c. [如果提示] 单击**确认**以确认选择。
   d. 返回到 **API 和服务** > **启用的 API 和服务**，然后禁用下一个 API。
4. 从导航菜单，选择 **API 和服务** > **库**。
5. 在 API 库中，依次启用以下 API：
   - Admin SDK API
   - Gmail API
   - Google Calendar API
   - Google Drive API
   - Google People API

   使用搜索栏查找所需的 API。要启用 API，请单击其名称，然后单击**启用**。要搜索下一个 API，请返回到 API 库，方法是从导航菜单选择 **API 和服务** > **库**。

配置 OAuth 同意屏幕

1. 从 Google Cloud Platform 中的导航菜单，选择 **API 和服务** > **OAuth 同意屏幕**。
2. 在打开的窗口中，为用户类型选择**内部**，然后单击**创建**。
3. 在**应用程序名称**字段中，为应用程序指定一个名称。
4. 在**用户支持电子邮件**字段中，输入超级管理员的电子邮件。
5. 在**开发人员联系信息**字段中，输入超级管理员的电子邮件。
6. 将所有其他字段保持空白，然后单击**保存并继续**。
7. 在**范围**页面上，单击**保存并继续**，无需更改任何内容。
8. 在**概要**页面中，验证您的设置，然后单击**返回到仪表板**。

为 Cyber Protection 服务创建和配置服务帐户

1. 从 Google Cloud Platform 的导航菜单中，选择 **IAM 和管理员** > **服务帐户**。
2. 单击**创建服务帐户**。
3. 指定服务帐户的名称。
4. [可选] 指定服务帐户的描述。

5. 单击**创建并继续**。
6. 在**授予此服务帐户对项目的访问权限**和**授予用户对此服务帐户的访问权限**步骤中，不要更改任何内容。
7. 单击**完成**。

   服务帐户页面即会打开。
8. 在**服务帐户**页面中，选择新的服务帐户，然后在**操作**下，单击**管理密钥**。
9. 在**密钥**下，单击**添加密钥** > **创建新密钥**，然后选择 **JSON** 密钥类型。
10. 单击**创建**。

    结果是，具有服务帐户的私钥的 JSON 文件将自动下载到您的计算机。请安全存储此文件，因为需要它来将 Google Workspace 组织添加到 Cyber Protection 服务。

将新项目访问权限授予 Google Workspace 帐户

1. 从 Google Cloud Platform 的导航菜单，选择 **IAM 和管理员** > **服务帐户**。
2. 在列表中，找到您创建的服务帐户，然后复制在 **OAuth 2.0 客户端 ID** 列中显示的客户端 ID。
3. 作为超级管理员登录到 Google Admin 中控台 (admin.google.com)。
4. 从导航菜单，选择**安全性** > **访问和数据控制** > **API 控件**。
5. 向下滚动 **API 控件**页面，然后在**域范围的委托**下，单击**管理域范围的委托**。将打开**域范围的委托**页面。
6. 在**域范围的委托**页面上，单击**添加新委托**。

   添加新客户端 ID 窗口即会打开。
7. 在**客户端 ID** 字段中，输入服务帐户客户端的客户端 ID。
8. 在 **OAuth 范围**字段中，复制并粘贴以下逗号分隔的范围列表：

   ```
   https://mail.google.com,https://www.googleapis.com/auth/contacts,https://www.googleapis.com/auth/calendar,https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.directory.domain.readonly,https://www.googleapis.com/auth/drive,https://www.googleapis.com/auth/gmail.modify
   ```

   或者，可以每行添加一个范围：
   - https://mail.google.com
   - https://www.googleapis.com/auth/contacts
   - https://www.googleapis.com/auth/calendar
   - https://www.googleapis.com/auth/admin.directory.user.readonly
   - https://www.googleapis.com/auth/admin.directory.domain.readonly
   - https://www.googleapis.com/auth/drive
   - https://www.googleapis.com/auth/gmail.modify
9. 单击**授权**。

结果是，新的 Google Cloud 项目可以访问 Google Workspace 帐户中的数据。若要备份数据，需要将此项目链接到 Cyber Protection 服务。有关如何执行此操作的详细信息，请参阅 "通过使用专用的个人版 Google Cloud 项目添加 Google Workspace 组织"(第 580 页)。

如果需要吊销 Google Cloud 项目对 Google Workspace 帐户的访问权限，以及各自的 Cyber Protection 服务访问权限，则删除项目所使用的 API 客户端。

吊销对 Google Workspace 帐户的访问权限

1. 在 Google Admin 中控台 (admin.google.com) 中，作为超级管理员登录。
2. 从导航菜单，选择**安全性** > **访问和数据控制** > **API 控件**。
3. 向下滚动 **API 控件**页面，然后在**域范围的委托**下，单击**管理域范围的委托**。将打开**域范围的委托**页面。
4. 在**域范围的委托**页面上，选择项目所使用的 API 客户端，然后单击**删除**。
   结果是，Google Cloud 项目和 Cyber Protection 服务将不能访问 Google Workspace 帐户并备份其中的数据。

发现 Google Workspace 资源

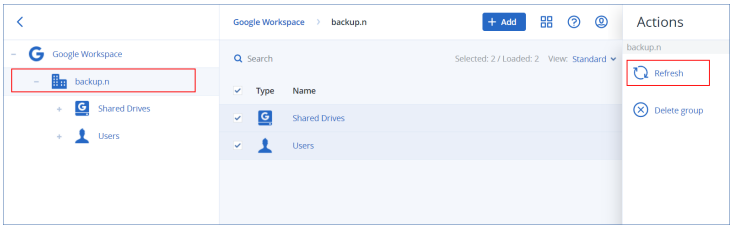
当将 Google Workspace 组织添加到 Cyber Protection 服务中时，该组织中的资源(如邮箱和 Google Drives) 会同步到 Cyber Protect 中控台。此操作称为“发现”，并会记录在**监控** > **活动**中。

在发现操作完成后，可以在 中控台的**设备** > **Google Workspace** 选项卡上查看 Google Workspace 组织的资源，并可以对这些资源应用备份计划。

自动发现操作每天运行一次，以使 Cyber Protect 中控台中的资源列表保持最新。还可以通过手动重新运行发现操作，来手动同步此列表。

手动重新运行发现操作

1. 在 Cyber Protect 中控台中，转到**设备** > **Google Workspace**。
2. 选择 Google Workspace 组织，然后在**操作**窗格中，单击**刷新**。



注意
每小时最多可以手动运行 10 次发现操作。达到此数量后，允许的运行数量重置为每小时一次，此后每小时再可运行一次，直到再次达到每小时总计 10 次运行。

设置 Google Workspace 备份的频率

默认条件下，Google Workspace 备份每日运行一次，并且不提供其他日程安排选项。

如果在您的租户中启用了 Advanced Backup 包，则默认情况下会启用 **每天两次** 选项，并且可供您选择的频率更多。

注意
可以选择每天的备份数，但不能配置备份开始时间。备份按大概的间隔时间自动开始，间隔时间取决于在数据中心服务多个客户的云代理程序的当前负载。这可确保当天的负载均匀，以及对所有客户同等的服务质量。

可使用以下选项。

日程安排选项	每个备份之间的大概间隔
每天一次*	24 小时
每天两次(默认) **	12 小时
每天 3 次**	8 小时
每天 6 次**	4 小时

* 虽然启用 Advanced Backup 时 **每天两次**选项是默认值，但根据存储可用性，某些数据中心可能会临时启用 **每天一次** 选项。

**需要 Advanced Backup 包

注意
根据 Google Workspace 方面的云代理程序负荷和可能的限制，备份可能晚于计划的时间开始或者花费更长时间结束。如果备份花费的时间长于两次备份之间的平均间隔时间，则下次备份将重新计划，这可能导致每天的备份比选择的备份少。例如，即使您选择了每天六次备份，但可能每天只能完成两次备份。

保护 Gmail 数据

可以备份哪些项目？

可以备份 Gmail 用户的邮箱。邮箱备份还包括日历和联系人数据。或者，可以选择备份共享的日历。

在备份期间*跳过*下列项目：

- **生日**、**提醒**、**任务**日历
- 附加到日历事件的文件夹
- 联系人中的**目录**文件夹

由于 Google Calendar API 限制，将*跳过*以下日历项目：

- 约会空档
- 事件的会议字段
- 日历设置**全天事件通知**
- 日历设置**自动接受邀请**(在房间或共享空间的日历中)

由于 Google People API 限制，将*跳过*以下联系人项目：

- **其他联系人**文件夹
- 联系人的外部配置文件(**目录配置文件**、**Google 配置文件**)
- 联系人字段**文件形式**

可以恢复哪些项目?

可从邮箱备份中恢复以下项目:

- 邮箱
- 电子邮件文件夹(根据 Google 术语,即"标签"。**标签**在备份软件中显示为文件夹,以便与其他数据显示保持一致。)
- 电子邮件
- 日历事件
- 联系人

您可以使用搜索以在备份中找到项目的位置。

在恢复邮箱和邮箱项目时,可以选择是否覆盖目标位置的项目。

限制

- 联系人照片无法恢复
- 由于 Google Calendar API 限制,**离开办公室**日历项目恢复为常规日历事件

选择 Gmail 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 Gmail 邮箱的步骤

1. 单击 **Google Workspace**。
2. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务,则选择要备份其用户数据的组织。否则,请跳过此步骤。
3. 请执行以下任一操作:
   - 若要备份所有用户的邮箱(包括将来要创建的邮箱),请展开**用户**节点,选择**所有用户**,然后单击**组备份**。
   - 若要备份单个用户邮箱,请展开**用户**节点,选择**所有用户**,选择您要备份其邮箱的用户,然后单击**备份**。
4. 在保护计划面板上:
   - 请确保已在**备份内容**中选择 **Gmail** i项目。
   - 如果要备份与选定用户共享的日历,请启用**包括共享日历**开关。
   - 确定备份的电子邮件中是否需要全文本搜索。若要访问此选项,请依次单击齿轮图标 > **备份选项** > **全文本搜索**。

恢复邮箱和邮箱项目

恢复邮箱

1. 单击 **Google Workspace**。
2. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 展开**用户**节点，选择**所有用户**，选择要恢复其邮箱的用户，然后单击**恢复**。

   如果用户已删除，请在备份存储选项卡的**云应用程序备份**部分中将该用户选中，然后单击**显示备份**。

   可以按名称搜索用户和组。不支持通配符。
4. 选择恢复点。

   注意

   若要仅查看包含邮箱的恢复点，请在**按内容过滤**中选择 **Gmail**。
5. 依次单击**恢复** > **整个邮箱**。
6. 如果多个 Google Workspace 组织添加到 Cyber Protection 服务，则单击 **Google Workspace 组织**即可查看、更改或指定目标组织。

   默认情况下，原始组织处于选中状态。如果该组织不再注册在 Cyber Protection 服务中，则必须从可用的注册组织中选择一个新的目标组织。
7. 在**恢复至邮箱**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组织，必须指定目标邮箱。

   无法在恢复期间创建新的目标邮箱。要将邮箱恢复至新邮箱，首先需要在所需的 Google Workspace 组织中创建目标邮箱，然后让云代理程序同步更改。云代理程序会每隔 24 小时与 Google Workspace 同步一次。要立即同步更改，请在 Cyber Protect 中控台中的 **Google Workspace** 页面上选择相应组织，然后单击**刷新**。
8. 单击**开始恢复**。
9. 选择任一覆盖选项：
   - **覆盖现有项目**
   - **不覆盖现有项目**
10. 单击**继续**以确认您的决定。

恢复邮箱项目

1. 单击 **Google Workspace**。
2. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 展开**用户**节点，选择**所有用户**，选择其邮箱最初包含要恢复的项目的用户，然后单击**恢复**。

   如果用户已删除，请在备份存储选项卡的**云应用程序备份**部分中将该用户选中，然后单击**显示备份**。

   可以按名称搜索用户和组。不支持通配符。

4. 选择恢复点。

   注意
   若要仅查看包含邮箱的恢复点，请在**按内容过滤**中选择 **Gmail**。

5. 依次单击**恢复** > **电子邮件**。
6. 浏览到所需文件夹。如果备份未加密，可以使用搜索功能获取所需项目的列表。
   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、日期、附件名称和邮件内容搜索。
     当按日期搜索时，可以在时间范围内选择开始日期或结束日期（包括两者），也可以同时选择两个日期进行搜索。
     仅当在备份期间启用了**全文搜索**选项时，才能按附件名称搜索或搜索邮件内容。可以指定将作为附加参数搜索的邮件片段的语言。
   - 对于事件：按标题和日期搜索。
   - 对于联系人：按名称、电子邮件地址和电话号码搜索。
7. 选择要恢复的项目。为了能够选择文件夹，请单击“恢复文件夹”图标： 
   此外，您可以执行以下任一操作：
   - 当已选择某个项目时，单击**显示内容**即可查看其内容，包括附件。单击附加文件的名称即可下载它。
   - 仅在备份未加密且您使用了搜索功能并在搜索结果中选择了单个项目时：单击**显示版本**以选择要恢复的项目版本。可以选择在选定的恢复点之前或之后的任何备份版本。
8. 单击**恢复**。
9. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务，则单击 **Google Workspace 组织**即可查看、更改或指定目标组织。
   默认情况下，原始组织处于选中状态。如果该组织不再注册在 Cyber Protection 服务中，则必须从可用的注册组织中选择一个新的目标组织。
10. 在**恢复至邮箱**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组织，必须指定目标邮箱。
11. 在**路径**中，查看或更改目标邮箱中的目标文件夹。默认情况下，选择原始文件夹。
12. 单击**开始恢复**。
13. 选择任一覆盖选项：
    - **覆盖现有项目**
    - **不覆盖现有项目**
14. 单击**继续**以确认您的决定。

保护 Google Drive 文件

可以备份哪些项目？

可以备份整个 Google Drive，也可以备份个别文件和文件夹。文件连同它们的共享权限一起备份。

重要事项
不备份以下项目：

- **与我共享**文件夹
- **计算机**文件夹(由备份和同步客户端创建)

限制

在 Google 特定文件格式中，完全支持备份和恢复 Google Docs、Google Sheets 和 Google Slides。其他 Google 特定格式可能不完全受支持或根本不受支持 - 例如，Google Drawings 文件恢复为 `.svg` 文件、Google Sites 文件恢复为 `.txt` 文件、Google Jamboard 文件恢复为 `.pdf` 文件，而 Google My Maps 文件在备份过程中会被跳过。

注意
完全支持备份和恢复的非 Google 特定的文件格式 - 例如，`.txt`、`.docx`、`.pptx`、`.pdf`、`.jpg`、`.png`、`.zip`。

可以恢复哪些项目？

可以恢复整个 Google Drive，也可以恢复备份的任何文件或文件夹。

可以选择是恢复共享权限，还是让文件从其恢复到的文件夹继承权限。

限制

- 不会恢复文件中的注释。
- 不恢复文件和文件夹的共享链接。
- 共享文件的只读**所有者设置(阻止编辑者更改访问权限和添加新用户**以及**禁用评论者和查看器的下载、打印和复制选项)**在恢复过程中无法更改。
- 如果**阻止编辑者更改访问权限和添加新用户**选项已为此文件夹启用，则共享文件夹的所有权无法在恢复过程中更改。此设置阻止 Google Drive API 列出文件夹权限。正确恢复文件夹中文件的所有权。

选择 Google Drive 文件

按如下所述选择文件，然后相应地指定保护计划的其他设置。

选择 Google Drive 文件的步骤

1. 单击 **Google Workspace**。
2. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务，则选择要备份其用户数据的组织。否则，请跳过此步骤。
3. 请执行以下任一操作：
   - 若要备份所有用户(包括将来将要创建的用户)的文件，请展开**用户**节点，选择**所有用户**，然后单击**组备份**。

- 若要备份单个用户的文件，请展开**用户**节点，选择**所有用户**，选择您要备份其文件的用户，然后单击**备份**。

4. 在保护计划面板上：
   - 请确保已在**备份内容**中选择 **Google Drive** 项目。
   - 在**要备份的项目**中，执行以下任一操作：
     - 保留默认设置 **[全部]**(所有文件)。
     - 通过添加名称或路径指定要备份的文件和文件夹。

       可以使用通配符(*、** 和 ?)。有关指定路径和使用通配符的更多详细信息，请参阅“文件过滤器”。
     - 通过浏览指定要备份的文件和文件夹。

       浏览链接仅在为单个用户创建保护计划时才可用。
   - [可选] 在**要备份的项目**中，单击**显示排除**，指定要在备份期间跳过的文件和文件夹。

     文件排除优先于文件选择；即，如果在这两个字段中指定相同的文件，将在备份期间跳过此文件。
   - 如果要启用为备份所选的所有文件的公证，请启用**公证**开关。有关公证的更多信息，请参阅“公证”。

恢复 Google Drive 和 Google Drive 文件

恢复整个 Google Drive

1. 单击 **Google Workspace**。
2. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 展开**用户**节点，选择**所有用户**，选择要恢复其 Google Drive 的用户，然后单击**恢复**。

   如果用户已删除，请在备份存储选项卡的**云应用程序备份**部分中将该用户选中，然后单击**显示备份**。

   可以按名称搜索用户。不支持通配符。
4. 选择恢复点。

   注意

   若要仅查看包含 Google Drive 文件的恢复点，请在**按内容过滤**中选择 **Google Drive**。
5. 依次单击**恢复** > **整个 Drive**。
6. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务，则单击 **Google Workspace 组织**即可查看、更改或指定目标组织。

   默认情况下，原始组织处于选中状态。如果该组织不再注册在 Cyber Protection 服务中，则必须从可用的注册组织中选择一个新的目标组织。
7. 在**恢复至驱动器**中，查看、更改或指定目标用户或目标 Shared Drive。

   默认情况下，选择原始用户。如果此用户不存在或者选择了非原始组织，必须指定目标用户或目标 Shared Drive。

   如果备份中包含共享文件，则文件将恢复到目标驱动器的根文件夹。

8. 选择是否恢复文件的共享权限。
9. 单击**开始恢复**。
10. 选择任一覆盖选项：

选项	描述
覆盖现有文件(如果较旧)	如果目标位置中的同名文件比源文件旧，则源文件将保存到目标位置，以替换旧版本。
覆盖现有文件	目标位置中的所有现有文件都将被覆盖，无论其上次修改日期如何。
不覆盖现有文件	如果目标位置中有同名文件，则不会对其应用任何更改，也不会将源文件保存到目标位置。

11. 单击**继续**以确认您的决定。

恢复 Google Drive 文件

1. 单击 **Google Workspace**。
2. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 展开**用户**节点，选择**所有用户**，选择要恢复其 Google Drive 文件的用户，然后单击**恢复**。

   如果用户已删除，请在备份存储选项卡的**云应用程序备份**部分中将该用户选中，然后单击**显示备份**。

   可以按名称搜索用户。不支持通配符。
4. 选择恢复点。

   注意
   若要仅查看包含 Google Drive 文件的恢复点，请在**按内容过滤**中选择 **Google Drive**。
5. 依次单击**恢复** > **文件/文件夹**。
6. 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。
7. 选择要恢复的文件。

   如果备份未加密且您选择了单个文件，则可以单击**显示版本**以选择要恢复的文件版本。可以选择在选定的恢复点之前或之后的任何备份版本。
8. 如果要下载某个文件，请选择该文件，单击**下载**，选择要将文件保存到的位置，然后单击**保存**。否则，请跳过此步骤。
9. 单击**恢复**。
10. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务，则单击 **Google Workspace 组织**即可查看、更改或指定目标组织。

    默认情况下，原始组织处于选中状态。如果该组织不再注册在 Cyber Protection 服务中，则必须从可用的注册组织中选择一个新的目标组织。
11. 在**恢复至驱动器**中，查看、更改或指定目标用户或目标 Shared Drive。

    默认情况下，选择原始用户。如果此用户不存在或者选择了非原始组织，必须指定目标用户或目标 Shared Drive。

12. 在**路径**中，查看或更改目标用户的 Google Drive 或目标 Shared Drive 中的目标文件夹。默认情况下，选择原始位置。
13. 选择是否恢复文件的共享权限。
14. 单击**开始恢复**。
15. 选择文件覆盖选项之一：

选项	描述
覆盖现有文件(如果较旧)	如果目标位置中的同名文件比源文件旧，则源文件将保存到目标位置，以替换旧版本。
覆盖现有文件	目标位置中的所有现有文件都将被覆盖，无论其上次修改日期如何。
不覆盖现有文件	如果目标位置中有同名文件，则不会对其应用任何更改，也不会将源文件保存到目标位置。

16. 单击**继续**以确认您的决定。

保护 Shared Drive 文件

可以备份哪些项目？

可以备份整个 Shared Drive，也可以备份个别文件和文件夹。文件连同它们的共享权限一起备份。

重要事项
不会备份**与我共享**文件夹。

限制

- 由于 Google Drive API 限制，无法备份没有成员的 Shared Drive。
- 在 Google 特定文件格式中，完全支持备份和恢复 Google Docs、Google Sheets 和 Google Slides。其他 Google 特定格式可能不完全受支持或根本不受支持 - 例如，Google Drawings 文件恢复为 `.svg` 文件、Google Sites 文件恢复为 `.txt` 文件、Google Jamboard 文件恢复为 `.pdf` 文件，而 Google My Maps 文件在备份过程中会被跳过。

  注意
  完全支持备份和恢复的非 Google 特定的文件格式 - 例如，`.txt`、`.docx`、`.pptx`、`.pdf`、`.jpg`、`.png`、`.zip`。

可以恢复哪些项目？

可以恢复整个 Shared Drive，也可以恢复备份的任何文件或文件夹。

可以选择是恢复共享权限，还是让文件从其恢复到的文件夹继承权限。

以下项目不会恢复：

- 如果在目标 Shared Drive 中禁用组织外部共享，则不会恢复与组织外部用户共享的文件的共享权限。

- 如果在目标 Shared Drive 中禁用**与非成员共享**，则不会恢复与非目标 Shared Drive 成员的用户共享的文件的共享权限。

限制

- 不会恢复文件中的注释。
- 不恢复文件和文件夹的共享链接。

选择 Shared Drive 文件

按如下所述选择文件，然后相应地指定保护计划的其他设置。

选择 Shared Drive 文件

1. 单击 **Google Workspace**。
2. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务，则选择要备份其用户数据的组织。否则，请跳过此步骤。
3. 请执行以下任一操作：
   - 要备份所有 Shared Drive(包括将来要创建的 Shared Drive) 的文件，请展开 **Shared Drive** 节点，选择**所有 Shared Drive**，然后单击**组备份**。
   - 要备份个别 Shared Drive 的文件，请展开 **Shared Drive** 节点，选择**所有 Shared Drive**，选择要备份的 Shared Drive，然后单击**备份**。
4. 在保护计划面板上：
   - 在**要备份的项目**中，执行以下任一操作：
     - 保留默认设置 **[全部]**(所有文件)。
     - 通过添加名称或路径指定要备份的文件和文件夹。

       可以使用通配符(*、** 和 ?)。有关指定路径和使用通配符的更多详细信息，请参阅“文件过滤器”。
     - 通过浏览指定要备份的文件和文件夹。

       浏览链接仅在为单个 Shared Drive 创建保护计划时才可用。
   - [可选] 在**要备份的项目**中，单击**显示排除**，指定要在备份期间跳过的文件和文件夹。

     文件排除优先于文件选择；即，如果在这两个字段中指定相同的文件，将在备份期间跳过此文件。
   - 如果要启用为备份所选的所有文件的公证，请启用**公证**开关。有关公证的更多信息，请参阅“公证”。

恢复 Shared Drive 和 Shared Drive 文件

恢复整个 Shared Drive

1. 单击 **Google Workspace**。
2. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 展开 **Shared Drive** 节点，选择**所有 Shared Drive**，选择要恢复的 Shared Drive，然后单击**恢复**。

如果 Shared Drive 已删除，请在备份存储选项卡的**云应用程序备份**部分中将它选中，然后单击**显示备份**。

可以按名称搜索 Shared Drive。不支持通配符。

4. 选择恢复点。
5. 依次单击**恢复** > **整个 Shared Drive**。
6. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务，则单击 **Google Workspace 组织**即可查看、更改或指定目标组织。

   默认情况下，原始组织处于选中状态。如果该组织不再注册在 Cyber Protection 服务中，则必须从可用的注册组织中选择一个新的目标组织。
7. 在**恢复至驱动器**中，查看、更改或指定目标 Shared Drive 或目标用户。如果指定用户，数据将恢复到该用户的 Google Drive。

   默认情况下，选择原始 Shared Drive。如果此 Shared Drive 不存在或者选择了非原始组织，必须指定目标 Shared Drive 或目标用户。
8. 选择是否恢复文件的共享权限。
9. 单击**开始恢复**。
10. 选择任一覆盖选项：

选项	描述
覆盖现有文件(如果较旧)	如果目标位置中的同名文件比源文件旧，则源文件将保存到目标位置，以替换旧版本。
覆盖现有文件	目标位置中的所有现有文件都将被覆盖，无论其上次修改日期如何。
不覆盖现有文件	如果目标位置中有同名文件，则不会对其应用任何更改，也不会将源文件保存到目标位置。

11. 单击**继续**以确认您的决定。

恢复 Shared Drive 文件

1. 单击 **Google Workspace**。
2. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务，则选择要恢复其备份数据的组织。否则，请跳过此步骤。
3. 展开 **Shared Drive** 节点，选择**所有 Shared Drive**，选择最初包含要恢复文件的 Shared Drive，然后单击**恢复**。

   如果 Shared Drive 已删除，请在备份存储选项卡的**云应用程序备份**部分中将它选中，然后单击**显示备份**。

   可以按名称搜索 Shared Drive。不支持通配符。
4. 选择恢复点。
5. 依次单击**恢复** > **文件/文件夹**。
6. 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。
7. 选择要恢复的文件。

如果备份未加密且您选择了单个文件，则可以单击**显示版本**以选择要恢复的文件版本。可以选择在选定的恢复点之前或之后的任何备份版本。

8. 如果要下载某个文件，请选择该文件，单击**下载**，选择要将文件保存到的位置，然后单击**保存**。否则，请跳过此步骤。
9. 单击**恢复**。
10. 如果多个 Google Workspace 组织已添加到 Cyber Protection 服务，则单击 **Google Workspace 组织**即可查看、更改或指定目标组织。

    默认情况下，原始组织处于选中状态。如果该组织不再注册在 Cyber Protection 服务中，则必须从可用的注册组织中选择一个新的目标组织。
11. 在**恢复至驱动器**中，查看、更改或指定目标 Shared Drive 或目标用户。如果指定用户，数据将恢复到该用户的 Google Drive。

    默认情况下，选择原始 Shared Drive。如果此 Shared Drive 不存在或者选择了非原始组织，必须指定目标 Shared Drive 或目标用户。
12. 在**路径**中，查看或更改目标 Shared Drive 或目标用户的 Google Drive 中的目标文件夹。默认情况下，选择原始位置。
13. 选择是否恢复文件的共享权限。
14. 单击**开始恢复**。
15. 选择文件覆盖选项之一：

选项	描述
覆盖现有文件(如果较旧)	如果目标位置中的同名文件比源文件旧，则源文件将保存到目标位置，以替换旧版本。
覆盖现有文件	目标位置中的所有现有文件都将被覆盖，无论其上次修改日期如何。
不覆盖现有文件	如果目标位置中有同名文件，则不会对其应用任何更改，也不会将源文件保存到目标位置。

16. 单击**继续**以确认您的决定。

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 Google Drive 文件和 Google Workspace Shared Drive 文件的备份。

如何使用公证

要对所有选择要备份的文件启用公证，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。

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. 请执行以下任一操作：
   - 若要验证 Google Drive 文件的真实性，请按“恢复 Google Drive 文件”部分中的第 1-7 步所述操作来选择文件。
   - 要验证 Google Workspace Shared Drive 文件的真实性，请按照“恢复 Shared Drive 文件”部分的第 1-7 步中所述操作来选择文件。
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。

在云到云备份中搜索

在恢复数据时，您可以搜索特定的备份项目，而不是浏览备份存档。

在非加密备份中，搜索始终可用。只支持增强（基于索引）的搜索。

基于索引的搜索更快，并提供额外的选项，例如显示备份项目的版本，搜索附件名称，以及在 Gmail 备份中进行全文搜索。

全文本搜索

全文搜索仅适用于 Gmail 备份，并且默认为启用状态。有了它，就可以在备份的电子邮件正文中进行搜索。如果此选项被禁用，您只能通过主题，发件人，收件人和日期进行搜索。

全文搜索索引占据了 Gmail 备份存储空间的 10% 到 30%。没有全文搜索数据的索引明显更小。为了节省存储空间，您可以禁用全文搜索并清除包含全文搜索数据的索引部分。

搜索索引

搜索索引在云到云备份存档中提供了增强的搜索能力。

每次备份操作后，存档会自动编制索引。编制索引的过程不会影响备份性能，因为编制索引和备份是由不同的软件组件完成的。

显示搜索结果需要在编制索引操作完成后才可用，这可能需要长达 24 小时。索引第一个完整备份通常比索引后续增量备份所需的时间更长。

所有索引都包含支持主要搜索功能的元数据 - 按主题、发件人、收件人或日期搜索。如果启用了全文搜索，则 Gmail 备份的索引将包含额外的数据。

检查搜索索引的大小

随着时间的推移，搜索索引会变得越来越大。对于启用了全文搜索的备份存档，其索引可能占据存档大小的 30%。

若要检查搜索索引的大小

1. 以管理员身份登录 Cyber Protect 中控台。
2. 在**备份存储**选项卡上，点击**云应用程序备份**。
3. 检查**索引大小**列中的值。

更新，重建或删除索引

要对云到云备份中与搜索相关的问题进行故障排除，可以更新、重建或删除搜索索引。

注意
我们建议您在更新、重建或删除索引之前联系支持团队。

若要更新，重建或删除索引

1. 以管理员身份登录到 Cyber Protect 中控台。
2. 在**备份存储**选项卡上，点击**云应用程序备份**。
   选择您想要更新、重建或删除索引的存档。
   这些操作的可用性取决于管理员的级别和角色，如下所示：

账户级别	角色	可以更新索引	可以重建索引	可以删除索引
合作伙伴租户	公司管理员	+	+	+
	保护网络安全管理员	+	-	-
	保护管理员	+	-	-
	保护只读管理员	-	-	-
客户租户	公司管理员	+	-	-
	保护管理员	+	-	-
	保护只读管理员	-	-	-
单元	单位管理员	+	-	-
	保护管理员	+	-	-
	保护只读管理员	-	-	-

3. 在**操作**窗格中，选择想要执行的操作：
   - **更新索引** — 检查存档中的恢复点，并添加丢失的索引。
   - **重建索引** — 删除存档中所有恢复点的索引，然后重新创建索引。
   - **删除索引** — 删除存档中所有恢复点的索引。
4. 选择操作的范围，然后点击**确定**。
   根据存档和所选操作，以下一个或多个选项可能可用：
   - **仅元数据**
   - **仅内容**
   - **元数据和内容搜索**

禁用 Gmail 备份的全文搜索

全文搜索仅适用于 Gmail 备份，并且默认为启用状态。有了它，就可以在备份的电子邮件正文中进行搜索。如果此选项被禁用，您只能通过主题，发件人，收件人和日期进行搜索。

如果您需要将搜索索引的大小保持在最小，则可能需要禁用全文搜索。

若要禁用全文搜索

1. 在创建或编辑备份计划时，点击右上角的齿轮图标。
2. 在**全文搜索**选项卡上，关闭开关。
3. 单击**完成**。
4. [创建计划时]点击**应用**。
5. [编辑计划时]点击**保存设置**。

注意
如果重新启用全文搜索，则所有由此备份计划创建的存档将会再次被编制索引。这是一个耗时的操作。

保护 Oracle 数据库

注意
该功能随 Advanced Backup 包提供。

在 https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper_en-US.pdf 处提供的单独文档中介绍了“保护 Oracle 数据库”

保护 SAP HANA

注意
该功能随 Advanced Backup 包提供。

在 https://dl.managed-protection.com/u/pdf/SAP_HANA_backup_whitepaper_en-US.pdf 处提供的单独文档中介绍了“保护 SAP HANA”

保护 MySQL 和 MariaDB 数据

可以使用应用程序感知备份来保护 MySQL 或 MariaDB 数据。它会收集应用程序元数据，并允许在实例、数据库或表级别上执行粒度恢复。

注意
通过 Advanced Backup 包，可以对 MySQL 或 MariaDB 数据进行应用程序感知备份。

要使用应用程序感知备份保护运行 MySQL 或 MariaDB 实例的物理机或虚拟机，需要在该计算机上安装适用于 MySQL/MariaDB 的代理程序。适用于 MySQL/MariaDB 的代理程序与适用于 Linux 的代理程序(64 位)捆绑在一起，因此只能安装在基于 64 位 Linux的操作系统上。请参阅 "支持的操作系统和环境"(第 23 页)。

下载适用于 Linux 的代理程序(64 位)安装文件

1. 登录到 Cyber Protect 中控台。
2. 单击右上角的帐户图标，然后选择**下载**。
3. 单击**适用于 Linux 的代理程序(64 位)**。

安装文件将下载到您的计算机上。要安装代理程序，请按照 "在 Linux 中安装保护代理程序"(第 74 页) 或 "在 Linux 中安装和卸载保护代理程序"(第 92 页) 中所述继续操作。确保选择适用于 MySQL/MariaDB 的代理程序，这是一个可选组件。

要将数据库和表恢复到实时实例，适用于 MySQL/MariaDB 的代理程序需要一个临时存储空间才能运行。默认情况下，使用 `/tmp` 目录。可以通过设置 `ACRONIS_MYSQL_RESTORE_DIR` 环境变量来更改此目录。

限制

- 不支持 MySQL 或 MariaDB 簇。
- 不支持在 Docker 容器中运行的 MySQL 或 MariaDB 实例。
- 不支持在使用 BTRFS 文件系统的操作系统上运行的 MySQL 或 MariaDB 实例。
- 系统数据库（`sys`、`mysql`、`information-schema` 和 `performance_schema`）和不包含任何表的数据库无法恢复为实时实例。但是，在恢复整个实例时，这些数据库可以作为文件进行恢复。
- 仅支持恢复到与备份实例版本相同或更高版本的目标实例，并具有以下限制：
  - 不支持从 MySQL 5.x 实例恢复到 MySQL 8.x 实例。
  - 仅支持通过将整个实例恢复为文件，来恢复到更高的 MySQL 5.x 版本（包括次要版本）。在尝试恢复之前，请参阅目标版本的官方 MySQL 升级指南（例如，MySQL 5.7 升级指南）。
- 不支持从存储在安全区上的备份进行恢复。
- 在安装有 AppArmor 的计算机上运行的适用于 MySQL/MariaDB 的代理程序无法恢复数据库和表。仍可以将实例恢复为文件，或恢复整台计算机。
- 不支持恢复到配置有符号链接的目标数据库。可以通过更改名称将备份的数据库恢复为新数据库。

已知问题

如果在从受密码保护的 Samba 共享中恢复数据时遇到问题，请从 Cyber Protect 中控台注销，然后重新登录。选择所需的恢复点，然后单击 **MySQL/MariaDB 数据库**。请勿单击**整台计算机**或**文件/文件夹**。

配置应用程序感知备份

先决条件

- 至少一个 MySQL 或 MariaDB 实例必须在选定计算机上运行。
- 在正在运行 MySQL 或 MariaDB 实例的计算机上，必须在根用户下启动保护代理程序。
- 仅当在保护计划中将**整台计算机**选择用作备份源时，应用程序感知备份才可用。
- 必须在保护计划中禁用**逐扇区**备份选项。否则，无法恢复应用程序数据。

配置应用程序感知备份

1. 在 Cyber Protect 中控台中，选择一台或多台正在运行 MySQL 或 MariaDB 实例的计算机。
   每台计算机上可以有一个或多个实例。
2. 创建启用备份模块的保护计划。
3. 在**要备份的内容**，选择**整个计算机**。
4. 单击**应用程序备份**，然后启用 **MySQL/MariaDB Server**旁边的开关。
5. 选择如何指定 MySQL 或 MariaDB 实例：

- **对于所有工作负载**

  如果在多台服务器上运行配置完全相同的实例，则使用此选项。相同的连接参数和访问凭据将用于所有实例。
- **对于特定工作负载**

  使用此选项来为每个实例指定连接参数和访问凭据。

6. 单击**添加实例**，以配置连接参数和访问凭据。
   a. 选择连接类型，然后指定以下内容：
      - [对于 TCP 套接字] IP 地址和端口。
      - [对于 Unix 套接字] 套接字路径。
   b. 指定有以下实例权限的用户帐户的凭据：
      - FLUSH_TABLES 或 RELOAD 用于所有数据库和表 (*.*)
      - SELECT 用于 information_schema.tables
   c. 单击**确定**。
7. 单击**完成**。

从应用程序感知备份恢复数据

从应用程序感知备份，可以恢复 MySQL 或 MariaDB 实例、数据库和表。还可以恢复正在运行实例的整个服务器，或从此服务器恢复文件和文件夹。

下表汇总了所有恢复选项。

恢复内容	恢复为	恢复至
MySQL 服务器 MariaDB 服务器	整台计算机	安装有适用于 Linux 的代理程序的计算机*
MySQL 服务器 MariaDB 服务器	文件或文件夹	安装有适用于 Linux 的代理程序的计算机*
实例	文件	安装有适用于 MySQL/MariaDB 的代理程序的计算机*
数据库	同一数据库 新数据库	安装有适用于 MySQL/MariaDB 的代理程序的计算机* • 原始实例 • 另一个实例 • 原始数据库 • 新数据库
Table	同一表 新表	安装有适用于 MySQL/MariaDB 的代理程序的计算机* • 原始实例 • 另一个实例 • 原始数据库

恢复内容	恢复为	恢复至
		• 原始表 • 新表

* 从备份的角度来看，内部附带代理程序的虚拟机会视为物理机。

恢复整个服务器

要了解如何恢复正在运行 MySQL 或 MariaDB 实例的整个服务器，请参阅 "恢复计算机"(第 446 页)。

恢复实例

从应用程序感知备份，可以将 MySQL 或 MariaDB 实例恢复为文件。

恢复实例

1. 在 Cyber Protect 中控台中，选择最初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)，则单击**选择计算机**、选择有适用于 MySQL/MariaDB 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用于恢复的目标计算机。
4. 依次单击**恢复** > **MySQL/MariaDB 数据库**。
5. 选择要恢复的实例，然单击**恢复为文件**。
6. 在**路径**下，选择文件将恢复到的目录。
7. 单击**开始恢复**。

恢复数据库

从应用程序感知备份，可以将数据库恢复到实时 MySQL 或 MariaDB 实例。

1. 在 Cyber Protect 中控台中，选择最初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)，则单击**选择计算机**、选择有适用于 MySQL/MariaDB 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用于恢复的目标计算机。
4. 依次单击**恢复** > **MySQL/MariaDB 数据库**。

5. 单击所需实例的名称，以深入查看其数据库。
6. 选择要恢复的一个或多个数据库。
7. 单击**恢复**。
8. 单击**目标 MySQL/MariaDB 实例**，以为目标实例指定连接参数和访问凭据。
   - 验证要将数据恢复到的实例。默认情况下，原始实例处于选中状态。
   - 指定可以访问目标实例的用户帐户的凭据。该用户帐户必须有为所有数据库和表 (*.*) 指派的以下权限：
     - INSERT
     - CREATE
     - DROP
     - LOCK_TABLES
     - ALTER
     - SELECT
   - 单击**确定**。
9. 验证目标数据库。

   默认情况下，原始数据库处于选中状态。

   要将某个数据库恢复为新数据库，请单击目标数据库的名称并进行更改。此操作仅在恢复单个数据库时才可用。
10. 在**覆盖现有数据库**下，选择覆盖模式。

    默认情况下，覆盖处于启用状态，并且备份的数据库将替换名称相同的目标数据库。

    如果覆盖处于禁用状态，则在恢复操作期间将跳过备份的数据库，并且不会替换名称相同的目标数据库。
11. 单击**开始恢复**。

恢复表

从应用程序感知备份，可以将表恢复到实时 MySQL 或 MariaDB 实例。

1. 在 Cyber Protect 中控台中，选择最初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)，则单击**选择计算机**、选择有适用于 MySQL/MariaDB 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用于恢复的目标计算机。
4. 依次单击**恢复** > **MySQL/MariaDB 数据库**。
5. 单击所需实例的名称，以深入查看其数据库。
6. 单击所需数据库的名称，以深入查看其表。
7. 选择要恢复的一个或多个表。
8. 单击**恢复**。

9. 单击**目标 MySQL/MariaDB 实例**，以为目标实例指定连接参数和访问凭据。
   - 验证要将数据恢复到的实例。默认情况下，原始实例处于选中状态。
   - 指定可以访问目标实例的用户帐户的凭据。该用户帐户必须有为所有数据库和表 (*.*) 指派的以下权限：
     - INSERT
     - CREATE
     - DROP
     - LOCK_TABLES
     - ALTER
     - SELECT
   - 单击**确定**。
10. 验证目标表。

    默认情况下，原始表处于选中状态。

    要将某个表恢复为新表，请单击目标表的名称并进行更改。此操作仅在恢复单个表时才可用。
11. 在**覆盖现有表**下，选择覆盖模式。

    默认情况下，覆盖处于启用状态，并且备份的表将替换名称相同的目标表。

    如果覆盖处于禁用状态，则在恢复操作期间将跳过备份的表，并且不会替换名称相同的目标表。
12. 单击**开始恢复**。

恢复存储的例程

当恢复整个 MySQL 实例时，存储的例程会自动恢复。

将单个数据库恢复到非原始实例或将其恢复为新数据库时，存储的例程不会自动恢复。可以手动恢复它们，方法是将它们导出到 SQL 文件中，然后将它们添加到恢复的数据库。

导出存储的例程并将其添加到恢复的数据库

1. 在具有原始 MySQL 实例的计算机上，打开终端。
2. 运行以下命令以导出存储的例程。
3. ```
   mysqldump -p [source_database_name] --routines --no-create-info --no-data >
   [exported_db_routines.sql]
   ```
4. 在恢复数据库的计算机上，打开 MySQL 命令行客户端。
5. 运行以下命令以将例程添加到恢复的数据库。

   ```
   mysql>  use [recovered_database_name];
   ```

   ```
   mysql>  source [path_to_exported_db_routines.sql];
   ```
   ```

保护网站和托管服务器

保护网站

未经授权的访问或恶意软件攻击会导致网站受损。如果您想要轻松将受损的网站还原到正常状态，请备份您的网站。

备份网站需要做些什么？

该网站必须可通过 SFTP 或 SSH 协议进行访问。您无需安装代理程序，只需添加一个网站，如本节稍后所述。

可以备份哪些项目？

您可以备份以下项目：

- **网站内容文件**
  您为 SFTP 或 SSH 连接指定的帐户可访问的所有文件。
- **MySQL 服务器上托管的已链接的数据库（如果有）。**
  您指定的 MySQL 帐户可以访问的所有数据库。

如果您的网站使用数据库，我们建议您同时备份文件和数据库，以便能将其恢复到一致状态。

限制

- 可用于网站备份的唯一备份位置为云存储。
- 可以将多个保护计划应用于网站，但其中只有一个可以按预定运行。其他计划需要手动启动。
- 唯一可用备份选项是“备份文件名”。
- 网站保护计划不会显示在**管理** > **保护计划**选项卡上。

备份网站

添加网站

1. 单击**设备** > **添加**。
2. 单击**网站**。
3. 为网站配置以下访问设置：
   - 在**网站名称**中，创建并键入网站名称。此名称将显示在 Cyber Protect 中控台中。
   - 在**主机**中，指定将用于通过 SFTP 或 SSH 访问网站的主机名或 IP 地址。例如：`my.server.com` 或 `10.250.100.100`。
   - 在**端口**中，指定端口号。
   - 在**用户名**和**密码**中，指定可用于通过 SFTP 或 SSH 访问网站的帐户凭据。

重要事项
将只备份指定帐户可访问的文件。

您可以指定您的 SSH 私钥而非密码。要执行此操作，请选择**使用 SSH 私钥而非密码**复选框，然后指定密钥。

4. 单击**下一步**。
5. 如果您的网站使用 MySQL 数据库，请为数据库配置访问设置。否则，单击**跳过**。
   a. 在**连接类型**中，选择如何从云中访问数据库：
      - **从主机上通过 SSH** - 通过在步骤 3 中指定的主机访问数据库。
      - **直接连接** - 直接访问数据库。仅在数据库可以从 Internet 进行访问时，才选择此设置。
   b. 在**主机**中，指定运行 MySQL 服务器的主机的名称或 IP 地址。
   c. 在**端口**中，指定 TCP/IP 与服务器连接的端口号。默认的端口号是 3306。
   d. 在**用户名**和**密码**中，指定 MySQL 帐户凭据。

   重要事项
   将只备份指定帐户可访问的数据库。

   e. 单击**创建**。

   该网站显示在 Cyber Protect 中控台中的**设备** > **网站**下。

更改连接设置

1. 请在**设备** > **网站**下选择网站。
2. 单击**详细信息**。
3. 单击网站或数据库连接设置旁边的铅笔图标。
4. 做出所需更改，然后单击**保存**。

为网站创建保护计划

1. 在**设备** > **网站**下选择一个网站或多个网站。
2. 单击**保护**。
3. [可选] 启用数据库备份。

   如果选择了多个网站，则数据库备份默认处于禁用状态。
4. [可选] 更改保留规则。
5. [可选] 启用备份加密。
6. [可选] 单击齿轮图标可编辑备份文件名选项。这一功能在两种情况下非常有用：
   - 如果您之前备份了此网站，并希望继续现有备份序列
   - 如果要在**备份存储**选项卡上查看自定义名称
7. 单击**应用**。

可以采用针对计算机的相同方式来编辑、吊销和删除网站的保护计划。这些操作在“保护计划的操作”中进行了介绍。

恢复网站

恢复网站

1. 请执行以下任一操作：
   - 在**设备** > **网站**下，选择要恢复的网站，然后单击**恢复**。
     您可以按名称搜索网站。不支持通配符。
   - 如果网站已删除，请在备份存储选项卡的**云应用程序备份**部分中将它选中，然后单击**显示备份**。
     要恢复已删除的网站，需要将目标站点添加为设备。
2. 选择恢复点。
3. 单击**恢复**，然后选择要恢复的内容：**整个网站**、**数据库**（如果有）或**文件/文件夹**。
   为了确保您的网站处于一致状态，建议您以任何顺序恢复文件和数据库。
4. 根据您的选择，执行以下所述步骤之一：

恢复整个网站

1. 在**恢复到网站**中，查看或更改目标网站。
   默认情况下，已选定原始网站。如果不存在，必须选择目标网站。
2. 选择是否恢复已恢复的项目的共享权限。
3. 单击**开始恢复**，然后确认操作。

恢复数据库

1. 选择要恢复的数据库。
2. 如果要将数据库下载为文件，请单击**下载**，选择要将文件保存到的位置，然后单击**保存**。否则，请跳过此步骤。
3. 单击**恢复**。
4. 在**恢复到网站**中，查看或更改目标网站。
   默认情况下，已选定原始网站。如果不存在，必须选择目标网站。
5. 单击**开始恢复**，然后确认操作。

要恢复网站文件/文件夹

1. 选择要恢复的文件/文件夹。
2. 如果要保存某个文件，请单击**下载**，选择要将文件保存到的位置，然后单击**保存**。否则，请跳过此步骤。
3. 单击**恢复**。
4. 在**恢复到网站**中，查看或更改目标网站。
   默认情况下，已选定原始网站。如果不存在，必须选择目标网站。
5. 选择是否恢复已恢复的项目的共享权限。
6. 单击**开始恢复**，然后确认操作。

保护 Web 托管服务器

可以保护基于 Linux 的 Web 托管服务器，这些服务器运行 Plesk、cPanel、DirectAdmin、VirtualMin 或 ISPManager 控制面板。运行来自其他供应商的 Web 托管控制面板的服务器作为常规工作负载受到保护。

限额

运行 Plesk、cPanel、DirectAdmin、VirtualMin 或 ISPManager 控制面板的服务被认为是 Web 托管服务器。每个备份的服务器均消耗 **Web 托管服务器**配额。如果禁用此配额或超过此配额的超额，将如下指派配额或备份将失败：

- 如果服务器为物理服务器，则将使用**服务器**配额。如果禁用此配额或超过此配额的超额，则备份将失败。
- 如果服务器为虚拟服务器，则将使用**虚拟机**配额。如果禁用此配额或超过此配额的超额，则备份将失败。

DirectAdmin、cPanel 和 Plesk 的集成

使用 DirectAdmin、Plesk 或 cPanel 的 Web 托管管理员可以将这些控制面板与 Cyber Protection 服务集成，以获得多个强大功能，包括：

- 使用磁盘级别备份将整个 Web 托管服务器备份到云存储
- 恢复整个服务器，包括所有网站和帐户
- 对帐户、网站、单个文件、邮箱或数据库执行粒度恢复和下载
- 使经销商和客户能够对自己的数据执行自助恢复

要执行集成，需要使用 Cyber Protection 服务扩展。有关详细信息，请参阅相应的集成指南：

- DirectAdmin 集成指南
- WHM 和 cPanel 集成指南
- Plesk 集成指南

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。

建议您让此临时虚拟机最多运行三天。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 Cyber Protection 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。
- 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。

注意
您可以在 Microsoft Azure 中对备份执行“作为虚拟机运行”(立即恢复)操作。然而，此操作会导致大量外出流量，这会增加您的 Microsoft Azure 订购许可帐单。对于从 Microsoft Azure 备份运行的 Windows 计算机，典型的外出流量从虚拟机开机到登录大约为 5 GB。

删除计算机

不建议您直接在 vSphere/Hyper-V 中删除临时虚拟机。这可能会导致在 Web 界面中出现人为错误。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。如果您计划执行终止化并有选项供您选择，建议您从本地备份运行虚拟机。

注意

终止化速度取决于代理程序是否连接到 VMware ESXi 主机或 vCenter，如 "配置虚拟设备"(第 121 页) 的步骤 3 所述。由于 VMware API 的特点，因此与 VMware vCenter 的连接可能会降低终止化操作的速度。要加快终止化操作，请将单独的适用于 VMware 的代理程序用于执行**以 VM 运行**操作，然后执行终止化，其中此代理程序将连接到 ESXi 主机(而不是 vCenter)。

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

- 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。
- 某些硬件更改(例如向 ESXi 主机添加网络接口卡 (NIC) 或从中删除 NIC) 会导致主机的内部 ID 发生更改。此更改会影响 VM 复制计划。进行此类更改后，必须重新创建虚拟机复制计划，其中选择了 ESXi 主机作为源或目标。否则，VM 复制计划将失败。

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

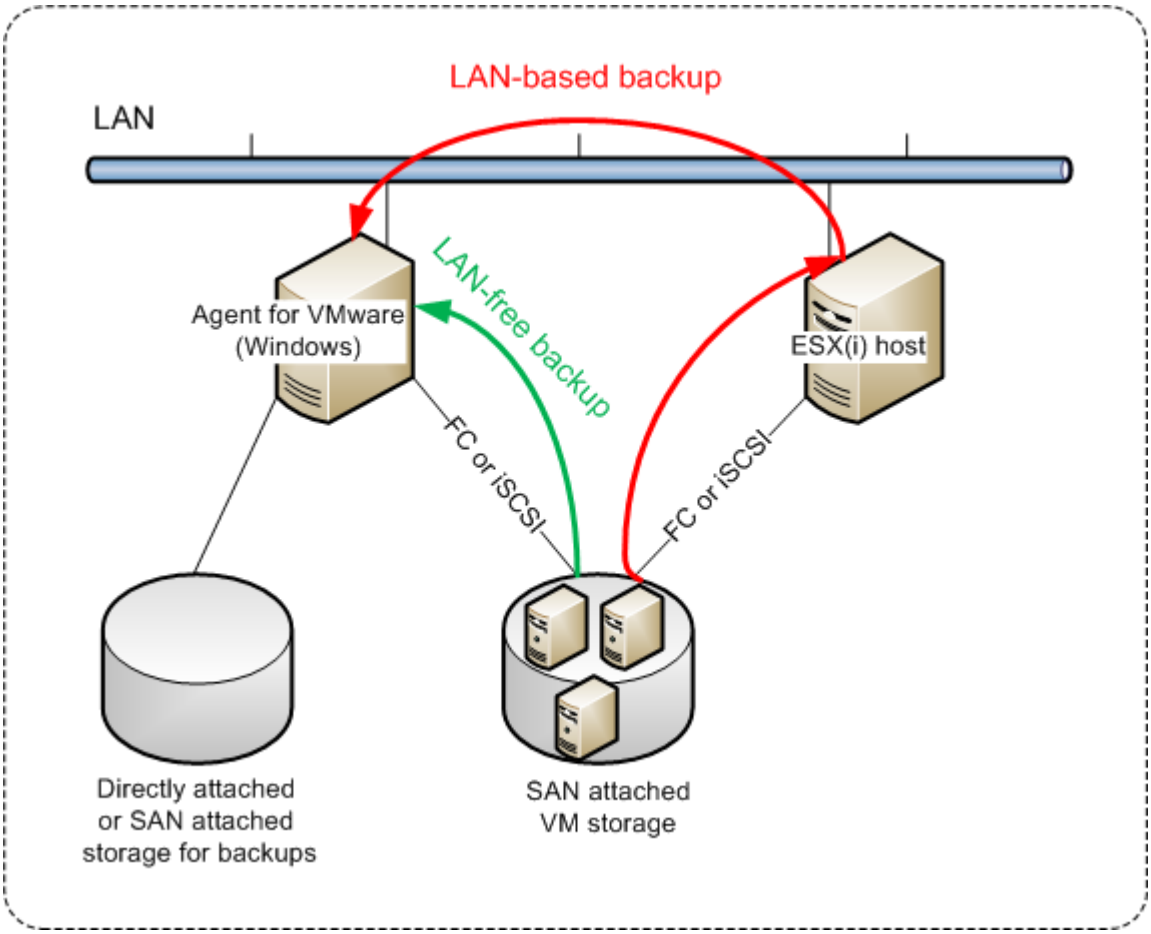
1. 请执行以下任一操作：
   - 如果可以关闭原始虚拟机，请关闭它，然后跳到步骤 4。
   - 如果不可以关闭原始虚拟机，请继续执行下一步。
2. 创建复制计划。
   在创建该计划时，请在**目标计算机**中选择**新副本**以及托管原始计算机的 ESXi。
3. 运行一次该计划。
   将在原始 ESXi 上创建一个副本。
4. 将虚拟机(或该副本)文件导出到外部硬盘驱动器。
   a. 将外部硬盘驱动器连接到运行 vSphere Client 的计算机。
   b. 将 vSphere Client 连接到原始 vCenter\ESXi。
   c. 选择库存中新创建的副本。
   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。

适用于 VMware 的代理程序 - 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。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。

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。

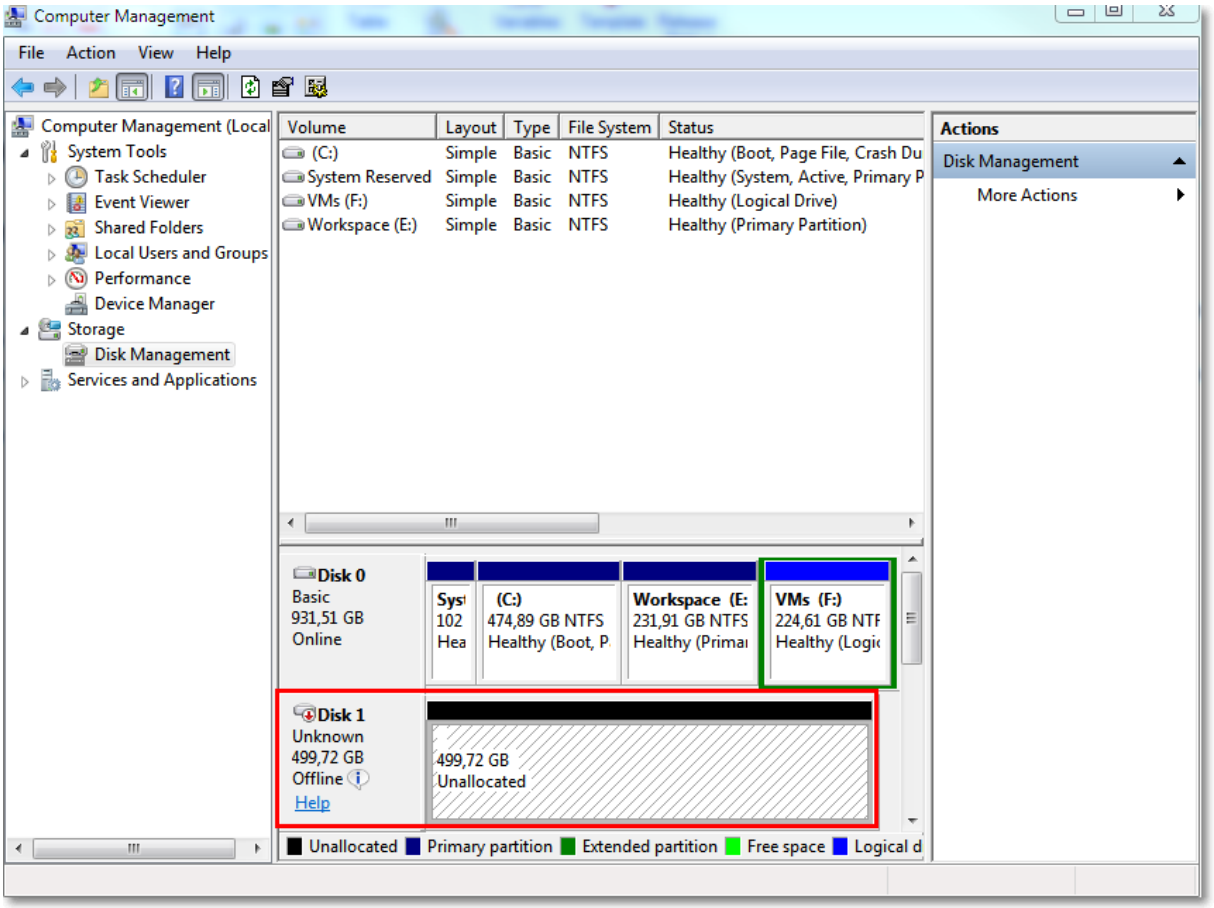
配置 iSCSI 启动程序

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:**。

注意
本地连接存储 (LAS) 专为具有单个代理程序（虚拟设备）的相对较小的环境而设计。我们已经测试了容量高达 5 TB 的本地连接存储单元。您可以连接更大的磁盘，风险由您自行承担，但不支持此类配置。对于超过 5TB 的备份数据，我们建议您使用其他类型的存储。例如，您可以创建 VMware 虚拟磁盘并将其附加到任意随机虚拟机，并在其上创建网络共享，然后将其用作备份目标而不是 LAS。

虚拟机绑定

本节概述了 Cyber Protection 服务如何在 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。如果发生这种情况，则 Cyber Protection 服务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。Cyber Protection 服务会将最适合的计算机指派给新的代理程序。将会减少旧代理程序的负载。

当从 Cyber Protection 服务中删除代理程序时，已指派给该代理程序的计算机将在剩余代理程序中进行分配。但是，如果代理程序遭破坏或从 vSphere 中手动删除代理程序，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。

自动运行冻结前和解冻后脚本

使用 VMware Tools，可以在无代理程序模式下备份的虚拟机上自动运行自定义冻结前和解冻后脚本。因此，例如可以运行自定义静默脚本并为运行不支持 VSS 感知的应用程序的虚拟机创建应用程序一致性备份。

先决条件

冻结前和解冻后脚本必须放置于虚拟机上的特定文件夹中。

- 对于 Windows 虚拟机，此文件夹的位置取决于主机的 ESXi 版本。
  例如，对于在 ESXi 6.5 主机上运行的虚拟机，该文件夹为 `C:\Program Files\VMware\VMware Tools\backupScripts.d\`。必须手动创建 `backupScritps.d` 文件夹。请勿在此文件夹中存储其他类型的文件，因为这可能会导致 VMware Tools 变得不稳定。
  有关其他 ESXi 版本的冻结前和解冻后脚本位置的详细信息，请参阅 VMware 文档。
- 对于 Linux 虚拟机，请将脚本分别复制到 `/usr/sbin/pre-freeze-script` 和 `/usr/sbin/post-thaw-script` 目录。`/usr/sbin/pre-freeze-script` 中的脚本在创建快照时运行，而 `/usr/sbin/post-thaw-script` 中的脚本在快照完成时运行。这些脚本必须可由 VMware Tools 用户执行。

自动运行冻结前和解冻后脚本

1. 确保 VMware Tools 已在虚拟机上安装。
2. 在虚拟机上，将自定义脚本放置于所需文件夹中。
3. 在这台计算机的保护计划中，启用**适用于虚拟机的卷影复制服务 (VSS)** 选项。
   这将创建一个已启用了**静默来宾文件系统**选项的 VMware 快照，进而触发虚拟机内的冻结前和解冻后脚本。

无需在运行 VSS 感知应用程序（例如 Microsoft SQL Server 或 Microsoft Exchange）的虚拟机上运行自定义静默脚本。要为此类计算机创建应用程序一致的备份，请在保护计划中启用**适用于虚拟机的卷影复制服务 (VSS)** 选项。

支持虚拟机迁移

本部分包含有关在 vSphere 环境中迁移虚拟机的信息，包括属于 vSphere 簇一部分的 ESXi 主机之间的迁移。

vMotion 允许将虚拟机的状态和配置迁移至另一台主机，而计算机磁盘保留在共享存储上的相同位置。Storage vMotion 允许将虚拟机的磁盘从一个数据存储迁移至另一个数据存储。

- 不支持运行代理程序 for VMware（虚拟设备）的虚拟机的 vMotion 迁移，包括 Storage vMotion，且必须在设备部署后禁用。为了避免在 vSphere 集群节点之间迁移设备虚拟机，您应在 vSphere 集群配置中的 VM 覆盖列表中添加此虚拟机。

- 开始备份虚拟机时，将会自动禁用使用 vMotion(包括 Storage vMotion) 进行迁移。此虚拟机将暂时添加到 vSphere 簇配置中的 **VM 覆盖**列表中。备份完成后，**VM 覆盖**设置会自动恢复到以前的状态。
- 在使用 vMotion(包括 Storage vMotion) 迁移虚拟机时，将无法开始备份该虚拟机。这台计算机的备份将在其迁移完成后开始。

保护虚拟化环境

在 Cyber Protect中控台，可以以本机呈现方式查看 vSphere、Hyper-V 和 Virtuozzo 环境。安装并注册相应的代理程序后，**设备**下将显示**VMware**、**Hyper-V** 或 **Virtuozzo**选项卡。

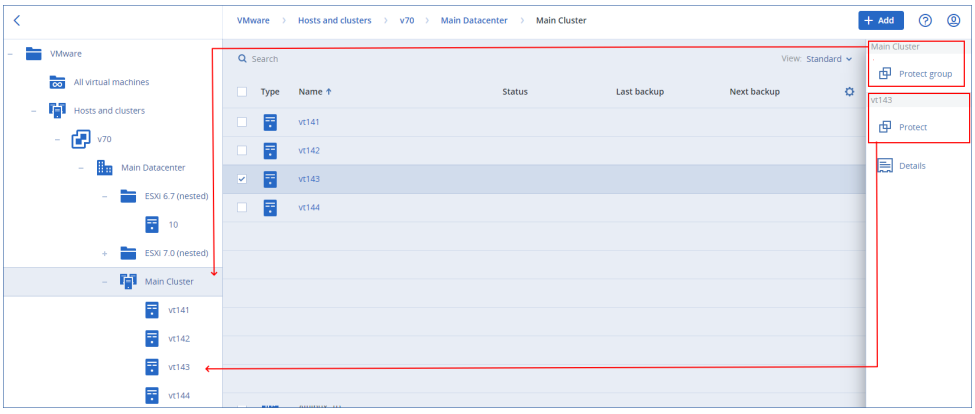
例如，在 **VMware** 选项卡中，可以备份以下 vSphere 基础架构对象：

- vCenter
- 数据中心
- 文件夹:
- 群集
- ESXi 主机
- 资源集区
- 虚拟机

若要将计划应用于选定的基础设施对象，请单击**"保护"**。所有子对象都将被备份。

若要将计划应用于所选基础设施对象的父对象，请单击**"保护组"**。父对象的所有子对象都将被备份。

例如，如果将计划应用于 ESXi 主机，则将备份该主机上的所有虚拟机。如果将计划应用于父集群，则将备份此集群中所有主机上的所有虚拟机。



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**

Agent for VMware 所需的权限

注意
若要启用虚拟机备份，请在 ESXi 主机上安装 vStorage API。有关更多信息，请参阅此知识库文章。

VMware 代理程序通过代理程序部署期间指定的用户帐户向 vCenter 或 ESXi 主机进行身份验证。用户帐户必须具有包含下表所列权限的角色。我们建议您使用专用帐户和角色，而不是使用具有管理员角色的现有帐户。

必须授予用户帐户访问 vSphere 基础架构所有级别的权限，例如 vCenter、数据中心、集群、ESXi 主机、资源池和虚拟机。若要了解如何在 vCenter 级别添加权限并将其传播到其他级别，请参阅 "授予用户账户访问权限"(第 627 页) 。

您可以更改 Agent for VMware 使用的用户帐户，而无需重新部署代理。若要了解如何更改帐户，请参阅 "更改 Agent for VMware 的用户帐户"(第 628 页) 。

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
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					
	禁用方法	+	+	+	

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
	启用方法	+	+	+	
	许可证	+	+	+	+
	管理自定义属性	+	+	+	
	设置自定义属性	+	+	+	
主机 > 配置					
	存储分区配置				+
	修改群集				
主机 > 本地操作					
	创建虚拟机				+
	删除虚拟机				+
	重新配置虚拟机				+
网络					
	分配网络		+	+	+
资源					
	将虚拟机分配到资源池		+	+	+
虚拟机 > 更改配置					
	获取磁盘租约	+		+	
	添加现有磁盘	+	+		+
	添加新磁盘		+	+	+
	添加或删除设备		+		+
	高级配置	+	+	+	
	更改 CPU 计数		+		

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
	改变内存		+		
	更改设置		+	+	+
	更改资源	+	+		
	修改设备设置	+	+		
	删除磁盘	+	+	+	+
	重命名		+		
	设置批注				+
	切换磁盘更改跟踪	+		+	
虚拟机 > 来宾操作					
	来宾操作修改	+**			
	来宾操作程序执行	+**			
	来宾操作查询	+**			
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		+	+	
	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 > 盘点					
	从现有基础上创建		+	+	+
	新建		+	+	+

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
	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				+

***** 仅备份加密计算机时才需要此权限。

****** 仅应用程序感知备份需要此权限。

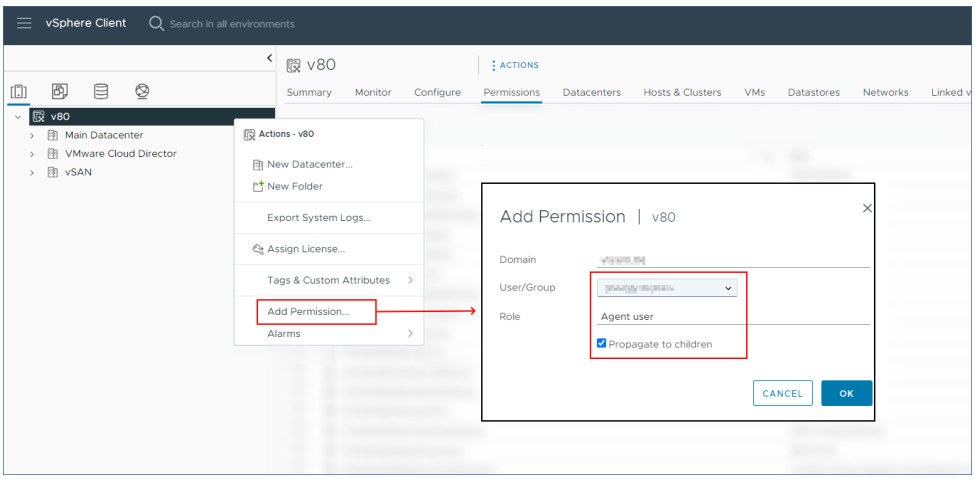
授予用户账户访问权限

Agent for VMware 使用的用户帐户必须具有对 vSphere 基础架构所有级别的访问权限，例如 vCenter、数据中心、集群、ESXi 主机、资源池和虚拟机。

授予用户帐户访问权限

1. 在 vSphere Client 中，转到**"盘点"**。
2. 右键单击要授予权限的 **vCenter** 对象，然后单击**添加权限**。
3. 在**添加权限**对话框中，选择一个用户帐户和一个角色。
   该角色必须在"Agent for VMware 所需的权限"(第 624 页) 中列出。

4. 选中**传播给子代**复选框。
5. 单击**确定**。



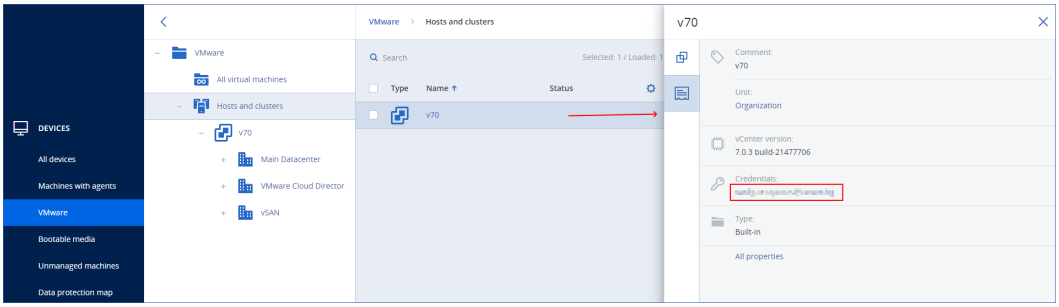
更改 Agent for VMware 的用户帐户

在Cyber Protect中控台中，可以更改 vCenter 或 ESXi 主机上单个代理或所有代理的用户帐户。

更改 Agent for VMware 的用户帐户

对于所有代理程序

1. 在Cyber Protect中控台中，转到**设备**> **VMware**。
2. 单击**主机和集群**。
3. 在主面板中，单击 vCenter 或独立 ESXi 主机名称旁边的空白处。
4. 在右侧面板上，单击**"详细信息"**。
5. 在**"凭据"**下，单击用户帐户。

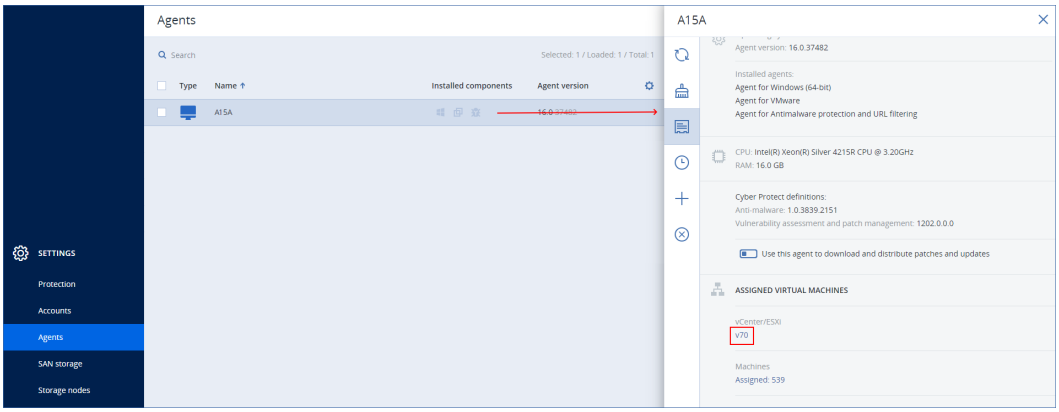


6. 指定新的用户帐户以及该帐户的密码。
7. 单击**确定**。

由此，此 vCenter 或 ESXi 主机上的所有代理都将使用新的用户帐户。

对于个人代理程序

1. 在 Cyber Protect 中控台中，转到**设置** > **代理程序**。
2. 选择代理程序。
3. 在右侧面板上，单击**"详细信息"**。
4. 在**已分配的虚拟机**下，单击 vCenter/ESXi 名称。



5. 在**添加 VMware vCenter 或 ESXi 主机**屏幕中，指定新用户帐户和该帐户的密码。
6. 单击**配置**。

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 Cyber Protection 服务中注册所有代理程序。

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。

在将备份的磁盘恢复至*新* Hyper-V 虚拟机时，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

在预定备份选项中，可以限制每个保护计划中同时备份的虚拟机的数量。

当一个代理程序同时运行多个计划时，同时备份的计算机数量会增加。这可能会影响备份性能，并使主机和虚拟机存储过载。可以通过在代理程序级别上配置限制，来避免出现此类问题。

在代理程序级别上限制同时备份的数量

适用于 VMware 的代理程序 (Windows)

1. 在具有代理程序的计算机上，创建新的文本文档，然后使用文本编辑器打开它。
2. 将以下各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. 重新启动代理程序。
   a. 在**开始**菜单中，单击**运行**。
   b. 键入 **cmd**，然后单击**确定**。
   c. 在命令行中，运行以下命令：

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

适用于 Hyper-V 的代理程序

1. 在具有代理程序的计算机上，创建新的文本文档，然后使用文本编辑器打开它。
2. 将以下各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. 重新启动代理程序。
   a. 在**开始**菜单中，单击**运行**。
   b. 键入 **cmd**，然后单击**确定**。
   c. 在命令行中，运行以下命令：

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

虚拟设备

此过程适用于以下代理程序:适用于 VMware 的代理程序(虚拟设备)、适用于 Scale Computing 的代理程序、适用于 Virtuozzo Hybrid Infrastructure 的代理程序和适用于 oVirt 的代理程序。

1. 在虚拟设备的中控台中,按 CTRL+SHIFT+F2 组合键以打开命令行界面。
2. 在文本编辑器中打开 `/etc/Acronis/MMS.config` 文件。
3. 找到以下部分:

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. 将 `10` 替换为要设置的最大同时备份数。
5. 保存文件。
6. 通过运行 `reboot` 命令,重新启动代理程序。

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		Virtuozzo Hybrid Infrastructure 虚拟机	Scale Computing HC3 虚拟机	RHV/oVirt 虚拟机
				虚拟机	容器			
物理机	+	+	+	-	-	+	+*	+
VMware ESXi 虚拟机	+	+	+	-	-	+	+*	+
Microsoft Azure 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	+	+	+	-	-	+	+*	+

*如果在源计算机上启用了安全启动，则除非在恢复后在 VM 中控台中禁用安全启动，否则恢复的 VM 将无法启动。

注意
无法将 macOS 虚拟机恢复为 Hyper-V 主机，因为 Hyper-V 不支持 macOS。可以将 macOS 虚拟机恢复为在 Mac 硬件上安装的 VMware 主机。

有关如何执行迁移操作的详细信息，请参阅以下主题：

- 有关物理到虚拟 (P2V) 迁移，请参阅 "物理机到虚拟机"(第 448 页)。
- 有关虚拟到虚拟 (V2V) 迁移，请参阅 "恢复虚拟机可以从虚拟机的备份中恢复它们。在 Cyber Protect 中控台中，无法为处于合规模式下的租户恢复备份。有关如何恢复此类备份的详细信息，请参阅 "在合规模式下恢复租户的备份"(第 1 页)。先决条件在恢复至此计算机时，该虚拟机必须处于停止状态。默认情况下，该软件会在无提示的情况下停止计算机运行。当完成恢复时，您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。步骤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。依次单击恢复 > 整台计算机。如果您希望恢复至物理机，请在恢复至中选择物理机。否则，请跳过此步骤。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，可以恢复至物理机。如果是这种情况，请继续执行“物理机”中的第 4 步。否则，我们建议使用可启动媒体执行 V2P 迁移。[可选] 默认情况下，该软件会自动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：选择虚拟机监控程序(VMware ESXi、Hyper-V、Virtuozzo、Virtuozzo Hybrid Infrastructure、Scale Computing HC3 或 oVirt)。仅 Virtuozzo 虚拟机可恢复至 Virtuozzo。有关 V2V 迁移的详细信息，请参阅“计算机迁移”。请注意，当选择 Microsoft Azure 作为目标时，可以选择相关的 Azure 订购许可、区域和资源组。选择恢复至新计算机还是现有计算机。选择主机并指定新计算机名称，或选择现有目标计算机。单击确定。设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)。要查看每个虚拟磁盘的数据存储(存储)、接口和调配模式，请单击磁盘映射。可以更改这些设置，除非您要恢复 Virtuozzo 容器或 Virtuozzo Hybrid Infrastructure 虚拟机。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。该映射部分也可让您选择个别磁盘进行恢复。对于 Microsoft Azure，可以通过选择相关存储类型(本地冗余存储 (LRS) 或区域冗余存储 (ZRS)) 来更改每个目标磁盘的存储类型。[可用于 VMware ESXi、Hyper-V 和 Virtuozzo] 要更改虚拟机的内存大小、处理器数量和网络连接，请单击 VM 设置。[适用于 Microsoft Azure] 若要更改虚拟机的可用性类型和区域、内存大小以及网络连接(包括子网和安全组)，请单击 VM 设置。[对于 Virtuozzo Hybrid Infrastructure] 要更改虚拟机的内存大小和处理

器数量，请选择规格。[仅适用于装有保护代理程序的 Windows 计算机] 启用安全恢复开关，以确保恢复后的数据无恶意软件。有关安全恢复如何工作的详细信息，请参阅 "安全恢复"(第 1 页)。单击开始恢复。当恢复至现有虚拟机时，请确认您希望覆盖磁盘。恢复进度显示在活动选项卡上。"(第 1 页)。

- 有关虚拟到物理 (V2P) 迁移，请参阅 "恢复虚拟机可以从虚拟机的备份中恢复它们。在 Cyber Protect 中控台中，无法为处于合规模式下的租户恢复备份。有关如何恢复此类备份的详细信息，请参阅 "在合规模式下恢复租户的备份"(第 1 页)。先决条件在恢复至此计算机时，该虚拟机必须处于停止状态。默认情况下，该软件会在无提示的情况下停止计算机运行。当完成恢复时，您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。步骤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。依次单击恢复 > 整台计算机。如果您希望恢复至物理机，请在恢复至中选择物理机。否则，请跳过此步骤。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，可以恢复至物理机。如果是这种情况，请继续执行“物理机”中的第 4 步。否则，我们建议使用可启动媒体执行 V2P 迁移。[可选] 默认情况下，该软件会自动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：选择虚拟机监控程序(VMware ESXi、Hyper-V、Virtuozzo、Virtuozzo Hybrid Infrastructure、Scale Computing HC3 或 oVirt)。仅 Virtuozzo 虚拟机可恢复至 Virtuozzo。有关 V2V 迁移的详细信息，请参阅“计算机迁移”。请注意，当选择 Microsoft Azure 作为目标时，可以选择相关的 Azure 订购许可、区域和资源组。选择恢复至新计算机还是现有计算机。选择主机并指定新计算机名称，或选择现有目标计算机。单击确定。设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)。要查看每个虚拟磁盘的数据存储(存储)、接口和调配模式，请单击磁盘映射。可以更改这些设置，除非您要恢复 Virtuozzo 容器或 Virtuozzo Hybrid Infrastructure 虚拟机。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。该映射部分也可让您选择个别磁盘进行恢复。对于 Microsoft Azure，可以通过选择相关存储类型(本地冗余存储 (LRS) 或区域冗余存储 (ZRS)) 来更改每个目标磁盘的存储类型。[可用于 VMware ESXi、Hyper-V 和 Virtuozzo] 要更改虚拟机的内存大小、处理器数量和网络连接，请单击 VM 设置。[适用于 Microsoft Azure] 若要更改虚拟机的可用性类型和区域、内存大小以及网络连接(包括子网和安全组)，请单击 VM 设置。[对于 Virtuozzo Hybrid Infrastructure] 要更改虚拟机的内存大小和处理器数量，请选择规格。[仅适用于装有保护代理程序的 Windows 计算机] 启用安全恢复开关，以确保恢复后的数据无恶意软件。有关安全恢复如何工作的详细信息，请参阅 "安全恢复"(第 1 页)。单击开始恢复。当恢复至现有虚拟机时，请确认您希望覆盖磁盘。恢复进度显示在活动选项卡上。"(第 1 页) 和 "使用可启动媒体恢复磁盘"(第 453 页)。

通过可启动媒体迁移

作为在 Cyber Protect 中控台中执行的计算机迁移的替代方案，可以使用可启动媒体恢复计算机。

在以下情况下，建议您使用可启动媒体：

- 执行本机不支持的迁移。
  例如，使用可启动媒体将物理机或非 Virtuozzo 虚拟机恢复为 Virtuozzo 主机上的 Virtuozzo 虚拟机。
- 执行包含逻辑卷 (LVM) 的 Linux 计算机的迁移。
  使用适用于 Linux 的代理程序或可启动媒体来创建备份，然后使用可启动媒体来恢复备份。
- 为对系统可启动性至关重要的特定硬件提供驱动程序。
  构建一个可使用所需驱动程序的可启动媒体。有关详细信息，请参阅 "可启动媒体生成器"(第 636 页)。

Microsoft Azure 和 Amazon EC2 虚拟机

要备份 Microsoft 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，Microsoft Azure 和 Amazon EC2 虚拟机无法从可启动媒体启动。如果需要恢复到新的 Microsoft Azure 或 Amazon EC2 虚拟机，请按照下面的步骤操作。

注意
以下恢复步骤仅适用于包含要在 Microsoft Azure 中本机运行的所有必要驱动程序的计算机的备份 (由 Azure VM、本地 Hyper-V 计算机或装有 Windows Server 2016 及更高版的源计算机创建的备份)。有关跨平台恢复的信息，请参阅此知识库文章。

将计算机恢复为 Microsoft Azure 或 Amazon EC2 虚拟机

1. 从 Microsoft Azure 或 Amazon EC2 中的映像/模板创建新的虚拟机。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。

创建可启动媒体以恢复操作系统

可启动媒体是让您可以在基于 Linux 的环境或 Windows 预安装环境/Windows 恢复环境 (WinPE/WinRE) 中运行保护代理程序的 CD、DVD、USB 闪存驱动器或其他可移动媒体，而无需操作系统的帮助。可启动媒体的主要用途是恢复无法启动的操作系统。

注意
可启动媒体不支持混合驱动器。

自定义还是现成可用的可启动媒体？

使用“可启动媒体生成器”，可以为 Windows、Linux 或 macOS 计算机创建自定义的可启动媒体 (“基于 Linux”或“基于 WinPE”)。在基于 Linux 和 WinPE/WinRE 的自定义可启动媒体中，您可以配置其他设置，例如自动注册、网络设置或代理服务器设置。在基于 WinPE/WinRE 的自定义可启动媒体中，还可以添加其他驱动程序。

或者，您可以下载现成可用的可启动媒体(仅基于 Linux)。可使用现成可用的可启动媒体来进行恢复操作和访问 Universal Restore 功能。

基于 Linux 还是基于 WinPE/WinRE 的可启动媒体?

基于 Linux

基于 Linux 的可启动媒体包含基于 Linux 内核的保护代理程序。代理程序可以在任何 PC 兼容硬件上启动并执行操作，包括裸机以及其文件系统已损坏或不受支持的计算机。

基于 WinPE/WinRE

基于 WinPE 的可启动媒体包含一个称为 Windows 预安装环境 (WinPE) 的最小 Windows 系统和适用于 WinPE 的 Cyber Protection 插件，即可在预安装环境中运行的改版保护代理程序。基于 WinRE 的可启动媒体使用 Windows 恢复环境，而且不需要安装其他 Windows 软件包。

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 Cyber Protection 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。

创建物理可启动媒体

强烈建议您在开始使用磁盘级别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 中创建物理可启动媒体

1. 创建自定义可启动媒体 ISO 文件或下载现成可用的 ISO 文件。
   若要创建自定义 ISO 文件，请使用 "可启动媒体生成器"(第 636 页)。
   要下载现成可用的 ISO 文件，请在 Cyber Protect 中控台中，选择一台计算机，然后依次单击**恢复** > **更多恢复方法...** > **下载 ISO 映像**。
2. [可选] 在 Cyber Protect 中控台中，生成注册令牌。在下载现成可用的 ISO 文件时，自动显示注册标记。

有了此标记，无需提示输入登录名和密码，即可从可启动媒体访问云存储。

3. 您可以通过下列途径之一创建物理可启动媒体：
   - 将 ISO 文件刻录到 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。

   对于虚拟机，可以将 ISO 文件作为 CD/DVD 驱动器连接到要恢复的计算机。

在 macOS 中创建物理可启动媒体

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。

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。它作为可选组件安装在安装有保护代理程序的计算机上。

为什么使用可启动媒体生成器？

在 Cyber Protect 中控台中可供下载的现成可用的可启动媒体是基于 Linux 内核的。不同于 Windows PE，它不允许在运行时插入自定义驱动程序。

可启动媒体生成器允许您创建自定义的基于 Linux 或基于 WinPE 的可启动媒体映像。

32 位或 64 位？

可启动媒体生成器创建包含 32 位和 64 位组件的可启动媒体。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. 在**可启动媒体类型**中，选择**默认（基于 Linux 的媒体）**。
3. 选择卷和网络资源的显示方式：
   - 具有类似 Linux 的卷表示形式的可启动媒体将卷显示为 hda1 和 sdb2 等。在开始恢复之前，它会尝试重建 MD 设备和逻辑卷 (LVM)。
   - 具有类似 Windows 的卷表示形式的可启动媒体将卷显示为 C:和 D: 等。它会提供对动态卷 (LDM) 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"(第 637 页)。
5. [可选] 选择可启动媒体的语言。
6. [可选] 选择恢复后 Windows 将使用的启动模式(BIOS 或 UEFI)。
7. 选择要置于媒体上的组件 – Cyber Protection 可启动代理程序。
8. [可选] 为启动菜单指定超时时间间隔。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。
9. [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。有关脚本的详细信息，请参阅 "可启动媒体中的脚本"(第 639 页)。
10. [可选] 选择如何在启动时在 Cyber Protection 服务上注册可启动媒体。有关注册设置的更多信息，请参阅 "注册可启动媒体"(第 647 页)。
11. 为已启动计算机的网络适配器指定网络设置，或保留自动 DHCP 配置。
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. 选择已创建可启动媒体的文件类型：
    - ISO 映像
    - ZIP 文件
14. 指定可启动媒体文件的文件名。
15. 在摘要窗口中查看您的设置，然后单击**继续**。

内核参数

当可启动媒体启动时，可以指定将自动应用的 Linux 内核的一个或多个参数。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。

如果删除了此参数，将显示所有启动消息，后跟命令提示符。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预定义的操作，可以在使用可启动媒体生成器创建媒体时指定一个脚本。这样，每次从媒体启动计算机时，将运行指定的脚本并且不会显示用户界面。

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：

- 从云存储恢复 (**entire_pc_cloud**)
- 从网络共享恢复 (**entire_pc_share**)

脚本位于安装了可启动媒体生成器的计算机的以下文件夹中：

- 在 Windows 中：**%ProgramData%\安克诺斯\MediaBuilder\scripts**
- 在 Linux 中：**/var/lib/安克诺斯/MediaBuilder/scripts/**

从云存储恢复

在可启动媒体生成器中，指定以下脚本参数：

1. 备份文件名。
2. [可选] 脚本将用于访问加密备份的密码。

从网络共享恢复

在可启动媒体生成器中，指定以下脚本参数：

- 网络共享的路径。
- 网络共享的用户名和密码。
- 备份文件名。要查找备份文件名，请执行以下操作：
  a. 在 Cyber Protect 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。

- [可选] 脚本将用于访问加密备份的密码。

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%\安克诺斯\MediaBuilder\scripts**
- 在 Linux 中：**/var/lib/安克诺斯/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	string	是	要在可启动媒体生成器中显示的脚本名称。
description	string	否	要在可启动媒体生成器中显示的脚本描述。
timeout	number	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	string	是	**<script_file>.sh** 中使用的变量名称。
type	string	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	string	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	number (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)	number	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)	number	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 spinner)	number	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。
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)	number	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	描述
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
            }
        }
}
```

基于 WinPE 和 WinRE 的可启动媒体

您可以创建 WinRE 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 WinPE 映像。

WinRE 映像

以下操作系统支持创建 WinRE 映像：

- Windows 7（32 位和 64 位）
- Windows 8（32 位和 64 位）
- Windows 8.1（32 位和 64 位）
- Windows 10（32 位和 64 位）
- Windows 11（64 位）
- Windows Server 2012（64 位）
- Windows Server 2016（64 位）
- Windows Server 2019（64 位）
- Windows Server 2022（64 位）

WinPE 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 10.0.1xxx)
- Windows 11 (PE 10.0.2xxx)

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。

注意
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。

创建 WinPE 或 WinRE 可启动媒体

可启动媒体生成器提供了将 Cyber Protection 与 WinPE 和 WinRE 相集成的两种方法：

- 使用 Cyber Protection 插件从头创建 ISO 文件。
- 将 Cyber Protection 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）。

创建 WinPE 或 WinRE 可启动媒体

1. 在已安装保护代理程序的计算机上，运行可启动媒体生成器。
2. 在**可启动媒体类型**中，选择 **Windows PE** 或 **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。
3. 选择可启动媒体的子类型：**WinRE** 或 **WinPE**。
   创建 WinRE 可启动媒体不需要安装任何其他软件包。
   要创建 64 位的 WinPE 媒体，必须下载 Windows 自动安装工具包 (AIK) 或 Windows 评估和部署工具包 (ADK)。要创建 32 位的 WinPE 媒体，除了下载 AIK 或 ADK，还需要执行以下操作：
   a. 单击**下载用于 WinPE（32 位）的插件**。
   b. 将插件保存到 **%PROGRAM_FILES%\BackupClient\BootableComponents\WinPE32**。
4. [可选] 选择可启动媒体的语言。
5. [可选] 选择恢复后 Windows 将使用的启动模式（BIOS 或 UEFI）。
6. 为已启动计算机的网络适配器指定网络设置，或保留自动 DHCP 配置。
7. [可选] 选择如何在启动时在 Cyber Protection 服务上注册可启动媒体。有关注册设置的更多信息，请参阅 "注册可启动媒体"（第 647 页）。
8. [可选] 指定要添加到可启动媒体的 Windows 驱动程序。
   在启动计算机进入 Windows PE 或 Windows RE 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 或 WinRE 分发，请添加 32 位驱动程序，如果使用 64 位 WinPE 或 WinRE 分发，请添加 64 位驱动程序。
   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 或 WinRE 媒体中包含的每个驱动程序重复该步骤。
9. 选择已创建可启动媒体的文件类型：

- ISO 映像
- WIM 映像

10. 指定所生成映像文件的完整路径，包括文件名。
11. 在摘要窗口中查看您的设置，然后单击**继续**。

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：

```
复制 c:\RecoveryWIMMedia.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。

准备：WinPE 2.x 和 3.x

为了能够创建或修改 PE 2.x 或 3.x 镜像，请在同一计算机上安装可启动媒体生成器和 Windows 自动安装工具包 (AIK)。

若要准备一台计算机

1. 从 Microsoft 网站下载 AIK 镜像文件，如下：
   - 对于 Windows Vista (PE 2.0): https://www.microsoft.com/en-us/download/details.aspx?id=10333
   - 对于 Windows Vista SP1 和 Windows Server 2008 (PE 2.1): https://www.microsoft.com/en-us/download/details.aspx?id=9085
   - 对于 Windows 7 (PE 3.0): https://www.microsoft.com/en-gb/download/details.aspx?id=5753
     对于 Windows 7 SP1 (PE 3.1)，您还需要 AIK 补充，可从 https://www.microsoft.com/en-us/download/details.aspx?id=5188 获取
2. 将镜像文件刻录到 DVD 磁盘或 USB 闪存驱动器。
3. 从镜像文件中，安装以下内容：
   - Microsoft .NET Framework(NETFXx86 或 NETFXx64，具体取决于您的硬件)
   - MSXML(Microsoft XML 解析器)
   - Windows AIK
4. 在同一计算机上安装可启动媒体生成器。

准备：WinPE 4.0 和更高版本

为了能够创建或修改 PE 4 或更高版本的镜像，请在同一台计算机上安装可启动媒体生成器和 Windows 评估和部署工具包 (ADK)。

若要准备一台计算机

1. 从 Microsoft 网站下载 ADK 安装程序。
   支持以下 Windows 版本：
   - Windows 11(PE 10.0.2xxx)
   - Windows 10 (PE 10.0.1xxx)
   - Windows 8.1 (PE 5.0)
   - Windows 8 (PE 4.0)
2. 安装评估和部署套件。
3. 安装可启动媒体生成器。

注册可启动媒体

在 Cyber Protection 服务中注册可启动媒体后，便可以访问您备份的云存储。创建可启动媒体时可以预配置注册。如果没有预配置注册，可以在启动具有媒体的计算机后注册该媒体。

在 Cyber Protection 服务中预配置注册

1. 在可启动媒体生成器中，导航到**可启动媒体注册**。
2. 在**服务 URL** 中，指定 Cyber Protection 服务地址。
3. [可选] 在**要显示的名称**中，指定已启动计算机的名称。
4. 要在 Cyber Protection 服务中设置自动注册，请选中**自动注册可启动媒体**复选框，然后选择自动注册级别：
   - **启动时要求提供注册标记**
     每次从此可启动媒体启动计算机时都必须提供该标记。
   - **使用以下标记**
     从此可启动媒体启动计算机时，会自动注册计算机。

从可启动媒体启动计算机后注册可启动媒体

1. 从可启动媒体启动计算机。
2. 在启动窗口中，单击**注册媒体**。
3. 在**服务器**中，指定 Cyber Protection 服务地址。
4. 在**注册标记**中，输入注册标记。
5. 单击**注册**。

网络设置

创建可启动媒体时，可预配置可启动代理程序将使用的网络连接。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

在可启动代理程序在计算机上启动后，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，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 (NIC) 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，其设置被选中并保存在该媒体上。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。

在可启动代理程序在服务器上启动后，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。

可启动代理程序会为每个已知 NIC 指派适合的设置，并通过其 MAC 地址识别 NIC。在配置带有已知 MAC 地址的 NIC 后，将从上部未指派的 NIC 开始，为剩余的 NIC 指派您为不存在的 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

可启动代理可以使用其中一个网络适配器，来通过生产网络与管理中控台通信。可以为此连接进行自动配置。可以通过第二个 NIC(通过使用静态 TCP/IP 设置的方式包含在专用备份网络中) 传输用于恢复的大量数据。

连接到从可启动媒体启动的计算机

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**。

计算机从可启动媒体启动后，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

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**。随后打开的**网络设置**窗口将允许您配置计算机的每个网卡 (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**。

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
   建议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已卸载（sda1、sda2...）。
3. 任务无法排程。如果您需要重复一项操作，则需要重新配置。
4. 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。

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 **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**）选择合适的模式，然后按 **Enter**。

如果在每次启动给定硬件配置时不想遵循此过程，请使用在**内核参数**字段中指定的适当的模式编号（在上例中，**vga=0x318**）重新创建可启动媒体。

本地使用可启动媒体恢复

1. 从可启动媒体启动计算机。
2. 单击**本地管理此计算机**。
3. 单击**恢复**。

4. 在**恢复内容**下，单击**选择数据**。
5. 选择要从中恢复的备份文件。
6. 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**确定**。
7. 配置覆盖规则。
8. 配置恢复排除。
9. 配置恢复选项。
10. 检查您的设置是否正确，然后单击 **OK**。

通过可启动媒体进行的远程操作

注意
该功能随 Advanced Backup 包提供。

要在 Cyber Protect 中控台中查看可启动媒体，首先需要注册它，如 "注册可启动媒体"(第 647 页) 中所述。

在 Cyber Protect 中控台中完成注册媒体后，它会显示在**设备** > **可启动媒体**选项卡上。当可启动媒体处于脱机状态超过 30 天时，它将从此选项卡中消失。

可以在 Cyber Protect 中控台中远程管理可启动媒体。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。

重要事项
在 中控台中的**设置** > **代理程序**选项卡上，无法远程更新可启动媒体。

要更新可启动媒体，请创建一个新的可启动媒体，如 "可启动媒体生成器"(第 636 页) 部分中所述。或者，下载现成可用的媒体，方法是在 中控台中依次单击您的帐户图标 > **下载** > **可启动媒体**。

使用可启动媒体远程恢复文件或文件夹

1. 在 Cyber Protect 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。

   搜索与语言无关。

   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(包含/排除)"(第 409 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 464 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 "恢复物理机本部分介绍使用 Web 界面恢复物理机。如果要恢复以下内容，请使用可启动媒体，而不是 Web 界面：运行 macOS 的计算机租户中的计算机处于“合规模式”下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。您不能恢复基于 Intel 的 Mac 对使用 Apple Silicon 处理器的 Mac 的磁盘级别备份，反之亦然。您可以恢复文件和文件夹。恢复至物理机选择已备份的计算机。单击恢复。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。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。如果您对映射结果不满意，或者磁盘映射失败，请单击卷映射以手动重新映射磁盘。该映射部分也可让您选择个别磁盘或卷进行恢复。可以使用右上角的切换至... 链接，在恢复磁盘和卷之间切换。[仅适用于装有保护代理程序的 Windows 计算机] 启用安全恢复开关，以确保恢复后的数据无恶意软件。有关安全恢复如何工作的详细信息，请参阅 "安全恢复"(第 1 页)。单击开始恢复。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。"(第 1 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 464 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 Cyber Protect 中控台中删除可启动媒体。
3. 确认要删除可启动媒体。

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。凭借 启动恢复管理器，您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。

如果出现故障，请重新启动计算机，等待提示**按 F11以使 安克诺斯启动恢复管理器** 出现，然后按 F11 或从启动菜单选择 启动恢复管理器(如果您使用 GRUB 引导加载程序)。启动恢复管理器 会启动，您即可执行恢复。

启动恢复管理器 支持 Windows 和 Linux 计算机。

重要事项
在具有加密系统卷的计算机上激活 启动恢复管理器 需要至少一个非加密卷。

磁盘空间要求

启动恢复管理器需要磁盘空间来存放临时文件。具体要求取决于所安装的计算机启动恢复管理器已激活。

下表总结了可用的选项。

启动模式	无安全区的计算机		有安全区的计算机
	使用非加密系统卷	使用加密系统卷	使用加密或非加密的系统卷
BIOS	系统卷上有 200 MB	未加密卷上有 400 MB	安全区上有 400 MB
UEFI	EFI 系统分区 (ESP) 上有 200 MB	以下之一： • EFI 系统分区 (ESP) 上有 400 MB • 启动过程中 EFI 系统分区 (ESP) 上有 200 MB，可访问的未加密分区上有 200 MB	安全区上有 400 MB

注意
重新启动恢复需要额外的磁盘空间。若要检查需要多少额外空间，请参阅"磁盘空间要求"(第 453 页)。

限制

- [不适用于安装到主启动记录的 GRUB] 激活启动恢复管理器用自己的启动代码覆盖主启动记录 (MBR)。因此，您可能需要在激活后重新激活任何第三方启动加载程序。
- [不适用于 GRUB] 激活之前启动恢复管理器在 Linux 中，我们建议您将启动加载程序安装到根分区的启动记录或 /启动分区的启动记录，而不是将其安装到主启动记录。否则，请在激活后手动重新配置启动加载程序。

激活 启动恢复管理器

若要启用启动时提示，**按 F11 以 安克诺斯 启动恢复管理器**(或添加 **启动恢复管理器** 项到 GRUB 菜单)，您必须激活 启动恢复管理器。

注意
在 启动恢复管理器 未激活情况下，创建一键恢复备份的备份操作将会失败。

若要激活 启动恢复管理器

在有代理程序的计算机上

1. 在 Cyber Protect 中控台中，选择要在其上激活 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** 转变。

在没有代理程序的计算机上

1. 使用可启动媒体启动计算机。
2. 在可启动媒体图形界面中，单击**"工具" > "激活"启动恢复管理器**。
3. 选择**激活**。
4. 单击**确定**。
5. 在**"详细信息"**选项卡上，检查**"结果"**行以验证激活是否成功。
6. 单击**关闭**。

取消激活 启动恢复管理器

停用会禁用启动时的提示**按 F11 进行 安克诺斯 启动恢复管理器**(或删除GRUB 菜单中的 **启动恢复管理器** 项目)。

如果 启动恢复管理器 未激活，您仍然可以使用单独的可启动媒体来恢复无法启动的计算机。

注意
在 启动恢复管理器 未激活情况下，创建一键恢复备份的备份操作将会失败。

若要停用 启动恢复管理器

在有代理程序的计算机上

1. 在 Cyber Protect 中控台中，选择您要停用 启动恢复管理器 的计算机。
2. 单击**详细信息**。
3. 禁用 **启动恢复管理器** 转变。

在没有代理程序的计算机上

1. 使用可启动媒体启动计算机。
2. 在可启动媒体图形界面中，单击**“工具”** > **“停用”启动恢复管理器**。
3. 选择**停用**。
4. 单击**确定**。
5. 在**“详细信息”**选项卡上，检查**“结果”**行以验证停用是否成功。
6. 单击**关闭**。

实施灾难恢复

注意
此功能不支持 Microsoft Azure 备份位置。

关于 Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR) 是 Cyber Protection 的一部分，它提供“灾难恢复即服务”(DRaaS)。在发生人为灾难或自然灾害时，Cyber Disaster Recovery Cloud 将向您提供快速且稳定的解决方案以在云站点上启动计算机的准确副本，并将工作负载从受损的原始计算机切换到云中的恢复服务器。

关键功能

注意
某些功能可能需要其他许可，具体取决于所应用的许可模式。

- 从单个中控台管理 Cyber Disaster Recovery Cloud 服务
- 通过使用安全的 VPN 隧道，可以将多达 23 个本地网络扩展到云
- 无需部署任何 VPN 设备[1]，即可建立与云站点的连接(“仅云”模式)
- 建立与本地站点和云站点的点到站点连接
- 通过在云中使用恢复服务器[2]来保护您的计算机
- 通过在云中使用主服务器[3]来保护应用程序和设备
- 针对加密备份执行自动灾难恢复操作
- 在隔离网络中执行测试故障转移
- 使用操作手册以在云中加速启动生产环境

软件要求

支持的操作系统

已针对以下操作系统对使用恢复服务器的保护进行了测试：

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x
- Red Hat Enterprise Linux 6.6, 7.x, 8.x

[1][灾难恢复] 一种特殊虚拟机，支持通过安全的 VPN 隧道在本地网络和云站点之间建立连接。VPN 设备部署在本地站点上。
[2][灾难恢复] 原始计算机的 VM 副本，基于存储在云中受保护的服务器备份。恢复服务器用于在发生灾难时切换原始服务器的工作负载。
[3][灾难恢复] 在本地站点(如恢复服务器)上没有链接计算机的虚拟机。主服务器用于保护应用程序或运行各种辅助服务(如 Web 服务器)。

- Ubuntu 18.04, 20.x, 21.x
- Oracle Linux 7.3 and 7.9 with Unbreakable Enterprise Kernel
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- 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

本软件可能适用于其他 Windows 操作系统和 Linux 发行版，但这一点不能保证。

注意
已针对以下操作系统，对 Microsoft Azure VM 的恢复服务器保护进行了测试。

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- 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
- Ubuntu Server 20.04 LTS - Gen2 (Canonical)。有关访问恢复服务器中控台的详细信息，请参阅 https://kb.acronis.com/content/71616。

所支持的虚拟化平台

已针对以下虚拟化平台对使用恢复服务器的虚拟机保护进行了测试：

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2 (包含 Hyper-V)
- Windows Server 2012/2012 R2(包含 Hyper-V)
- Windows Server 2016(包含 Hyper-V) - 所有安装选项，Nano Server 除外
- Windows Server 2019(包含 Hyper-V) – 所有安装选项，Nano Server 除外
- Windows Server 2022(包含 Hyper-V) – 所有安装选项，Nano Server 除外
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- 基于内核的虚拟机 (KVM) - 仅限完全虚拟化的来宾 (HVM)。不支持半虚拟化的来宾 (PV)。
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

已针对以下虚拟化平台对 VPN 设备进行了测试：

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 (包含 Hyper-V)
- Windows Server 2012/2012 R2(包含 Hyper-V)
- Windows Server 2016(包含 Hyper-V) - 所有安装选项，Nano Server 除外

- Windows Server 2019(包含 Hyper-V) – 所有安装选项，Nano Server 除外
- Windows Server 2022(包含 Hyper-V) – 所有安装选项，Nano Server 除外
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

支持来宾操作系统的无代理程序备份和具有逻辑卷管理器 (LVM) 配置的卷的 Linux 工作负载。

支持来宾操作系统进行无代理程序备份且具有动态磁盘 (LDM) 配置的 Windows 工作负载。

本软件可能适用于其他虚拟化平台和版本，但这一点不能保证。

限制

以下平台和配置在 Cyber Disaster Recovery Cloud 中不受支持：

1. 不受支持的平台：
   - 适用于 Virtuozzo 的代理程序
   - macOS
   - 因 Microsoft 产品条款限制，Windows 桌面操作系统不受支持。
   - Windows Server Azure 版本

     Azure 版本是 Windows Server 的特殊版本，专为在 Azure 中作为 Azure IaaS 虚拟机 (VM) 或在 Azure Stack HCI 集群上作为 VM 而构建。与标准版和 Datacenter 版不同，Azure 版本未获得在裸机硬件、Windows 客户端 Hyper-V、Windows Server Hyper-V、第三方虚拟机管理程序或第三方云中运行的许可。
2. 不受支持的配置：

   Microsoft Windows
   - 不支持 Windows 桌面操作系统(由于 Microsoft 产品条款) 。
   - 不支持使用 FRS 复制的 Active Directory 服务。
   - 不支持未使用 GPT 或 MBR 格式化的可移动媒体(所谓的“超级软盘”) 。

   Linux
   - 没有分区表的文件系统。
   - Linux 工作负载使用来宾操作系统的代理程序进行备份，并且具有包含以下高级逻辑卷管理器 (LVM) 配置的卷：带区卷、镜像卷、RAID 0、RAID 4、RAID 5、RAID 6 或 RAID 10 卷。

   注意
   不支持装有多个操作系统的工作负载。
3. 不支持的租户模式：
   - 当为租户启用“合规模式”时，灾难恢复不可用。
4. 不支持的备份类型：
   - 持续数据保护 (CDP) 恢复点不兼容。

     重要事项
     如果从具有 CDP 恢复点的备份创建恢复服务器，则在故障恢复或创建恢复服务器的备份期

间，将丢失 CDP 恢复点中包含的数据。

- 取证备份无法用于创建恢复服务器。

恢复服务器具有一个网络接口。如果原始计算机具有多个网络接口，则只有一个是模拟的。

云服务器未加密。

操作 Microsoft Azure 虚拟机

注意
某些功能可能需要其他许可，具体取决于所应用的许可模式。

可以将 Microsoft Azure 虚拟机故障转移到 安克诺斯 Cyber Protect Cloud。有关详细信息，请参阅 "执行故障转移"(第 711 页)。

之后，可以从 安克诺斯 Cyber Protect Cloud 执行故障恢复回 Azure 虚拟机。该故障恢复过程与物理机的故障恢复过程相同。有关详细信息，请参阅 "执行基于代理程序通过可启动媒体的故障恢复"(第 715 页)。

注意
要注册用于故障恢复的新 Azure 虚拟机，可以使用 Azure 中提供的 安克诺斯 Backup VM 扩展。

可以在 安克诺斯 Cyber Protect Cloud 和 Azure VPN 网关之间配置多站点 IPsec VPN 连接。有关详细信息，请参阅 "配置多站点 IPsec VPN"(第 674 页)。

Cyber Disaster Recovery Cloud 试用版

可以使用 安克诺斯 Cyber Disaster Recovery Cloud 的试用版 30 天。在这种情况下，灾难恢复对合作伙伴租户有以下限制：

- 无法通过公共 Internet 访问恢复和主服务器。无法将公共 IP 地址指派给服务器。
- IPsec 多站点 VPN 不可用。

使用 Geo-redundant Cloud Storage 时的限制

Geo-redundant Cloud Storage 会为备份数据提供辅助位置。辅助位置位于地理上与主存储位置不同的区域中。区域的地理分离确保：如果发生影响其中一个区域的灾难并使备份数据不可恢复，则另一个区域不会受到影响，操作将继续。

重要事项
如果备份存储位置从主要位置切换到地理冗余辅助位置，则不支持灾难恢复服务。

Disaster Recovery与加密软件的兼容性

灾难恢复与以下磁盘级加密软件兼容：

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

注意
- 对于具有磁盘级加密的工作负载，我们建议您在工作负载的来宾操作系统中安装保护代理程序，并执行基于代理程序的备份。
- 加密工作负载的无代理备份将不支持故障转移和故障恢复。

有关与加密软件 Cyber Protection 兼容性的更多信息，请参见"与加密软件的兼容性"(第 39 页)。

自动删除云站点上未使用的客户环境

灾难恢复服务会跟踪为灾难恢复目的而创建的客户环境的使用情况，并会自动删除未使用的客户环境。

以下条件用于定义客户租户是否处于活动状态：

- 当前，至少有一台云服务器或过去七天内有云服务器。
  或
- 启用了**对本地站点进行 VPN 访问**选项，并且建立了“站点到站点 Open VPN”隧道或过去 7 天从 VPN 设备报告了数据。

所有其他租户均被视为非活动租户。对于此类租户，系统会执行以下操作：

- 删除 VPN 网关和与租户相关的所有云资源。
- 注销 VPN 设备。

不活跃租户将回滚到其在配置连接之前所处的状态。

使用灾难恢复云

注意
某些功能可能需要其他许可，具体取决于所应用的许可模式。

使用灾难恢复的基本工作流程如下：

1. 使用以下一种方式创建要保护的工作负载的恢复服务器：
   - a. 创建包含“**灾难恢复**”模块和“**备份**”模块的保护计划，其中**备份内容**设置为**整个计算机**或系统和启动卷。
   - b. 将计划应用于您的设备。这将自动设置默认的灾难恢复基础结构。有关详细信息，请参阅创建灾难恢复保护计划。
   - 手动设置灾难恢复云基础架构，并控制每个步骤。请参阅 "创建恢复服务器"(第 694 页)。
2. 配置与云站点的连接。
   - “仅云”模式
   - 站点到站点 OpenVPN 连接

- 多站点 IPsec VPN 连接
- 点到站点连接

3. 配置自动测试故障转移。
4. 执行测试故障转移。
5. [发生灾难时] 执行生产故障转移。
6. [灾难发生后] 对本地站点执行故障恢复。
7. [可选] 配置操作手册。

创建灾难恢复保护计划

灾难恢复保护计划是启用了**"灾难恢复"**模块的保护计划。

在启用灾难恢复功能并将计划应用于设备后，会将创建云网络基础架构。有关详细信息，请参阅 "默认云网络基础架构"(第 662 页)。

注意

- 仅当恢复云网络基础架构不存在时，应用灾难恢复保护计划才会创建该基础架构。将不会更改现有云网络，也不会重新创建云网络。
- 在配置灾难恢复后，您将能够从为设备创建恢复服务器后生成的任何恢复点，执行测试或生产故障转移。在设备受到灾难恢复保护之前(例如，在创建恢复服务器之前)生成的恢复点(备份)不能用于故障转移。
- 如果无法检测到设备的 IP 地址，则无法启用灾难恢复保护计划。例如，当虚拟机进行无代理程序备份且未指派有 IP 地址时。
- 当应用保护计划时，将在云站点中指派相同的网络和 IP 地址。IPsec VPN 连接要求云和本地站点的网段不重叠。如果配置了多站点 IPsec VPN 连接，并且稍后将保护计划应用于一个或多个设备，则必须另外更新云网络并重新指派云服务器的 IP 地址。有关详细信息，请参阅 "重新指派 IP 地址"(第 688 页)。

创建灾难恢复保护计划

1. 在 Cyber Protect 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**。
   将打开保护计划的默认设置。
4. 配置备份选项。
   要使用灾难恢复功能，该计划必须将整台计算机或仅磁盘(启动和提供必要服务所需的磁盘)备份到云存储。
5. 通过单击模块名称旁边的开关，即可启用**灾难恢复**模块。
6. 单击**创建**。
   已创建计划并将其应用于所选计算机。已创建默认网络基础结构和默认参数的恢复服务器。有关详细信息，请参阅 "编辑恢复服务器的默认设置"(第 661 页) 和 "默认云网络基础架构"(第 662 页)。

下一步操作

- 可以编辑恢复服务器的默认配置。有关详细信息，请参阅 "编辑恢复服务器的默认设置"(第 661 页)。
- 可以编辑默认的网络连接配置。有关详细信息，请参阅 "连接和网络"(第 662 页)。

编辑恢复服务器的默认设置

创建并应用灾难恢复保护计划时，将使用默认设置创建恢复服务器。必要时，可以编辑这些默认设置。

注意
仅当恢复服务器不存在时，才会创建它。将不会更改现有恢复服务器，也不会重新创建恢复服务器。

若要编辑恢复服务器的默认配置

1. 转到**设备** > **所有设备**。
2. 选择一个设备，并单击**灾难恢复**。
3. 编辑恢复服务器的默认设置。
   恢复服务器设置如下表所示。

设置	默认值	描述
CPU 和 RAM	自动	恢复服务器的虚拟 CPU 数量和 RAM 量。将根据原始设备的 CPU 和 RAM 配置自动确定默认设置。
云网络	自动	服务器将连接到的云网络。有关如何配置云网络的详细信息，请参阅云网络基础架构。
生产网络中的 IP 地址	自动	服务器将在生产网络中拥有的 IP 地址。默认情况下，将设置原始计算机的 IP 地址。
测试 IP 地址	已禁用	测试 IP 地址让您可以在隔离的测试网络中测试故障转移，以及在测试故障转移期间通过 RDP 或 SSH 连接到恢复服务器。在“测试故障转移”模式下，VPN 网关会使用 NAT 协议将测试 IP 地址替换为生产 IP 地址。如果未指定测试 IP 地址，则中控台将是测试故障转移期间访问服务器的唯一途径。
Internet 访问	已启用	使恢复服务器能够在实际或测试故障转移期间访问 Internet。默认情况下，TCP 端口 25 被拒绝用于出站连接。
使用公共地址	已禁用	拥有公共 IP 地址使恢复服务器能够在故障转移或测试故障转移期间通过 Internet 进行访问。如果

		不使用公共 IP 地址，则服务器将仅在生产网络中可进行访问。要使用公共 IP 地址，必须启用 Internet 访问。公共 IP 地址将在配置完成后显示。默认情况下，TCP 端口 443 处于打开状态，用于入站连接。
设置 RPO 阈值	已禁用	RPO 阈值定义上一个恢复点与当前时间之间允许的最大时间间隔。该值可以设置的范围为 15 – 60 分钟，1 – 24 小时，1 – 14 天。

默认云网络基础架构

将灾难恢复保护计划应用于工作负载时，自动创建的云网络基础架构包括以下组件：

- 每个受保护设备的恢复服务器。

  恢复服务器是云中的虚拟机，是一个选定设备的副本。

  对于所选设备中的每一台设备，都会创建一个带有默认设置的恢复服务器，其状态为**待机**（即虚拟机未运行）。恢复服务器的大小会根据受保护设备的 CPU 和 RAM 自动调整。
- 云站点上的 VPN 网关。
- 恢复服务器所连接的云网络。

系统将检查设备的 IP 地址，如果现有云网络中不存在对应的 IP 地址，它会自动创建合适的云网络。如果现有云网络中已存在对应的恢复服务器 IP 地址，则将不会更改现有云网络，也不会重新创建云网络。

- 如果没有现有的云网络，或首次设置灾难恢复配置，则将根据您设备的 IP 地址范围使用 IANA 为专用而建议的最大范围（10.0.0.0/8、172.16.0.0/12、192.168.0.0/16）创建云网络。可以通过编辑网络掩码来缩小网络范围。
- 如果您的设备位于多个本地网络上，则云站点上的网络可能会成为本地网络的超集。可以在**连接**部分中重新配置网络。请参阅 "管理站点到站点 OpenVPN 网络"（第 670 页）。
- 如果需要设置站点到站点 Open VPN 连接，请下载 VPN 设备并对它进行配置。请参阅 "配置站点到站点 Open VPN"（第 668 页）。确保云网络范围与连接到 VPN 设备的本地网络范围相匹配。
- 若要更改默认网络配置，请导航至**灾难恢复** > **连接**，或在保护计划的 **灾难恢复** 模块中，单击 **转到连接**。

如果吊销、删除或关闭保护计划的**灾难恢复**模块，将不会自动删除恢复服务器和云网络。必要情况下，可以手动删除灾难恢复基础架构。

连接和网络

注意

某些功能可能需要其他许可，具体取决于所应用的许可模式。

借助 Cyber Disaster Recovery Cloud，可以为云站点定义以下连接类型：

- **“仅云”模式**

  此类连接不需要在本地站点上部署 VPN 设备。

  本地网络和云网络都是独立网络。此类连接意味着会故障转移所有本地站点的受保护服务器，或部分故障转移不需要与本地站点通信的独立服务器。

  可通过点到站点 VPN 和公共 IP 地址(如果已指派)访问云中的云服务器。
- **站点到站点 Open VPN 连接**

  此类连接需要在本地站点上部署 VPN 设备。

  通过使用“站点到站点 Open VPN 连接”，可以将您的网络扩展到云并保留 IP 地址。

  您的本地站点通过安全的 VPN 隧道连接到云站点。此类连接适合在本地站点上具有紧密相关服务器(如 Web 服务器和数据库服务器)的情况。在发生部分故障转移的情况下，当其中一个服务器在云站点上重新创建而其他服务器驻留在本地站点上时，它们仍然可以通过 VPN 隧道相互通信。

  可通过本地网络、点到站点 VPN 和公共 IP 地址(如果已指派)访问云中的云服务器。
- **多站点 IPsec VPN 连接**

  此类连接需要支持 IPsec IKE v2 的本地 VPN 设备。

  当开始配置多站点 IPsec VPN 连接时，Cyber Disaster Recovery Cloud 将会自动创建具有公共 IP 地址的云 VPN 网关。

  使用多站点 IPsec VPN，您的本地站点会通过安全的 IPsec VPN 隧道连接到云站点。

  当您有一个或多个托管重要工作负载或紧密相关服务的本地站点时，此类型的连接适用于灾难恢复。

  在其中一个服务器发生部分故障转移的情况下，将在云站点上重新创建该服务器而其他服务器驻留在本地站点上，而且它们仍然可以通过 IPsec VPN 隧道相互通信。

  在其中一个本地站点发生部分故障转移的情况下，本地站点的其余部分保持运行，而且它们仍然可以通过 IPsec VPN 隧道相互通信。
- **点到站点远程 VPN 访问**

  从外部使用端点设备对您云和本地站点的工作负载进行安全的点到站点远程 VPN 访问。

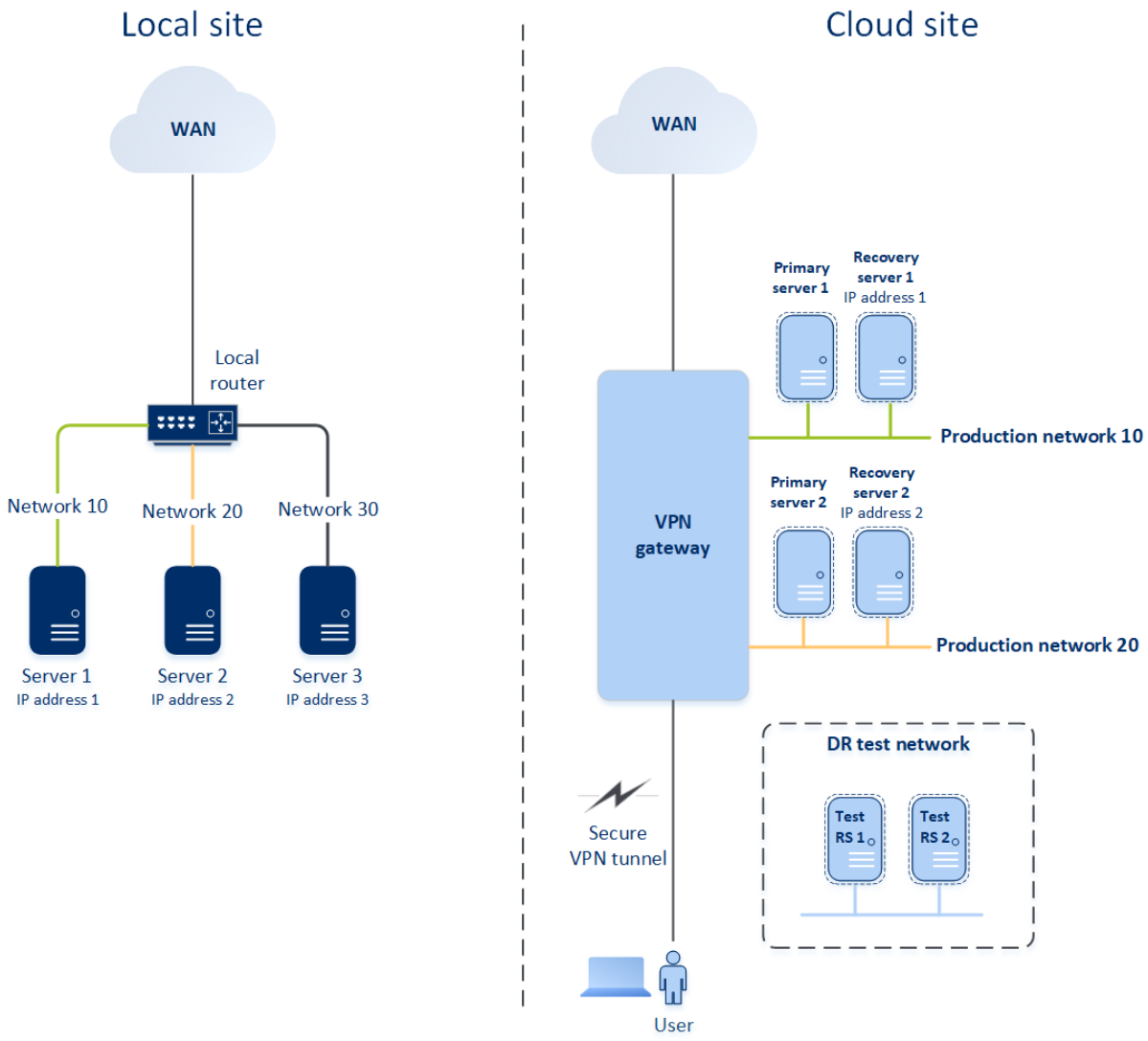
  对于本地站点访问，此类连接需要在本地站点上部署 VPN 设备。

“仅云”模式

“仅云”模式不需要在本地站点上部署 VPN 设备。这意味着您有两个独立的网络：一个在本地站点上，另一个在云站点上。使用云站点上的路由器执行路由。

路由如何工作

如果建立了仅云模式，则会使用云站点上的路由器执行路由，以便不同云网络中的服务器可以相互通信。



配置“仅云”模式

云模式是将灾难恢复计划应用于工作负载时自动创建的默认连接类型。

若要在“仅云”模式下配置连接

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **连接**。
2. 选择**仅云**，然后单击**配置**。

   结果，VPN 网关和云网络（具有已定义的地址和掩码）将部署在云站点上。

在仅云模式下管理网络

可以在云中添加和管理多达 23 个网络。

添加网络

添加新的云网络

1. 转到**灾难恢复** > **连接**。
2. 在**云站点**上，单击**添加云网络**。
3. 定义云网络参数：网络地址和掩码。准备就绪后，单击**完成**。

由此，具有已定义地址和掩码的其他云网络将在云站点上创建。

删除网络

先决条件

要删除的网络中的所有云服务器都将被删除。

删除云网络

1. 转到**灾难恢复** > **连接**。
2. 在**云站点**上，单击要删除的网络地址。
3. 单击**删除**并确认操作。

更改参数

更改云网络参数

1. 转到**灾难恢复** > **连接**。
2. 在**云站点**上，单击要编辑的网络地址。
3. 单击**编辑**。
4. 定义网络地址和掩码，然后单击**完成**。

站点到站点 Open VPN 连接

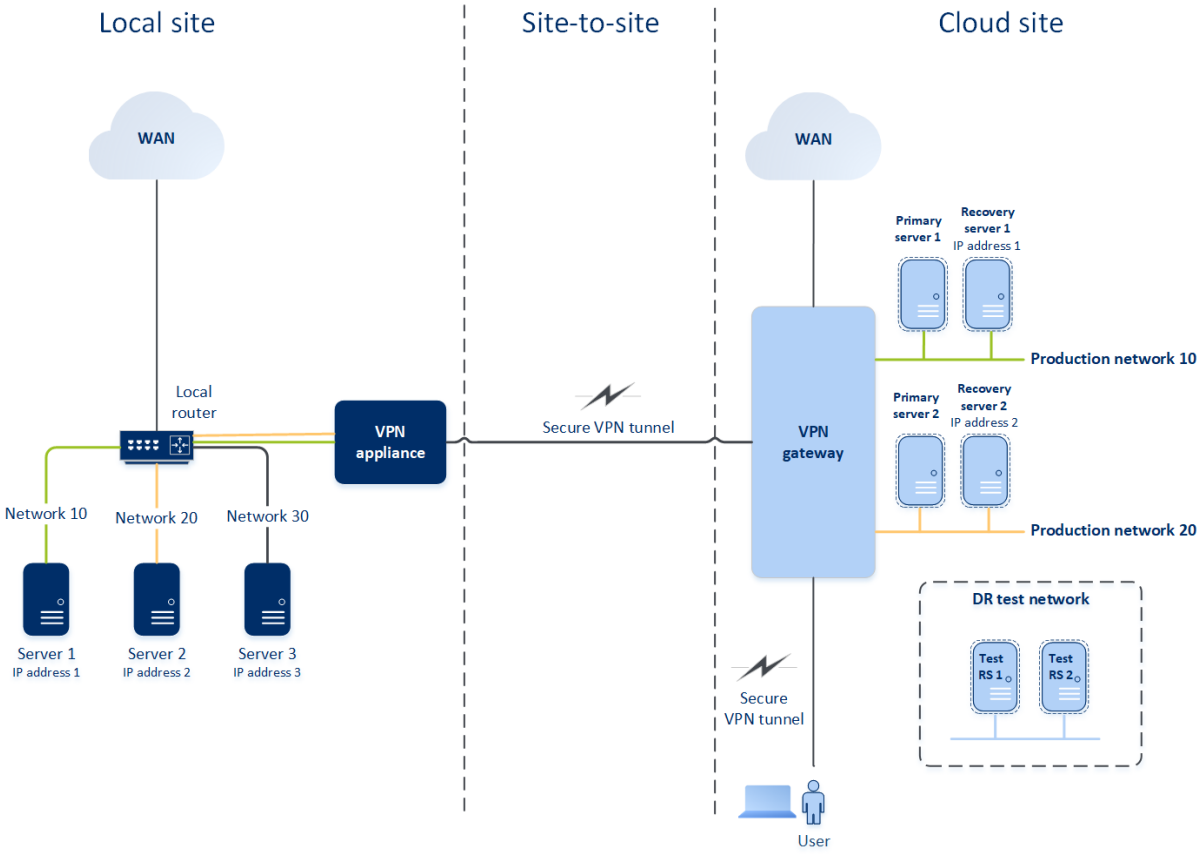
注意
此功能的可用性取决于为您的帐户启用的服务配额。

要了解网络连接如何在 Cyber Disaster Recovery Cloud 中工作，我们会考虑到以下情形：当您有三个网络时，每个网络在本地站点中都有一台计算机。您将为两个网络（Network 10 和 Network 20）配置灾难保护。

在下图中，您可以看到托管您计算机的本地站点，以及发生灾难时启动云服务器的云站点。

使用 Cyber Disaster Recovery Cloud，您可以将本地站点中受损计算机的所有工作负载故障转移到云中的云服务器。

可以在云中添加和管理多达 23 个网络。



要在本地站点和云站点之间建立站点到站点 Open VPN 连接，请使用 **VPN 设备**和 **VPN 网关**。

当在 Cyber Protect 中控台中开始配置站点到站点 Open VPN 连接时，VPN 网关将自动部署在云站点中。

部署 VPN 网关后，您必须执行以下操作：

- 在本地站点部署 VPN 服务器。
- 添加希望得到保护的网络。
- 在云中注册 VPN 设备。

Cyber Disaster Recovery Cloud 将在云中创建本地网络的副本。VPN 网关和 VPN 服务器之间将建立安全的 VPN 隧道。此 VPN 隧道将为您的本地网络提供云扩展。云中的生产网络将与本地网络桥接。本地服务器和云服务器将通过此 VPN 隧道进行通信，就好像它们都在同一以太网段中一样。路由将由本地路由器执行。

对于要保护的每台源计算机，必须在云站点上创建恢复服务器。它会一直保持在**待机**状态，直到发生故障转移事件。如果发生灾难并启动故障转移过程(在**生产模式**下)，则代表受保护计算机的确切副本的恢复服务器会在云中开始。可以为其指派与源计算机相同的 IP 地址，并在同一个以太网段中开始。您的客户端可以继续使用服务器，而不会注意到任何后台更改。

还可以在**测试模式**下启动故障转移过程。这意味着源计算机仍在工作，与此同时在云中启动具有相同 IP 地址的相应恢复服务器。为了防止出现 IP 地址冲突，系统会在云中创建一个特殊虚拟网络 - **测试网络**。系统会隔离测试网络，以防止一个以太网段中重复出现源计算机 IP 地址。要在“测试故

障转移"模式下访问恢复服务器，在创建恢复服务器时必须将**测试 IP 地址**指派给该恢复服务器。还可以配置恢复服务器的其他参数。

路由如何工作

当建立了站点到站点连接时，会使用本地路由器执行云网络之间的路由。VPN 服务器不会执行位于不同云网络中云服务器之间的路由。如果一个网络中的云服务器想要与另一个云网络中的服务器通信，流量将通过 VPN 隧道转到本地站点上的本地路由器、接着本地路由器将其路由到另一个网络，然后再通过该隧道转到云站点上的目标服务器。

VPN 网关

VPN 网关是允许本地站点和云站点之间通信的主要组件。它是云中安装有特殊软件的虚拟机，并且网络经过专门配置。VPN 网关提供以下功能：

- 在 L2 模式下，将本地网络的以太网段与云中的生产网络相连接。
- 提供 iptables 和 ebtables 规则。
- 用作测试网络和生产网络中计算机的默认路由器和 NAT。
- 用作 DHCP 服务器。生产和测试网络中的所有计算机都通过 DHCP 获取网络配置(IP 地址，DNS 设置)。云服务器每次都会从 DHCP 服务器获取相同的 IP 地址。如果需要设置自定义 DNS 配置，应与支持团队联系。
- 用作缓存 DNS。

VPN 网关网络配置

VPN 网关有几个网络接口：

- 外部接口，与 Internet 连接
- 生产接口，与生产网络连接
- 测试接口，与测试网络连接

此外，还添加了两个虚拟接口，用于点到站点连接和站点到站点连接。

在部署并初始化 VPN 网关时，系统会创建网桥 - 一个用于外部接口，另一个用于客户端和生产接口。虽然客户端-生产网桥和测试接口使用相同的 IP 地址，但 VPN 网关可以使用特定技术来正确路由数据包。

VPN 设备

VPN 设备是本地站点上安装了带有特殊软件的 Linux 的虚拟机，并且网络经过专门配置。它允许本地站点和云站点之间通信。

启用站点到站点连接

注意
此功能的可用性取决于为您的帐户启用的服务配额。

在以下情况下，可以启用站点到站点连接：

- 如果需要使用云站点上的云服务器来与本地站点上的服务器进行通信。
- 故障转移到云后，本地基础架构恢复，您希望将服务器故障恢复到本地站点。

若要启用站点到站点连接

1. 转到**灾难恢复** > **连接**。
2. 单击**显示属性**，然后启用**站点到站点连接**选项。

结果，在本地站点和云站点之间启用站点到站点 VPN 连接。Cyber Disaster Recovery Cloud 服务从 VPN 设备获取网络设置，并将本地网络扩展到云站点。

配置站点到站点 Open VPN

注意
此功能的可用性取决于为您的帐户启用的服务配额。

VPN 设备要求

系统要求

- 1 CPU
- 1 GB RAM
- 8 GB 磁盘空间

端口

- TCP 443(出站) - 用于 VPN 连接
- TCP 80(出站) - 用于自动更新设备

请确保防火墙和网络安全系统的其他组件允许通过任何 IP 地址连接这些端口。

配置站点到站点 Open VPN 连接

VPN 设备通过安全的 VPN 隧道将本地网络扩展到云。此种连接通常称为“站点到站点”(S2S) 连接。可以按照以下步骤操作，或者观看视频教程。

通过 VPN 设备配置连接

1. 在 Cyber Protect 中控台中，转到**Disaster Recovery** > **连接**。
2. 选择**站点到站点 Open VPN 连接**，然后单击**配置**。
   系统开始在云中部署 VPN 网关。这需花费一些时间。与此同时，您可以继续进行下一步。

   注意
   VPN 网关免费提供。如果未使用Disaster Recovery功能，即连续七天云中没有主服务器或恢复服务器，则会删除它。

3. 在 **VPN 设备**块中，单击**下载并部署**。根据您使用的虚拟化平台，下载适用于 VMware vSphere 或 Microsoft Hyper-V 的 VPN 设备。

4. 部署设备并将其连接到生产网络。

   在 vSphere 中，请确保**混杂模式**和**伪传输**已启用，并针对所有将 VPN 设备连接到生产网络的虚拟交换机设置为**接受**。要访问这些设置，请在 vSphere Client 中依次选择主机 > **概要** > **网络**，然后依次选择交换机 > **编辑设置...** > **安全**。

   在 Hyper-V 中，创建一个具有 1024 MB 内存的**第 1 代**虚拟机。此外，建议您为计算机启用**动态内存**。在创建计算机后，转到**设置** > **硬件** > **网络适配器**> **高级功能**，然后选中**启用 MAC 地址欺骗**复选框。
5. 接通设备电源。
6. 打开设备中控台，然后使用“admin”/“admin”用户名和密码进行登录。
7. [可选] 更改密码。
8. [可选] 更改网络设置（如有需要）。定义将哪个接口用作 Internet 连接的 WAN 接口。
9. 使用公司管理员的凭据在 Cyber Protection 服务中注册设备。

   这些凭据仅可用于检索证书一次。数据中心 URL 已预定义。

   注意

   如果为您的帐户配置了双重身份验证，则系统还会提示您输入 TOTP 代码。如果启用了双重身份验证，但未为您的帐户进行配置，则无法注册 VPN 设备。首先，必须转到 Cyber Protect 中控台登录页面并完成您帐户的双重身份验证配置。有关双重身份验证的更多详细信息，请转到“管理门户管理员指南”。

完成配置后，设备的状态将为**在线**。设备连接到 VPN 网关，并开始将有关网络的信息从所有活动接口报告给 Cyber Disaster Recovery Cloud 服务。Cyber Protect 中控台会根据 VPN 设备的信息显示接口。

管理 VPN 设备设置

注意

此功能的可用性取决于为您的帐户启用的服务配额。

在**灾难恢复** > **连接**选项卡中，您可以：

- 下载日志文件。
- 注销设备（如果需要重置 VPN 设备设置或切换到“仅云”模式）。

若要访问这些设置，请单击 **VPN 设备**块中的 **i** 图标。

在 VPN 设备中控台中，可以：

- 更改设备的密码。
- 查看/更改网络设置，并定义要用作用于 Internet 连接的 WAN 的接口。
- 注册/更改注册帐户（通过重复注册）。
- 重新启动 VPN 服务。
- 重启 VPN 设备。
- 运行 Linux shell 命令（仅针对高级故障排除情况）。

管理站点到站点 OpenVPN 网络

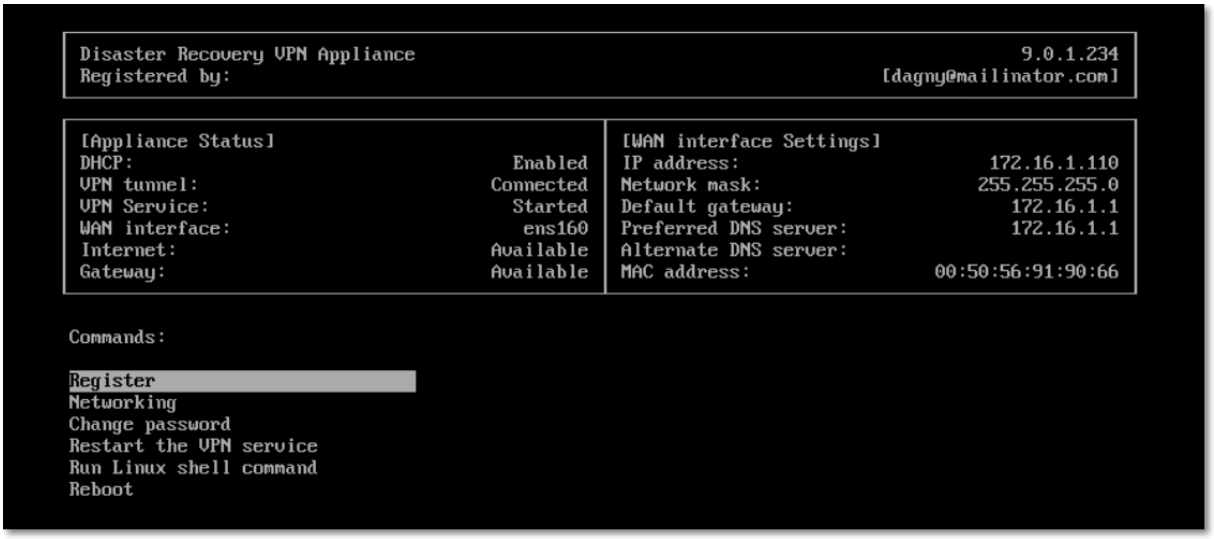
注意
某些功能可能需要其他许可，具体取决于所应用的许可模式。

可以在云中添加和管理多达 23 个网络。

添加网络

在本地站点上添加网络并将其扩展到云

1. 在 VPN 设备上，设置要在云中扩展的本地网络的新网络接口。
2. 登录 VPN 设备中控台。
3. 在**网络**部分中，为新接口设定网络设置。



VPN 设备开始将有关网络的信息从所有活动接口报告给 Cyber Disaster Recovery Cloud。Cyber Protect 中控台会根据 VPN 设备的信息显示接口。

删除网络

删除已扩展到云的网络

1. 登录 VPN 设备中控台。
2. 在**网络**部分中，选择要删除的接口，然后单击**清除网络设置**。
3. 确认操作。

结果，将停止通过安全的 VPN 隧道至云的本地网络扩展。该网络将作为独立的云段运行。如果此接口用于与云站点之前传递流量，将断开您的所有网络与云站点之间的连接。

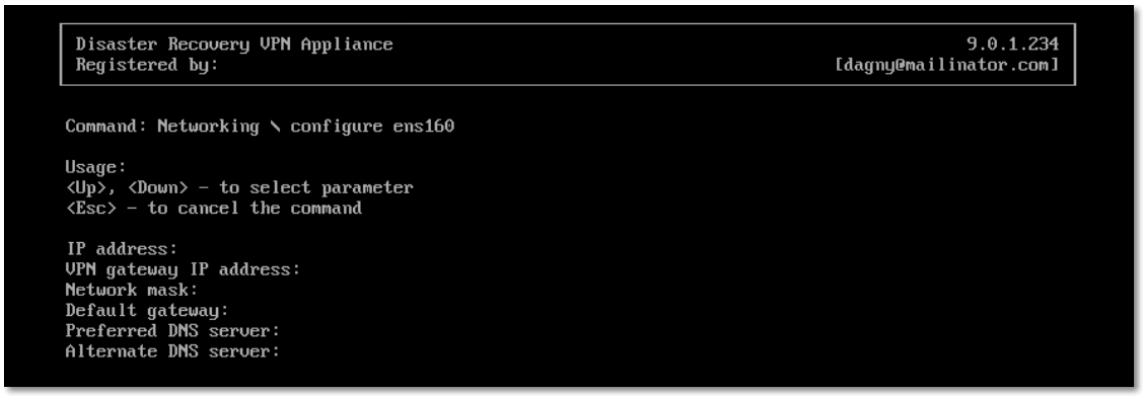
更改参数

更改网络参数

1. 登录 VPN 设备中控台。
2. 在**网络**部分中，选择要编辑的接口。

3. 单击**编辑网络设置**。
4. 选择其中一个选项：
   - 对于通过 DHCP 的自动网络配置，请单击**使用 DHCP**，然后确认操作。
   - 若要手动配置网络，请单击**设置静态 IP 地址**，配置设置，然后单击**输入**。

设置	描述
IP 地址	本地网络中接口的 IP 地址。
VPN 网关 IP 地址	为了使 Cyber Disaster Recovery Cloud 服务正常工作而保留用于网络云段的特殊 IP 地址。
网络掩码	本地网络的网络掩码。
默认网关	本地站点上的默认网关。
首选 DNS 服务器	本地站点上的主 DNS 服务器。
备用 DNS 服务器	本地站点上的辅助 DNS 服务器。



允许通过 L2 VPN 的 DHCP 流量

如果本地站点上的设备从 DHCP 服务器获取其 IP 地址，则可以使用灾难恢复保护 DHCP 服务器、将其故障转移到云，然后允许 DHCP 流量通过 L2 VPN 运行。因此，您的 DHCP 服务器将在云中运行，但会继续为本地设备指派 IP 地址。

先决条件

必须将站点到站点 L2 VPN 连接类型设置为云站点。

允许通过 L2 VPN 连接的 DHCP 流量

1. 转到**灾难恢复** > **连接**选项卡。
2. 单击**显示属性**。
3. 启用**允许通过 L2 VPN 的 DHCP 流量**开关。

从站点到站点 OpenVPN 切换到多站点 IPsec VPN

注意
此功能的可用性取决于为您的帐户启用的服务配额。

您可以轻松地从“站点到站点 Open VPN”连接切换到“多站点 IPsec VPN”连接，以及从“多站点 IPsec VPN”连接切换到“站点到站点 Open VPN”连接。

当切换连接类型时，将删除活动的 VPN 连接，但会保留云服务器和网络配置。但是，仍然需要重新指派云网络和服务器的 IP 地址。

下表比较了“站点到站点 Open VPN”连接和“多站点 IPsec VPN”连接的基本特征。

	站点到站点 Open VPN	**多站点 IPsec VPN**
本地站点支持	单个	单个，多个
VPN 网关模式	L2 Open VPN	L3 IPsec VPN
网段	将本地网络扩展到云网络	本地网段和云网段不应重叠
支持对本地站点的点对站点访问	是	否
支持对云站点的点对站点访问	是	是
需要公共 IP 提供项	否	是

从“站点到站点 Open VPN”连接切换到“多站点 IPsec VPN”连接

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **连接**。
2. 单击**显示属性**。
3. 单击**切换到多站点 IPsec VPN**。
4. 单击**重新配置**。
5. 重新指派云网络和云服务器的 IP 地址。
6. 配置多站点 IPsec 连接设置。

禁用站点到站点连接

注意
此功能的可用性取决于为您的帐户启用的服务配额。

如果不需要使用云站点上的云服务器来与本地站点上的服务器进行通信，可以禁用站点到站点连接。

若要禁用站点到站点连接

1. 转到**灾难恢复** > **连接**。
2. 单击**显示属性**，然后禁用**站点到站点连接**选项。

结果，本地站点与云站点断开连接。

多站点 IPsec VPN 连接

注意
此功能的可用性取决于为您的帐户启用的服务配额。

可以使用多站点 IPsec VPN 连接，以通过安全的 L3 IPsec VPN 连接将单个本地站点或多个本地站点连接到 Cyber Disaster Recovery Cloud。

如果您遇到以下使用案例之一，则此连接类型对灾难恢复方案很有用：

- 您有一个本地站点托管重要的工作负载。
- 您有多个本地站点托管重要的工作负载，例如位于不同位置的办公室。
- 可以使用第三方软件站点或受控服务提供商站点，并通过 IPsec VPN 隧道与这些站点连接。

为了在本地站点和云站点之间建立多站点 IPsec VPN 通信，将使用 **VPN 网关**。当在 Cyber Protect 中控台中开始配置多站点 IPsec VPN 连接时，VPN 网关将自动部署在云站点中。您应配置云网段，并确保它们与本地网段不重叠。将在本地站点和云站点之间建立安全的 VPN 隧道。本地服务器和云服务器可以通过此 VPN 隧道进行通信，就好像它们都位于同一个以太网段中一样。

对于要保护的每台源计算机，必须在云站点上创建恢复服务器。它会一直保持在**待机**状态，直到发生故障转移事件。如果发生灾难并启动故障转移过程（在**生产模式**下），则代表受保护计算机的确切副本的恢复服务器会在云中启动。您的客户端可以继续使用服务器，而不会注意到任何后台更改。

还可以在**测试模式**下启动故障转移过程。这意味着源计算机仍在工作，与此同时相应恢复服务器将在云中的特殊虚拟网络中启动，该特殊虚拟网络即是在云中创建的**测试网络**。测试网络处于隔离状态，以防止其他云网段中出现重复的 IP 地址。

VPN 网关

允许本地站点和云站点之间通信的主要组件是 **VPN 网关**。它是云中安装有特殊软件的虚拟机，并且网络经过专门配置。VPN 网关会提供以下功能：

- 在 L3 IPsec 模式下，将本地网络的以太网段与云中的生产网络相连接。
- 用作测试网络和生产网络中计算机的默认路由器和 NAT。
- 用作 DHCP 服务器。生产和测试网络中的所有计算机都通过 DHCP 获取网络配置（IP 地址，DNS 设置）。云服务器每次都会从 DHCP 服务器获取相同的 IP 地址。
  如果愿意，可以设置自定义 DNS 配置。有关详细信息，请参阅 "配置自定义 DNS 服务器"（第 689 页）。
- 用作缓存 DNS。

路由如何工作

云网络之间的路由将由云站点上的路由器执行，以便不同云网络中的服务器可以相互通信。

配置多站点 IPsec VPN

注意
此功能的可用性取决于为您的帐户启用的服务配额。

可以通过以下两种方法配置多站点 IPsec VPN 连接：

- 从**灾难恢复** > **连接**选项卡。
- 通过在一个或多个设备上应用保护计划，然后从自动创建的站点到站点 Open VPN 连接手动切换到多站点 IPsec VPN 连接、配置多站点 IPsec VPN 设置并重新指派 IP 地址。

连接选项卡

从连接选项卡配置多站点 IPsec VPN 连接

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **连接**。
2. 在**多站点 VPN 连接**部分中，单击**配置**。
   VPN 网关将部署在云站点上。
3. 配置多站点 IPsec VPN 设置。

保护计划

基于保护计划配置多站点 IPsec VPN 连接

1. 在 Cyber Protect 中控台中，转到**设备**。
2. 将保护计划应用于列表中的一个或多个设备。
   将为站点到站点 Open VPN 连接配置恢复服务器和云基础架构设置。
3. 转到**灾难恢复** > **连接**。
4. 单击**显示属性**。
5. 单击**切换到多站点 IPsec VPN**。
6. 配置多站点 IPsec VPN 设置。
7. 重新指派云网络和云服务器的 IP 地址。

配置多站点 IPsec VPN 设置

注意
此功能的可用性取决于为您的帐户启用的服务配额。

在配置多站点 IPsec VPN 后，必须在**灾难恢复** > **连接**选项卡上配置云站点和本地站点设置。

先决条件

- 多站点 IPsec VPN 连接已配置。有关配置多站点 IPsec VPN 连接的详细信息，请参阅 "配置多站点 IPsec VPN"(第 674 页)。
- 每个本地 IPsec VPN 网关都有一个公共 IP 地址。

- 您的云网络有足够 IP 地址可提供给用作受保护计算机副本的云服务器(在生产网络中)和恢复服务器(需要一个或两个 IP 地址,具体取决于您的需求)。
- [如果在本地站点和云站点之间使用防火墙]在本地站点上允许以下 IP 协议和 UDP 端口:IP 协议 ID 50 (ESP)、UDP 端口 500 (IKE) 和 UDP 端口 4500。
- 本地站点上的 NAT-T 配置已禁用。

配置多站点 IPsec VPN 连接

1. 将一个或多个网络添加到云站点。
   a. 单击**添加网络**。

      注意
      当添加云网络时,将自动添加具有相同网络地址和掩码的相应测试网络,以执行测试故障转移。测试网络中的云服务器将具有与云生产网络中相同的 IP 地址。如果在测试故障转移期间需要从生产网络访问云服务器,则在创建恢复服务器时,向其指派第二个测试 IP 地址。

   b. 在**网络地址**字段中,键入网络的 IP 地址。

      注意
      确保云网络不与您环境中的任何本地网络重叠。否则无法建立隧道。

   c. 在**网络掩码**字段中,键入网络的掩码。
   d. 单击**添加**。
2. 按照本地站点的建议,为每个要连接到云站点的本地站点配置设置。有关这些建议的详细信息,请参阅 "本地站点的一般建议"(第 676 页)。
   a. 单击**添加连接**。
   b. 输入本地 VPN 网关的名称。
   c. 输入本地 VPN 网关的公共 IP 地址。
   d. [可选]输入本地 VPN 网关的描述。
   e. 单击**下一步**。
   f. 在**预共享密钥**字段中,键入预共享密钥,或单击**生成新的预共享密钥**以使用自动生成的值。

      注意
      必须对本地和云 VPN 网关使用相同的预共享密钥。

   g. 单击 **IPsec/IKE 安全设置**以配置设置。有关可以配置的设置的详细信息,请参阅 "IPsec/IKE 安全设置"(第 676 页)。

      注意
      可以使用自动填充的默认设置,也可以使用自定义值。仅支持 IKEv2 协议连接。建立 VPN 时,默认的**启动操作**是**添加**(本地 VPN 网关发起连接),但可以将其更改为**启动**(云 VPN 网关发起连接)或**路由**(适用于支持路由选项的防火墙)。

   h. 配置**网络策略**。

网络策略指定 IPsec VPN 连接到的网络。使用 CIDR 格式键入网络的 IP 地址和掩码。本地网段和云网段不应重叠。

i. 单击**保存**。

本地站点的一般建议

注意
此功能的可用性取决于为您的帐户启用的服务配额。

在为多站点 IPsec VPN 连接配置本地站点时，请考虑以下建议：

- 对于每个 IKE 阶段，请为以下参数设置至少一个在云站点中配置的值：加密算法、哈希算法和 Diffie-Hellman 组号。
- 使用在 IKE 阶段 2 的云站点中配置的 Diffie-Hellman 组号的至少一个值，启用完全转发保密。
- 为 IKE 阶段 1 和 IKE 阶段 2 配置与云站点相同的**生命周期**值。
- 不支持使用 NAT 穿越 (NAT-T) 的配置。在本地站点上禁用 NAT-T 配置。否则，无法协商其他 UDP 封装。
- **启动操作**配置定义哪一侧发起连接。默认值**添加**表示本地站点发起连接，而云站点将等待连接发起。如果希望云站点发起连接，则将值更改为**启动**；如果希望两侧都能够发起连接，则将值更改为**路由**（适用于支持路由选项的防火墙）。

有关不同解决方案的更多信息和配置示例，请参阅：

- 此系列知识库文章
- 此视频示例

IPsec/IKE 安全设置

注意
此功能的可用性取决于为您的帐户启用的服务配额。

下表提供了有关 Psec/IKE 安全性参数的更多信息。

参数	描述
加密算法	将用于确保数据在传输过程中不可见的加密算法。默认情况下，所有算法都处于选中状态。必须在本地网关设备上为每个 IKE 阶段配置至少一种选定的算法。
哈希算法	将用于验证数据完整性和真实性的哈希算法。默认情况下，所有算法都处于选中状态。必须在本地网关设备上为每个 IKE 阶段配置至少一种选定的算法。
Diffie-Hellman 组号	Diffie-Hellman 组号定义 Internet 密钥交换 (IKE) 过程中所使用密钥的强度。

参数	描述
	组号越高越安全，但需要更多时间来计算密钥。 默认情况下，所有组都处于选中状态。必须在本地网关设备上为每个 IKE 阶段配置至少一个选定组。
生命周期(秒)	生命周期值通过一组用户数据包的加密/身份验证密钥来确定连接实例的持续时间(从成功协商到到期)。 阶段 1 的范围：900-28800 秒(默认值为 28800)。 阶段 2 的范围:900-3600 秒(默认值为 3600)。 阶段 2 的生命周期必须短于阶段 1 的生命周期。 连接将在其到期之前通过密钥通道重新协商，请参阅**密钥更新等待时间**。如果本地端和远程端的生命周期不一致，则生命周期较长的一侧将出现连接废弃的混乱情况。另请参见**密钥更新时间**和**密钥更新模糊**。
密钥更新等待时间(秒)	连接到期或密钥通道到期之前的等待时间，在此期间 VPN 连接的本地端会尝试协商替换。根据**密钥更新模糊**值随机选择密钥更新的确切时间。仅在本地相关，远端无需对此达成协商。范围：900-3600 秒。默认值为 3600。
重播窗口大小(数据包)	此连接的 IPsec 重播窗口大小。 默认值 -1 使用 strongswan.conf 文件中 charon.replay_window 配置的值。 仅当使用 Netlink 后端时才支持大于 32 的值。 值为 0 将禁用 IPsec 重播保护。
密钥更新模糊(%)	随机增加 marginbytes、marginpackets 和 margintime 以随机化密钥更新间隔的最大百分比(对于具有多个连接的主机很重要)。 密钥更新模糊值可以超过 100%。随机增加后，marginTYPE 的值不得超过 lifeTYPE，其中 TYPE 是字节、数据包或时间之一。 值 0% 表示禁用随机功能。仅在本地相关，远端无需对此达成协商。
DPD 超时(秒)	失效对等检测 (DPD) 超时发生的时间。可以指定 30 或更高的值。默认值为 30。
失效对等检测(DPD)超时操作	失效对等检测 (DPD) 超时发生后采取的操作。 **重新启动** - DPD 超时发生后重新启动会话。

参数	描述
	清除 - DPD 超时发生后结束会话。 **无** - DPD 超时发生后不采取任何操作。
启动操作	确定哪一侧发起连接，并建立 VPN 连接的隧道。 **添加** - 本地 VPN 网关发起连接。 **开始** - 云 VPN 网关发起连接。 **路由** - 适用于支持路由选项的 VPN 网关。仅当有从本地 VPN 网关或云 VPN 网关发起的流量时，隧道才会建立。

从多站点 IPsec VPN 切换到站点对站点 Open VPN

可以轻松从“多站点 IPsec VPN” 连接切换到“站点到站点 Open VPN” 连接。

当切换连接类型时，将删除活动的 VPN 连接，但会保留云服务器和网络配置。但是，仍然需要重新指派云网络和服务器的 IP 地址。

下表比较了“站点到站点 Open VPN”连接和“多站点 IPsec VPN”连接的基本特征。

	站点到站点 Open VPN	多站点 IPsec VPN
本地站点支持	单个	单个，多个
VPN 网关模式	L2 Open VPN	L3 IPsec VPN
网段	将本地网络扩展到云网络	本地网段和云网段不应重叠
支持对本地站点的点对站点访问	是	否
支持对云站点的点对站点访问	是	是
需要公共 IP 提供项	否	是

若要从“多站点 IPsec VPN”连接切换到“站点到站点 Open VPN”连接

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **连接**。
2. 单击**显示属性**。
3. 单击**切换到站点到站点 Open VPN**。
4. 单击**重新配置**。
5. 重新指派云网络和云服务器的 IP 地址。
6. 配置站点到站点连接设置。

IPsec VPN 配置故障排除

注意
此功能的可用性取决于为您的帐户启用的服务配额。

当配置或使用 IPsec VPN 连接时，可能遇到问题。

可以在 IPsec 日志文件中了解有关问题的详细信息，并查看“IPsec VPN 配置问题故障排除”主题，获取某些可能发生的常见问题的可能解决方案。

IPsec VPN 配置问题故障排除

注意
此功能的可用性取决于为您的帐户启用的服务配额。

下表描述了最经常发生的 IPsec VPN 配置问题，并解释了如何解决它们。

问题	可能的解决方案
我看到以下错误消息：**IKE 阶段 1 协商错误。检查云和本地站点上的 IPsec IKE 设置。**	单击**重试**并查看是否显示更具体的错误消息。例如，更具体的错误消息可能是有关算法不匹配或预共享的密钥错误的错误消息。 **注意** 出于安全原因，将以下限制应用到 IPsec VPN 连接： • 出于安全风险，IKEv1 在 RFC8247 中要求弃用并且不受支持。仅支持 IKEv2 协议连接。 • 以下加密算法被认为不安全并且不受支持：DES 和 3DES。 • 以下哈希算法被认为不安全并且不受支持：SHA1 和 MD5。 • Diffie-Hellman 组编号 2 被认为不安全并且不受支持。
我的本地站点和云站点之间的连接保持为**正在连接**状态。	检查： • UDP 端口 500 是否是开放的（当使用防火墙时）。 • 本地站点和云站点之间的连接。 • 本地站点的 IP 地址是否正确。
我的本地站点和云站点之间的连接保持为**正在等待连接**状态。	当云站点的**启动操作**设置为**添加**时，您会看到此状态，它云站点正在等待本地站点发起连接。 从本地站点发起连接。

问题	可能的解决方案
我的本地站点和云站点之间的连接保持为**正在等待流量**状态。	当云站点的**启动操作**设置为**路由**时，您会看到此状态。 如果希望从本地站点发起连接，请执行以下操作： • 从本地站点中，尝试在云站点中对虚拟机执行 ping 操作。这是为某些设备（例如 Cisco ASA）建立隧道所必需的标准行为。（路由模式） • 通过将本地站点的**启动操作**设置为**启动**，确保本地站点建立了隧道。
我的本地站点和云站点之间建立了连接，但我看到一个或多个网络策略已停用。	此问题可能由以下原因导致： • 云 IPsec 站点中的网络映射不同于本地站点中的网络映射。 请确保本地和云站点中的网络映射和网络策略序列精确匹配。 • 当本地站点和/或云站点的**启动操作**设置为**路由**时（例如，在 Cisco ASA 设备上），此状态是正确的，并且当前没有流量。可以尝试执行 ping 操作以确保建立了隧道。如果 ping 操作不起作用，则检查本地和云站点上的网络映射。
我想要重新启动特定 IPsec 连接。	要重新启动特定 IPsec 连接： 1. 在**灾难恢复** > **连接**屏幕中，单击 IPsec 连接。 2. 单击**禁用连接**。 3. 再次单击 IPsec 连接。 4. 单击**启用连接**。

下载 IPsec VPN 日志文件

注意
此功能的可用性取决于为您的帐户启用的服务配额。

可以在 VPN 服务器上的日志文件中找到有关 IPsec 连接的其他信息。日志文件压缩为可以下载和解压缩的 .zip 存档。

先决条件

多站点 IPsec VPN 连接已配置。

下载含有日志文件的 .zip 存档

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **连接**。
2. 单击云站点的 VPN 网关旁边的齿轮图标。
3. 单击**下载日志**。

4. 单击**完成**。
5. 当 .zip 存档可供下载时，单击**下载日志**，然后将其保存在本地。

多站点 IPSec VPN 日志文件

注意
此功能的可用性取决于为您的帐户启用的服务配额。

以下列表描述了作为 Zip 存档一部分的 IPsec VPN 日志文件及其包含的信息。

- `ip.txt` - 该文件包含来自网络接口配置的日志。必须看到两个 IP 地址 - 一个公共 IP 地址和一个本地 IP 地址。如果在日志中没有看到这些 IP 地址，则表示有问题。请与支持团队联系。

  注意
  公共 IP 地址的掩码必须为 32。

- `swanctl-list-loaded-config.txt` - 该文件包含有关所有 IPsec 站点的信息。
  如果在该文件中看不到站点，则表示未应用 IPsec 配置。尝试更新配置并保存配置，或者与支持团队联系。
- `swanctl-list-active-sas.txt` - 该文件包含处于活动状态或处于连接状态的连接和策略。

点到站点远程 VPN 访问

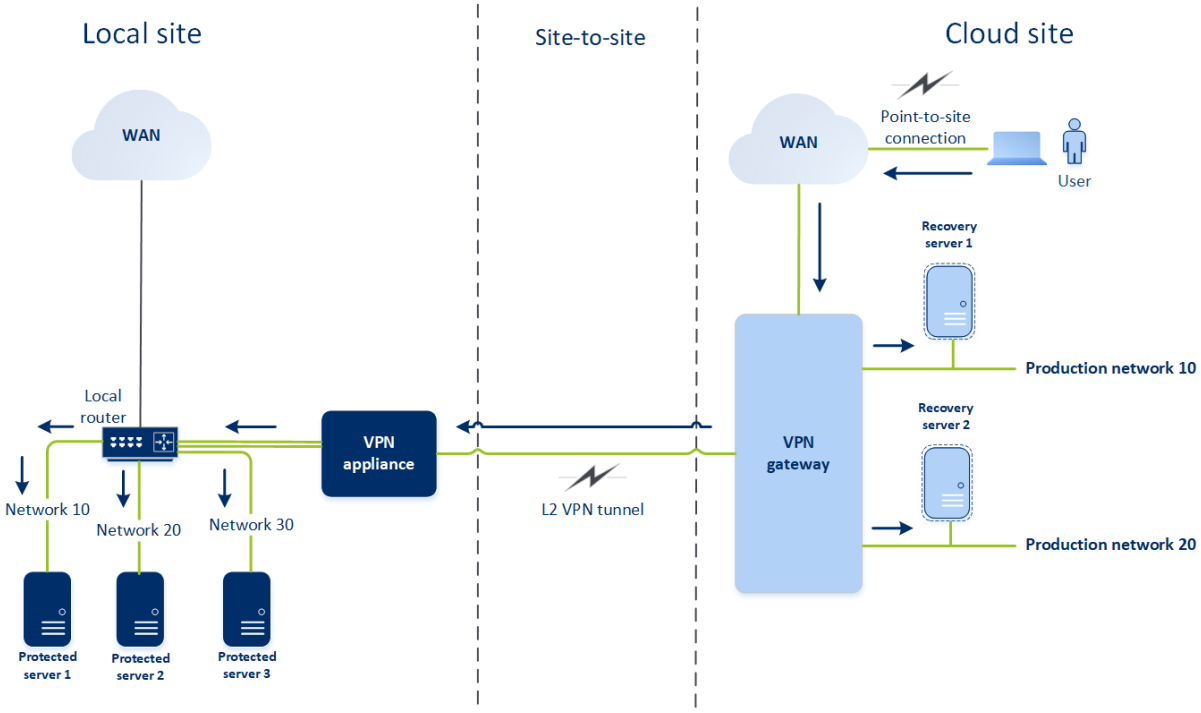
注意
此功能的可用性取决于为您的帐户启用的服务配额。

点到站点连接是一种安全的连接，即从外部使用端点设备（如计算机或笔记本电脑）通过 VPN 与云和本地站点进行安全连接。在与 Cyber Disaster Recovery Cloud 站点建立站点到站点的 Open VPN 连接后，它即可用。在下列情况下此类型的连接将很有用：

- 在许多公司中，公司服务和 Web 资源仅可从公司网络中获得。您可以使用点到站点连接安全地连接到本地站点。
- 如果发生灾难，当工作负载切换到云站点并且本地网络出现故障时，您可能需要直接访问云服务器。这可以通过与云站点建立点到站点连接来实现。

对于与本地站点建立点到站点连接，您需要在本地站点上安装 VPN 设备、配置站点到站点连接，然后配置与本地站点的点到站点连接。这样，远程员工将能够通过 L2 VPN 访问公司网络。

下面的方案显示了本地站点、云站点以及绿色亮显的服务器之间的通信。L2 VPN 隧道连接您的本地站点和云站点。当用户建立点到站点连接时，与本地站点的通信是通过云站点执行的。



点到站点配置使用证书来对 VPN 客户端进行身份验证。此外，用户凭据用于身份验证。请注意有关与本地站点建立点到站点连接的以下事项：

- 用户应使用其 Cyber Protect Cloud 凭据以在 VPN 客户端中进行身份验证。他们必须具有“公司管理员”或“网络安全保护”用户角色。
- 如果您重新生成 OpenVPN 配置，则需要向使用“点到站点连接”访问云站点的所有用户提供更新后的配置。

配置点到站点远程 VPN 访问

注意
此功能的可用性取决于为您的帐户启用的服务配额。

如果需要远程连接到本地站点，可以配置与本地站点的点到站点连接。可以按照以下步骤操作，或者观看视频教程。

先决条件

- 已配置站点到站点 Open VPN 连接。
- VPN 设备安装在本地站点上。

配置与本地站点的点到站点连接

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **连接**。
2. 单击**显示属性**。
3. 启用**对本地站点进行 VPN 访问**选项。
4. 确保需要与本地站点建立点到站点连接的用户具有：

- Cyber Protect Cloud 中的用户帐户。这些凭据用于 VPN 客户端中的身份验证。否则，请在 Cyber Protect Cloud 中创建一个用户帐户。
- “公司管理员”或“网络安全保护”用户角色。

5. 配置 OpenVPN 客户端：
   a. 从以下位置下载 OpenVPN 客户端版本 2.4.0 或更高版本：https://openvpn.net/community-downloads/。

      注意
      不支持 OpenVPN Connect 客户端。

   b. 在要从其连接到本地站点的计算机上安装 OpenVPN 客户端。
   c. 单击**下载 OpenVPN 的配置**。该配置文件适用于您组织中用户角色为“公司管理员”或“网络安全保护”的用户。
   d. 将下载的配置导入到 OpenVPN 客户端。
   e. 使用 Cyber Protect Cloud 用户凭据登录到 OpenVPN 客户端（请参阅上述步骤 4）。
   f. [可选] 如果为组织启用了双重身份验证，则应提供一次性生成的 TOTP 代码。

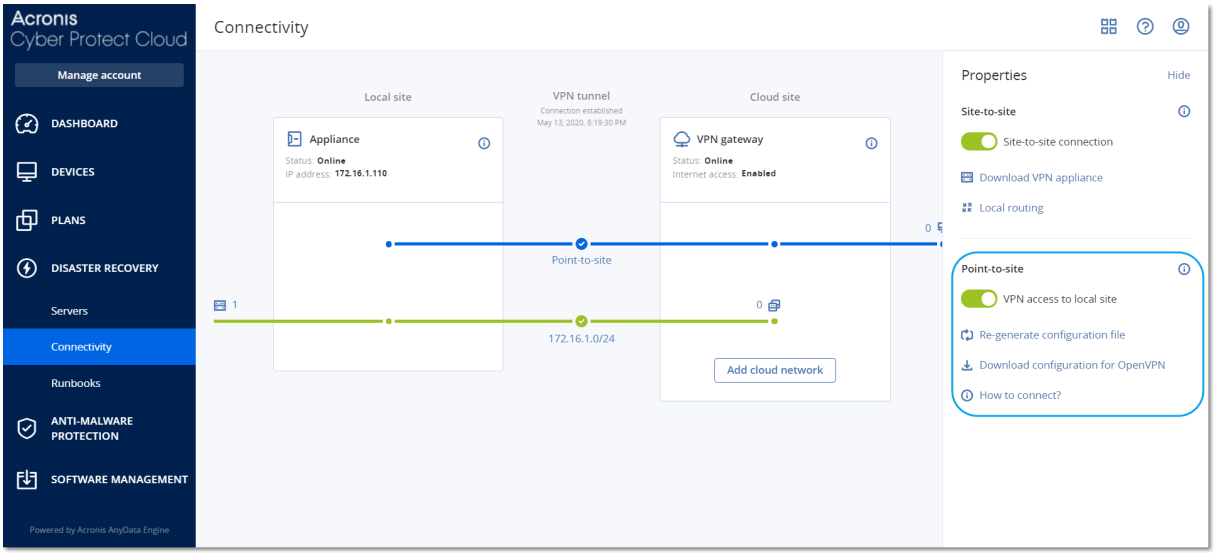
重要事项
如果已为帐户启用双重身份验证，您需要重新生成配置文件，并为现有 OpenVPN 客户端续订它。用户必须重新登录到 Cyber Protect Cloud，才能为其帐户设置双重身份验证。

因此，您将能够连接到本地站点上的计算机。

管理点到站点连接设置

注意
此功能的可用性取决于为您的帐户启用的服务配额。

在 Cyber Protect 中控台中，转到**灾难恢复** > **连接**，然后单击右下角的**显示属性**。



对本地站点进行 VPN 访问

此选项用于管理对本地站点进行 VPN 访问。默认情况下，该选项处于启用状态。如果该选项处于禁用状态，将不允许对本地站点进行点到站点访问。

下载 OpenVPN 的配置

此操作将下载 OpenVPN 客户端的配置文件。需要此文件才能建立与云站点的点到站点连接。

重新生成配置

可以为 OpenVPN 客户端重新生成配置文件。

需要在以下情况下执行此操作：

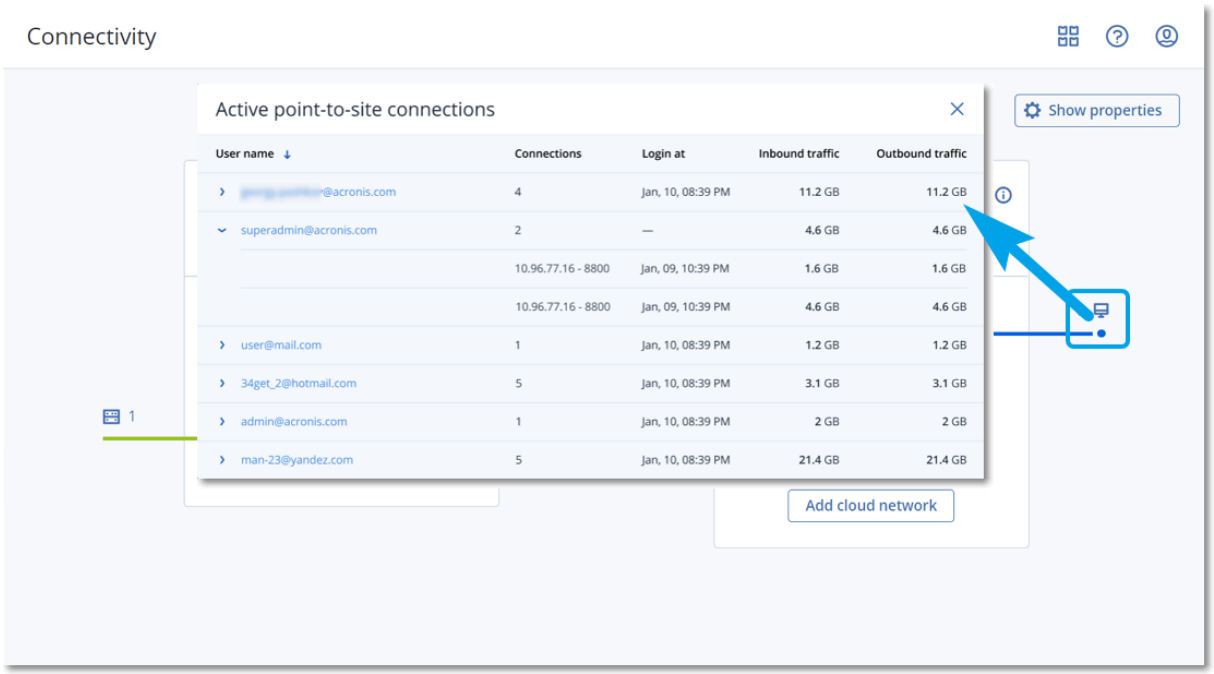
- 如果您怀疑配置文件已泄露。
- 如果已为您的帐户启用了双重身份验证。

在配置文件更新后，即无法通过旧配置文件进行连接。确保将新文件分发给允许其使用点到站点连接的用户。

活动的点到站点连接

注意
此功能的可用性取决于为您的帐户启用的服务配额。

可以在**灾难恢复** > **连接**中查看所有活动的点到站点连接。单击蓝色**点到站点**行上的计算机图标，您将看到有关按用户名分组的活动点到站点连接的详细信息。



Active Directory 域服务可用性的建议

如果您的受保护工作负载需要在域控制器中进行身份验证，建议您在灾难恢复站点上拥有一个 Active Directory 域控制器 (AD DC) 实例。

用于 L2 Open VPN 连接的 Active Directory 域控制器

使用 L2 Open VPN 连接时，在测试故障转移或生产故障转移期间，受保护工作负载的 IP 地址将保留在云站点中。因此，在测试故障转移或生产故障转移期间，AD DC 具有与本地站点相同的 IP 地址。

使用自定义 DNS 时，可以为所有云服务器设置自己的自定义 DNS 服务器。有关详细信息，请参阅 "配置自定义 DNS 服务器"(第 689 页)。

用于 L3 IPsec VPN 连接的 Active Directory 域控制器

使用 L3 IPsec VPN 连接时，受保护工作负载的 IP 地址将不会保留在云站点中。因此，建议您在执行生产故障转移之前，将一个额外的专用 AD DC 实例作为云站点中的主服务器。

对配置为云站点中主服务器的专用 AD DC 实例的建议如下所述：

- 关闭 Windows 防火墙。
- 将主服务器加入 Active Directory 服务。
- 确保主服务器可以访问 Internet。
- 添加 Active Directory 功能。

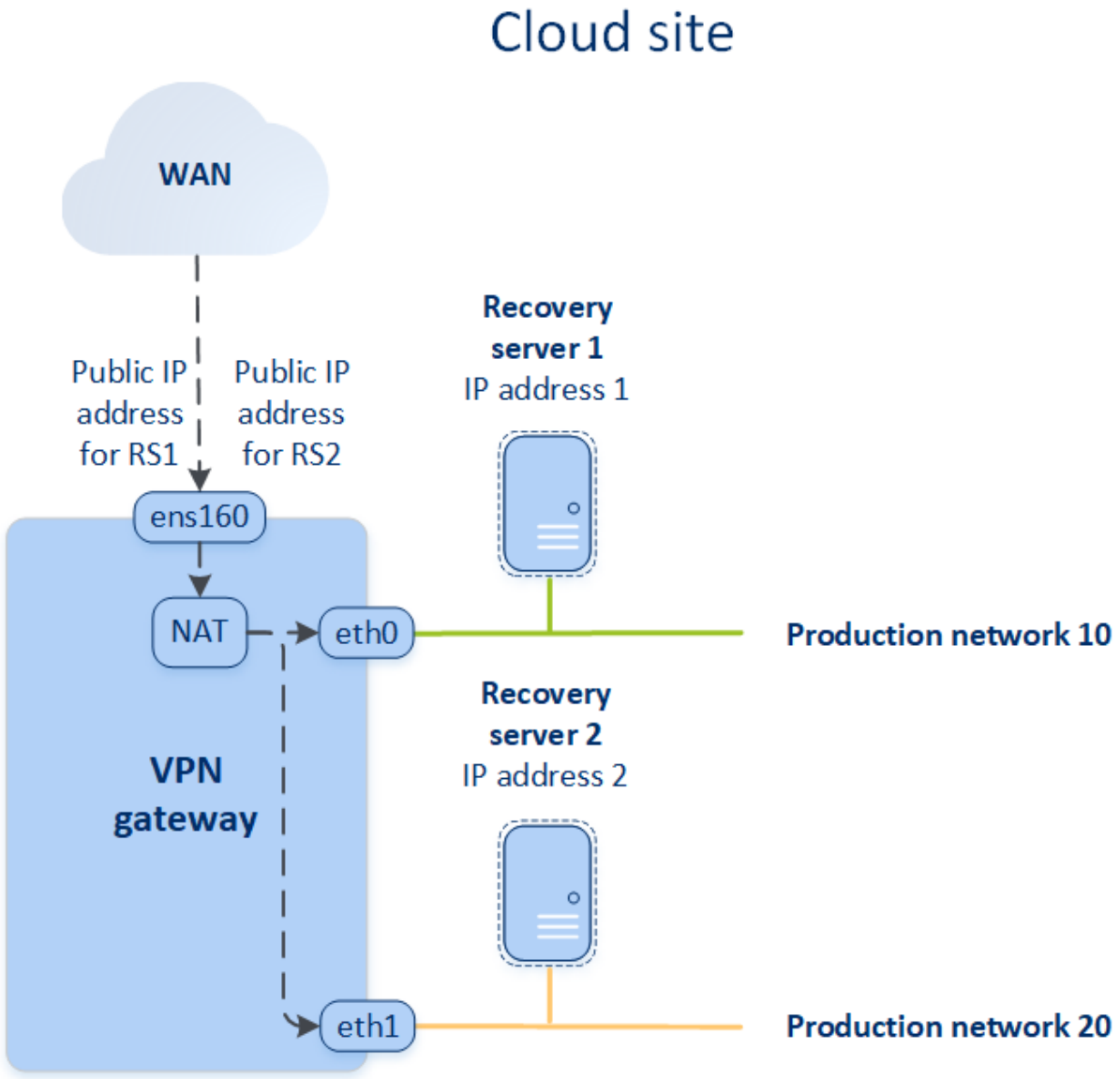
使用自定义 DNS 时，可以为所有云服务器设置自己的自定义 DNS 服务器。有关详细信息，请参阅 "配置自定义 DNS 服务器"(第 689 页)。

网络管理

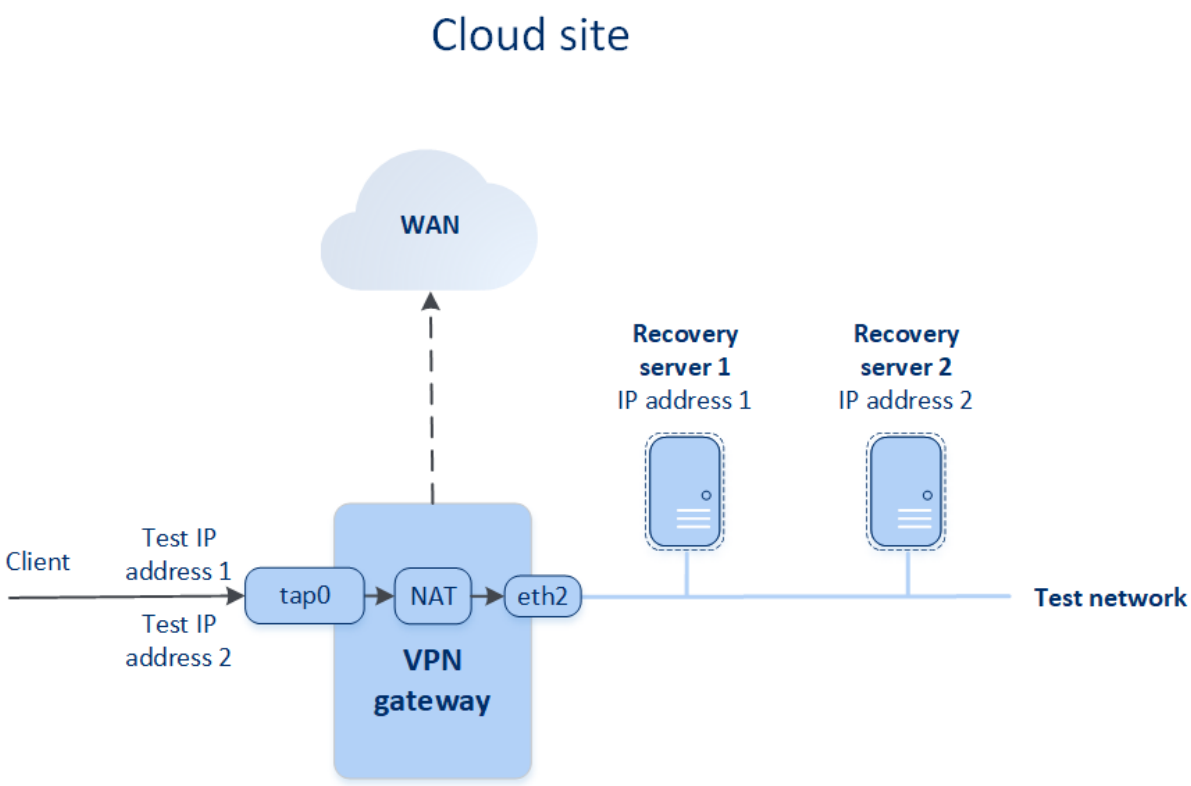
本节介绍网络管理方案。

公共和测试 IP 地址

如果在创建恢复服务器时指派公共 IP 地址，则可从 Internet 通过此 IP 地址访问恢复服务器。当来自 Internet 的数据包具有目标公共 IP 地址时，VPN 网关会使用 NAT 将它重新映射到相应的生产 IP 地址，然后将它发送到对应的恢复服务器。



如果在创建恢复服务器时指派测试 IP 地址，则在测试网络中可通过此 IP 地址访问恢复服务器。执行测试故障转移时，原始计算机仍在运行，同时具有相同 IP 地址的恢复服务器会在云中的测试网络中启动。不会发生 IP 地址冲突，因为测试网络处于隔离状态。测试网络中的恢复服务器可通过其测试 IP 地址进行访问，这些地址通过 NAT 重新映射到生产 IP 地址。



有关站点到站点 Open VPN 的详细信息，请参阅 "站点到站点 Open VPN - 附加信息"(第 1001 页)。

IP 地址重新配置

为了获得适当的灾难恢复性能，指派给本地服务器和云服务器的 IP 地址必须一致。如果 IP 地址存在任何不一致或不匹配，您会在**灾难恢复** > **连接**中相应网络的旁边看到感叹号。

下面列出了 IP 地址不一致的一些常见原因：

1. 恢复服务器从一个网络迁移到另一个网络，或者云网络的网络掩码已更改。结果，云服务器具有来自未与其连接的网络的 IP 地址。
2. 连接类型从不使用站点到站点连接切换到站到站点连接。结果，本地服务器置于的网络与为云站点上的恢复服务器创建的网络不同。
3. 连接类型从“站点到站点 Open VPN”切换到“多站点 IPsec VPN”，或“从多站点 IPsec VPN”切换到“站点到站点 Open VPN”。有关此方案的详细信息，请参阅切换连接、"从多站点 IPsec VPN 切换到站点对站点 Open VPN"(第 678 页) 和重新指派 IP 地址。
4. 在 VPN 设备站点上编辑以下网络参数：
   - 通过网络设置添加接口
   - 通过接口设置手动编辑网络掩码
   - 通过 DHCP 编辑网络掩码
   - 通过接口设置手动编辑网络地址和掩码
   - 通过 DHCP 编辑网络掩码和地址

   以上所列操作的结果，云站点上的网络可能成为本地网络的子集或超集，或者 VPN 设备接口可能会针对不同接口报告相同的网络设置。

解决网络设置存在的问题

1. 单击需要重新配置 IP 地址的网络。
   您会看到所选网络中服务器的列表、其状态和 IP 地址。网络设置不一致的服务器标有感叹号。
2. 要更改服务器的网络设置，请单击**转到服务器**。要一次更改所有服务器的网络设置，请单击通知块中的**更改**。
3. 根据需要更改 IP 地址，方法是在**新 IP** 和**新测试 IP** 字段中定义它们。
4. 准备就绪后，单击**确认**。

将服务器移动到合适的网络

当创建灾难恢复保护计划并将其应用于选定设备时，系统会检查设备的 IP 地址，并在现有云网络中不存在对应的 IP 地址的情况下自动创建云网络。默认情况下，使用 IANA 为专用而建议的最大范围(10.0.0.0/8、172.16.0.0/12、192.168.0.0/16)配置云网络。可以通过编辑网络掩码来缩小网络范围。

如果所选设备位于多个本地网络上，则云站点上的网络可能会成为本地网络的超集。在这种情况下，要重新配置云网络，请执行以下操作：

1. 单击需要重新配置网络大小的云网络，然后单击**编辑**。
2. 使用正确设置重新配置网络大小。
3. 创建需要的其他网络。
4. 单击与网络连接的设备数量旁边的通知图标。
5. 单击**移动到合适的网络**。
6. 选择要移动到合适网络的服务器，然单击**移动**。

重新指派 IP 地址

注意
此功能的可用性取决于为您的帐户启用的服务配额。

在以下情况下，必须重新指派云网络和云服务器的 IP 地址，以便完成配置：

- 从“站点到站点 Open VPN”切换到“多站点 IPsec VPN”，或反之。
- 应用保护计划之后(如果多站点 IPsec VPN 连接已配置)。

云网络

重新指派云网络的 IP 地址

1. 在**连接**选项卡中，单击云网络的 IP 地址。
2. 在**网络**弹出菜单中，单击**编辑**。
3. 键入新的网络地址和网络掩码。
4. 单击**完成**。

重新指派云网络的 IP 地址后，必须重新指派属于重新指派的云网络的云服务器。

云服务器

重新指派服务器的 IP 地址

1. 在**连接**选项卡中，单击云网络中服务器的 IP 地址。
2. 在**服务器**弹出窗口中，单击**更改 IP 地址**。
3. 在**更改 IP 地址**弹出窗口中，键入服务器的新 IP 地址，或者使用自动生成的 IP 地址，它属于重新指派的云网络一部分。

   注意
   在重新指派网络 IP 地址之前，Cyber Disaster Recovery Cloud 为所有属于云网络一部分的云服务器从云网络中自动指派 IP 地址。可以使用建议的 IP 地址立即重新指派所有云服务器的 IP 地址。

4. 单击**确认**。

重新安装 VPN 网关

如果 VPN 网关存在无法解决的问题，您可能想要重新安装 VPN 网关。可能的问题包括：

- VPN 网关处于**错误**状态下。
- VPN 网关长时间处于**待处理**状态下。
- VPN 网关状态长时间未确定。

重新安装 VPN 网关过程包括以下自动操作：完全删除现有 VPN 网关虚拟机、从模板安装新虚拟机，以及在新虚拟机上应用之前 VPN 网关的设置。

先决条件：

必须设置与云站点的一种连接类型。

重新安装 VPN 网关

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **连接**。
2. 单击 VPN 网关的齿轮图标，然后选择**重新安装 VPN 网关**。
3. 在**重新安装 VPN 网关**对话框中，输入您的登录名。
4. 单击**重新安装**。

配置自定义 DNS 服务器

注意
此功能的可用性取决于为您的帐户启用的服务配额。

当配置连接时，Cyber Disaster Recovery Cloud 会创建云网络基础架构。云 DHCP 服务器会自动将默认 DNS 服务器指派给恢复服务器和主服务器，但您可以更改默认设置并配置自定义 DNS 服务器。新的 DNS 设置将在下次向 DHCP 服务器发出请求时应用。

先决条件

必须设置与云站点的一种连接类型。

配置自定义 DNS 服务器

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **连接**。
2. 单击**显示属性**。
3. 单击**默认(由云站点提供)**。
4. 选择**自定义服务器**。
5. 键入 DNS 服务器的 IP 地址。
6. [可选] 如果要添加另一个 DNS 服务器，请单击**添加**，然后键入该 DNS 服务器的 IP 地址。

   注意
   在添加自定义 DNS 服务器，还可以添加默认 DNS 服务器。这样，如果自定义 DNS 服务器不可用，Cyber Disaster Recovery Cloud 将使用默认 DNS 服务器。

7. 单击**完成**。

删除自定义 DNS 服务器

注意
此功能的可用性取决于为您的帐户启用的服务配额。

可以从自定义 DNS 列表中删除 DNS 服务器。

先决条件：

自定义 DNS 服务器已配置。

删除自定义 DNS 服务器

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **连接**。
2. 单击**显示属性**。
3. 单击**自定义服务器**。
4. 单击 DNS 服务器旁边的删除图标。

   注意
   当只有一个自定义 DNS 服务器可用时，删除操作处于禁用状态。如果要删除所有自定义 DNS 服务器，选择**默认(由云站点提供)**。

5. 单击**完成**。

配置本地路由

除了通过 VPN 设备扩展到云的本地网络之外，您可能还有其他未在 VPN 设备中注册的本地网络，但其中的服务器需要与云服务器通信。要在此类本地服务器和云服务器之间建立连接，您需要配置本地路由设置。

配置本地路由

1. 转到**灾难恢复** > **连接**。
2. 单击**显示属性**，然后单击**本地路由**。
3. 采用 CIDR 表示法指定本地网络。
4. 单击**保存**。

结果，指定本地网络中的服务器可以与云服务器通信。

下载 MAC 地址

可以下载 MAC 地址列表，然后提取它们并将其导入到自定义 DHCP 服务器的配置中。

先决条件：

- 必须设置与云站点的一种连接类型。
- 必须配置至少一个具有 MAC 地址的主服务器或恢复服务器。

下载 MAC 地址列表

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **连接**。
2. 单击**显示属性**。
3. 单击**下载 MAC 地址列表**，然后保存 CSV 文件。

使用日志

灾难恢复收集 VPN 设备和 VPN 网关的日志。日志保存为 .txt 文件，这些文件压缩在 .zip 存档中。可以下载并提取该存档，并将其中的信息用于故障排除或监视目的。

以下列表描述了作为 .zip 存档一部分的日志文件及其包含的信息。

`dnsmasq.config.txt` - 该文件包含有关提供 DNS 和 DHCP 地址的服务的配置信息。

`dnsmasq.leases.txt` - 该文件包含有关当前 DHCP 地址租约的信息。

`dnsmasq_log.txt` - 该文件包含 dnsmasq 服务的日志。

`ebtables.txt` - 该文件包含有关防火墙表的信息。

`free.txt` - 该文件包含有关可用内存的信息。

`ip.txt` - 该文件包含来自网络接口配置的日志，包括可用于配置**捕获网络数据包**设置的名称。

`NetworkManager_log.txt` - 该文件包含来自 NetworkManager 服务的日志。

`NetworkManager_status.txt` - 该文件包含有关 NetworkManager 服务状态的信息。

`openvpn@p2s_log.txt` - 该文件包含来自 OpenVPN 服务的日志。

`openvpn@p2s_status.txt` - 该文件包含有关 VPN 隧道状态的信息。

`ps.txt` - 该文件包含有关 VPN 网关或 VPN 设备上当前正在运行的进程的信息。

`resolf.conf.txt` - 该文件包含有关 DNS 服务器配置的信息。

`routes.txt` - 该文件包含有关网络路由的信息。

`uname.txt` - 该文件包含有关操作系统内核当前版本的信息。

`uptime.txt` - 该文件包含有关操作系统尚未重新启动的时长信息。

`vpnserver_log.txt` - 该文件包含来自 VPN 服务的日志。

`vpnserver_status.txt` - 该文件包含有关 VPN 服务器状态的信息。

有关特定于 IPsec VPN 连接的日志文件的详细信息，请参阅 "多站点 IPSec VPN 日志文件"(第 681 页)。

下载 VPN 设备的日志

可以下载并提取包含 VPN 设备日志的存档，并将这些信息用于故障排除或监视目的。

下载 VPN 设备的日志

1. 在**连接**页面上，单击 VPN 设备旁边的齿轮图标。
2. 单击**下载日志**。
3. [可选] 选择**捕获网络数据包**，然后配置设置。有关详细信息，请参阅 "捕获网络数据包"(第 692 页)。
4. 单击**完成**。
5. 当 .zip 存档可供下载时，单击**下载日志**，然后将其保存在本地。

下载 VPN 网关的日志

可以下载并提取包含 VPN 网关日志的存档，并将这些信息用于故障排除或监视目的。

下载 VPN 网关的日志

1. 在**连接**页面上，单击 VPN 网关旁边的齿轮图标。
2. 单击**下载日志**。
3. [可选] 选择**捕获网络数据包**，然后配置设置。有关详细信息，请参阅 "捕获网络数据包"(第 692 页)。
4. 单击**完成**。
5. 当 .zip 存档可供下载时，单击**下载日志**，然后将其保存在本地。

捕获网络数据包

要对本地生产站点与主服务器或恢复服务器之间的通信进行故障排除和分析，可以选择收集 VPN 网关或 VPN 设备上的网络数据包。

在收集到 32,000 个网络数据包或达到时间限制后，会停止捕获网络数据包，并将结果写入一个 .libpcap 文件，该文件将添加到日志 .zip 存档中。

下表提供了有关可以配置的**捕获网络数据包**设置的更多信息。

设置	描述
网络接口	捕获其网络数据包的网络接口。如果要捕获所有网络接口上的网络数据包，请选择**任何**。

设置	描述
名称	
时间限制(秒)	捕获网络数据包的时间限制。可以设置的最大值为 1800。
过滤	应用于捕获的网络数据包的额外过滤器。 可以输入包含协议、端口、方向及其组合的字符串，以空格分隔，例如：“and”、“or”、“not”、“(”、“)”、“src”、“dst”、“net”、“host”、“port”、“ip”、“tcp”、“udp”、“icmp”、“arp”、“esp”。 如果要使用括号，请用空格将它们括起来。还可以输入 IP 地址和网络地址，例如：“icmp or arp”和“port 67 or 68”。 有关可以输入的值的详细信息，请参阅 Linux tpcdump 帮助。

云服务器

使用“灾难恢复”，您可以使用两种类型的云服务器：主服务器和恢复服务器。

主服务器是一个未与本地站点上的计算机关联的虚拟机。您可以使用主服务器来保护特定应用程序或运行各种辅助服务(如 Web 服务器)。

恢复服务器是原始计算机(受保护服务器)的副本。恢复服务器基于存储在云中的受保护服务器备份。发生灾难时，将使用恢复服务器将工作负载从原始服务器切换到恢复服务器。

配置恢复服务器

恢复服务器 - 原始计算机的副本，基于存储在云中受保护的服务器备份。恢复服务器用于在发生灾难时切换原始服务器的工作负载。

创建恢复服务器时，必须指定以下网络参数：

参数	描述
云网络	(必选)恢复服务器将连接到的云网络。
生产网络中的 IP 地址	(必选)用于启动恢复服务器的虚拟机的 IP 地址。该地址用于生产网络和测试网络。在启动之前，虚拟机配置为通过 DHCP 获取 IP 地址。
测试 IP 地址	(可选)：在测试故障转移期间，用于从客户端-生产网络访问恢复服务器的 IP 地址，以防止生产 IP 地址在同一网络中重复出现。此 IP 地址与生产网络中的 IP 地址不同。本地站点中的服务器可以在测试故障转移期间通过测试 IP 地址访问恢复服务器，但反向访问不可行。如果在创建恢复服务器期间选择了 **Internet 访问**选项，则可以从测试网络中的恢复服务器访问 Internet。

参数	描述
公共 IP 地址	(可选)用于从 Internet 访问恢复服务器的 IP 地址。如果服务器没有公共 IP 地址,则只能从本地网络访问它。
Internet 访问	(可选)它允许恢复服务器访问 Internet(在生产和测试故障转移情况下)。

创建恢复服务器

要创建将作为工作负载副本的恢复服务器,请按照下面的步骤操作。您还可以观看演示该过程的视频教程。

重要事项
执行故障转移时,只能选择在创建恢复服务器后创建的恢复点。

先决条件

- 必须将保护计划应用于要保护的原始计算机。此计划必须将整个计算机或仅磁盘(需要启动和提供必要服务)备份到云存储。
- 必须设置与云站点的一种连接类型。

创建恢复服务器的步骤

1. 在**所有设备**选项卡上,选择要保护的计算机。
2. 单击**灾难恢复**,然后单击**创建恢复服务器**。
3. 在**创建恢复服务器**向导中的**服务器配置**选项卡上,执行以下操作:
   a. 选择虚拟核心的数量和 RAM 的大小。

      注意
      可以查看每个选项的计算点。计算点的数量反映每小时运行恢复服务器的成本。有关详细信息,请参阅 "计算点"(第 705 页)。

   b. [可选]更改恢复服务器的默认名称。
   c. [可选]添加说明。
4. 在**网络**选项卡上,执行以下操作:
   a. 指定服务器将连接到的云网络。
   b. 选择 **DHCP** 选项。

DHCP 选项	描述
由云站点提供	这是默认设置。服务器的 IP 地址将由云中自动配置的 DHCP 服务器提供。
自定义	服务器的 IP 地址将由云中您自己的 DHCP 服务器提供。

   c. 指定 **MAC 地址**。

MAC 地址是指派给服务器的网络适配器的唯一标识符。如果使用自定义 DHCP，则可以将其配置为始终将特定 IP 地址指派给特定 MAC 地址。因此，将确保恢复服务器始终获得相同的 IP 地址。可以运行有使用 MAC 地址注册的许可证的应用程序。

d. 指定服务器将在生产网络中拥有的 IP 地址。默认情况下，将设置原始计算机的 IP 地址。

注意

如果使用 DHCP 服务器，请将此 IP 地址添加到服务器排除列表，以避免 IP 地址冲突。

如果使用自定义 DHCP 服务器，则必须在**生产网络中的 IP 地址**中指定与 DHCP 服务器中配置的 IP 地址相同的 IP 地址。否则，测试故障转移将无法正常工作，并且无法通过公共 IP 地址访问服务器。

e. [可选] 选中**测试 IP 地址**复选框，然后指定 IP 地址。

如果选择此设置，则您可以在隔离的测试网络中测试故障转移，以及在测试故障转移期间通过 RDP 或 SSH 连接到恢复服务器。在“测试故障转移”期间下，VPN 网关会使用 NAT 协议将测试 IP 地址替换为生产 IP 地址。

如果您不选择该设置，则中控台将是测试故障转移期间访问服务器的唯一途径。

注意

如果使用 DHCP 服务器，请将此 IP 地址添加到服务器排除列表，以避免 IP 地址冲突。

可以选择其中一个建议的 IP 地址，或输入其他 IP 地址。

f. [可选] 选择 **Internet 访问**复选框。

如果选择此选项，恢复服务器能够在生产或测试故障转移期间访问 Internet。默认情况下，TCP 端口 25 处于打开状态，用于与公用 IP 地址的出站连接。

g. [可选] 选中**使用公共 IP 地址**复选框。

使用公共 IP 地址，恢复服务器将可在故障转移或测试故障转移期间从 Internet 进行访问。如果不选择此选项，则服务器仅可在生产网络中使用。

使用公共 IP 地址选项需要选择 **Internet 访问**选项。

公共 IP 地址将在配置完成后显示。默认情况下，TCP 端口 443 处于打开状态，用于与公用 IP 地址的入站连接。

注意

如果取消选中**使用公共 IP 地址**复选框或删除恢复服务器，则不会保留其公共 IP 地址。

5. 在 **设置** 选项卡上，选择 **设置 RPO 阈值**，然后设置该值。

RPO 阈值定义故障转移的上一个合适恢复点与当前时间之间的最大时间间隔。该值可以设置的范围为 15 – 60 分钟，1 – 24 小时，1 – 14 天。

6. [可选] [如果所选计算机的备份已使用加密作为计算机属性进行加密]，指定从加密备份为恢复服务器创建虚拟机时将自动使用的密码。

a. 单击**输入密码**，然后输入加密备份的密码，并定义凭据的名称。

默认情况下，您会在列表中看到最新备份。

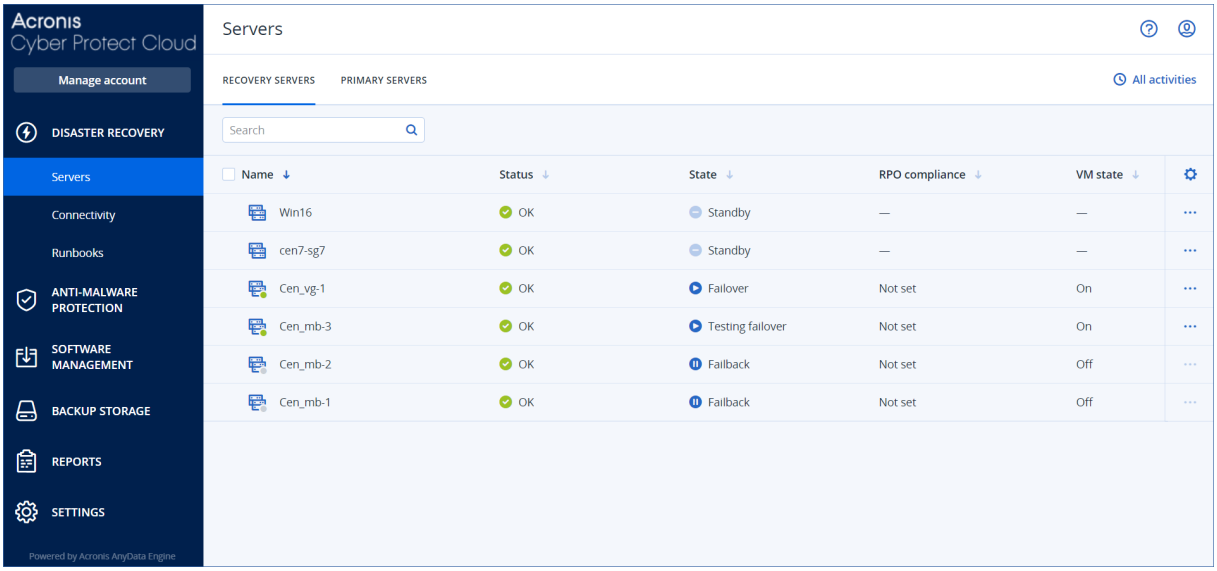
b. 要查看所有备份，请选择**显示所有备份**。

c. 单击**保存**。

注意
尽管您指定的密码将存储在安全凭据存储中，但保存密码可能违反您的合规义务。

7. 单击**云防火墙规则**选项卡以编辑默认防火墙规则。有关详细信息，请参阅 "设置云服务器的防火墙规则"(第 703 页)。
8. 单击**创建**。

恢复服务器将显示在 中控台的**灾难恢复** > **服务器** > **恢复服务器**选项卡中。



可对恢复服务器执行的操作

在 Cyber Protect 中控台中，主服务器显示在 **灾难恢复** > **服务器** > **恢复服务器**选项卡中。

接通电源

若要启动恢复服务器

1. 在**恢复服务器**选项卡中，单击恢复服务器。
2. 单击**开机**。

关闭电源

若要关闭恢复服务器

1. 在**恢复服务器**选项卡中，单击恢复服务器。
2. 单击**关闭电源**。
3. 在**关闭服务器**屏幕上，单击**关闭**。

强制关闭电源

若要强制关闭恢复服务器

1. 在**恢复服务器**选项卡中，单击恢复服务器。
2. 单击**关闭电源**。

3. 在**关闭服务器**屏幕，选择**强制关闭服务器**，然后单击**关闭电源**。

停止

若要停止恢复服务器

1. 在**恢复服务器**选项卡中，单击恢复服务器。
2. 单击**停止**。

编辑设置

若要编辑恢复服务器的设置

1. 在**恢复服务器**选项卡中，单击恢复服务器。
2. 单击**停止**。
3. 单击**编辑**，然后编辑设置。

应用保护计划

若要将计划应用于组

1. 在**主服务器**选项卡上，单击主服务器。
2. 在**计划**选项卡上，单击**创建**。
   您将看到一个预定义的保护计划，您在其中只能更改预定和保留规则。有关详细信息，请参阅"备份云服务器"。

配置主服务器

主服务器是在本地站点上没有链接计算机的虚拟机(与恢复服务器相比)。主服务器用于通过复制保护应用程序，或运行各种辅助服务(如 Web 服务器)。

通常，主服务器用于在运行关键应用程序的服务器之间进行实时数据复制。可以使用应用程序的原生工具自行设置复制。例如，可以在本地服务器和主服务器之间配置 Active Directory 复制或 SQL 复制。

或者，主服务器可以包含在 AlwaysOn 可用性组 (AAG) 或数据库可用性组 (DAG) 中。

两种方法都需要对应用程序及其管理员权限有深入了解。主服务器不断消耗快速灾难恢复存储上的计算资源和空间。需要您这一方对其进行维护：监控复制、安装软件更新以及备份。优点是最小的 RPO 和 RTO，生产环境上的负载最小(与将整个服务器备份到云相比)。

主服务器始终仅在生产网络中启动，并具有以下网络参数：

参数	描述
云网络	(必选) 主服务器将连接到的云网络。
生产网络中的 IP 地址	(必选) 主服务器将在生产网络中拥有的 IP 地址。默认情况下，将设置生产网络中的第一个可用 IP 地址。
公共 IP 地址	(可选) 用于从 Internet 访问主服务器的 IP 地址。如果服务器没有公共 IP 地址，则只能从本地网络(无法通过 Internet) 访问它。

参数	描述
Internet 访问	(可选) 允许主服务器访问 Internet。

创建主服务器

先决条件

- 必须设置与云站点的一种连接类型。

创建主服务器的步骤

1. 转到**Disaster Recovery** > **服务器** > **主服务器**选项卡。
2. 单击**创建**。
3. 在**创建主服务器**向导中的**服务器配置**选项卡上，执行以下操作：
   a. 为新虚拟机选择一个模板。
   b. 选择配置的规格(虚拟核心的数量和 RAM 的大小)。
      下表显示了每个规则的最大磁盘空间总量 (GB)。

类型	vCPU	RAM (GB)	最大磁盘空间总量 (GB)
F1	1	2	500
F2	1	4	1,000
F3	2	8	2,000
F4	4	16	4,000
F5	8	32	8,000
F6	16	64	16,000
F7	16	128	32,000
F8	16	256	64,000

   c. [可选] 更改虚拟磁盘大小。如果需要多个硬盘，请单击**添加磁盘**，然后指定新磁盘大小。你可以为一个主服务器添加最多 10 个磁盘。
   d. 更改恢复服务器的默认名称。
   e. 添加说明。
4. 在**网络**选项卡上，执行以下操作：
   a. 指定将包含主服务器的云网络。
   b. 选择 **DHCP** 选项。

DHCP 选项	描述
由云站点提供	这是默认设置。服务器的 IP 地址将由云中自动配置的 DHCP 服务器提供。
自定义	服务器的 IP 地址将由云中您自己的 DHCP 服务器提供。

c. 指定 **MAC 地址**。

MAC 地址是指派给服务器的网络适配器的唯一标识符。如果使用自定义 DHCP，则可以将其配置为始终将特定 IP 地址指派给特定 MAC 地址。这会确保主服务器始终获得相同的 IP 地址。可以运行有使用 MAC 地址注册的许可证的应用程序。

d. 指定服务器将在生产网络中拥有的 IP 地址。

默认情况下，将设置生产网络中的第一个可用 IP 地址。

注意

如果使用 DHCP 服务器，请将此 IP 地址添加到服务器排除列表，以避免 IP 地址冲突。

如果使用自定义 DHCP 服务器，则必须在**生产网络中的 IP 地址**中指定与 DHCP 服务器中配置的 IP 地址相同的 IP 地址。否则，测试故障转移将无法正常工作，并且无法通过公共 IP 地址访问服务器。

e. [可选] 选中 **Internet 访问**复选框。

如果选择此选项，则主服务器能够访问 Internet。默认情况下，TCP 端口 25 处于打开状态，用于与公用 IP 地址的出站连接。

f. [可选] 选中**使用公共 IP 地址**复选框。

使用公共 IP 地址，主服务器将可从 Internet 进行访问。如果不选择此设置，则服务器仅可在生产网络中使用。

公共 IP 地址将在配置完成后显示。默认情况下，TCP 端口 443 处于打开状态，用于与公用 IP 地址的入站连接。

注意

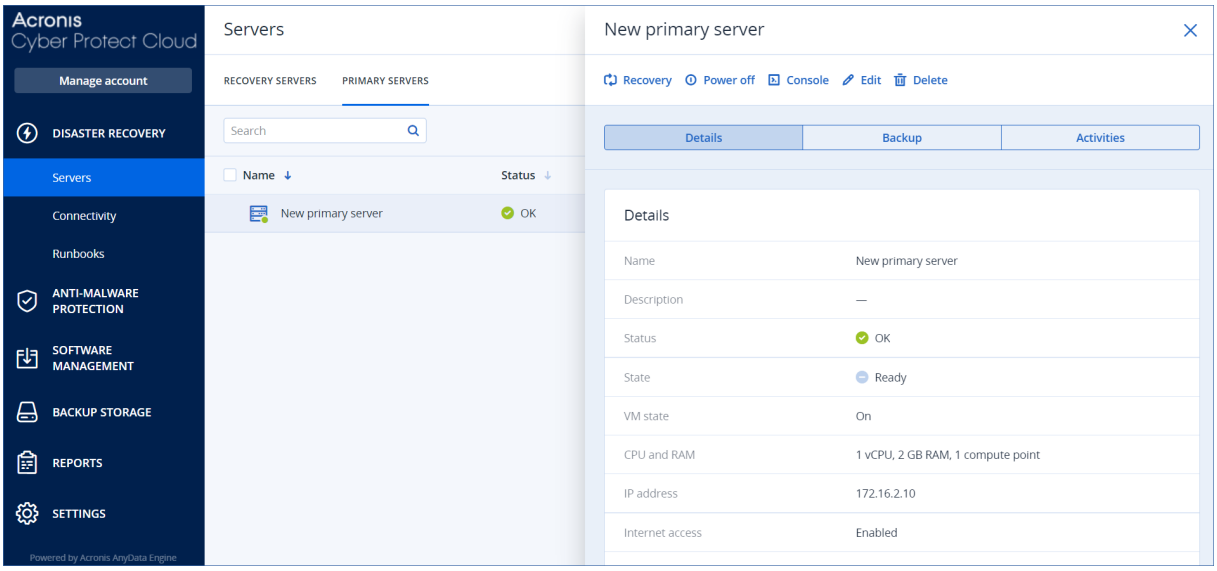
如果取消选中**使用公共 IP 地址**复选框或删除恢复服务器，则不会保留其公共 IP 地址。

5. [可选] 在 **设置** 选项卡上，选择 **设置 RPO 阈值**，然后设置该值。

RPO 阈值会定义上一个恢复点与当前时间之间的最大时间间隔。该值可以设置的范围为 15 – 60 分钟，1 – 24 小时，1 – 14 天。

6. [可选] 单击**云防火墙规则**选项卡以编辑默认防火墙规则。有关详细信息，请参阅 "设置云服务器的防火墙规则"(第 703 页)。
7. 单击**创建**。

主服务器将在生产网络中可用。可以通过使用服务器的中控台、RDP、SSH 或 TeamViewer 来管理服务器。



使用主服务器的操作

在 Cyber Protect 中控台中，主服务器显示在 **灾难恢复** > **服务器** > **主服务器**选项卡中。

接通电源

若要开启主服务器

1. 在**主服务器**选项卡上，单击主服务器。
2. 单击**开机**。

关闭电源

若要关闭主服务器

1. 在**主服务器**选项卡上，单击主服务器。
2. 单击**关闭电源**。
3. 在**关闭服务器**屏幕上，单击**关闭**。

强制关闭电源

若要强制关闭主服务器

1. 在**主服务器**选项卡上，单击主服务器。
2. 单击**关闭电源**。
3. 在**关闭服务器**屏幕，选择**强制关闭服务器**，然后单击**关闭电源**。

停止

若要停止主服务器

1. 在**主服务器**选项卡上，单击主服务器。
2. 单击**停止**。

编辑设置

若要编辑主服务器的设置

1. 在**主服务器**选项卡上，单击主服务器。
2. 单击**停止**。
3. 单击**编辑**，然后编辑设置。

应用保护计划

若要将计划应用于组

1. 在**主服务器**选项卡上，单击主服务器。
2. 在**计划**选项卡上，单击**创建**。
   您将看到一个预定义的保护计划，您在其中只能更改预定和保留规则。有关详细信息，请参阅"备份云服务器"。

查看有关云服务器的详细信息

若要查看云服务器详细信息，请转到**灾难恢复 > 服务器**。有以下两个选项卡：**恢复服务器**和**主服务器**。要在表中显示所有可选列，请单击齿轮图标。

通过选择每个云服务器，即可找到该云服务器的以下相关信息。

列名称	描述
名称	由您定义的云服务器名称
状态	反映云服务器最严重问题的状态(基于活动警告)
状态	云服务器状态
VM 状态	与云服务器关联的虚拟机的电源状态
活动位置	托管云服务器的位置。例如，**云**。
RPO 阈值	故障转移的上一个合适恢复点与当前时间之间允许的最大时间间隔。该值可以设置的范围为 15 – 60 分钟，1 – 24 小时，1 – 14 天。
RPO 合规性	RPO 合规性是实际 RPO 与 RPO 阈值之间的比率。如果定义了 RPO 阈值，则会显示 RPO 合规性。 计算方法如下所示： **RPO 合规性 = 实际 RPO / RPO 阈值** 其中： **实际 RPO = 当前时间 – 上次恢复点时间** **RPO 合规性状态** 根据实际 RPO 与 RPO 阈值之间的比率值，使用的状态如下所示： • **合规**。RPO 合规性 < 1x。服务器满足 RPO 阈值。 • **超出**。RPO 合规性 <= 2x。服务器违反 RPO 阈值。

	• **严重超出**。RPO 合规性 <= 4x。服务器违反 RPO 阈值超过 2 倍。 • **极其严重超出**。RPO 合规性 > 4x。服务器违反 RPO 阈值超过 4 倍。 • **待处理(无备份)**。该服务器受保护计划保护，但备份正在创建中，尚未完成。
实际 RPO	自上次创建恢复点以来经过的时间
上次恢复点	上次创建恢复点的日期和时间

云服务器的备份

主服务器和恢复服务器会在云站点上进行无代理程序备份。这些备份有以下限制。

- 唯一可能的备份位置是云存储。主服务器将备份到**主服务器备份**存储。

  注意
  不支持 Microsoft Azure 备份位置。

- 备份计划无法应用于多个服务器。每个服务器必须具有自己的备份计划，即使所有备份计划设置都相同。
- 一个服务器只能应用一个备份计划。
- 不支持应用程序感知备份。
- 加密不可用。
- 备份选项不可用。

删除主服务器时，也会删除其备份。

仅在故障转移状态下备份恢复服务器。其备份继续原始服务器的备份序列。执行故障恢复时，原始服务器可以继续此备份序列。因此，恢复服务器的备份只能手动删除，或作为应用保留规则的结果。删除恢复服务器后，其备份将始终保留。

注意
云服务器的备份计划会根据 UTC 时间执行。

云服务器的防火墙规则

可以配置防火墙规则，来控制云站点上主服务器和恢复服务器的入站和出站流量。

在为云服务器调配公共 IP 地址之后，即可配置入站规则。默认情况下，允许使用 TCP 端口 443，并且拒绝所有其他入站连接。可以更改默认防火墙规则，并添加或删除入站例外。如果未调配公共 IP，则只能查看入站规则，而不能对其进行配置。

在为云服务器调配 Internet 访问之后，即可配置出站规则。默认情况下，拒绝使用 TCP 端口 25，并且允许所有其他出站连接。可以更改默认防火墙规则，并添加或删除出站例外。如果未调配 Internet 访问，则只能查看出站规则，而不能对其进行配置。

注意
出于安全原因，存在无法更改的预定义防火墙规则。

对于入站和出站连接：

- 允许 ping：ICMP echo-request (type 8, code 0) 和 ICMP echo-reply (type 0, code 0)
- Permit ICMP need-to-frag (type 3, code 4)
- Permit TTL exceeded (type 11, code 0)

仅限入站连接：

- 不可配置的部分：全部拒绝

仅限出站连接：

- 不可配置的部分：全部拒绝

设置云服务器的防火墙规则

可以编辑云中主服务器和恢复服务器的默认防火墙规则。

编辑云站点上服务器的防火墙规则

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **服务器**。
2. 如果要编辑恢复服务器的防火墙规则，请单击**恢复服务器**选项卡。或者，如果要编辑主服务器的防火墙规则，请单击**主服务器**选项卡。
3. 单击相应服务器，然后单击**编辑**。
4. 单击**云防火墙规则**选项卡。
5. 如果要更改入站连接的默认操作，请执行以下操作：
   a. 在**入站**下拉字段中，选择默认操作。

操作	描述
全部拒绝	拒绝任何入站流量。 可以添加例外，并允许来自特定 IP 地址、协议和端口的流量。
全部允许	允许所有入站 TCP 和 UDP 流量。 可以添加例外，并拒绝来自特定 IP 地址、协议和端口的流量。

   注意
   更改默认操作会使现有入站规则的配置无效并删除该配置。

   b. [可选] 如果要保存现有例外，请在确认窗口中选择**保存填充的例外**。
   c. 单击**确认**。
6. 如果要添加例外：
   a. 单击**添加例外**。
   b. 指定防火墙参数。

防火墙参数	描述
协议	选择连接协议。支持以下选项： • **TCP** • **UDP** • **TCP+UDP**
服务器端口	选择将应用规则的端口。可以指定以下内容： • 特定端口号（例如，2298） • 端口号范围（例如，6000-6700） • 任何端口号。如果要将规则应用于任何端口号，请使用 *。
客户端 IP 地址	选择将应用规则的 IP 地址。可以指定以下内容： • 特定 IP 地址（例如，192.168.0.0） • 使用 CIDR 表示法的 IP 地址范围（例如，192.168.0.0/24） • 任何 IP 地址。如果要将规则应用于任何 IP 地址，请使用 *。

7. 如果要删除现有入站例外，请单击其旁边的回收站图标。
8. 如果要更改出站连接的默认操作，请执行以下操作：
   a. 在**出站**下拉字段中，选择默认操作。

操作	描述
全部拒绝	拒绝任何出站流量。 可以添加例外，并允许流量流向特定的 IP 地址、协议和端口。
全部允许	允许所有出站流量。 可以添加例外，并拒绝来自特定 IP 地址、协议和端口的流量。

注意
更改默认操作会使现有出站规则的配置无效并删除该配置。

   b. [可选] 如果要保存现有例外，请在确认窗口中选择**保存填充的例外**。
   c. 单击**确认**。
9. 如果要添加例外：
   a. 单击**添加例外**。
   b. 指定防火墙参数。

防火墙参数	描述
协议	选择连接协议。支持以下选项： • **TCP** • **UDP** • **TCP+UDP**
服务器端口	选择将应用规则的端口。可以指定以下内容： • 特定端口号（例如，2298）

防火墙参数	描述
	• 端口号范围(例如,6000-6700) • 任何端口号。如果要将规则应用于任何端口号,请使用 *。
客户端 IP 地址	选择将应用规则的 IP 地址。可以指定以下内容: • 特定 IP 地址(例如,192.168.0.0) • 使用 CIDR 表示法的 IP 地址范围(例如,192.168.0.0/24) • 任何 IP 地址。如果要将规则应用于任何 IP 地址,请使用 *。

10. 如果要删除现有出站例外,请单击其旁边的回收站图标。
11. 单击**保存**。

检查云防火墙活动

在更新云服务器的防火墙规则的配置后,即会在 Cyber Protect 中控台中提供更新活动的日志。可以查看该日志并检查以下信息:

- 更新配置的用户的用户名
- 更新的日期和时间
- 入站和出站连接的防火墙设置
- 入站和出站连接的默认操作
- 入站和出站连接的例外的协议、端口和 IP 地址

查看有关云防火墙规则配置更改的详细信息

1. 在 Cyber Protect 中控台中,依次单击**监视** > **活动**。
2. 单击相应活动,然后单击**所有属性**。
   活动的描述应为**正在更新云服务器配置**。
3. 在**上下文**字段中,检查您感兴趣的信息。

计算点

在Disaster Recovery中,计算点用于测试故障转移和生产故障转移期间的主服务器和恢复服务器。计算点反映了用于在云中运行服务器(虚拟机)的计算资源。

灾难恢复期间消耗的计算点取决于服务器的参数,以及服务器处于故障转移状态下的持续时长。服务器功能越强大,时长越长,将消耗的计算点就越多。消耗的计算点越多,您将支付的金额就越高。

所有正在 安克诺斯 Cloud 中运行的服务器将根据计算点的配置进行收费,无论其状态如何(打开或关闭)。

处于待机状态的恢复服务器不会消耗计算点,也不会产生计算点费用。

在下表中，可以看到云中八台不同类型的服务器的示例，以及它们每小时消耗的相应计算点。可以在**"详细信息"**选项卡中更改服务器类型。

类型	CPU	RAM	计算点
F1	1 vCPU	2 GB	1
F2	1 vCPU	4 GB	2
F3	2 vCPU	8 GB	4
F4	4 vCPU	16 GB	8
F5	8 vCPU	32 GB	16
F6	16 vCPU	64 GB	32
F7	16 vCPU	128 GB	64
F8	16 vCPU	256 GB	128

使用表中的信息，可以轻松估算服务器（虚拟机）将消耗的计算点。

例如，如果要使用Disaster Recovery保护一个 4 vCPU*（共 16 GB RAM）的虚拟机和一个 2 vCPU（共 8 GB RAM）的虚拟机，则第一个虚拟机将每小时消耗 8 个计算点，而第二个虚拟机将每小时消耗 4 个计算点。如果两个虚拟机都处于故障转移状态下，则总消耗量将为每小时 12 个计算点，或一整天 288 个计算点（12 个计算点 x 24 小时 = 288 个计算点）。

*vCPU 指的是指派给虚拟机的物理中央处理单元 (CPU)，是一个时间相关实体。

注意
如果**计算点**配额超额，则所有主服务器和恢复服务器将被关闭。在下一个计费周期开始之前或在您增加配额之前，将无法使用这些服务器。默认计费周期是一个完整的日历月。

测试故障转移

执行测试故障转移是指在与生产网络隔离的测试 VLAN 中启动恢复服务器。可以一次测试多个恢复服务器并检查它们的互动。在测试网络中，服务器使用其生产 IP 地址进行通信，但它们无法发起与本地网络中工作负载的 TCP 或 UDP 连接。

在测试故障转移期间，不会最终确定虚拟机（恢复服务器）。代理程序直接从备份中读取虚拟磁盘的内容，并随机访问备份的不同部分。这可能会使处于测试故障转移状态的恢复服务器的性能低于其正常性能。

执行测试故障转移

尽管执行测试故障转移是可选的，但建议您以自己在成本和安全性方面觉得合适的频率定期执行此过程。最佳做法是创建一个 Runbook - 描述如何在云中启动生产环境的一组说明。

重要事项

必须先创建恢复服务器，才能保护设备免遭灾难的影响。

只能从在创建了设备的恢复服务器后创建的恢复点(备份)执行故障转移。

在故障转移到恢复服务器之前，必须创建至少一个恢复点。支持的最大恢复点数为 100。

执行测试故障转移

1. 选择原始计算机或选择要测试的恢复服务器。
2. 单击**灾难恢复**。

   将打开恢复服务器的描述。
3. 单击**故障转移**。
4. 选择故障转移类型**测试故障转移**。
5. 选择恢复点(备份)，然后单击**启动**。
6. 如果您选择的备份是通过使用加密作为计算机属性进行加密的：
   a. 输入备份集的加密密码。

      注意

      该密码将仅临时保存，将仅用于当前测试故障转移操作。如果测试故障转移停止，或在测试故障转移完成后，该密码会自动从凭据存储中删除。

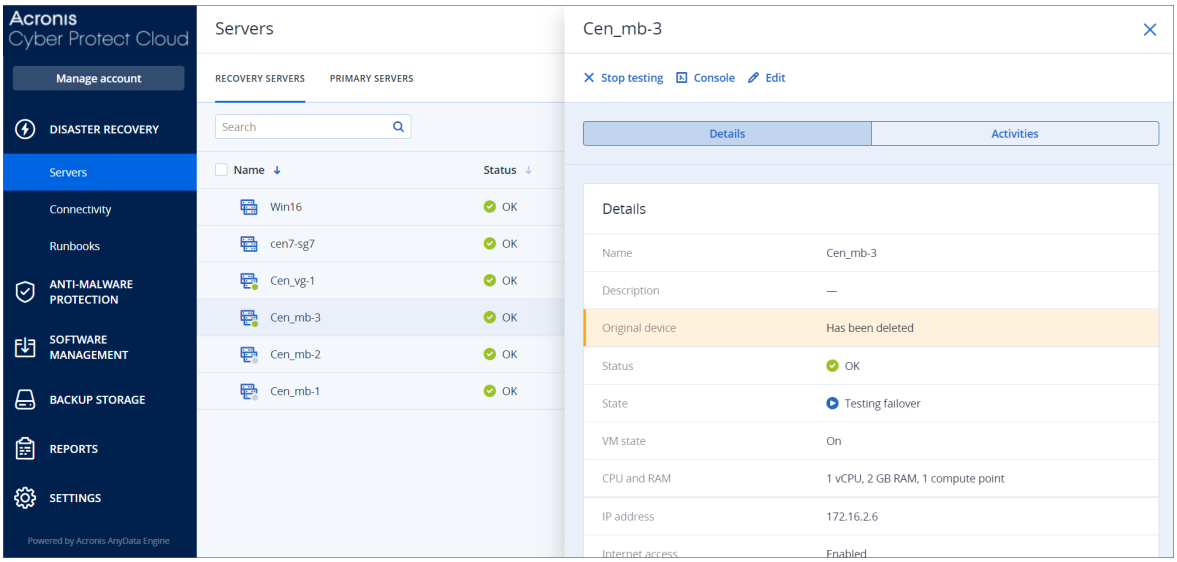
   b. [可选]要保存备份集的密码并在后续故障转移操作中使用它，请选中**将密码存储在安全凭据存储中...**复选框，然后在**凭据名称**字段中输入凭据的名称。

      重要事项

      该密码将存储在安全凭据存储中，将在后续故障转移操作中自动应用。但是，保存密码可能与您的合规义务冲突。

   c. 单击**完成**。

   恢复服务器启动时，其状态将更改为**测试故障转移**。



7. 使用以下任一方法测试恢复服务器：
   - 在**灾难恢复** > **服务器**中，选择恢复服务器，然后单击**中控台**。
   - 使用 RDP 或 SSH 以及创建恢复服务器时指定的测试 IP 地址连接到恢复服务器。尝试同时从生产网络的内部和外部连接（如“点到站点连接”中所述）。
   - 在恢复服务器内运行脚本。

     脚本可能会检查登录屏幕、应用程序是否已启动、Internet 连接以及其他计算机是否能够连接到恢复服务器。
   - 如果恢复服务器可以访问 Internet 和公共 IP 地址，您可能想要使用 TeamViewer。
8. 测试完成后，单击**停止测试**。

   恢复服务器将停止。测试故障转移期间对恢复服务器所做的所有更改都不会保留。

注意

无论是在 Runbook 中还是手动启动测试故障转移时，**启动服务器**和**停止服务器**操作都不适用于测试故障转移操作。如果尝试执行此类操作，它将失败并显示以下错误消息：
已失败：操作不适用于当前服务器状态。

自动测试故障转移

通过使用自动测试故障转移，将每月对恢复服务器自动测试一次，无需任何手动互动。

自动测试故障转移过程由以下各部分组成：

1. 从上一个恢复点创建虚拟机
2. 对虚拟机进行屏幕截图
3. 分析虚拟机的操作系统是否成功启动
4. 向您发送测试故障转移状态的通知

注意

自动测试故障转移会消耗计算点。

可以在恢复服务器的设置中配置自动测试故障转移。有关详细信息，请参阅 "配置自动测试故障转移"(第 709 页)。

请注意，在极少数情况下，自动测试故障转移可能会跳过，并可能不会在预定时间执行。这是因为生产故障转移的优先级高于自动测试故障转移，因此为自动测试故障转移分配的硬件资源(CPU 和 RAM) 可能会临时受限制，以确保有足够的资源可用于并发生产故障转移。

如果自动测试故障转移因某种原因而跳过，将会发出警报。

注意
如果使用加密作为计算机属性来加密原始计算机的备份，并且在创建恢复服务器时未指定加密密码，自动测试故障转移将会失败。有关指定加密密码的更多信息，请参见"创建恢复服务器"(第 694 页)。

配置自动测试故障转移

通过配置自动测试故障转移，可以每月测试恢复服务器，而无需执行任何手动操作。

配置自动测试故障转移

1. 在中控台中，转到**灾难恢复** > **服务器** > **恢复服务器**，然后选择相应恢复服务器。
2. 单击**编辑**。
3. 在**自动测试故障转移**选项卡的**预定**字段中，选择**每月**。
4. 在**屏幕截图超时**中，更改系统尝试执行自动测试故障转移的最长时间段的默认值(以分钟为单位)。
5. 如果要将**屏幕截图超时**值保存为默认值，并在为其他恢复服务器启用自动测试故障转移时自动填充该值，请选择**设为默认超时**。
6. 单击**保存**。

查看自动测试故障转移状态

可以查看已完成的自动测试故障转移的详细信息，如状态、开始时间、结束时间、持续时间和虚拟机的屏幕截图。

注意
虚拟机的屏幕截图将保留，直到自动化测试故障转移再次运行并生成新的屏幕截图。

查看恢复服务器的自动测试故障转移状态

1. 在中控台中，转到**灾难恢复** > **服务器** > **恢复服务器**，然后选择相应恢复服务器。
2. 在**自动测试故障转移**部分中，查看上次自动测试故障转移的详细信息。
3. 若要查看虚拟机的屏幕截图，请单击**显示屏幕截图**。

禁用自动测试故障转移

如果要节省资源，或者不需要为某个恢复服务器执行自动测试故障转移，则可以禁用自动测试故障转移。

禁用自动测试故障转移

1. 在中控台中，转到**灾难恢复** > **服务器** > **恢复服务器**，然后选择相应恢复服务器。
2. 单击**编辑**。
3. 在**自动测试故障转移**部分的**预定**字段中，选择**从不**。
4. 单击**保存**。

生产故障转移

注意
此功能的可用性取决于为您的帐户启用的服务配额。

创建恢复服务器后，它会一直保持在**待机**状态。在启动故障转移之前，相应虚拟机并不存在。在启动故障转移过程之前，必须创建至少一个原始计算机的磁盘映像备份（具有可启动卷）。

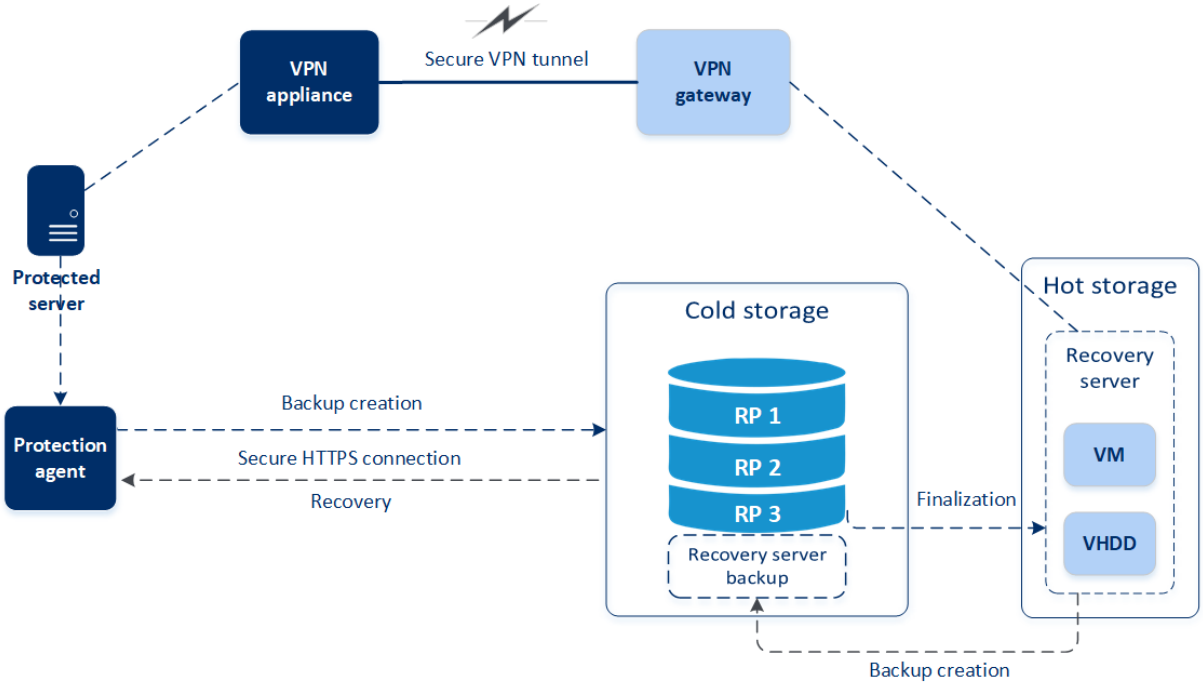
当启动故障转移过程时，选择原始计算机（将基于其创建带有预定义参数的虚拟机）的恢复点（备份）。故障转移操作使用“从备份运行 VM”功能。恢复服务器获取转移状态**最终确定**。此过程意味着将服务器的虚拟磁盘从备份存储（“冷”存储）传输到灾难恢复存储（“热”存储）。

注意
在**最终确定**期间，尽管性能低于正常水平，但服务器仍可以访问并操作。可以通过单击**中控台准备就绪**链接来打开服务器中控台。该链接位于**灾难恢复** > **服务器**屏幕上的 **VM 状态列**中，以及服务器的**详细信息**视图中。

最终确定完成后，服务器性能达到正常值。服务器状态更改为**故障转移**。现在，工作负载从原始计算机切换到云站点中的恢复服务器。

如果恢复服务器内部装有保护代理程序，则系统会停止运行代理程序服务以避免干扰（例如，开始备份或向备份组件报告过期状态）。

在下图中，您可以查看故障转移和故障恢复过程。



执行故障转移

注意
此功能的可用性取决于为您的帐户启用的服务配额。

故障转移是将工作负载从您本地移动到云的过程，也是工作负载保留在云中时的状态。

当启动故障转移时，恢复服务器会在生产网络中启动。为了避免干扰和出现不必要的问题，请确保原始工作负载不在线并且无法通过 VPN 进行访问。

为了避免对同一云存档造成备份干扰，请从当前处于**故障转移**状态下的工作负载中手动撤消保护计划。有关撤消计划的详细信息，请参阅撤消保护计划。

重要事项
必须先创建恢复服务器，才能保护设备免遭灾难的影响。

只能从在创建了设备的恢复服务器后创建的恢复点(备份)执行故障转移。

在故障转移到恢复服务器之前，必须创建至少一个恢复点。支持的最大恢复点数为 100。

可以按照以下步骤操作，或者观看视频教程。

执行故障转移的步骤

1. 确保原始计算机在网络上不可用。
2. 在 Cyber Protect 中控台中，转到**灾难恢复** > **服务器** > **恢复服务器**，然后选择相应恢复服务器。
3. 单击**故障转移**。
4. 选择**生产故障转移**。
5. 选择恢复点(备份)，然后单击**启动**。

6. [如果您选择的备份是通过使用加密作为计算机属性进行加密的]
   a. 输入备份集的加密密码。

   注意
   该密码将仅临时保存，将仅用于当前故障转移操作。在故障转移操作完成并且服务器返回到**待机**状态后，该密码会自动从凭据存储中删除。

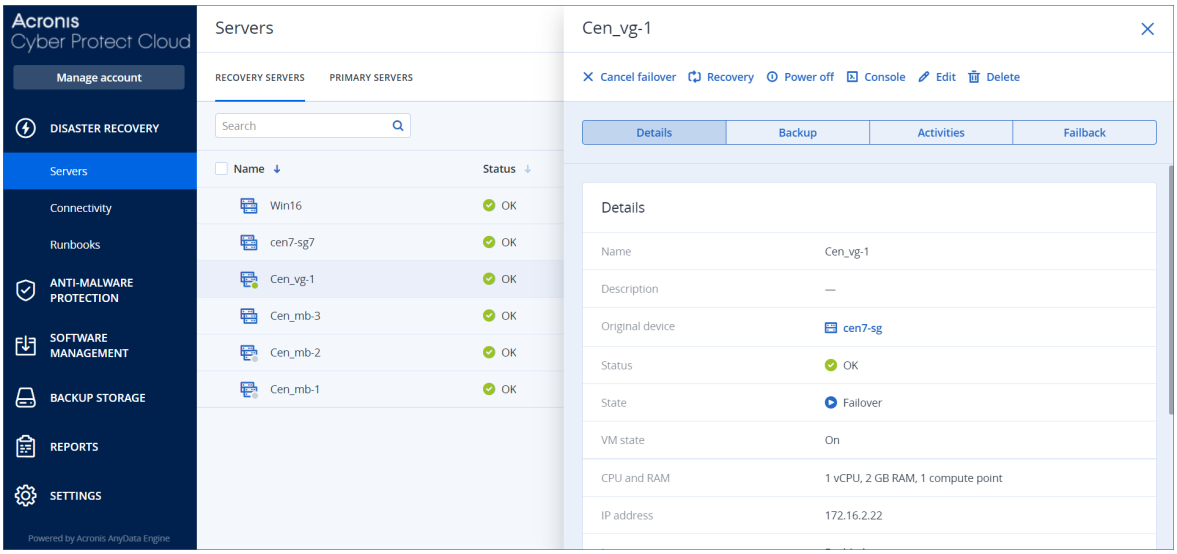
   b. [可选] 要保存备份集的密码并在后续故障转移操作中使用它，请选中**将密码存储在安全凭据存储中...**复选框，然后在**凭据名称**字段中输入凭据的名称。

   重要事项
   该密码将存储在安全凭据存储中，将在后续故障转移操作中自动应用。但是，保存密码可能与您的合规义务冲突。

   c. 单击**完成**。

   恢复服务器启动时，其状态更改为**最终确定**，然后更改后**故障转移**。

重要事项
了解服务器在**最终确定**和**故障转移**状态下都可用是至关重要的。在**最终确定**状态期间，可以通过单击**中控台准备就绪**链接来访问服务器中控台。该链接位于**灾难恢复 > 服务器**屏幕上的 **VM 状态**列中，以及服务器的**详细信息**视图中。



7. 查看恢复服务器的中控台，确保它已启动。依次单击**灾难恢复 > 服务器**、选择相应恢复服务器，然后单击**中控台**。
8. 确保可以使用在创建恢复服务器时指定的生产 IP 地址访问恢复服务器。

在恢复服务器终止后，将自动创建一个新的保护计划并对其应用该计划。该保护计划基于用于创建恢复服务器的保护计划，但有一定限制。在此计划中，只能更改预定和保留规则。有关详细信息，请参阅“备份云服务器”。

如何使用本地 DNS 执行服务器的故障转移

如果将本地站点上的 DNS 服务器用于解析计算机名称，那么在故障转移后，恢复服务器(对应于依赖 DNS 的计算机)将无法通信，因为云中使用 DNS 服务器并不相同。默认情况下，云站点的 DNS 服务器用于新创建的云服务器。如果需要应用自定义 DNS 设置，请与支持团队联系。

如何执行 DHCP 服务器的故障转移

您的本地基础架构可能具有位于 Windows 或 Linux 主机上的 DHCP 服务器。当此类主机故障转移到云站点时，DHCP 服务器重复问题会发生，因为云中的 VPN 网关也履行 DHCP 角色。要解决该问题，请执行以下任一操作：

- 如果仅 DHCP 主机故障转移到云，而其余本地服务器仍位于本地站点上，那么必须登录云中的 DHCP 主机，然后关闭其上的 DHCP 服务器。如此一来，将不会发生冲突，仅 VPN 网关将用作 DHCP 服务器。
- 如果云服务器已从 DHCP 主机获得 IP 地址，那么必须登录云中的 DHCP 主机，然后关闭其上的 DHCP 服务器。还必须登录云服务器并续订 DHCP 租约，以指派从正确的 DHCP 服务器(托管在 VPN 网关中)分配得到的新 IP 地址。

注意
当云 DHCP 服务器是使用**自定义 DHCP** 选项配置的时，这些说明无效，并且某些恢复服务器或主服务器将从该 DHCP 服务器获取其 IP 地址。

停止故障转移

您可以在处理的每个阶段的任何时候停止生产故障转移。

注意
停止故障转移会还原自故障转移开始以来所做的所有更改，但不包括恢复服务器备份。

若要停止故障转移

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **服务器** > **恢复服务器**。
2. 选择处于**故障转移**状态的恢复服务器。
3. 点击恢复服务器。
4. 单击**停止故障转移**。
5. 在出现的确认窗口中，选择复选框，然后单击**停止故障转移**。
   故障转移已停止。恢复服务器会返回到**待机**状态。

故障恢复

注意
此功能的可用性取决于为您的帐户启用的服务配额。

故障恢复是将工作负载从云移回本地站点上的物理机或虚拟机的过程。可以在处于**故障转移**状态下的恢复服务器上执行故障恢复，然后继续在本地站点上使用该服务器。

可以执行自动故障转移到本地站点上的虚拟或物理目标计算机。在故障恢复过程中，可以将备份数据传输到本地站点，同时云中的虚拟机继续运行。该技术有助于您实现非常短的停机时间(在 Cyber Protect 中控台中进行估算并显示)。可以查看它并使用此信息来计划您的活动，并在必要时提醒客户即将发生的停机时间。如果通过可启动媒体执行基于代理程序的故障恢复，停机时间甚至会更短，因为只有增量更改会传输到本地站点。

若要将数据故障恢复到目标物理机，可通过可启动媒体使用基于代理程序的故障恢复。有关详细信息，请参阅 "执行基于代理程序通过可启动媒体的故障恢复"(第 715 页)。

若要将故障恢复到目标虚拟机，可使用通过可启动媒体的基于代理程序的故障恢复，或通过虚拟机监控程序代理程序的无代理程序故障恢复。有关详细信息，请参阅 "执行基于代理程序通过可启动媒体的故障恢复"(第 715 页) 和 "通过虚拟机监控程序代理程序执行无代理程序的故障恢复"(第 718 页)。

在无法使用自动故障恢复过程的特定情况下，可以执行手动故障恢复。有关详细信息，请参阅 "手动故障恢复"(第 721 页)。

注意
Runbook 操作仅支持手动模式下的故障恢复。这意味着，如果通过执行包含**故障恢复服务器**步骤的 Runbook 来启动故障恢复过程，则该过程需要手动互动：必须手动恢复计算机，然后从**灾难恢复** > **服务器**选项卡来确认或取消故障恢复过程。

基于代理程序通过可启动媒体进行故障恢复

注意
此功能的可用性取决于为您的帐户启用的服务配额。

已经优化通过可启动媒体的基于代理程序的故障恢复流程，以便将故障恢复到原始物理或虚拟机。在此过程中，仅增量更改会传输到本地站点。

通过可启动媒体到目标物理机或虚拟机的基于代理程序的故障恢复过程包括以下各阶段：

1. **计划**。在此阶段，将还原本地站点上的 IT 基础架构(如主机和网络配置)、配置故障恢复参数并计划何时启动数据传输。
2. **数据传输**。在此阶段中，数据会从云站点传输到本地站点，同时云中虚拟机继续运行。可以在数据传输阶段的任何时候开始下一阶段(即切换)，但应考虑以下关系。

   停留在数据传输阶段的时间越长，
   - 云中虚拟机继续运行的时间越长。
   - 将传输到本地站点的数据越多。
   - 将支付的费用越高(花费更多计算点)。
   - 切换阶段的停机时间就越短。

   如果要最大程度地减少停机时间，请在 90% 以上的数据传输到本地站点后开始切换阶段。

如果可以承受更长的停机时间，并且不希望花费更多计算点用于运行云中的虚拟机，则可以更早地开始切换阶段。

注意
数据传输过程使用闪回技术。此技术将目标计算机上的可用数据与云中虚拟机的数据进行比较。如果部分数据已在目标计算机上可用，则不会再次传输它。此技术使数据传输阶段更快。
因此，建议您将服务器还原到本地站点上的原始计算机。

3. **切换**。在此阶段，将关闭云中虚拟机，并将剩余数据(包括上一备份增量)传输到本地站点。如果没有在恢复服务器上应用备份计划，则在切换阶段会自动执行备份，这将减慢该过程。
4. **验证**。在此阶段，本地站点上的计算机已准备就绪，可以使用基于 Linux 的可启动媒体重新启动它。可以验证虚拟机是否正常运行，以及：
   - 如果一切正常，请确认故障恢复。确认故障恢复后，将删除云中的虚拟机，并且恢复服务器会返回到**待机**状态。这表示故障恢复过程结束。
   - 如果出现问题，可以取消故障转移并返回到计划阶段。

注意
可启动媒体重新启动后，您将无法再次使用它。如果在验证阶段发现问题，则必须注册新的可启动媒体，然后再次启动故障恢复过程。
然而，由于将使用闪回技术，因此本地站点上已存在的数据将不会再次传输，并且故障恢复过程将更快。

执行基于代理程序通过可启动媒体的故障恢复

注意
此功能的可用性取决于为您的帐户启用的服务配额。

可以通过可启动媒体对本地站点上的目标物理机或虚拟机执行基于代理程序的故障恢复。

注意
数据传输过程使用闪回技术。此技术将目标计算机上的可用数据与云中虚拟机的数据进行比较。如果部分数据已在目标计算机上可用，则不会再次传输它。此技术使数据传输阶段更快。

因此，建议您将服务器还原到本地站点上的原始计算机。

先决条件

- 将用于执行故障恢复的代理程序处于联机状态，并且当前未用于其他故障恢复操作。
- Internet 连接稳定。
- 注册的可启动媒体可用。有关详细信息，请参阅《Cyber Protection 用户指南》中的“创建可启动媒体以恢复操作系统”。
- 目标计算机是本地站点上的原始计算机，或者有与原始计算机相同的固件。
- 云中至少有一个虚拟机的完整备份。

执行故障恢复至物理机

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **服务器**。
2. 选择处于**故障转移**状态的恢复服务器。
3. 单击**故障恢复**选项卡。
4. 在**故障恢复类型**字段中，选择**通过可启动媒体、基于代理程序的**。
5. 在**目标可启动媒体**字段中，单击**指定**、选择可启动媒体，然后单击**完成**。

注意
由于现成的可启动媒体已完成配置，因此建议您使用该可启动媒体。有关详细信息，请参阅《Cyber Protection 用户指南》中的“创建可启动媒体以恢复操作系统”。

6. [可选] 要更改默认磁盘映射，请在**磁盘映射**字段中，单击**指定**、将备份的磁盘映射到目标计算机的磁盘，然后单击**完成**。
7. 单击**开始数据传输**，然后在确认窗口中，单击**开始**。

注意
如果云中没有虚拟机的备份，系统将在数据传输阶段之前自动执行备份。

数据传输阶段即会开始。中控台会显示以下信息：

现场	描述
进度	此参数显示已传输到本地站点的数据量，以及必须传输的数据总量。 由于虚拟机在数据传输阶段继续运行，因此数据总量包括数据传输阶段开始之前上次备份的数据以及新生成数据的备份（备份增量）。因此，**进度**值会随着时间的推移而增大。 由于系统在数据传输过程中使用闪回技术，并且不会传输目标计算机上的已可用数据，因此进度可能比中控台最初计算的要快。
停机时间估计	如果现在开始切换阶段，则此参数会显示云中虚拟机将不可用的时长。该值根据**进度**参数的值计算得出，并随着时间的推移而减小。 由于系统在数据传输过程中使用闪回技术，并且不会传输目标计算机上的已可用数据，因此停机时间可能比中控台最初显示的值短得多。

8. 单击**切换**，然后在确认窗口中，再次单击**切换**。
切换阶段即会开始。中控台会显示以下信息：

现场	描述
进度	此参数显示在本地站点上还原计算机的进度。
估计的完成时间	此参数显示切换阶段将完成的大致时间，然后您将能够在本地站点上启动计算机。

注意
如果未对云中的虚拟机应用备份计划，则在切换阶段会自动执行备份，这将导致停机时间更长。

9. 在**切换**阶段完成后，重新启动可启动媒体，然后验证本地站点上的物理机是否按预期运行。

有关详细信息，请参阅《Cyber Protection 用户指南》中的“使用可启动媒体恢复磁盘”。

10. 单击**确认故障恢复**，然后在确认窗口中，单击**确认**以完成该过程。
    将删除云中的虚拟机，并且恢复服务器会返回到**待机**状态。

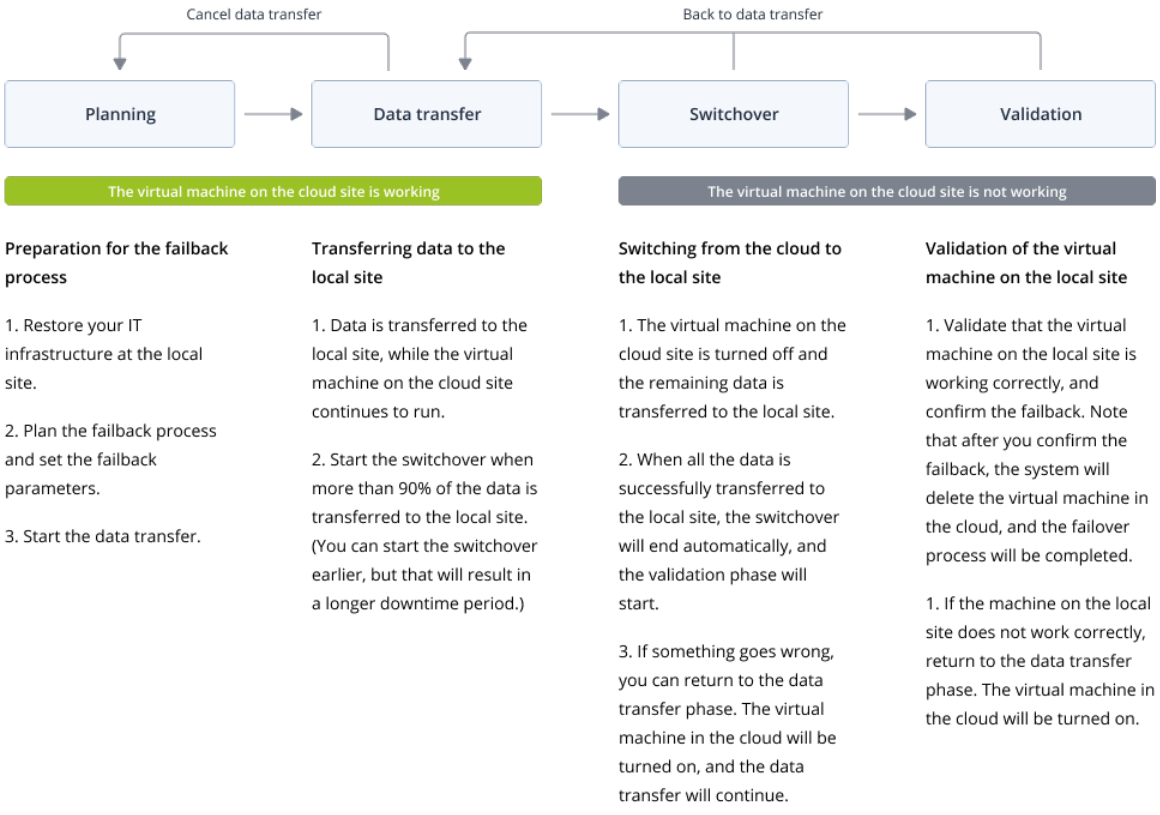
注意
在恢复的服务器上应用保护计划不是故障恢复过程的一部分。在故障恢复过程完成后，在恢复的服务器上应用保护计划以确保它再次受到保护。可以应用原始服务器上已应用的相同保护计划，也可以应用已启用**灾难恢复**模块的新保护计划。

通过虚拟机监控程序代理程序进行的无代理程序故障恢复

注意
此功能的可用性取决于为您的帐户启用的服务配额。

已优化通过虚拟机监控程序代理程序进程进行的无代理程序故障恢复，可用于将故障恢复到新的虚拟机。若要将故障恢复到原始虚拟机，请按照通过可启动媒体的基于代理程序的故障恢复的程序操作。

通过虚拟机监控程序代理程序进行的无代理程序故障恢复包括四个阶段。



1. **计划**。在此阶段，将还原本地站点上的 IT 基础架构(如主机和网络配置)、配置故障恢复参数并计划何时启动数据传输。

注意
为了最大程度地减少故障恢复过程的总时间，建议您在完成设置本地服务器后立即开始数据传输阶段，然后在数据传输阶段继续配置网络和本地基础架构的其余部分。

2. **数据传输**。在此阶段中，数据会从云站点传输到本地站点，同时云中虚拟机继续运行。可以在数据传输阶段的任何时候开始下一阶段(即切换)，但应考虑以下关系。

   停留在数据传输阶段的时间越长，
   - 云中虚拟机继续运行的时间越长。
   - 将传输到本地站点的数据越多。
   - 将支付的费用越高(花费更多计算点)。
   - 切换阶段的停机时间就越短。

   如果要最大程度地减少停机时间，请在 90% 以上的数据传输到本地站点后开始切换阶段。

   如果可以承受更长的停机时间，并且不希望花费更多计算点用于运行云中的虚拟机，则可以更早地开始切换阶段。

   如果在数据传输阶段取消故障恢复过程，将不会从本地站点中删除已传输的数据。为避免出现潜在问题，请在开始新的故障恢复过程之前先手动删除已传输的数据。后续数据传输过程将从头开始。
3. **切换**。在此阶段，将关闭云中虚拟机，并将剩余数据(包括上一备份增量)传输到本地站点。如果没有在恢复服务器上应用备份计划，则在切换阶段会自动执行备份，这将减慢该过程。

   可以在 Cyber Protect 中控台中查看此阶段的估计完成时间(停机时间)。在所有数据都传输到本地站点(没有数据丢失，并且本地站点上的虚拟机是云中虚拟机的精确副本)后，切换阶段完成。将恢复本地站点上的虚拟机，然后验证阶段会自动开始。
4. **验证**。在此阶段中，本地站点上的虚拟机已准备就绪并自动启动。可以验证虚拟机是否正常运行，以及：
   - 如果一切正常，请确认故障恢复。确认故障恢复后，将删除云中的虚拟机，并且恢复服务器会返回到**待机**状态。这表示故障恢复过程结束。
   - 如果出现问题，可以取消切换并返回到数据传输阶段。

通过虚拟机监控程序代理程序执行无代理程序的故障恢复

注意
此功能的可用性取决于为您的帐户启用的服务配额。

可以通过虚拟机监控程序代理程序在本地站点对目标虚拟机执行无代理程序的故障恢复。

先决条件

- 将用于执行故障恢复的代理程序处于联机状态，并且当前未用于其他故障恢复操作。
- Internet 连接稳定。
- 云中至少有一个虚拟机的完整备份。

通过虚拟机监控程序代理程序执行无代理程序的虚拟机故障恢复

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **服务器**。
2. 选择处于**故障转移**状态的恢复服务器。
3. 单击**故障恢复**选项卡。
4. 在**故障恢复参数**部分，**故障恢复类型**字段中，选择**通过虚拟机监控程序的无代理程序**，然后配置其他参数。

   请注意，默认情况下，某些**故障恢复参数**会自动填充建议值，但可以进行更改。

   下表提供了有关**故障恢复参数**的更多信息。

参数	描述
备份大小	在故障恢复过程中将传输到本地站点的数据量。 在启动对目标虚拟机的故障恢复过程之后，**备份大小**会在数据传输阶段增加，因为云中的虚拟机会继续运行并生成新数据。 要计算对目标虚拟机的故障恢复过程期间的估计停机时间，请取 10% 的**备份大小**值（因为我们建议您在 90% 的数据传输到本地站点之后开始切换阶段），然后将其除以 Internet 速度值。 **注意** 当同时执行多个故障恢复过程时，Internet 的速度值会降低。
目标计算机位置	故障恢复位置：VMware ESXi 主机或 Microsoft Hyper-V 主机。 可以从具有代理程序（已在网络安全保护服务中进行注册）的所有主机中进行选择。
代理程序	将执行故障恢复操作的代理程序。 可以同时使用一个代理程序执行一项故障恢复操作。 可以选择一个处于联机状态的代理程序，并且该代理程序当前未用于另一个故障恢复过程、其版本支持故障恢复功能以及有权访问备份。 请注意，可以在 VMware ESXi 主机上安装多个代理程序，然后使用每个代理程序启动一个单独故障恢复过程。可以同时执行这些故障恢复过程。
目标计算机设置	虚拟机设置： • **虚拟处理器**。选择虚拟处理的数量。 • **内存**。选择虚拟机将拥有多少内存。 • **单位**。选择内存的单位。 • [可选] **网络适配器**。要添加网络适配器，请单击**添加**，然后在**网络**字段中选择一个网络。 准备好进行更改时，单击**完成**。
路径	（对于 Microsoft Hyper-V 主机）将存储计算机的主机上的文件夹。 确保主机上有可用于计算机的足够内存空间。
数据存储	（对于 VMware ESXi 主机）将存储计算机的主机上的数据存储。 确保主机上有可用于计算机的足够内存空间。
调配	虚拟磁盘的分配方法。

参数	描述
模式	对于 Microsoft Hyper-V 主机： • **动态扩展**(默认值)。 • **固定大小**。 对于 Microsoft Hyper-V 主机： • **精简**(默认值)。 • **完整**。
目标计算机名称	目标计算机的名称。默认情况下，目标计算机名称与恢复服务器名称相同。 目标计算机名称在所选**目标计算机位置**上必须是唯一的。

5. 单击**启动数据传输**，然后在确认窗口中单击**启动**。

注意
如果云中没有虚拟机的备份，系统将在数据传输阶段之前自动执行备份。

数据传输阶段将开始。中控台会显示以下信息：

现场	描述
进度	此参数显示已传输到本地站点的数据量，以及必须传输的数据总量。 由于虚拟机在数据传输阶段继续运行，因此数据总量包括数据传输阶段开始之前上次备份的数据以及新生成数据的备份(备份增量)。因此，**进度**参数的两个值都会随时间增加。
停机时间估计	如果现在开始切换阶段，则此参数会显示云中虚拟机将不可用的时长。该值根据**进度**参数的值计算得出，并随着时间的推移而减小。

6. 单击**切换**，然后在确认窗口中，再次单击**切换**。
切换阶段即会开始。中控台会显示以下信息：

现场	描述
进度	此参数显示在本地站点上还原计算机的进度。
估计的完成时间	此参数显示切换阶段将完成的大致时间，然后您将能够在本地站点上启动计算机。

注意
如果未对云中的虚拟机应用备份计划，则在切换阶段会自动执行备份，这将导致停机时间更长。

7. **切换**阶段完成，且本地站点上的虚拟机自动启动后，验证其是否按预期工作。
8. 单击**确认故障恢复**，然后在确认窗口中单击**确认**以完成该过程。
将删除云中的虚拟机，并且恢复服务器会返回到**待机**状态。

注意
在恢复的服务器上应用保护计划不是故障恢复过程的一部分。在故障恢复过程完成后，在恢复的服务器上应用保护计划以确保它再次受到保护。可以应用原始服务器上已应用的相同保护计划，也可以应用已启用**灾难恢复**模块的新保护计划。

手动故障恢复

注意
建议您仅当支持团队建议您在手动模式下使用故障恢复过程时才这样做。

还可以在手动模式下启动故障恢复过程。在这种情况下，将不会自动执行从云中备份到本地站点的数据传输。必须在云中虚拟机关机后手动执行数据传输。这使手动模式下的故障恢复过程较慢，您应该会预计到停机时间较长。

手动模式下的故障恢复过程包括以下几个阶段：

1. **计划**。在此阶段，将还原本地站点上的 IT 基础架构（如主机和网络配置）、配置故障恢复参数并计划何时启动数据传输。
2. **切换**。在此阶段，将关闭云中虚拟机，并备份新生成的数据。如果没有在恢复服务器上应用备份计划，则在切换阶段会自动执行备份，这将减慢该过程。完成备份后，将计算机手动恢复到本地站点。可以使用可启动媒体来恢复磁盘，也可以从云备份存储恢复整个计算机。
3. **验证**。在此阶段，将验证本地站点上的物理机或虚拟机是否正常运行，并确认故障恢复。确认后，将删除云站点上的虚拟机，并且恢复服务器会返回到**待机**状态。

执行手动故障恢复

注意
此功能的可用性取决于为您的帐户启用的服务配额。

可以对本地站点上的目标物理机或虚拟机执行手动故障恢复。

执行手动故障恢复

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **服务器**。
2. 选择处于**故障转移**状态的恢复服务器。
3. 单击**故障恢复**选项卡。
4. 在**目标**字段中，选择**物理机**。
5. 单击齿轮图标，然后启用**使用手动模式**开关。
6. [可选] 通过将**备份大小**值除以您 Internet 的速度值，计算故障恢复过程期间的估计停机时间。

注意
当同时执行多个故障恢复过程时，Internet 的速度值会降低。

7. 单击**切换**，然后在确认窗口中，再次单击**切换**。

将关闭云站点上的虚拟机。

注意
如果未对云中的虚拟机应用备份计划，则在切换阶段会自动执行备份，这将导致停机时间更长。

8. 将服务器从云备份恢复到本地站点上的物理机或虚拟机。有关详细信息，请参阅《Cyber Protection 用户指南》中的“恢复计算机”。
9. 确保恢复完成并且恢复的计算机工作正常，然后单击**计算机已还原**。
10. 如果一切正常，则单击**确认故障恢复**，然后在确认窗口中再次单击**确认**。
    恢复服务器和恢复点现在可用于下一次故障转移。要创建新的恢复点，请将保护计划应用于新的本地服务器。

注意
在恢复的服务器上应用保护计划不是故障恢复过程的一部分。在故障恢复过程完成后，在恢复的服务器上应用保护计划以确保它再次受到保护。可以应用原始服务器上已应用的相同保护计划，也可以应用已启用**灾难恢复**模块的新保护计划。

编排 (Runbook)

注意
某些功能可能需要其他许可，具体取决于所应用的许可模式。

操作手册是一组说明，用于介绍如何在云中启动生产环境。您可以在 Cyber Protect 中控台中创建操作手册。

使用操作手册，你可以：

- 自动进行一个或多个服务器的故障转移。
- 通过对服务器 IP 地址执行 Ping 操作并检查与指定端口的连接，来自动检查故障转移结果。
- 设置运行分布式应用程序的服务器的操作顺序。
- 将手动操作包含在工作流程中。
- 通过在测试模式下执行 Runbook，验证灾难恢复解决方案的完整性。

若要访问 **操作手册** 屏幕，请依次选择**灾难恢复** > **操作手册**。

创建 Runbook

操作手册由连续执行的步骤组成。步骤由同时启动的操作组成。

若要创建操作手册，请按照以下程序或 视频教程中的说明进行操作。

若要创建操作手册

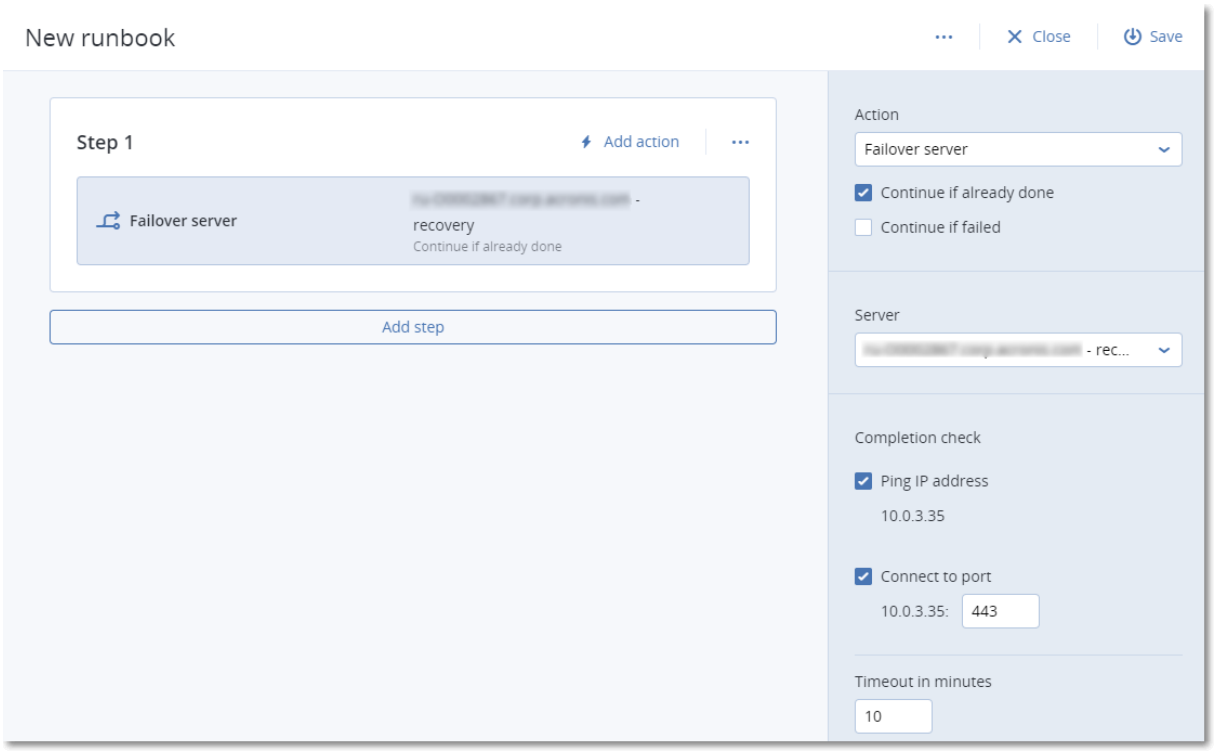
1. 在 Cyber Protection 中控台中，转到**灾难恢复** > **操作手册**。
2. 点击**创建操作手册**。

3. 点击**添加步骤**。
4. 点击**添加操作**，然后选择想要添加到步骤的操作。

操作	描述
对服务器进行故障转移	执行云服务器的故障转移。要定义此操作，您必须选择一个云服务器并配置可用于此操作的操作手册参数。有关这些参数的更多信息，请参见"操作手册参数"(第 724 页)。 **注意** 如果选择的服务器的备份使用加密作为计算机属性进行加密，**对服务器进行故障转移**的操作将被暂停，并将自动更改为**需要互动**。若要继续执行操作手册，您将必须提供加密备份的密码。
对服务器进行故障恢复	执行云服务器的故障恢复。要定义此操作，您必须选择一个云服务器并配置可用于此操作的操作手册参数。有关这些设置的更多信息，请参见"操作手册参数"(第 724 页)。 **注意** Runbook 操作仅支持手动模式下的故障恢复。这意味着，如果通过执行包含**对服务器进行故障恢复**步骤的 Runbook 来启动故障恢复过程，则该过程需要手动互动：必须手动恢复计算机，然后从**灾难恢复** > **服务器**选项卡来确认或取消故障恢复过程。
启动服务器	启动云服务器。若要定义此操作，您必须选择一个云服务器并配置可用于此操作的操作手册参数。有关这些设置的更多信息，请参见"操作手册参数"(第 724 页)。 **注意** **启动服务器**操作在操作手册中的测试故障转移操作中不适用。如果您尝试执行此类操作，它将失败并出现以下错误消息： 失败：该操作不适用于当前服务器状态。
停止服务器	停止云服务器。若要定义此操作，您必须选择一个云服务器并配置可用于此操作的操作手册参数。有关这些设置的更多信息，请参见"操作手册参数"(第 724 页)。 **注意** **停止服务器**操作在操作手册中的测试故障转移操作中不适用。如果您尝试执行此类操作，它将失败并出现以下错误消息： 失败：该操作不适用于当前服务器状态。
手动操作	手动操作需要用户的互动。若要定义此操作，您必须输入描述。 当操作手册序列达到手动操作时，操作手册将会暂停，直到用户执行所需的手动操作(例如点击确认按钮)才会继续进行。
执行操作手册	执行另一个操作手册。若要定义此操作，您必须选择一个操作手册。 在 Runbook 中，仅可执行一次指定的 Runbook。例如，如果已添加操作“执行 Runbook A”，则可以添加操作“执行 Runbook B”，但不能再次添加操作“执行

操作	描述
	Runbook A”。

5. 为该操作定义操作手册参数。有关这些参数的更多信息，请参见"操作手册参数"(第 724 页)。
6. [可选] 若要添加步骤的描述：
   a. 单击省略号图标，然后单击**描述**。
   b. 输入步骤的描述。
   c. 单击**完成**。
7. 重复步骤 3-6，直到你创建出所需的步骤和行动序列。
8. [可选] 更改操作手册的默认名称：
   a. 点击省略号图标。
   b. 输入操作手册的名称。
   c. 输入操作手册的描述。
   d. 单击**完成**。
9. 单击**保存**。
10. 单击**关闭**。



操作手册参数

操作手册参数是您必须配置的特定设置，以定义操作手册动作。操作手册参数有两类 - 操作参数和完成检查参数。

操作参数根据操作的初始状态或结果定义操作手册的行为。

完成检查参数会确保服务器可用并提供必要的服务。如果完成检查失败，则该操作会被视为失败。

以下表格描述了每个操作的可配置操作手册参数。

操作手册参数	类别	可供进行操作	描述
如果已经完成则继续	操作参数	• **对服务器进行故障转移** • **启动服务器** • **停止服务器** • **对服务器进行故障恢复**	此参数定义所需操作已完成(例如，已执行故障转移或服务器已在运行)时的操作手册行为。如果启用，操作手册会发出警告并进行运行。如果禁用，操作将失败，且操作手册也将无法运行。 默认情况下会启用此参数。
如果失败则继续	操作参数	• **对服务器进行故障转移** • **启动服务器** • **停止服务器** • **对服务器进行故障恢复**	此参数定义所需操作失败时的操作手册行为。如果启用，操作手册会发出警告并继续运行。如果禁用，操作将失败，且操作手册无法运行。 默认情况下会禁用此参数。
对 IP 地址执行 Ping 操作	完成检查	• **启动服务器**	软件将对云服务器的生产 IP 地址执行 ping 操作，直到服务器回复或超时到期为止，以先到者为准。
连接到端口(默认为 443 端口)	完成检查	• **对服务器进行故障转移** • **启动服务器**	软件将尝试使用其生产 IP 地址和指定的端口来连接到云服务器，直到建立连接或超时到期为止，以先到者为准。这样一来，您可以检查侦听指定端口的应用程序是否正在运行。
超时(以分钟为单位)	完成检查	• **对服务器进行故障转移** • **启动服务器**	默认超时为 10 分钟。

使用 Runbook 进行的操作

注意
此功能的可用性取决于为您的帐户启用的服务配额。

若要访问操作列表，请将鼠标悬停在 Runbook 上并单击省略号图标。Runbook 未运行时以下操作可用：

- **执行**
- **编辑**
- **克隆**
- **删除**

执行 Runbook

每次单击**执行**，会提示您输入执行参数。这些参数适用于 Runbook 中包含的所有故障转移和故障恢复操作。**执行 Runbook** 操作中指定的 Runbook 从主 Runbook 继承这些参数。

- **故障转移和故障恢复模式**

  选择是要运行测试故障转移(默认情况下)还是实际(生产)故障转移。故障恢复模式将与所选的故障转移模式有关。
- **故障转移恢复点**

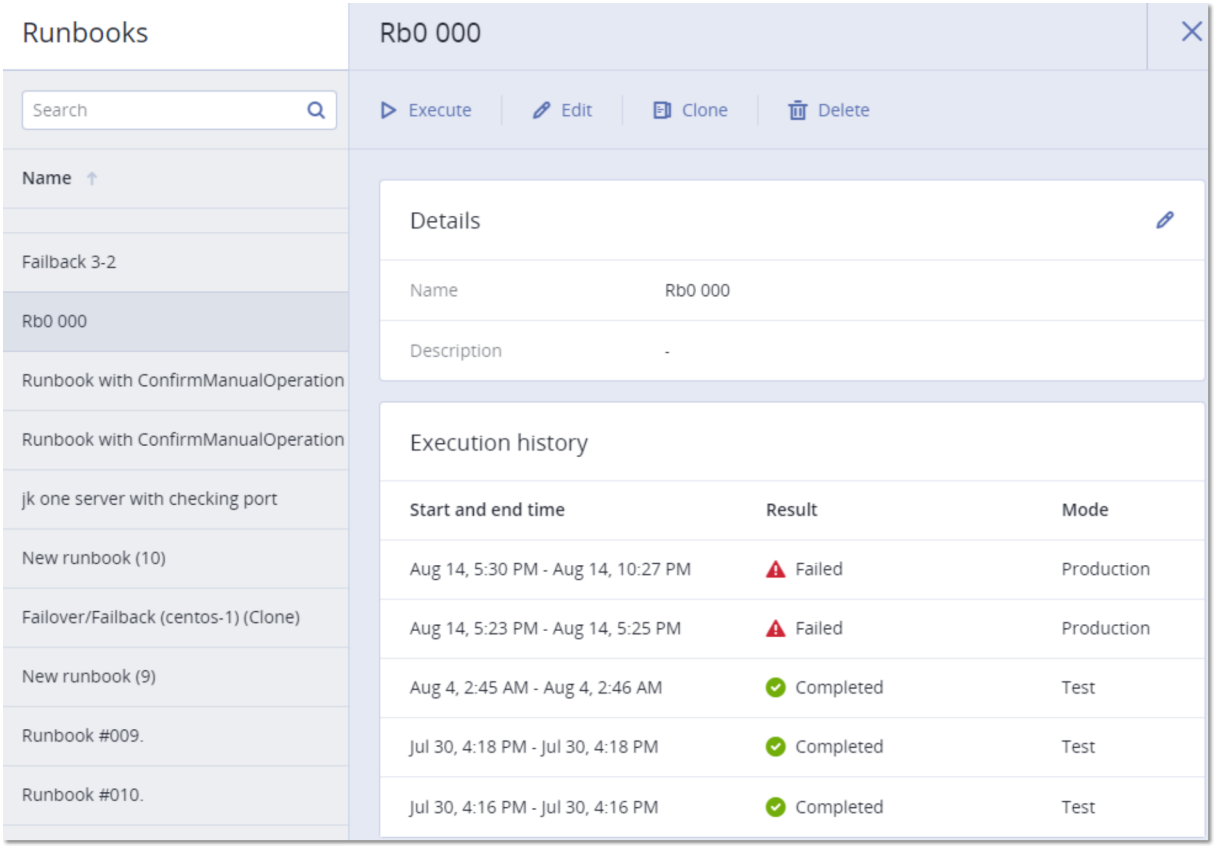
  选择最近的恢复点(默认情况下)或选择过去的某个时间点。如果是后者,则将为每个服务器选择指定日期和时间之前最接近的恢复点。

停止 Runbook 执行

在 Runbook 执行期间,您可以在操作列表中选择**停止**。软件将完成所有已启动的操作,需要用户交互的操作除外。

查看执行历史记录

在 **Runbooks** 选项卡上选择一个 Runbook 后,软件将显示此 runbook 详细信息和执行历史记录。单击对应于特定执行的行以查看执行日志。



正在移除灾难恢复站点

可以删除灾难恢复站点。此操作将自动删除 VPN 网关、VPN 连接和站点上配置的所有操作手册。

先决条件

灾难恢复站点上无可用的云服务器。

若要移除灾难恢复站点

1. 在 Cyber Protect 中控台中，转到**灾难恢复** > **连接**。
2. 单击**显示属性**。
3. 点击**移除灾难恢复站点**。
4. 在确认窗口中，单击**删除**。

配置防病毒和防恶意软件保护

注意
在 Windows 计算机上，防恶意软件防护功能需要安装防恶意软件防护代理，URL 筛选功能需要安装 URL 筛选代理程序。如果在其保护计划中启用了**防病毒和防恶意软件保护**和/或**URL 筛选**模块，将自动为受保护的工作负载安装这些代理程序。

Cyber Protection 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 Microsoft Defender Antivirus。

  注意
  此功能的可用性取决于为您的帐户启用的服务配额。

重要事项
仅当在保护计划中启用了**高级防恶意软件**选项时，才会检测到 EICAR 测试文件。但是，检测不到 EICAR 文件并不会影响 Cyber Protection 的反恶意软件功能。

支持的防病毒和防恶意软件保护操作系统

以下平台支持 Active Protection、防病毒和防恶意软件保护功能。

操作系统	版本/发行版
Windows	Windows 7 Service Pack 1 及更高版本 Windows Server 2008 R2 Service Pack 1 及更高版本 **注意** 对于 Windows 7，必须先安装 Microsoft 发布的以下更新，然后再安装保护代理程序。 • 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。
Linux	Red Hat Linux 7.x, 8.x, 9.x CloudLinux 6.10, 7.x, 8.x CentOS 6.5 及更高的 6.x 版本、7.x、8.x Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 Debian 8.x, 9.x, 10,x, 11.x

操作系统	版本/发行版
	Oracle Linux 7.x, 8.x, 9.x SUSE Enterprise Linux 15.x openSUSE Leap 15.x
macOS	macOS 10.13.x 及更高版本

每个平台支持的功能

注意
高级防恶意软件包提供有针对 Linux 和 macOS 的防恶意软件保护。

功能集	Windows	Linux	macOS
防病毒和反恶意软件保护			
完全集成的 Active Protection 功能	是	否	否
实时防恶意软件保护	是	是，装有高级防恶意软件包	是，装有高级防恶意软件包
具有本地基于签名检测的高级实时防恶意软件保护	是	是	是
便携式可执行文件的静态分析	是	否	是*
手动反恶意软件扫描	是	是**	是
网络文件夹保护	是	是	否
服务器端保护	是	否	否
扫描存档文件	是	否	是
扫描可移动驱动器	是	否	是
仅扫描新文件和更改的文件	是	否	是
文件/文件夹排除	是	是	是***
进程排除	是	否	是
行为分析引擎	是	否	是
漏洞利用预防	是	否	否
隔离	是	是	是

功能集	Windows	Linux	macOS
防病毒和反恶意软件保护			
隔离区自动清除	是	是	是
URL 过滤 (http/https)	是	否	否
公司范围的白名单	是	否	是
防火墙管理****	是	否	否
Microsoft Defender Antivirus 管理*****	是	否	否
Microsoft Security Essentials 管理	是	否	否
通过 Windows Security Center 注册和管理防病毒和反恶意软件保护	是	否	否
有关受支持操作系统及其版本的详细信息，请参阅 "支持的防病毒和防恶意软件保护操作系统"(第 728 页)。			

* 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。

** 对于 Linux 上的手动扫描，不支持开始条件。

*** 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。

**** Windows 8 及更高版本支持防火墙管理。不支持 Windows Server。

***** Windows 8.1 及更高版本支持 Microsoft Defender Antivirus 管理。

功能集	Windows	Linux	macOS
Active Protection			
进程注入检测	是	否	否
自动从本地缓存恢复受影响的文件	是	是	是
安克诺斯 备份文件的自我防御	是	否	否
安克诺斯 软件的自我防御	是	否	是 (仅限 Active Protection 和防恶意软件组件)
受信任/已阻止的进程管理	是	否	是
进程/文件夹排除	是	是	是

功能集	Windows	Linux	macOS
Active Protection			
基于进程行为的勒索软件检测(基于人工智能 (AI))	是	是	是
基于进程行为的加密挖矿进程检测	是	否	否
外部驱动器保护(HDD、闪存驱动器、SD 卡)	是	否	是
网络文件夹保护	是	是	是
服务器端保护	是	否	否
Zoom、Cisco Webex、Citrix Workspace 和 Microsoft Teams 保护	是	否	否
有关受支持操作系统及其版本的详细信息,请参阅 "支持的防病毒和防恶意软件保护操作系统"(第 728 页)。			

防病毒和反恶意软件保护

注意
某些功能可能需要其他许可,具体取决于所应用的许可模式。

防病毒和反恶意软件模块会保护 Windows、Linux 和 macOS 计算机免受所有最新恶意软件威胁的影响。查看 "支持的防病毒和防恶意软件保护操作系统"(第 728 页) 中支持的防恶意软件功能的完整列表。

防病毒和反恶意软件保护在 Windows Security Center 中受支持并进行注册。

防恶意软件功能

- 在实时保护和手动模式下检测文件中的恶意软件
- 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允许列表

扫描类型

可以将防病毒和防恶意软件保护配置为在后台持续运行或按需运行。

实时保护

注意
此功能的可用性取决于为您的帐户启用的服务配额。

“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。

为了防止出现潜在的兼容性和性能问题，“实时保护”不能与其他也使用实时保护功能的防病毒解决方案并行工作。其他已安装的防病毒解决方案的状态通过 Windows Security Center 进行确定。如果 Windows 计算机已由另一种防病毒解决方案提供保护，则实时保护会自动关闭。

要启用“实时保护”，请禁用或卸载其他防病毒解决方案。“实时保护”可以自动替换 Microsoft Defender 实时保护。

注意
在运行 Windows Server 操作系统的计算机上，启用“实时保护”后，Microsoft Defender 不会自动关闭。管理员必须手动关闭 Microsoft Defender，以避免出现潜在的兼容性问题。

可以选择以下扫描模式之一：

- **访问时智能**检测是指防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。在执行某个文件时，以及对该文件进行各种操作（例如打开文件以进行读取或编辑）的情况下，都会检测到恶意软件。
- **执行时**检测是指只会在可执行文件运行时进行扫描，以确保这些文件未受感染并且不会对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。

预定的扫描

根据时间表执行反恶意软件扫描。

可以选择以下扫描模式之一。

- **快速扫描** - 仅检查工作负载系统文件。
- **完整扫描** - 检查工作负载上的所有文件。
- **自定义扫描** - 检查管理员已添加到保护计划的文件/文件夹。

防恶意软件扫描完成后，可以在**监控** > **概述** > 最近受影响小组件中查看有关受威胁影响的工作负载的详细信息。

防病毒和反恶意软件保护设置

本部分介绍可以在保护计划的**防病毒和防恶意软件保护**模块中配置的功能。要了解如何创建保护计划，请参阅 "创建保护计划"（第 192 页）。

可以在保护计划的“防病毒和防恶意软件保护”模块中配置以下功能：

- "Active Protection"（第 733 页）
- "高级防恶意软件"（第 733 页）
- "网络文件夹保护"（第 734 页）
- "服务器端保护"（第 734 页）
- "自我保护"（第 735 页）
- "Cryptomining 进程检测"（第 736 页）
- "隔离设置"（第 736 页）

- "行为引擎"(第 737 页)
- "漏洞利用预防"(第 737 页)
- "实时保护"(第 739 页)
- "预定扫描"(第 739 页)
- "保护排除"(第 742 页)

注意
并非所有操作系统都支持防病毒和防恶意软件保护功能。有关支持的操作系统和功能的更多信息,请参阅 "支持的防病毒和防恶意软件保护操作系统"(第 728 页)。某些功能需要特定许可证才能在您的保护计划中使用。

Active Protection

Active Protection 保护系统免受称为勒索软件(它会加密文件并要求支付赎金才会提供加密密钥)的恶意软件攻击。

默认设置:**已启用**。

注意
必须在受保护的计算机上安装保护代理程序。有关受支持操作系统和功能的详细信息,请参阅 "支持的防病毒和防恶意软件保护操作系统"(第 728 页)。

配置 Active Protection

1. 在**创建保护计划**窗口中,展开**防病毒和防恶意软件保护**模块。
2. 单击 **Active Protection**。
3. 在**检测到时的操作**部分中,选择可用选项之一:
   默认设置:**使用缓存还原**
   - **仅通知** - 软件生成有关涉嫌勒索软件活动的进程的警报。
   - **停止进程** - 软件生成警报并停止涉嫌勒索软件活动的进程。
   - **使用缓存还原** - 软件生成警报、停止进程并使用服务缓存还原文件更改。
4. 单击**完成**,以将选定选项应用于保护计划。

高级防恶意软件

此引擎使用增强的病毒库,来提高在快速扫描和完整扫描下防恶意软件检测的效率。

重要事项
仅当 Advanced Security 护包已启用时,此功能才可用。有关详细信息,请访问 https://www.acronis.com/zh-cn/products/cloud/cyber-protect/security/。

注意
此功能的可用性取决于为您的帐户启用的服务配额。

配置高级防恶意软件

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 在**高级防恶意软件**部分中，使用开关可启用基于本地签名的引擎。

注意
适用于 macOS 和 Linux 的防病毒和反恶意软件保护也需要基于本地签名的引擎。对于 Windows，无论有没有此引擎，都可以使用防病毒和反恶意软件保护。

网络文件夹保护

网络文件夹保护功能定义防病毒和防恶意软件保护是否会保护映射为本地驱动器的网络文件夹。对通过 SMB 或 NFS 协议共享的文件夹应用保护。

配置网络文件夹保护

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**网络文件夹保护**。
3. 添加要备份网络文件夹的文件：
   - 例如，如果工作负载是 Windows，请在 **Windows** 字段中输入要备份网络文件夹的 Windows 文件的路径。默认值：C:\ProgramData\Acronis\Restored Network Files。
   - 例如，如果工作负载是 macOS，请在 **macOS** 字段中输入要备份网络文件夹的 macOS 文件的路径。默认值：/Library/Application Support/Acronis/Restored Network Files/。

   注意
   输入本地文件夹的路径。网络文件夹(包括映射驱动器上的文件夹) 不支持作为网络文件夹的备份目标。
4. 单击**完成**，以将选定选项应用于保护计划。

服务器端保护

此功能定义 Active Protection 是否会保护网络文件夹，此类文件夹由您从网络中可能会带来威胁的其他服务器的外部传入连接共享。

默认设置：**关闭**。

注意
Linux 不支持服务器端保护。

设置受信任的连接

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**服务器端保护**。
3. 使用**服务器端保护**开关以启用它。
4. 选择**受信任**选项卡。
5. 在**受信任的连接**字段中，单击**添加**以定义将允许修改数据的连接。

6. 在**计算机名称/帐户**字段中，键入计算机的名称和装有保护代理程序的计算机的帐户。例如，`MyComputer\TestUser`。
7. 在**主机名**字段中，键入允许使用保护代理程序连接到计算机的计算机的主机名。
8. 单击右侧的复选标记保存连接定义。
9. 单击**完成**。

设置阻止的连接

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**服务器端保护**。
3. 使用**服务器端保护**开关以启用它。
4. 选择**已阻止**选项卡。
5. 在**阻止的连接**字段中，单击**添加**以定义将不允许修改数据的连接。
6. 在**计算机名称/帐户**字段中，键入计算机的名称和装有保护代理程序的计算机的帐户。例如，`MyComputer\TestUser`。
7. 在**主机名**字段中，键入允许使用保护代理程序连接到计算机的计算机的主机名。
8. 选中右侧的复选框以保存连接定义。
9. 单击**完成**。

自我保护

“自我保护”会阻止未经授权更改软件的自身进程、注册表记录、可执行文件和配置文件、以及位于本地文件夹中的备份。

管理员可以启用**自我保护**，而无需启用 **Active Protection**。

默认设置：**开启**。

注意
Linux 不支持自我保护。

启用自我保护

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**自我保护**。
3. 使用**自我保护**开关以启用它。

启用密码保护

1. 在**自我保护**功能已启用后，可以使用开关启用**密码保护**功能。
2. 单击**生成新密码**，以生成用于修改或删除本地代理程序的密码。
3. 单击**复制**，然后将其粘贴到安全位置，因为当您要在本地修改组件列表时，将要求输入该密码。

   重要事项
   在关闭窗口后，该密码将不可用。要将此密码应用到设备，必须保存保护计划设置。

4. 单击**关闭**。

密码保护会阻止未经授权用户或软件卸载适用于 Windows 的代理程序或修改其组件。这些操作只能使用管理员可以提供的密码才能执行。

以下操作不再需要密码：

- 通过本地运行安装程序来更新安装
- 通过使用 Cyber Protect 中控台来更新安装
- 修复安装

默认设置：**已禁用**

有关如何启用**密码保护**的详细信息，请参阅阻止未经授权卸载或修改代理程序。

Cryptomining 进程检测

加密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，甚至可能因滥用而导致硬件损坏。**Cryptomining 进程检测**功能保护设备免受加密挖矿恶意软件影响，以防止未经许可使用计算机资源。

管理员可以启用 **Cryptomining 进程检测**，而无需启用 **Active Protection**。默认设置：**已启用**。

注意
Linux 不支持 Cryptomining 进程检测。

配置网络文件夹保护

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**Cryptomining 进程检测**。
3. 使用**检测加密挖矿进程**开关，可启用或禁用该功能。
4. 选择如何处理涉嫌加密挖矿活动的进程：
   默认设置：**停止进程**
   - **仅通知** - 软件将生成警报。
   - **停止进程** - 软件将生成警报并停止进程。
5. 单击**完成**，以将选定选项应用于保护计划。

隔离设置

隔离区是一个用于隔离可疑(可能已感染)或潜在危险文件的文件夹。

配置隔离

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**隔离**。
3. 在**在以下时间过后删除隔离文件**字段中，可以定义将删除隔离文件所需经过的天数。
   默认设置：**30 天**
4. 单击**完成**。

有关此功能的详细信息，请参阅隔离。

行为引擎

行为引擎功能通过使用行为启发式方法来识别恶意进程，从而保护系统免受恶意软件的侵害。

默认设置：**已启用**。

注意
Linux 不支持行为引擎。

配置网络文件夹保护

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**行为引擎**。
3. 使用**行为引擎**开关，可启用或禁用该功能。
4. 在**检测到时的操作**部分中，选择软件在检测到恶意软件活动时将执行的操作：
   默认设置：**隔离**
   - **仅通知** - 软件生成有关涉嫌恶意软件活动的进程的警报。
   - **停止进程** - 软件生成警报并停止涉嫌恶意软件活动的进程。
   - **隔离** - 软件生成警报、停止过程，并将可执行文件移动到隔离文件夹。
5. 单击**完成**，以将选定选项应用于保护计划。

漏洞利用预防

重要事项
仅当 Advanced Security 护包已启用时，此功能才可用。有关详细信息，请访问 https://www.acronis.com/zh-cn/products/cloud/cyber-protect/security/。

注意
此功能的可用性取决于为您的帐户启用的服务配额。

“漏洞利用预防”会检测并阻止被感染进程传播和利用系统上的软件漏洞。检测到漏洞利用时，该软件可能会生成警告并停止漏洞利用活动的可疑进程。

“漏洞利用预防”仅适用于代理程序版本 12.5.23130(21.08，在 2020 年 8 月发布) 或更高版本。

默认设置：**已启用**(针对新创建的保护计划) 和**已禁用**(针对使用以前的代理程序版本创建的现有保护计划) 。

注意
Linux 不支持漏洞防御。

可以选择检测到漏洞利用时该程序应采取的措施，以及程序所采用的漏洞利用预防方法。

配置漏洞利用预防

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**漏洞利用预防**。
3. 在**检测到时的操作**部分中，选择可用选项之一：
   默认设置：**停止进程**
   - **仅通知**
     软件将生成有关涉嫌漏洞利用活动的进程的警报。
   - **停止进程**
     软件将生成警报并停止涉嫌漏洞利用活动的进程。
4. 在**已启用漏洞利用预防技术**部分中，从要应用的可用选项中选择：
   默认设置：**所有方法都已启用**
   - **内存保护**
     检测并阻止对内存页的执行权限的可疑修改。恶意进程会对页面属性进行此类修改，以便能够从非可执行内存区域（如堆栈和堆）执行壳代码。
   - **返回导向编程 (ROP) 保护**
     检测和阻止使用 ROP 漏洞利用技术的尝试。
   - **特权升级保护**
     检测并阻止未经授权的代码或应用程序尝试提升特权。恶意代码使用特权升级来获取对受攻击计算机的完全访问权限，然后执行关键而敏感的任务。未经授权的代码禁止访问关键系统资源或修改系统设置。
   - **代码注入保护**
     检测并阻止恶意代码注入到远程进程中。代码注入用于将应用程序的恶意意图隐藏在干净或良性进程之后，以逃避反恶意软件产品的检测。
5. 单击**完成**，以将选定选项应用于保护计划。

注意
将不会扫描“排除”列表中列为受信任进程的进程，以查找漏洞利用。

允许进程修改备份

仅当启用**自我保护**设置后，**允许特定进程修改备份**设置才可用。

它适用于位于本地文件夹中扩展名为 .tibx、.tib、.tia 的文件。

通过使用此设置，可以指定允许修改备份文件的进程，即使这些文件由“自我保护”提供保护。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。

如果禁用此设置，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。

如果启用此设置，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**。

实时保护

注意
此功能的可用性取决于为您的帐户启用的服务配额。

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，除非计算机用户暂停"实时保护"。

默认设置：**已启用**。

重要事项
仅当 Advanced Security 护包已启用时，此功能才可用。有关详细信息，请访问 https://www.acronis.com/zh-cn/products/cloud/cyber-protect/security/。

配置实时保护

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**实时保护**。
3. 在**检测到时的操作**下拉列表中，选择可用选项之一：
   默认设置：**隔离**
   - **仅通知**
     软件会生成有关涉嫌勒索软件活动的进程的警报。
   - **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**
4. 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。
5. 在**扫描模式**部分中，选择软件在检测到病毒或其他恶意威胁时将执行的操作：
   默认设置：**访问时智能**
   - **访问时智能** - 在访问文件进行读取或写入或者启动程序时，该功能会监视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这些文件，以确保它们未受感染并且不会对计算机或数据造成任何损害。
6. 单击**完成**。

预定扫描

手动扫描会根据指定的预定检查计算机系统以查找病毒。完整扫描会检查计算机上的所有文件，而快速扫描仅检查计算机系统文件。

配置预定扫描

默认设置：

- **自定义扫描**处于禁用状态。
- **快速** 且 **完整** 扫描已排程。

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**预定扫描**。
3. 使用该开关，可启用要应用于计算机的扫描类型。

可用的扫描类型：

- **完整** - 与“快速扫描”相比，完成“完整扫描”所需的时间更长，因为会检查每个文件。
- **快速** - 仅扫描恶意软件在计算机上通常驻留的常规区域。
- **自定义** - 检查 保护 计划的管理员已选择的文件/文件夹。

注意
可以在一个保护计划中预定所有三类扫描：**快速**、**完整**和**自定义**。

配置自定义扫描

- 使用**自定义扫描开关**，可启用或禁用此类扫描。
- 在**检测到时的操作**下拉列表中，选择可用选项之一：

默认设置：**隔离**

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。

现场	描述
使用以下事件预定任务运行	此设置定义任务将何时运行。 以下值可用： • **按时间预定** - 这是默认设置。任务将根据指定的时间运行。 • **用户登录系统时** - 默认情况下，任何用户登录都会触发任务。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，任何用户注销都会触发任务。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。
预定类型	如果在**使用以下事件预定任务运行**中选择了**按时间预定**，则该字段会显示。

现场	描述
	以下值可用： • **月** – 选择运行任务的月份和月份中的特定周或特定天。 • **每日** - 这是默认设置。选择任务将在星期几运行。 • **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。
启动时间	如果在**使用以下事件预定任务运行**中选择了**按时间预定**，则该字段会显示。 选择任务将运行的确切时间。
在日期范围内运行	如果在**使用以下事件预定任务运行**中选择了**按时间预定**，则该字段会显示。 设置配置的预定将有效的日期范围。
指定登录到操作系统将启动任务的用户帐户	如果在**使用以下事件预定任务运行**中选择了**用户登录系统时**，则该字段会显示。 以下值可用： • **任何用户** - 如果希望任何用户的登录触发任务，请使用此选项。 • **以下用户** - 如果仅希望特定用户帐户的登录触发任务，请使用此选项。
指定从操作系统注销将启动任务的用户帐户	如果在**使用以下事件预定任务运行**中选择了**用户注销系统时**，则该字段会显示。 以下值可用： • **任何用户** - 如果希望任何用户的注销触发任务，请使用此选项。 • **以下用户** - 如果仅希望特定用户帐户的注销触发任务，请使用此选项。
开始条件	定义为了任务能够运行而必须同时满足的所有条件。 防恶意软件扫描的开始条件类似于“开始条件”中所述的**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 10:00 点，延迟时间为 60 分钟，则任务将在上午 10:00 点到上午 11:00 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。

- 如果要仅扫描新创建和修改的文件，请选中**仅扫描新文件和已更改的文件**复选框。

默认设置：**已启用**

- 为**自定义扫描**显示的其他两个选项仅适用于**完整扫描**:

1. **扫描存档文件**

   默认设置:**已启用**。

   最大递归深度

   默认设置:**16**

   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。

   最大大小

   默认设置:**100**

   要扫描的存档文件的最大大小。

2. **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**(如数码笔和外部硬盘驱动器)
- **CD/DVD**

注意
Linux 不支持扫描可移动驱动器。

保护排除

当受信任的程序被视为勒索软件或恶意软件时,保护排除使您能够消除误报。可以通过将受信任和阻止的项目添加到保护排除列表中来定义它们。

在受信任的项目列表中,可以添加文件、进程和文件夹,以认为它们在系统中是安全的,防止将来对它们进行任何检测。

在阻止的项目列表中,可以添加进程和哈希。此选项确保这些进程将被阻止,并且您的工作负载将是安全的。

保护排除项目	已阻止	受信任
哈希	将哈希添加到被阻止列表中后,系统将根据提供的哈希停止进程。 例如,添加 MD5 哈希 938c2cc0dcc05f2b68c4287040cfcf71 后,系统将阻止与该哈希关联的进程。	将哈希添加到受信任列表中后,系统将根据提供的哈希知道哪些进程必须被监视忽略。 例如,添加 MD5 哈希 938c2cc0dcc05f2b68c4287040cfcf71 后,系

保护排除项目	已阻止	受信任
		统将信任并排除监视与该哈希关联的进程。
进程	将进程添加到被阻止列表中后，系统将知道必须监视这些进程，并将始终阻止这些进程。 例如，如果将路径 C:\Users\user1\application\nppInstaller.exe 添加到被阻止列表中，系统将阻止此特定进程；当尝试打开此进程时，系统将不会允许启动它。	将进程添加到受信任列表中后，系统将知道必须排除监视这些进程。 **注意** 始终信任由 Microsoft 签名的进程。 例如，如果添加路径 C:\Users\user1\application\nppInstaller.exe，系统将排除监视此特定进程，并且防病毒不会干扰此进程。
文件/文件夹		将文件或文件夹添加到受信任列表中后，系统将知道应始终将这些文件或文件夹认为是安全的，无需扫描/监视这些文件或文件夹。

指定将始终受信任的项目

1. 打开保护计划。
2. 展开**防病毒和防恶意软件保护**模块。
3. 选择**排除**选项。
   保护排除窗口即会打开。
4. 在**受信任的项目**部分中，单击**添加**以从可用选项中选择：
   - 要信任文件、文件夹或进程，请选择**文件/文件夹/进程**选项。**添加文件/文件夹/进程**窗口即会打开。
     - 在**文件/进程/文件夹**字段中，在新行中输入每个进程、文件夹或文件的路径。在**描述**部分中，输入简短描述，以便可以识别受信任的项目列表中的更改。
     - 选中**添加为文件/文件夹**复选框，以信任文件/文件夹。
       文件夹描述示例：D:\folder\, /home/Folder/folder2, F:\
     - 选中**添加为进程**复选框，以信任进程。选定的进程将排除监视。

       注意
       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`。

注意
支持本地网络路径。例如：\\localhost\folderpath\file.exe

- 选择**哈希**选项，以将 MD5 哈希添加到受信任的项目列表中。**添加哈希**窗口即会打开。
  - 在此处，可以在单独行中插入 MD5 哈希，以将其作为受信任的哈希包含在保护排除列表中。基于这些哈希，Cyber Protection 会将 MD5 哈希所述的进程排除监视。

默认设置：默认情况下，不会定义任何例外。

指定将始终被阻止的项目

1. 打开保护计划。
2. 展开**防病毒和防恶意软件保护**模块。
3. 选择**保护排除**选项。**保护排除**窗口即会打开。

在**阻止的项目**部分中，单击**添加**以从可用选项中选择：

- 要阻止进程，请选择**进程**选项。**添加进程**窗口即会打开。
  - 在**进程**字段中，在新行中输入每个进程的路径。在**描述**字段中，输入简短描述，以便可以识别阻止的项目列表中的更改。

注意
只要在计算机上启用 Active Protection，这些进程就无法启动。

- 要阻止哈希，请选择**哈希**选项。**添加哈希**窗口即会显示。
  - 在**哈希**字段中，在新行中输入每个进程的哈希。在**描述**字段中，输入简短描述，以便可以识别阻止的项目列表中的更改。

默认设置：默认情况下，不会定义任何例外。

通配符

要指定文件夹，可以使用通配符 * 和 ?。星号 (*) 可替代零个或多个字符。问号 (?)只能替代一个字符。不能使用环境变量，例如 `%AppData%`。

可以使用通配符 (*) 来将项目添加到排除列表中。

- 通配符可以用在描述的中间或结尾。

描述中接受的通配符示例：

C:*.pdf

D:\folders\file.*

C:\Users*\AppData\Roaming

- 通配符不能用在描述的开头。

描述中不接受的通配符示例：

*.docx

*:\folder\

变量

还可以使用变量将项目添加到保护排除列表中，但有以下限制：

- 对于 Windows，仅支持 SYSTEM 变量。不支持用户特定的变量，例如，%USERNAME%、%APPDATA%。不支持 {username} 的变量。有关详细信息，请参阅 https://ss64.com/nt/syntax-variables.html。
- 对于 macOS，不支持环境变量。
- 对于 Linux，不支持环境变量。

支持的格式示例：

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

描述

可以使用**描述**字段来记录您在保护排除列表中添加的排除。有关您可以做记录的一些建议：

- 排除的原因和目的。
- 哈希排除的实际文件名。
- 时间戳。

如果在一个条目中添加了多个项目，则针对多个项目只能捕获 1 条评论。

Cyber Backup Standard 版中的 Active Protection

在 Cyber Backup Standard 版中，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。

在所有其他版本的网络安全保护服务中，Active Protection 是保护计划的**防病毒和防恶意软件**模块的一部分。

默认设置：**已启用**。

注意
必须在受保护的计算机上安装保护代理程序。有关受支持操作系统和功能的详细信息，请参阅 "支持的防病毒和防恶意软件保护操作系统"(第 728 页)。

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，并执行保护计划中所指定的其他操作。

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。

Cyber Backup Standard 中的 Active Protection 设置

在 Cyber Backup Standard 版中，可以配置以下 Active Protection 功能：

- 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

注意
适用于 Linux 的 Active Protection 支持以下设置：对检测、网络文件夹保护和排除的操作。网络文件夹保护始终处于启用状态，并且不可配置。

对检测的操作

在**检测到时的操作**部分中，选择可用选项之一：

- **仅通知**
  软件将生成有关涉嫌勒索软件活动的进程的警报。
- **停止进程**
  软件将生成警报并停止涉嫌勒索软件活动的进程。
- **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**

“自我保护”会阻止未经授权更改软件的自身进程、注册表记录、可执行文件和配置文件、以及位于本地文件夹中的备份。

管理员可以启用**自我保护**，而无需启用 **Active Protection**。

默认设置：**开启**。

注意
Linux 不支持自我保护。

启用自我保护

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**自我保护**。
3. 使用**自我保护**开关以启用它。

启用密码保护

1. 在**自我保护**功能已启用后，可以使用开关启用**密码保护**功能。
2. 单击**生成新密码**，以生成用于修改或删除本地代理程序的密码。
3. 单击**复制**，然后将其粘贴到安全位置，因为当您要在本地修改组件列表时，将要求输入该密码。

   重要事项
   在关闭窗口后，该密码将不可用。要将此密码应用到设备，必须保存保护计划设置。

4. 单击**关闭**。

密码保护会阻止未经授权用户或软件卸载适用于 Windows 的代理程序或修改其组件。这些操作只能使用管理员可以提供的密码才能执行。

以下操作不再需要密码：

- 通过本地运行安装程序来更新安装
- 通过使用 Cyber Protect 中控台来更新安装
- 修复安装

默认设置：**已禁用**

有关如何启用**密码保护**的详细信息，请参阅阻止未经授权卸载或修改代理程序。

网络文件夹保护

保护映射为本地驱动器的网络文件夹设置定义 Active Protection 是否会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。

此设置适用于通过 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。而是将其保存到在此设置中指定的文件夹。默认文件夹为 `C:\ProgramData\Acronis\Restored Network Files`（对于 Windows）和 `Library/Application Support/Acronis/Restored Network Files/`（对于 macOS）。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：**开启**。

此功能定义 Active Protection 是否会保护网络文件夹，此类文件夹由您从网络中可能会带来威胁的其他服务器的外部传入连接共享。

默认设置：**关闭**。

注意
Linux 不支持服务器端保护。

设置受信任的连接

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**服务器端保护**。
3. 使用**服务器端保护**开关以启用它。
4. 选择**受信任**选项卡。
5. 在**受信任的连接**字段中，单击**添加**以定义将允许修改数据的连接。
6. 在**计算机名称/帐户**字段中，键入计算机的名称和装有保护代理程序的计算机的帐户。例如，`MyComputer\TestUser`。
7. 在**主机名**字段中，键入允许使用保护代理程序连接到计算机的计算机的主机名。
8. 单击右侧的复选标记保存连接定义。
9. 单击**完成**。

设置阻止的连接

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**服务器端保护**。
3. 使用**服务器端保护**开关以启用它。
4. 选择**已阻止**选项卡。
5. 在**阻止的连接**字段中，单击**添加**以定义将不允许修改数据的连接。
6. 在**计算机名称/帐户**字段中，键入计算机的名称和装有保护代理程序的计算机的帐户。例如，`MyComputer\TestUser`。
7. 在**主机名**字段中，键入允许使用保护代理程序连接到计算机的计算机的主机名。
8. 选中右侧的复选框以保存连接定义。
9. 单击**完成**。

加密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，甚至可能因滥用而导致硬件损坏。**Cryptomining 进程检测**功能保护设备免受加密挖矿恶意软件影响，以防止未经许可使用计算机资源。

管理员可以启用 **Cryptomining 进程检测**，而无需启用 **Active Protection**。默认设置：**已启用**。

注意
Linux 不支持 Cryptomining 进程检测。

配置网络文件夹保护

1. 在**创建保护计划**窗口中，展开**防病毒和防恶意软件保护**模块。
2. 单击**Cryptomining 进程检测**。
3. 使用**检测加密挖矿进程**开关，可启用或禁用该功能。
4. 选择如何处理涉嫌加密挖矿活动的进程：
   默认设置：**停止进程**
   - **仅通知** - 软件将生成警报。
   - **停止进程** - 软件将生成警报并停止进程。
5. 单击**完成**，以将选定选项应用于保护计划。

当受信任的程序被视为勒索软件或恶意软件时，保护排除使您能够消除误报。可以通过将受信任和阻止的项目添加到保护排除列表中来定义它们。

在受信任的项目列表中，可以添加文件、进程和文件夹，以认为它们在系统中是安全的，防止将来对它们进行任何检测。

在阻止的项目列表中，可以添加进程和哈希。此选项确保这些进程将被阻止，并且您的工作负载将是安全的。

保护排除项目	已阻止	受信任
哈希	将哈希添加到被阻止列表中后，系统将根据提供的哈希停止进程。 例如，添加 MD5 哈希 938c2cc0dcc05f2b68c4287040cfcf71 后，系统将阻止与该哈希关联的进程。	将哈希添加到受信任列表中后，系统将根据提供的哈希知道哪些进程必须被监视忽略。 例如，添加 MD5 哈希 938c2cc0dcc05f2b68c4287040cfcf71 后，系统将信任并排除监视与该哈希关联的进程。
进程	将进程添加到被阻止列表中后，系统将知道必须监视这些进程，并将始终阻止这些进程。 例如，如果将路径 C:\Users\user1\application\nppInstaller.exe 添加到被阻止列表中，系统将阻止此特定进程；当尝试打开此进程时，系统将不会允许启动它。	将进程添加到受信任列表中后，系统将知道必须排除监视这些进程。 **注意** 始终信任由 Microsoft 签名的进程。 例如，如果添加路径 C:\Users\user1\application\nppInstaller.exe，系统将排除监视此特定进程，并且防病毒不会干扰此进程。
文件/文件夹		将文件或文件夹添加到受信任列表中后，系统将知道应始终将这些文件或文件夹认为是安全的，无需扫描/监视这些文件或文件夹。

指定将始终受信任的项目

1. 打开保护计划。
2. 展开**防病毒和防恶意软件保护**模块。
3. 选择**排除**选项。
   保护排除窗口即会打开。

4. 在**受信任的项目**部分中，单击**添加**以从可用选项中选择：
   - 要信任文件、文件夹或进程，请选择**文件/文件夹/进程**选项。**添加文件/文件夹/进程**窗口即会打开。
     - 在**文件/进程/文件夹**字段中，在新行中输入每个进程、文件夹或文件的路径。在**描述**部分中，输入简短描述，以便可以识别受信任的项目列表中的更改。
     - 选中**添加为文件/文件夹**复选框，以信任文件/文件夹。
       文件夹描述示例：D:\folder\, /home/Folder/folder2, F:\
     - 选中**添加为进程**复选框，以信任进程。选定的进程将排除监视。

       注意
       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`。

       注意
       支持本地网络路径。例如：\\localhost\folderpath\file.exe
   - 选择**哈希**选项，以将 MD5 哈希添加到受信任的项目列表中。**添加哈希**窗口即会打开。
     - 在此处，可以在单独行中插入 MD5 哈希，以将其作为受信任的哈希包含在保护排除列表中。基于这些哈希，Cyber Protection 会将 MD5 哈希所述的进程排除监视。

默认设置：默认情况下，不会定义任何例外。

指定将始终被阻止的项目

1. 打开保护计划。
2. 展开**防病毒和防恶意软件保护**模块。
3. 选择**保护排除**选项。**保护排除**窗口即会打开。

   在**阻止的项目**部分中，单击**添加**以从可用选项中选择：
   - 要阻止进程，请选择**进程**选项。**添加进程**窗口即会打开。
     - 在**进程**字段中，在新行中输入每个进程的路径。在**描述**字段中，输入简短描述，以便可以识别阻止的项目列表中的更改。

       注意
       只要在计算机上启用 Active Protection，这些进程就无法启动。
   - 要阻止哈希，请选择**哈希**选项。**添加哈希**窗口即会显示。
     - 在**哈希**字段中，在新行中输入每个进程的哈希。在**描述**字段中，输入简短描述，以便可以识别阻止的项目列表中的更改。

默认设置：默认情况下，不会定义任何例外。

通配符

要指定文件夹，可以使用通配符 * 和 ?。星号 (*) 可替代零个或多个字符。问号 (?)只能替代一个字符。不能使用环境变量，例如 `%AppData%`。

可以使用通配符 (*) 来将项目添加到排除列表中。

- 通配符可以用在描述的中间或结尾。

描述中接受的通配符示例：

C:*.pdf

D:\folders\file.*

C:\Users*\AppData\Roaming

- 通配符不能用在描述的开头。

描述中不接受的通配符示例：

*.docx

*:\folder\

变量

还可以使用变量将项目添加到保护排除列表中，但有以下限制：

- 对于 Windows，仅支持 SYSTEM 变量。不支持用户特定的变量，例如，%USERNAME%、%APPDATA%。不支持 {username} 的变量。有关详细信息，请参阅 https://ss64.com/nt/syntax-variables.html。
- 对于 macOS，不支持环境变量。
- 对于 Linux，不支持环境变量。

支持的格式示例：

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

描述

可以使用**描述**字段来记录您在保护排除列表中添加的排除。有关您可以做记录的一些建议：

- 排除的原因和目的。
- 哈希排除的实际文件名。
- 时间戳。

如果在一个条目中添加了多个项目，则针对多个项目只能捕获 1 条评论。

URL 过滤

注意
此功能的可用性取决于为您的帐户启用的服务配额。

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。可以通过阻止用户访问可能含有恶意内容的网站来保护组织。

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。可以根据与网站相关的类别来配置对网站的访问。URL 过滤当前支持 44 个网站类别并允许管理对它们的访问。

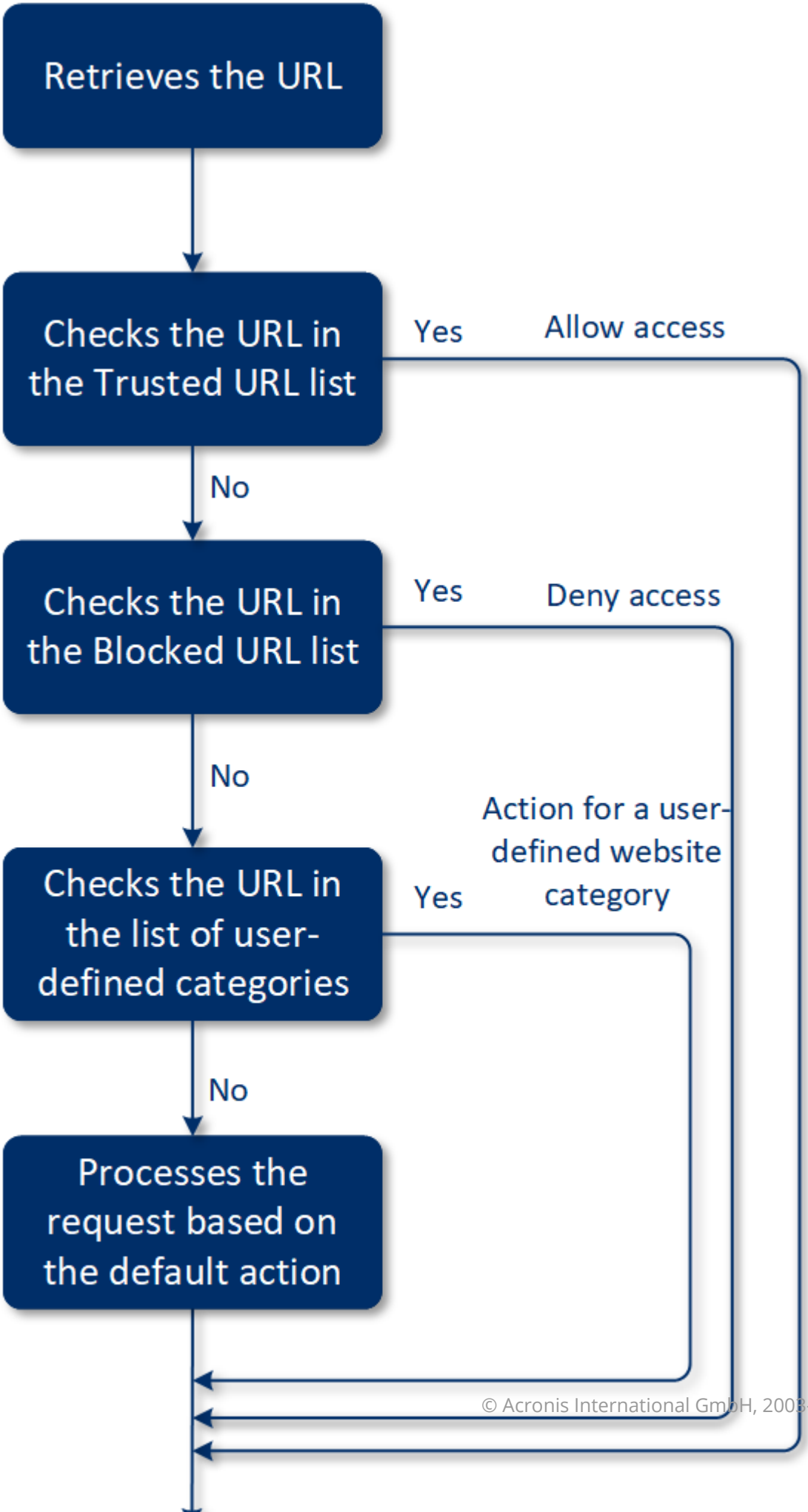
当前，Windows 计算机上的 HTTP/HTTPS 连接将由保护代理程序进行检查。

URL 过滤功能需要连接 Internet，才能起作用。

注意
为了防止可能与保护代理程序版本 15.0.26692(C21.03 HF1 版) 及更早版本出现兼容性问题，将在以下情况下自动禁用 URL 过滤功能：如果检测到另一个防病毒解决方案，或 Windows Security Center 服务不存在于系统上。
在将来版本的保护代理程序中，将解决兼容性问题，以便始终根据策略启用 URL 过滤。

工作方式

用户在浏览器中输入 URL 链接。拦截器获取链接，并将它发送到保护代理程序。代理程序获取 URL、对其进行解析，然后检查判决。拦截器将用户重定向到带有消息的页面，该消息中提供的操作可用于手动访问请求的页面。

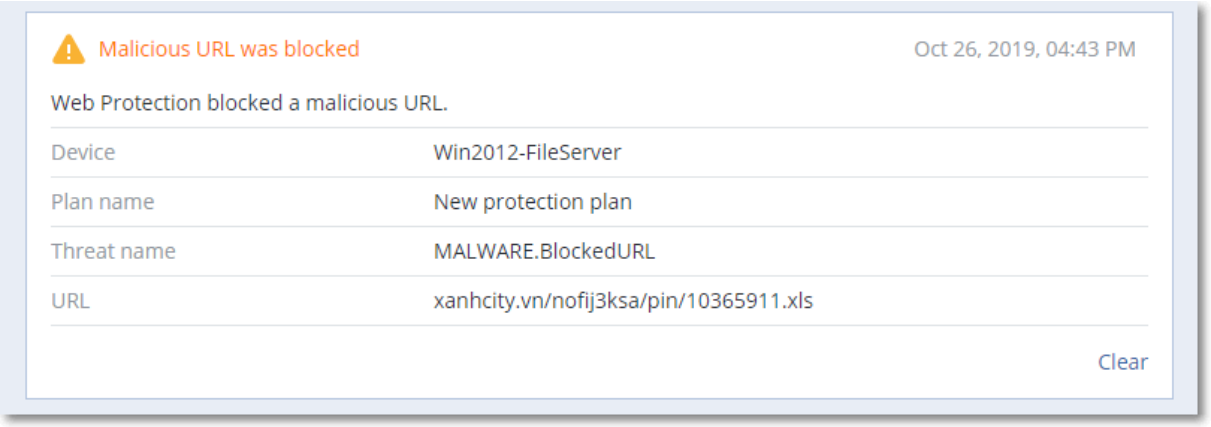


URL 过滤配置工作流程

通常，URL 过滤配置包括以下步骤：

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**监控** > **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：

- **仅通知** - 软件生成有关涉嫌勒索软件活动的进程的警报。
- **阻止** - 阻止访问恶意网站。用户将无法访问该网站，并且会生成警告警报。
- **始终询问用户** - 询问用户是继续访问该网站还是返回。

要过滤的类别

有 44 个可以配置访问的网站类别：

- **允许** - 允许访问与选定类别相关的网站。
- **拒绝** - 拒绝访问与选定类别相关的网站。

默认情况下，允许所有类别。

按类别显示被阻止 URL 的所有通知 - 如果启用，您将在任务栏中获得按类别显示的被阻止 URL 的所有通知。如果某个网站有多个子域，则系统还会为它们生成通知，因此通知的数量可能很多。

在下表中，可以找到类别说明：

	网站类别	描述
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	**通俗小报**	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。

URL 排除

可以将已知安全的 URL 添加到受信任的域列表中。可以将构成威胁的 URL 添加到阻止的域列表中。

指定将始终受信任或被阻止的 URL

1. 在保护计划的 URL 过滤模块中，单击 **URL 排除**。
   URL 排除窗口即会打开。
   以下选项会显示：

受信任的项目 - 单击**添加**以从可用选项中选择：

- **域** - 当选择此选项时，**添加域**窗口即会显示。
  - 在**域**字段中，在新行中输入每个域。在**描述**字段中，输入简短描述，以便可以识别受信任的项目列表中的更改。
- **进程** - 当选择此选项时，**添加进程**窗口即会显示。
  - 在**进程**字段中，在新行中输入每个进程的路径。在**描述**部分中，输入简短描述，以便可以识别受信任的项目列表中的更改。

阻止的项目 - 单击**添加**。**添加域**窗口即会显示。

在**域**字段中，在新行中输入每个域。在**描述**字段中，输入简短描述，以便可以识别阻止的项目列表中的更改。

> **注意**
> 支持本地网络路径。例如，\\localhost\folderpath\file.exe。

描述

可以使用**描述**字段，来记录您在 URL 排除列表中添加的排除。有关您可以做记录的一些建议：

- 排除的原因和目的。
- 时间戳。

如果在一个条目中添加了多个项目，则针对多个项目只能捕获 1 条评论。

Microsoft Defender Antivirus 和 Microsoft Security Essentials

注意
此功能的可用性取决于为您的帐户启用的服务配额。

Microsoft Defender Antivirus

Microsoft Defender Antivirus 是 Microsoft Windows 的一个内置反恶意软件组件，从 Windows 8 开始提供。

Microsoft Defender Antivirus (WDA) 模块让您可以配置 Microsoft Defender Antivirus 安全策略，并通过 Cyber Protect 中控台跟踪其状态。

该模块适用于安装有 Microsoft Defender Antivirus 的工作负载。

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 Cyber Protect 中控台跟踪其状态。

该模块适用于安装有 Microsoft Security Essentials 的工作负载。

Microsoft Security Essentials 的设置与 Microsoft Defender Antivirus 的设置相似，但无法配置实时保护，也无法通过 Cyber Protect 中控台定义排除。

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 Microsoft Defender Antivirus 的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** - 清除工作负载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** - 从工作负载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 Microsoft Defender Antivirus 的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工作负载上安装或运行。

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 Microsoft Defender Antivirus 的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#real-time-protection-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 WDA 用户界面将不会提供给用户使用。可以通过 Cyber Protect 中控台管理 WDA 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 Microsoft Defender Antivirus 的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 Microsoft Defender Antivirus 的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

防火墙管理

注意
此功能的可用性取决于为您的帐户启用的服务配额。

防火墙管理允许您轻松配置受保护工作负载上的防火墙设置。

Cyber Protect 中的此功能是通过 Microsoft Windows 的内置 Microsoft Defender 防火墙组件提供的。Microsoft Defender 防火墙会阻止未经授权的网络流量流入/流出工作负载。

防火墙管理适用于安装有 Microsoft Defender 防火墙的工作负载。

支持的 Windows 操作系统

防火墙管理支持以下 Windows 操作系统：

Windows

- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

不支持 Windows Server。

启用和禁用防火墙管理

当创建保护计划时，可以启用防火墙管理。可以更改现有保护计划以启用或禁用防火墙管理。

启用或禁用防火墙管理

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 执行以下任一操作以打开保护计划面板：
   - 如果想要创建新的保护计划，请选择要保护的计算机、单击**保护**，然后单击**创建计划**。
   - 如果想要更改现有保护计划，请选择受保护的计算机、单击**保护**、单击保护计划名称旁边的省略号 (...)，然后单击**编辑**。
3. 在保护计划面板中，导航到**防火墙管理**区域，然后启用或禁用**防火墙管理**。
4. 执行以下任一操作以应用更改：
   - 如果创建保护计划，请单击**创建**。
   - 如果编辑保护计划，请单击**保存**。

保护计划面板的**防火墙管理**区域中的 **Microsoft Defender 防火墙状态**显示为**打开**或**关闭**，具体取决于您是启用还是禁用了防火墙管理。

还可以从"管理"选项卡访问保护计划面板。但是，此功能在 Cyber Protection 服务的所有版本中不可用。

隔离

隔离区是受保护设备的硬盘上的一个特殊的隔离文件夹。如果防病毒和防恶意软件保护检测到任何可疑文件，这些文件将被移至隔离区，以防止威胁的进一步传播。

在**隔离区**选项卡的 Cyber Protection 中控台，可以查看所有受保护设备中的可疑和潜在危险的文件，并决定是否要删除或还原它们。

注意
如果从环境中移除设备，则将自动移除隔离的文件。

文件如何进入隔离文件夹?

1. 在保护计划中，选择**隔离**作为针对感染或可疑文件的默认操作。
   若要了解如何创建保护计划，请参阅 "创建保护计划"(第 192 页)。
2. 在扫描时，防病毒和防恶意软件保护模块会检测恶意文件，并将其移至安全的隔离文件夹。
3. 该模块会更新隔离列表以添加有关移动到隔离区的文件的信息。

注意
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删除。请参阅 "隔离设置"(第 736 页)。

管理隔离的文件

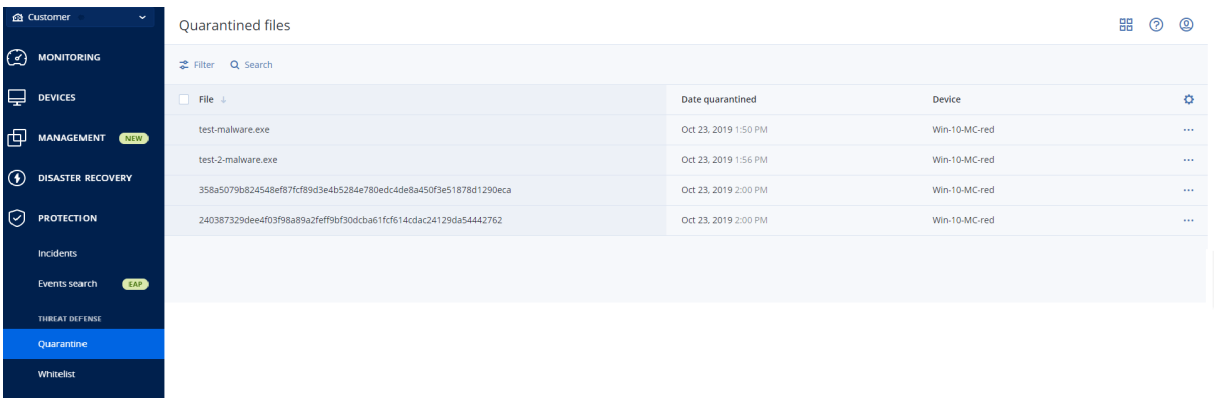
若要管理隔离的文件，请转至**保护>隔离**。所有受保护设备的隔离文件列表包含以下信息。

名称	描述
文件	隔离文件的名称。
隔离日期	文件移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	将可疑文件移入隔离区所依据的保护计划。

可以对隔离的文件执行以下操作：

- **删除** - 从所有计算机中永久删除隔离的文件。可以删除文件哈希相同的所有文件。可以恢复文件哈希相同的所有文件。按哈希分组文件、选择所需文件，然后将这些文件删除。
- **还原** - 将隔离的文件无任何修改地还原到其原始位置。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。

  注意
  还原的文件将被添加到允许列表，并在进一步反恶意软件扫描过程中被跳过。



计算机上的隔离区位置

以下是每个操作系统的隔离文件的默认位置列表。

- 对于 Windows 计算机：`%programdata%\Acronis\NGMP\quarantine`
- 对于 Mac 计算机：`/Library/Application Support/Acronis/NGMP/quarantine`
- 对于 Linux 计算机：`/var/lib/Acronis/NGMP/quarantine`

隔离区存储由服务提供商的自我防御保护提供保护。

自助服务按需自定义文件夹

可以选择工作负载上的自定义文件夹，并直接从上下文菜单扫描它们。

使用上下文菜单中的 Cyber Protect 选项访问扫描

对于保护计划中启用了防病毒和防恶意软件的工作负载，请右键单击要扫描的文件/文件夹。

注意
此选项仅适用于工作负载的管理员。

公司白名单

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。

注意
公司白名单不会影响对备份执行防恶意软件扫描。

Cyber Protection 可以自动执行此过程：防病毒和防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防恶意软件扫描性能。

白名单是针对每个客户创建的，并且仅基于该客户的数据。

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。

注意
仅具有管理员角色的帐户（例如，Cyber Protection 管理员；公司管理员；代表公司管理员行事的合作伙伴管理员；单位管理员）才能配置和管理白名单。此功能不适用于只读管理员帐户或用户帐户。

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 Cyber Protect 中控台中，转到**防恶意软件保护 > 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 Cyber Protect 中控台中，转到**防恶意软件保护 > 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**
  公司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

在对备份执行防恶意软件扫描后，可以通过检查备份是否没有恶意软件来防止恢复被感染的文件。防恶意软件扫描将由位于 Cyber Protection 数据中心中的云代理程序执行，不会使用本地计算资源。

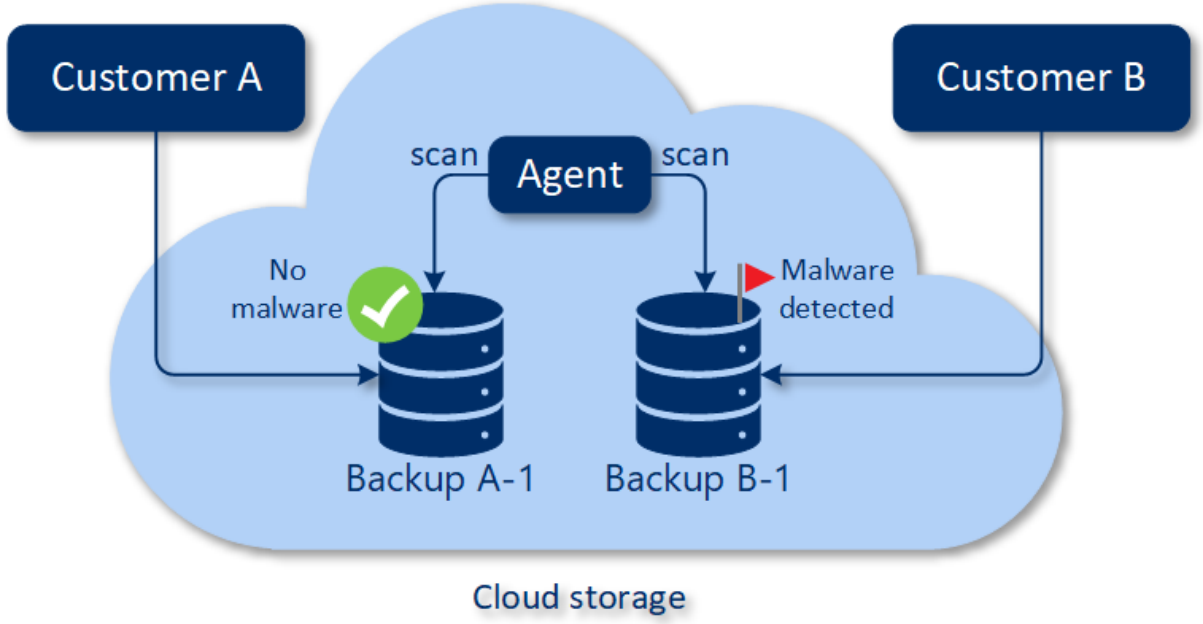
注意
此功能的可用性取决于为您的帐户启用的服务配额。

要执行防恶意软件扫描，需要配置备份扫描计划。有关如何执行此操作的详细信息，请参阅 "备份扫描计划"(第 211 页)。

每个备份扫描计划都会为云代理程序创建扫描任务，并将该任务添加到队列中(即每个数据中心一个)。扫描任务将根据其在队列中的顺序进行处理。此外，扫描所需时间取决于备份大小。这就是创建备份扫描计划和完成扫描之间存在延迟的原因。

选择进行扫描的备份可能处于以下状态之一：

- 未扫描
- 无恶意软件
- 检测到恶意软件



可以在**备份扫描详细信息(威胁)**小组件中，检查备份扫描的结果。可以在 Cyber Protect 中控台中的**监控** > **概述**选项卡上找到它。

限制

- 支持针对以下工作负载的**整台计算机**或**磁盘/卷**备份执行防恶意软件扫描：
  - 已安装保护代理程序的 Windows 计算机。
  - 由适用于 Hyper-V 的代理程序和适用于 VMware 的代理程序 (Windows) 在虚拟机监控程序级别(无代理程序备份)上备份的 Windows 虚拟机。

  不支持针对由虚拟设备(如适用于 VMware 的代理程序(虚拟设备)、适用于 Virtuozzo 的代理程序、适用于 Scale Computing HC3 的代理程序、Agent for Azure 和适用于 oVirt 的代理程序)创建的备份执行防恶意软件扫描。

- 将仅扫描文件系统为 NTFS 且有 GPT 或 MBR 分区的卷。
- 仅支持默认云存储作为备份位置。不支持本地存储和合作伙伴拥有的云存储。
- 合规模式的租户不支持防恶意软件扫描。
- 当选择要扫描的备份时，可以选择包含持续数据保护 (CDP) 备份的备份集。但是，仅会扫描这些备份集中的非 CDP 备份。有关 CDP 备份的详细信息，请参阅 "连续数据保护 (CDP)"(第 364 页)。
- 当对整台计算机执行安全恢复时，可以选择包含 CDP 备份的备份集。但是，此恢复操作不会使用 CDP 备份中的数据。要恢复 CDP 数据，请另外运行**文件/文件夹**恢复操作。

使用高级保护功能

默认情况下，Cyber Protect 包含涵盖大多数网络安全威胁的功能。可以免费使用这些功能。此外，还可以启用高级功能来增强对工作负载的保护。

- 如果高级保护功能可供您使用，则它会显示在保护计划中并标有高级功能图标  。
- 如果您无法使用高级保护功能，请联系您的管理员以启用所需的高级保护包。
- 如果管理员允许您购买额外的安全包，则您可以选择启用高级功能。一条消息将提示您进入屏幕，以告知您需要额外计费。

注意
如果至少一个功能已启用，则必须购买相应的高级保护包。

注意
如果所有高级功能在您的保护计划中都处于禁用状态，则将禁用相应高级保护包。

高级保护包	高级保护功能
Advanced Backup	持续保护您的工作负载，并确保即使是最后一刻的工作更改也不会丢失。特点包括： • 单击恢复 • 连续数据保护 • Microsoft SQL Server 集群和 Microsoft Exchange 集群的备份支持 - Always On 可用性组 (AAG) 和数据库可用性组 (DAG) • MariaDB、MySQL、Oracle DB 和 SAP HANA 的备份支持 • 数据保护地图和合规性报告 • 脱离主机数据处理 • Microsoft 365 和 Google Workspace 工作负载的备份频率 • 通过可启动媒体进行的远程操作 • 直接备份至 Microsoft Azure、Amazon S3 和 Wasabi 公共云存储
Advanced Security + XDR	Advanced Security + XDR 套餐由 "Extended Detection and Response (XDR)"(第 861 页)、"Endpoint Detection and Response (EDR)"(第 792 页) 和 受控检测与响应 (MDR) 组成，可持续保护您的工作负载免受所有恶意软件威胁。功能包括： • 与 Perception Point、Microsoft 365 协作应用程序和 Microsoft Entra ID 等第三方解决方案的集成 • 在集中式事件页面中管理事件 • 可视化事件的范围和影响 • 建议和补救措施 • 使用威胁源检查对您工作负载的公开披露的攻击 • 将安全事件存储 180 天 • 基于本地签名检测的防病毒和反恶意软件保护(有实时保护) • 漏洞利用预防 • URL 过滤

	• 终端防火墙管理 • 取证备份、扫描备份以查找恶意软件、安全恢复、企业允许列表 • 智能保护计划(与 CPOC 警报集成) • 集中式备份扫描恶意软件 • 远程擦除 • Microsoft Defender Antivirus • Microsoft Security Essentials
Advanced Management	允许您修补受保护工作负载上的漏洞。特点包括: • 修补程序管理 • 磁盘运行状况 • 软件库存记录 • 故障安全修补 • 网络安全脚本 • 远程协助 • 文件传输和共享 • 选择要连接的会话 • 在多视图中观察工作负载 • 连接模式:控制、仅查看和隔离 • 通过“Quick Assist”应用程序连接 • 远程连接协议:NEAR 和 Apple 屏幕共享 • NEAR 连接的会话记录 • 屏幕截图传输 • 会话历史记录报告 • 24 个监视器 • 基于阈值的监视 • 基于异常的监视 • 远程软件部署
Advanced Data Loss Prevention	防止受保护工作负载中的敏感信息泄露。特点包括: • 内容感知预防工作负载通过外围设备和网络通信丢失数据 • 预建自动检测个人身份信息 (PII)、受保护的运行状况信息 (PHI) 和支付卡行业数据安全标准 (PCI DSS) 数据以及“标记为机密”类别中的文档 • 通过可选的最终用户帮助自动创建数据丢失预防策略 • 通过基于学习的自动策略调整实现自适应数据丢失预防 • 基于云的集中式审核日志记录、警报和最终用户通知

Advanced Data Loss Prevention

Advanced Data Loss Prevention 模块会分析受保护工作负载上数据传输的内容和上下文,并根据数据流策略防止敏感数据通过外围设备或公司网络内外的网络传输泄漏。

如果为此客户启用了保护服务和 Advanced Data Loss Prevention 包,则 Advanced Data Loss Prevention 功能可以包含在客户租户的任何保护计划中。

在开始使用 Advanced Data Loss Prevention 模块之前，请确认您已阅读并理解基础指南中所述的 Advanced DLP 管理的基本概念和逻辑。

您可能还想要查看技术规范文档。

创建数据流策略和策略规则

数据丢失防护的关键原则要求公司 IT 系统的用户只允许在履行其工作职责所需的范围内处理敏感数据。应阻止任何其他与业务流程无关的敏感数据传输。因此，区分业务相关数据传输或数据流与流氓数据传输或数据流是至关重要的。

数据流策略包含指定允许哪些数据流和禁止哪些数据流的规则，从而在保护计划中已启用数据丢失防护模块并在“执行”模式下运行时可阻止未经授权传输敏感信息。

策略中的每个敏感度类别都包含一个标有星号 (*) 的默认规则，以及一个或多个用于定义特定用户或组的数据流的明确（非默认）规则。阅读基础指南中有关策略规则类型的详细信息。

数据流策略通常是在 Advanced Data Loss Prevention 处于“观察”模式下运行时自动创建的。构建具有代表性的数据流策略所需的时间大约为 1 个月，但可能会有所不同，具体取决于贵组织中的业务流程。数据流策略也可以由公司或部门管理员手动创建、配置或编辑。

开始自动创建数据流策略

1. 以管理员身份登录到 Cyber Protect 中控台。
2. 导航到**管理** > **保护计划**。
3. 单击**创建计划**。
4. 展开**数据丢失防护**部分，并单击**模式**行。
5. 在“模式”对话框中，选择**观察模式**，然后选择处理数据传输的方式：

选项	描述
全部允许	所有来自用户工作负载的敏感数据传输都会被视为业务流程所必需的并且是安全的。将为每个检测到的与策略中已定义规则不匹配的数据流创建一个新规则。
全部正当	所有来自用户工作负载的敏感数据传输都会被视为业务流程所必需的，但存在风险。因此，对于每一次向组织内外的任何接收者或目的地传输敏感数据但遭拦截的传输（不匹配先前创建的数据流规则），用户都必须提供一次性业务正当理由。提交正当理由时，将会在数据流策略中创建一个新的数据流规则。
混合	“全部允许”逻辑适用于所有内部敏感数据流，而“全部正当”逻辑适用于所有外部数据流。 **注意** 有关内部和外部数据的详细信息，请参阅自动检测目的地

6. 保存保护计划并将其应用于要从中收集数据以构建策略的工作负载。

注意
在观察模式下，无法阻止数据泄露。

手动配置数据流策略

1. 在 Cyber Protect 中控台中，导航到**保护** > **数据流策略**。
2. 单击**新数据流规则**。
   “新数据流规则”窗格会在右侧展开。
3. 选择敏感度类别，添加发送者和接收者，并为选定类别、发送者和接收者定义数据传输权限。

选项	描述
允许	允许该发送者将此敏感度类别的数据发送给此接收者。
例外	不允许该发送者将此敏感度类别的数据传输给此接收者，但允许发送者针对特定传输提交规则例外。 当该发送者尝试将此敏感度类别的数据传输给此接收者时，将会阻止该传输并要求发送者提交例外以允许该传输。提交例外后，将允许数据传输继续进行。 **重要事项** 在提交例外后，在该发送者和接收者之间将允许此敏感度类别的所有后续数据传输进行五分钟。
拒绝	不允许该发送者将此敏感度类别的数据传输给此接收者，也不允许发送者请求规则例外。

4. (可选) 选择触发规则时应执行的操作。

操作	描述
写入日志	触发规则时，将事件记录存储在审核日志中。建议您为具有**例外**权限的规则选择此操作。
生成警报	触发规则时，将在 Cyber Protect **警告**选项卡中生成警报。如果为管理员启用通知，还会发送电子邮件通知。
当数据传输被拒绝时通知最终用户	当数据传输触发规则时，将通过屏幕警告实时通知用户。

5. 单击**保存**。
6. 重复步骤 2 到 5 以创建不同敏感度类别和选项的多个规则，并验证生成的规则是否与您选择的选项相对应。

数据流策略结构

在**数据流策略**视图中，策略规则会根据它们所控制的敏感数据类别进行分组。敏感度类别标识符会显示在策略规则组的正上方。

- 敏感
  - 受保护的运行状况信息(PHI)
  - 个人身份信息(PII)
  - 支付卡行业数据安全标准 (PCI DSS),
  - 标记为机密
- 不敏感

有关数据流策略概念和功能的详细信息，请参阅基础指南。

规则结构

每个策略规则都包含以下元素。

- **敏感度类别**
  - **受保护的运行状况信息(PHI)**
  - **个人身份信息(PII)**
  - **支付卡行业数据安全标准(PCI DSS)**
  - **标记为机密**

    请参阅 "敏感数据定义"(第 780 页)
- **发送者** - 指定由该规则控制的数据传输的发起者。它可以是单个用户、用户列表或用户组。
  - **任何内部** - 包括组织所有内部用户的用户组。
  - **联系人/从组织** - 组织中的一个 Windows 帐户，由 Advanced Data Loss Prevention 识别，还可以由以前已使用的给定 Windows 帐户的所有其他帐户(包括由第三方通信应用程序使用的帐户)识别。
  - **联系人/自定义标识** - 以下列格式之一指定的内部用户的标识符：电子邮件地址、Skype ID、ICQ 标识符、IRC 标识符、Jabber 电子邮件地址、Mail.ru 代理程序电子邮件地址、Viber 电话号码、Zoom 电子邮件地址。

    以下通配符可用于指定一组联系人：
    - ***** - 任意数量的符号
    - **?** - 任何一个符号
- **接收者** - 指定由该规则控制的数据传输的目的地。它可以是单个用户、用户列表或用户组，也可以是下面指定的其他类型的目的地。
  - **任何** - Advanced DLP 支持的任何接收者类型。
  - **联系人/任何联系人** - 任何内部或外部联系人。
  - **联系人/任何内部联系人** - 内部用户的任何联系人(请参阅 "自动检测目的地"(第 780 页))。
  - **联系人/任何外部联系人** - 外部人员或实体的任何联系人。
  - **联系人/从组织** - 与“发送者”字段中所述的原则相同。
  - **联系人/自定义标识** - 与“发送者”字段中所述的原则相同。
  - **文件共享服务** - 受控文件共享服务的标识符。
  - **社交网络** - 受控社交网络的标识符。
  - **主机/任何主机** - 由 Advanced DLP 识别为内部或外部的任何计算机。
  - **主机/任何内部主机** - 由 Advanced DLP 识别为内部的任何计算机。
  - **主机/任何外部主机** - 由 Advanced DLP 识别为外部的任何计算机。

- **主机/特定主机** - 指定为主机名(例如 FQDN)或 IP 地址(IPv4 或 IPv6)的计算机标识符。
- **设备/任何设备** - 连接到工作负载的任何外围设备。
- **设备/外部存储** - 连接到工作负载的可移动存储或重定向的映射驱动器。
- **设备/可移动的加密设备** - 使用 BitLocker To Go 加密的可移动存储设备。
- **设备/重定向的剪贴板** - 连接到工作负载的重定向的剪贴板。
- **打印机** - 连接到工作负载的任何本地或网络打印机。

- **权限** - 对受该规则控制的数据传输强制执行的防护控制。在数据流策略规则中的权限主题中进行了更详细的说明。
- **操作** - 触发此规则时执行的非防护操作。默认情况下,此字段设置为"无操作"。选项包括:
  - **写入日志** - 触发规则时将事件记录存储在审核日志中。
  - **当数据传输被拒绝时通知最终用户** - 当数据传输触发规则时,通过实时屏幕警告通知用户。
  - **生成警报** - 触发规则时提醒管理员。

警告!
如果**无操作**处于选中状态并触发规则:
- 事件记录不会添加到审核日志;
- 不会向管理员发送警报;
- 不会向最终用户显示屏幕通知。

哪些内容会触发策略规则?

如果以下所有条件都为真,则数据传输与数据流策略规则匹配:

- 此数据传输的所有发送者列出或属于规则的**发送者**字段中指定的用户组。
- 此数据传输的所有接收者列出或属于规则的**接收者**字段中指定的用户组。
- 正在传输的数据与规则的**敏感度类别**匹配。

调整数据流策略规则中的权限

Advanced Data Loss Prevention 在数据流策略规则中支持三种类型的权限。权限是在策略的每个规则中单独配置的。

允许(允许)
允许与规则中定义的敏感度类别、发送者和接收者的组合相匹配的数据传输。

例外(禁止)
不允许与规则中定义的敏感度类别、发送者和接收者的组合相匹配的数据传输,但发送者可以提交规则例外以允许特定传输。

重要事项
在提交例外后,在该发送者和接收者之间将允许此敏感度类别的所有后续数据传输进行五分钟。

拒绝(禁止)
不允许与规则中定义的敏感度类别、发送者和接收者的组合相匹配的数据传输,并且发送者无法选择提交例外。

此外，可以将优先级标志指派给**允许**和**例外**权限，以增加策略管理的灵活性。使用此设置，可以覆盖策略中其他数据流规则中为特定组设置的权限。可以使用它仅将组数据流规则应用于其部分成员。为此，必须为要从组规则中排除的特定用户创建数据流规则，然后将他们的权限优先于这些用户所属组的规则中配置的数据流限制。有关组合规则时的权限优先级的信息，请参阅 "组合数据流策略规则"(第 774 页)。

重要事项
在将公司或部门策略从“观察”模式切换到“执行”模式之前，将每个敏感数据类别的默认规则从“允许”状态调整为“禁止”状态至关重要。在**数据流策略**视图中，默认规则标有星号 (*)。阅读基础指南中有关策略规则类型的详细信息。

在策略规则中编辑权限

1. 以管理员身份登录到 Cyber Protect 中控台。
2. 导航到**保护** > **数据流策略**。
3. 选择要编辑的策略规则，然后单击规则列表上方的**编辑**。
   编辑数据流规则窗口将打开。
4. 在**权限**部分中，选择**允许**、**例外**或**拒绝**。
5. (可选) 要将此规则的**允许**或**例外**权限优先于其他规则中的权限，请选中**优先**复选框。
   无需使用此复选框即可将某个数据流规则优先于“任何 > 其他”默认规则，因为它的优先级在策略中默认为最低。
   有关组合规则时的权限优先级的信息，请参阅 "组合数据流策略规则"(第 774 页)。
6. (可选) 选择触发规则时要执行的操作。
7. 保存对策略规则的更改。

组合数据流策略规则

当数据传输匹配多个规则时，为所有规则配置的权限和操作会按如下方式组合和应用。

权限

如果数据传输与多个规则匹配，并且这些规则对同一数据类别具有不同的权限，则根据以下权限优先级列表(按降序排列)，覆盖规则为优先级权限较高的优先：

1. 带有**已划分优先级**标志的例外
2. 带有**已划分优先级**标志的允许
3. 拒绝
4. 例外
5. 允许

如果数据传输匹配多个规则，并且这些规则对不同的数据类别具有不同的权限，则以下逻辑适用于覆盖：

1. 为数据传输匹配的每个敏感类别都定义最严格的规则权限。
2. 强制执行第 1 点中定义的最严格规则权限。

示例

文件传输匹配不同敏感类别的三个规则，如下所示：

敏感度类别	权限
PII	允许 - 已划分优先级
PHI	例外 - 已划分优先级
PCI	拒绝

将应用的权限是“拒绝”。

操作

如果数据传输匹配多个规则，并且这些规则在**操作**字段中配置了不同的选项，则会执行所有触发规则中配置的所有操作。

策略审核和管理

在强制执行自动创建的基准数据流策略之前，必须由客户对该策略进行审核、验证和批准，因为客户本身就了解其业务流程的所有详情，并且可以评估它们在该基准策略中是否会一致执行。此外，客户还可以识别不准确之处，然后由合作伙伴管理员进行修复。

在策略审核期间，合作伙伴管理员会向客户展示基准数据流策略，客户会审核策略中的每个数据流并验证其与业务流程的一致性。验证不需要任何技术技能，因为策略规则会在 Cyber Protect 中控台中直观地清楚显示：每条规则都会描述敏感数据流的发送者和接收者。

根据客户的指示，合作伙伴管理员通过编辑、删除和创建数据流策略规则来手动调整基准策略。在客户批准后，通过将已应用于这些工作负载的保护计划切换到执行模式，以对受保护的工作负载强制执行已审核的策略。

在强制执行已审核的策略之前，请务必将为敏感数据类别自动创建的所有默认策略规则中的**允许**权限更改为**拒绝**或**例外**。**拒绝**权限无法由用户覆盖，而**例外**权限会阻止与规则匹配的传输，但允许用户在紧急情况下通过提交与业务相关的例外来覆盖该阻止。

数据流策略更新

当公司或其部门的业务流程发生重大变化时，必须更新其 DLP 策略，才能使其与更新后业务流程的敏感数据流的变化保持一致。如果员工的岗位职责发生变化，也需要更新策略 - 在这种情况下，也必须更新用于保护员工工作负载的部分部门策略。

Advanced DLP 策略管理工作流允许管理员为整个公司、一个部门、一个用户或一个部门中的部分用户自动更新策略。

更新公司或部门的策略

“观察”模式的所有选项都可用于更新公司或部门范围的策略，以及部门中一个或多个用户的一部分部门策略。

更新公司或部门的策略

更新过程包括必须由公司管理员或管理公司工作负载的合作伙伴执行的以下步骤。

1. 删除强制执行策略中的所有非默认规则。
2. 要开始更新，请将 Advanced DLP 已应用于公司或部门的保护计划切换到观察模式选项之一（具体取决于哪个选项最适合此特定公司或部门），然后将该计划应用于公司或部门中的所有工作负载。
3. 更新期结束后，与客户一起审核新的公司或部门策略、必要时进行调整，然后由客户批准。
4. 将已应用于公司或部门工作负载的保护计划切换到合适的执行模式选项，客户认为这是防止部门工作负载泄露数据的最佳选择。

更新公司或部门中一个或多个用户的策略

可以使用观察模式的任何选项以及自适应执行模式来更新用户级策略。

使用观察模式更新用户策略

使用观察模式更新公司（或部门）中某个用户或一部分用户的策略有以下特点：在更新期间，不会针对用户的数据传输强制执行为整个公司（或部门）强制执行的数据流策略。因此，可以在更新期间为用户创建新的个人规则，这些规则可能与为公司（或部门）强制执行策略中的现有组规则相矛盾或匹配。在更新完成并针对用户的数据传输重新强制执行策略后，为用户创建的这些新的个人规则是否会实际应用于用户的数据传输取决于它们的优先级与策略中这些数据传输匹配的其他规则的比较结果。

通过观察模式更新用户的策略

更新过程包括必须由公司管理员或管理公司工作负载的合作伙伴执行的以下步骤。

1. 删除为公司（或部门）强制执行策略中将用户作为其单一发送者的所有非默认规则。
2. 从强制执行策略中所有非默认数据流规则的发送者列表中删除用户。
3. 在观察模式下创建使用 Advanced DLP 的新保护计划，并将其应用于用户的工作负载以开始更新（观察）期。
   更新期的持续时间取决于用户完成执行所有或 90-95% 的常规业务活动（这些活动涉及从其工作负载传输敏感数据）可能需要的时长。
4. 在更新期结束后，审核已添加到强制执行策略中与此用户有关的新规则、必要时进行调整，然后由客户批准。
5. 将已应用于用户的工作负载的保护计划切换到**严格执行**模式或**自适应执行**模式 - 具体取决于客户将哪个选项视为防止用户工作负载泄露数据的最佳选择。
   或者，可以将已应用于公司（或部门）的保护计划重新应用于用户的工作负载。

使用自适应执行模式更新用户策略

可以通过使用 Advanced DLP 已应用于用户工作负载的保护计划的自适应强制模式，来为公司（或部门）中单个用户或所有用户中的一部分执行策略更新。

注意

此策略更新方法的详情如下所示:在更新期间,对具有用户成员资格(即"任何内部")的发送者组强制执行的公司(部门)策略也会针对此用户的数据传输强制执行。因此,更新将不会为用户创建与发送者组的这些已存在策略规则相矛盾或匹配的新个人规则。这两种方法中的哪一种对特定客户的用户策略更新更有效取决于其特定的 IT 安全要求

通过自适应执行模式更新用户的策略

更新过程包括必须由公司管理员或管理公司工作负载的合作伙伴执行的以下步骤。

1. 删除为公司(部门)强制执行策略中将用户作为其单一发送者的所有非默认规则。
2. 从强制执行策略中所有非默认数据流规则的发送者列表中删除用户。
3. 对于为公司(或部门)强制执行策略中的所有默认规则,将其权限设置为**例外**,然后在**操作**字段中选择**写入日志**操作。
4. 如果将当前已应用于用户的工作负载的保护计划设置为**严格执行**模式,则会创建使用 Advanced DLP 的新保护计划并将其应用于**自适应执行**模式下的用户工作负载以开始更新期。更新期的持续时间取决于用户完成执行所有或 90-95% 的常规业务活动(这些活动涉及从其工作负载传输敏感数据)可能需要的时长。
5. 在更新期结束后,审核已添加到强制执行策略中与此用户有关的新规则、必要时进行调整,然后由客户批准。
6. 将已应用于用户的工作负载的保护计划切换到**严格执行**模式或将其保留在**自适应执行**模式下 - 具体取决于客户将哪个选项视为防止用户工作负载泄露数据的最佳选择。
   或者,可以将已应用于公司(或部门)的保护计划重新应用于用户的工作负载。

在保护计划中启用 Advanced Data Loss Prevention

如果为此客户启用了保护服务和 Advanced Data Loss Prevention 包,则 Advanced Data Loss Prevention 功能可以包含在客户租户的任何保护计划中。

Advanced DLP 是数据丢失预防功能组的高级模块。Advanced DLP 功能和设备控制可以独立使用,也可以一起使用(在一个保护计划中,或在两个保护同一工作负载的计划中)。如果一起使用,他们的功能能力将按照以下方式进行协调。

- 设备控制停止控制用户对 Advanced DLP 检查传输数据内容的那些本地通道的访问。然而,如果它们被配置为只读或拒绝访问,则设备控制仍保留对以下设备类型的控制:
  - 可携式
  - 加密的可移动设备
  - 已映射的驱动器

  例如,如果您在单个保护计划中或在保护同一工作负载的两个计划中同时启用了设备控制和 Advanced DLP,并且在设备控制中为 USB 设备配置了只读访问,那么无论 Advanced DLP 模块中的访问设置如何,只读访问将应用于所有 USB 设备(白名单中的设备除外)。如果在设备控制中配置了默认的启用访问,那么将应用 Advanced DLP 中的访问设置。

- 用户对白名单中以下本地通道和外围设备的访问由设备控制强制执行：
  - 光盘驱动器
  - 软盘驱动器
  - MTP 连接的移动设备
  - 蓝牙适配器
  - Windows 剪贴板
  - 屏幕截图捕获
  - USB 设备和设备类型(可移动存储和加密存储除外)

创建使用 Advanced DLP 的保护计划

1. 导航到**管理** > **保护计划**。
2. 单击**创建计划**。
3. 展开**数据丢失防护**部分，并单击**模式**行。
   模式对话框将打开。
   - 要开始创建或更新数据流策略，请选择**观察模式**，然后选择处理数据传输的方式：

选项	描述
全部允许	所有来自用户工作负载的敏感数据传输都会被视为业务流程所必需的并且是安全的。将为每个检测到的与策略中已定义规则不匹配的数据流创建一个新规则。
全部正当	所有来自用户工作负载的敏感数据传输都会被视为业务流程所必需的，但存在风险。因此，对于每一次向组织内外的任何接收者或目的地传输敏感数据但遭拦截的传输(不匹配先前创建的数据流规则)，用户都必须提供一次性业务正当理由。提交正当理由时，将会在数据流策略中创建一个新的数据流规则。
混合	“全部允许”逻辑适用于所有内部传输的敏感数据，而“全部正当”逻辑适用于所有外部传输的敏感数据。 有关内部目的地的定义，请参阅 "自动检测目的地"(第 780 页)

警告！
- 仅当以前没有创建过数据流策略或正在更新策略时，才选择**观察模式**。在开始更新策略之前，请参阅 "数据流策略更新"(第 775 页)。
- 在观察模式下，无法阻止数据泄露。请参阅 《基础指南》中的观察模式。

   - 要强制执行现有数据流策略，请选择**执行模式**，然后选择强制执行数据流策略规则的严格程度：

选项	描述
严格执行	数据流策略会按原样执行，并且不会在检测到以前未观察到的敏感数据流时使用新的允许策略规则进行扩展。请参阅 《基础指南》中的严格执行。

选项	描述
自适应执行(具有学习能力的执行)	强制执行的策略会继续其自动适应在观察期间未执行的业务操作或业务流程的变化。此模式允许强制执行的数据流策略基于在工作负载中检测到的新学习的数据流进行扩展。请参阅 基础指南》中的自适应执行。

重要事项
在将公司或部门策略从“观察”模式切换到“执行”模式之前，将每个敏感数据类别的默认规则从“允许”状态调整为“禁止”状态至关重要。在**数据流策略**视图中，默认规则标有星号 (*)。阅读基础指南中有关策略规则类型的详细信息。

4. 单击**完成**以关闭“模式”对话框。
5. (可选) 要配置光符识别、白名单和更多保护选项，请单击**高级设置**。
   有关可用选项的信息，请参阅 "高级设置"(第 779 页)。
6. 保存保护计划并将其应用于要保护的工作负载。

高级设置

可以将保护计划中的高级设置与 Advanced Data Loss Prevention 结合使用，以提高 Advanced Data Loss Prevention 所控制通道中数据内容检查的质量，并从任何防护控制中排除到白名单中外围设备类型、网络通信类别、目标主机的数据传输以及由白名单中应用程序发起的数据传输。可以配置以下高级设置：

- **光符识别**
  此设置可打开/关闭光符识别 (OCR)，以便从图形文件以及文档、消息、扫描、屏幕截图和其他对象中的图像中提取 31 种语言的文本片段，来进一步执行内容检查。
- **传输受密码保护的数据**
  受密码保护的存档和文档的内容无法检查。使用此设置，Advanced DLP 允许管理员选择是允许还是阻止传出传输受密码保护的数据。
- **出现错误时阻止数据传输**
  有时，对正在发送的内容进行分析可能会失败，或者 DLP 代理程序操作中可能会出现其他控制错误。如果启用此选项，将阻止传输。如果禁用此选项，将允许传输而不管错误。
- **设备类型和网络通信的白名单**
  允许对外围设备类型以及在此列表中选中的网络通信中的数据传输，不管其数据敏感性和强制执行的数据流策略。

警告！
如果特定设备类型或协议出现问题，则使用此选项。除非支持代表建议启用，否则不要启用它。

- **远程主机的白名单**
  允许对在此列表中指定的目标主机的数据传输，不管其数据敏感性和强制执行的数据流策略。
- **应用程序的白名单**
  允许对在此列表中指定的应用程序执行的数据传输，不管其数据敏感性和强制执行的数据流策略。

在**创建保护计划**视图和保护计划的"详细信息"视图中显示的高级设置的**安全性级别**指示器有以下级别指示器逻辑：

- **基本**指示没有任何一个高级设置已打开。
- **中等**指示一个或多个设置已打开，但 **OCR**、**传输受密码保护的数据**和**出现错误时阻止数据传输**组合未激活。
- **严格**指示至少 **OCR**、**传输受密码保护的数据**和**出现错误时阻止数据传输设置**组合已激活。

自动检测目的地

在"混合观察"模式下，Advanced Data Loss Prevention 会根据检测到的数据传输目的地(内部或外部)来应用不同的规则。将目的地确定为内部的逻辑如下所述。所有其他目的地都会被视为外部。

对于每个拦截的数据传输，Advanced Data Loss Prevention 会通过执行 DNS 请求并比较运行数据丢失防护代理程序的计算机和远程服务器的 FQDN 名称，来自动检测目标 HTTP、FTP 或 SMB 服务器是否为内部。如果 DNS 请求失败，它还会检查受保护的工作负载和远程服务器是否位于同一网络中。与运行数据丢失防护代理程序的计算机具有相同域名(或位于同一子网中)的服务器会被视为内部。

对于电子邮件通信，如果收件人电子邮件地址与发件人电子邮件地址都位于同一域中并且收件人邮件服务器名称相同，则 Advanced Data Loss Prevention 会将使用公司邮件服务器从公司电子邮件地址发送的所有电子邮件都视为内部传输。

除非收件人帐户已知，否则非公司电子邮件会被视为外部通信。当数据丢失防护监视网络上的用户活动并在后端使用与用户关联的电子邮件地址数据更新数据库时，将会更新已知电子邮件地址。

除非收件人帐户已知，否则通过信使进行的通信都会被视为外部通信。当数据丢失防护监视网络上的用户活动并在后端使用与用户关联的帐户数据更新数据库时，将会更新已知帐户。

敏感数据定义

本主题介绍了在内容分析过程中识别敏感数据的逻辑。

为了减少误报的数量，对于所有描述的逻辑表达式组而言，相同的匹配会被计数为一个匹配。

重要事项
用于内容识别的逻辑表达式仅供参考，并不会详细描述解决方案。

受保护的运行状况信息(PHI)

支持的语言

- 美国英语、英国英语、英语-国际
- 芬兰语
- 意大利语
- 法语
- 波兰语

- 俄语
- 匈牙利语
- 挪威语
- 西班牙语

数据被视为受保护的运行状况信息

以下数据被视为受保护的运行状况信息。

- 名字和姓氏
- 地址(街道、城市、县、区、邮政编码及其等效的地理编码)
- 电话号码
- 电子邮件地址
- 社会保障号码
- 健康计划受益人号码
- 银行帐号
- URL
- IP 地址编号
- ICD-10-CM 码
- ICD-10-PCS-and-GEMs
- HIPAA
- 其他医疗保健相关信息
- 信用卡号

用于内容检测的逻辑表达式

逻辑表达式由以下由逻辑运算符 OR 连接的字符串组成。如果未明确指定 AND 逻辑运算符，则 OR 运算符用于连接上面列表中的不同数据组。括号中的数字表示检测到的将返回阳性检测结果的实例数。

- **社会保障号码** (5)
- (名字和姓氏 (3) OR 地址 (3) OR 电话号码 (3) OR 电子邮件地址 (3) OR 银行帐号 (3) OR 信用卡号码 (3)) AND (社会保障号码 (3) OR 健康计划受益人号码 (3) * OR ICD-10-CM 代码 (3) OR ICD-10-PCS-and-GEMs (3) OR HIPAA (3) OR * 其他医疗保健相关信息 (3))

个人身份信息(PII)

支持的语言

- 美国英语、英国英语、英语-国际
- 保加利亚语
- 中文
- 捷克语
- 丹麦语

- 荷兰语
- 芬兰语
- 法语
- 德语
- 匈牙利语
- 印度尼西亚语
- 意大利语
- 韩语
- 马来语
- 挪威语
- 波兰语
- 葡萄牙语(巴西)
- 葡萄牙语(葡萄牙)
- 罗马尼亚语
- 俄语
- 塞尔维亚语
- 新加坡
- 西班牙语
- 瑞典语
- 台湾
- 土耳其语
- 泰国语
- 日语

数据被视为个人身份信息(PII)

- 名字和姓氏
- 地址(街道、城市、县、邮政编码)
- 银行帐号
- 个人和财政身份证号码
- 护照号码
- 社会保障号码
- 电话号码
- 车牌号
- 驾驶证号码
- 标识符和序列号
- IP 地址
- 电子邮件地址
- 信用卡号

用于内容检测的逻辑表达式

适用于所有支持语言(日语除外)的逻辑表达式

逻辑表达式由以下由逻辑运算符 OR 或 AND 连接的字符串组成。括号中的数字表示检测到的将返回阳性检测结果的实例数。

- 个人和财政身份证号码 (5)
- 名字和姓氏 (3) AND **(**信用卡号 (3) OR 社会保障号码 (3) OR 银行帐号 (3) OR 个人和财政身份证号码 (3) OR 驾驶证号码 (3) OR 护照号码 (3) OR 社会保障号码 (3) OR IP 地址 (3) OR 车牌号 (3) OR 标识符和序列号**)**
- 电话号码 (3) AND **(**信用卡号 (3) OR 社会保障号码 (3) OR 银行帐号 (3) OR 地址 (3) OR 个人和财政身份证号码 (3) OR 驾驶证号码 (3) OR 护照号码 (3) OR 社会保障号码 (3) OR 车牌号 (3) OR 标识符和序列号 (3)**)**
- **(**名字和姓氏 (30) OR 地址 (30)**)** AND **(**电子邮件地址 (30) OR 电话号码 (30) OR IP 地址 (30)**)**
- 电子邮件地址 (3) AND **(**信用卡号 (3) OR 社会保障号码 (3) OR 银行帐号 (3) OR 个人和财政身份证号码 (3) OR 驾驶证号码 (3) OR 护照号码 (3) OR 社会保障号码 (3) OR 车牌号 (3) OR 标识符和序列号 (3)**)**
- 电子邮件地址 (30) AND **(**地址 (30) OR 电话号码 (30)**)**
- 名字和姓氏 (30) AND 地址 (30)
- 电话号码 (30) AND 地址 (30)
- 名字和姓氏 (3) AND 银行帐号 (3)
- 电话号码 (3) AND **(**信用卡号 (3) OR 银行帐号 (3) OR 社会保障号码 (3) OR 个人和财政身份证号码 (3) OR 驾驶证号码 (3) OR 护照号码 (3)**)**

适用于日语的逻辑表达式

注意
内容检测仅会计算唯一匹配项。

逻辑表达式由以下由逻辑运算符 OR 连接的字符串组成。如果未明确指定逻辑运算符 AND, 则运算符 OR 用于连接不同的组。

- 社会保障号码 (5)
- 名字和姓氏 (3) AND **(**信用卡号 (3) OR 银行帐户 (3) OR 驾驶证号码 (3) OR 护照号码 (3) OR 社会保障号码 (3)**)**
- 名字和姓氏 (30) AND **(**电子邮件地址 (30) OR 电话号码 (30) OR IP 地址 (30) OR 地址 (30)**)**
- 地址 (3) AND **(**信用卡号 (3) OR 银行帐户 (3) OR 驾驶证号码 (3) OR 护照号码 (3) OR 社会保障号码 (3)**)**
- 电子邮件地址 (3) AND **(**信用卡号 (3) OR 银行帐户 (3) OR 社会保障号码 (3) OR 驾驶证号码 (3)**)**
- 地址 (5) AND **(**电子邮件地址 (5) OR 名字和姓氏 (5) OR 电话号码 (5) OR IP 地址 (5)**)**
- 名字和姓氏 (3) AND 银行帐号 (3)

- 电话号码 (3) AND **(**信用卡号 (3) OR 银行帐户 (3) OR 地址 (3) OR 社会保障号码 (3) OR 驾驶证号码 (3)**)**

支付卡行业数据安全标准 (PCI DSS)

支持的语言

该敏感度组与语言无关。PCI DSS 数据在所有国家/地区中都是英语版。

数据被视为 PCI DSS

- 持卡人资料
  - 主帐号(PAN)
  - 持卡人姓名
  - 失效日期
  - 服务代码
- 敏感的身份验证数据
  - 完整磁道数据(磁条数据或芯片上的等效数据)
  - CAV2/CVC2/CVV2/CID
  - PIN/PIN 块

用于内容检测的逻辑表达式

逻辑表达式由以下由逻辑运算符 OR 连接的字符串组成。括号中的数字表示检测到的将返回阳性检测结果的实例数。

- 信用卡号 (5)
- 信用卡号 (3) AND (美国人姓名 (Ex) (3) OR 美国人姓名 (3) OR PCI DSS 关键字 (3) OR 日期 (月/年) (3))
- 信用卡转储 (5)

标记为机密

通过关键字组检测到标记为机密的数据。

匹配条件是基于权重的，每个单词的权重 == 1。如果权重 > 3 时匹配，则内容检测被认为是阳性检测。

支持的语言

- 英式英语
- 保加利亚语
- 简体中文
- 繁体中文
- 捷克语
- 丹麦语

- 荷兰语
- 芬兰语
- 法语
- 德语
- 匈牙利语
- 印度尼西亚语
- 意大利语
- 日语
- 韩语
- 马来语
- 挪威语
- 波兰语
- 葡萄牙语 - 巴西
- 葡萄牙语 - 葡萄牙
- 俄语
- 塞尔维亚语
- 西班牙语
- 瑞典语
- 土耳其语

关键字组

每种语言的关键字组包含以下用于英语的特定国家/地区的等效关键字(不区分大小写)。

- 机密的
- 内部分发
- 不适用于分发
- 请勿分发
- 不适用于公开
- 不适用于外部分发
- 仅供内部使用
- 高质量文档
- 专用
- 特权信息
- 仅供内部使用
- 仅供官方使用

数据丢失防护事件

Advanced Data Loss Prevention 会在 DLP 事件视图中生成事件，如下所示。

- 在“观察”模式期间，将会为所有正当的数据传输生成事件。
- 在“执行”模式期间，将会根据为每个触发的策略规则配置的**写入日志**操作生成事件。

查看数据流策略中规则的事件

1. 以管理员身份登录到 Cyber Protect 中控台。
2. 导航到**保护** > **数据流策略**。
3. 找到要查看其事件的规则，然后单击规则行末尾的省略号。
4. 选择**查看事件**。

在 DLP 事件视图中查看有关事件的详细信息

1. 以管理员身份登录到 Cyber Protect 中控台。
2. 导航到**保护** > **DLP 事件**。
3. 单击列表中的事件以查看有关它的更多详细信息。
   “事件详细信息”窗格会向右侧展开。
4. 在“事件详细信息”窗格中上下滚动以查看可用信息。
   在该窗格中显示的详细信息取决于触发事件的规则类型和规则设置。

在 DLP 事件列表中过滤事件

1. 以管理员身份登录到 Cyber Protect 中控台。
2. 导航到**保护** > **DLP 事件**。
3. 在左上角，单击**过滤器**。
4. 从下拉菜单中选择敏感度类别、工作负载、操作类型、用户和通道。
   可以在下拉菜单中选择多个项目。过滤会在同一菜单中的各项目之间应用逻辑运算符 OR，但在不同菜单中的各项目之间使用逻辑运算符 AND。
   例如，如果选择 **PHI** 和 **PII** 敏感度类别，则结果将返回包含 PHI 或 PII 或者两者的所有事件。如果选择 **PHI** 敏感度类别和**写入访问**操作，则在过滤结果中只会显示与这两个类别匹配的事件。
5. 单击**应用**。
6. 要再次查看所有事件，请单击**过滤器**、然后单击**重置为默认值**，最后单击**应用**。

在 DLP 事件列表中搜索事件

1. 重复上述过程中的步骤 1-2。
2. 从过滤器右侧的下拉列表中，选择要搜索的类别：**发送者**、**目的地**、**流程**、**消息主题**或**原因**。
3. 在文本框中，输入您感兴趣的短语并按键盘上的 Enter 进行确认。
   只有与您输入的短语匹配的事件才会显示在列表中。
4. 要重置事件列表，请单击搜索文本框中的 **X** 符号并按 Enter。

查看与数据流策略中的特定规则相关的事件列表

1. 以管理员身份登录到 Cyber Protect 中控台。
2. 导航到**保护** > **数据流策略**。
3. 选中您感兴趣的策略规则名称前面的复选框。
   如果需要，可以选择多个策略规则。

4. 单击**查看事件**。
   视图会切换到**保护** > **DLP 事件**，然后与您选择的策略规则相关的事件显示在列表中。

概述仪表板上的 Advanced Data Loss Prevention 小组件

概述仪表板提供了若干可自定义的小组件，这些小组件会提供与 Cyber Protection 服务（包括 Advanced Data Loss Prevention）相关操作的概述。可以在**概述**仪表板上的**监控**下找到以下 Advanced Data Loss Prevention 小组件。

- **敏感数据传输** - 显示对内外接收者的敏感数据传输操作总数。该图表按权限类型划分：允许、正当或阻止。可以通过选择所需的时间范围（1 天、7 天、30 天或本月）来自定义此小组件。
- **出站敏感数据类别** - 显示对外部接收者的敏感数据传输总数。该图表按敏感类别划分：受保护的运行状况信息 (PHI)、个人身份信息 (PII)、PCI DSS 并标记为机密（机密）。
- **已出站敏感数据的前几名发送者** - 显示从组织到外部接收者的敏感数据传输总数，以及传输次数最多的前五名用户的列表（连同这些次数）。该统计数据包括允许的传输和正当的传输。可以通过选择所需的时间范围（1 天、7 天、30 天或本月）来自定义此小组件。
- **已阻止敏感数据传输的前几名发送者** - 显示已阻止敏感数据传输的总数以及尝试传输次数最多的前五名用户的列表（连同这些次数）。可以通过选择所需的时间范围（1 天、7 天、30 天或本月）来自定义此小组件。
- **最近的 DLP 事件** - 显示选定时间范围内最近数据丢失防护事件的详细信息。可以使用以下选项自定义此小组件：
  - **范围(发布日期)**（1 天、7 天、30 天或本月）。
  - **工作负载**的名称
  - **操作状态**（允许、正当或阻止）
  - **敏感度**（PHI、PII、机密、PCI DSS）
  - **目的地类型**（外部，内部）
  - **分组**（工作负载、用户、通道、目的地类型）

小组件每五分钟更新一次。小部件具有可单击元素，可让您调查和解决问题。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。

自定义敏感度类别

自定义敏感数据类别可以通过扩展与法规遵从性相关的内容定义的 Advanced DLP 内置目录，来帮助组织保护特定于该组织的知识产权和机密数据。

创建自定义敏感类别

1. 以管理员身份登录到 Cyber Protect 中控台。
2. 导航到**保护** > **数据丢失预防** > **数据分类器**。
3. 选择**敏感度类别**。
4. 您会看到一个敏感度列表，其中包括内置敏感度（如受保护的运行状况信息或个人身份信息）和自定义敏感度。
5. 单击窗口右上角的**创建敏感度**。
6. 在下一个窗口中，输入其名称。

7. 默认情况下，始终禁用新的自定义敏感度。在完成配置敏感度的所有参数后，就可以启用它们。
8. 在创建新的敏感度后，需要设置其内容检测器。单击箭头以展开新敏感度的内容，然后选择**添加内容检测器**。
9. 在下一个窗口中，可以使用任何现有的内容检测器（方法是单击其名称旁边的复选标记，然后单击右下角的**添加**），也可以定义新的内容检测器。
10. 还可以通过克隆现有敏感度并调整其参数来重新使用该敏感度（内置敏感度或现有自定义敏感度），而无需从头开始创建新的敏感度。
    - 要克隆现有敏感度，请单击其名称旁边的复选标记，然后从左上角的“操作”下拉菜单（由省略号指示）中选择**克隆**。可以一次选择多个项目以克隆多个敏感度。
    - 在下一个窗口中，可以通过单击每个参数旁边的复选标记，来选择要保留的现有敏感度的参数。

注意
复制一个租户内的内置敏感度时，将创建一个包含相同检测器的新敏感度（复制后的检测器将成为自定义检测器）

创建新内容检测器

1. 以管理员身份登录到 Cyber Protect 中控台。
2. 导航到**保护 > 数据丢失预防 > 数据分类器**。
3. 选择**内容检测器**。
4. 您会看到一个内容检测器列表，其中包括内置检测器和自定义检测器。
5. 单击窗口右上角的**创建内容检测器**。
6. 一个下拉菜单即会打开，可以在其中选择要创建的检测器类型；此时，只有**文件类型**内容检测器可用，更多内容检测器会通过将来更新提供。
7. 在下面的窗口中，可以配置内容检测器。

内容检测器的类型	描述
文件类型内容检测器	a. 有两个列表可供选择：**支持的文件类型**和**选定的文件类型**。通过单击受支持文件类型右侧的“+”图标，可以将其移动到“选定的文件类型”列表中。还可以选择多个受支持文件类型，方法是单击文件类型名称旁边的复选标记，然后使用右上角的**添加选定项**按钮。 b. 要从“选定的文件类型”列表中删除某个文件类型，请单击其名称右侧的垃圾桶图标。还可以使用复选标记和**删除选定项**按钮，来一次删除多个文件类型。
关键字内容检测器	a. 创建新的关键字内容检测器时，需要通过文件导入关键字。成功导入后，可以将新关键字与现有关键字列表合并，也可以将现有关键字替换为导入的关键字。 b. 还需要确定是希望内容检测器匹配列表中的所有关键字、列表中的任何关键字还是自定义数量的关键字。

8. 还可以通过克隆现有内容检测器并调整其参数来重新使用该内容检测器（内置内容检测器或现有自定义内容检测器），而无需从头开始创建新的内容检测器。

- 要克隆现有内容检测器，请单击其名称旁边的复选标记，然后从左上角的“操作”下拉菜单（由省略号指示）中选择**克隆**。可以一次选择多个项目以克隆多个内容检测器。

注意
复制内置内容检测器时，会导致相应检测器变为自定义检测器。

组织结构图

注意
此功能仅可供公司管理员用户访问。

组织地图是一个数据库，其中包含用户及其所有帐户的数据，这些帐户用于通过即时消息、电子邮件或任何其他方式传输数据，这些数据已被 Advanced DLP 拦截。

组织地图提供了在 Advanced DLP 中创建和管理用户组以及管理与 Advanced DLP 中的用户关联的用户和帐户的方法。然后，用户组可用于基于组的 DLP 策略管理。

若要找到组织地图

- 在 Cyber Protect Cloud 中控台中，导航到**保护>数据丢失防护>组织地图**。

它是如何工作的？

注意
当 Advanced DLP 模块在观察模式下运行时，会填充组织图。

对于 DLP 代理程序拦截的每个数据传输，后端都会收集以下属性。

属性	描述	用户界面中的标签
组织单位	手动创建的组。该组织单元可以有一个或多个嵌套的组织单元。	组名称，如定义所述
安全 ID	唯一安全标识符。	在用户详细信息页面 > **SID**
	从用户的帐户名称派生的用户友好的显示名称。此名称并不总是在组织地图中可用。	**名称**
电脑\用户名	终端（工作负载）的用户名称。 一个用户名只能指派给一个组织单位。	**用户名**
设备（工作负	终端（工作负载）的名称。	**工作负载**

属性	描述	用户界面中的标签
载)		
帐户	用户用于通过即时消息和电子邮件进行通信且已被 DLP 代理程序拦截的帐户。例如，如果代理程序检测到用户名 “PC\John”使 用 john@gmail.com 发送电子邮件，则此帐户将链接到 PC\John 用户名。	**账户**

在组织地图中，您可以查看和搜索帐户、用户和组，以及创建、编辑和删除组。

搜索特定帐户

作为事件调查的一部分，管理员用户可能需要找到涉及潜在数据泄露的特定帐户的所有者。

1. 在 Cyber Protect Cloud 中控台中，导航到**保护>数据丢失防护>组织地图**。
2. 在用户列表上方的**搜索**文本框中，开始键入或粘贴帐户。
   该列表会在您键入时进行筛选。

若要搜索特定用户名

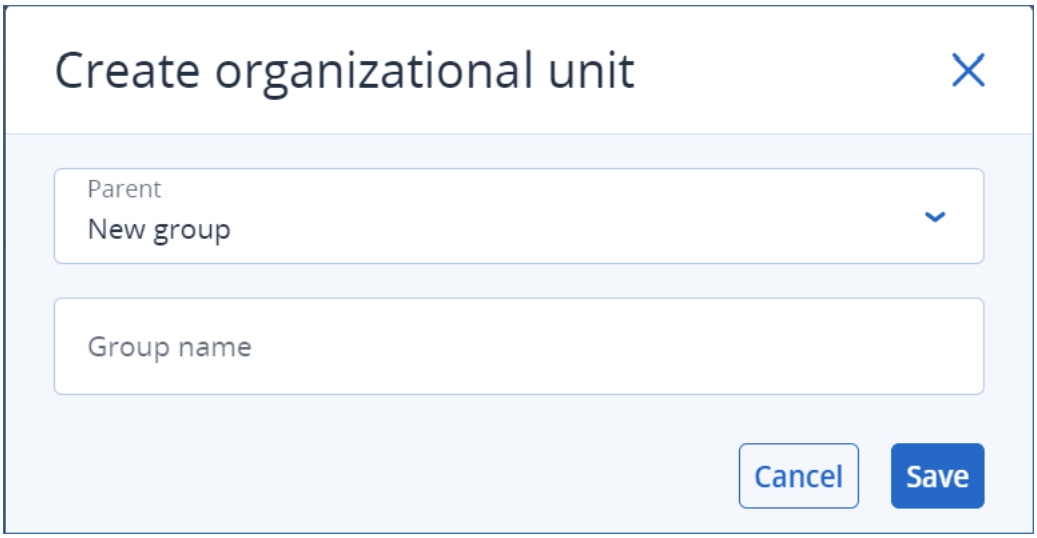
1. 在 Cyber Protect Cloud 中控台中，导航到**保护>数据丢失防护>组织地图**。
2. 若要在特定组中进行搜索，请单击列表中的组名称。
3. 在用户列表上方的**搜索**文本框中，开始键入或粘贴用户名。
   该列表会在您键入时进行筛选。

查看特定用户名使用的帐户

1. 在用户列表中找到该用户。
2. 单击用户行末尾的三个点，然后选择**“查看”**。
3. 在用户详细信息对话框中，找到**关联帐户**部分。
4. 您可以在描述文本框中添加注释。

若要创建用户组

1. 在 Cyber Protect Cloud 中控台中，导航到**保护>数据丢失防护>组织地图**。
2. 在组列表的左下部分中，单击**“创建组”**。
   将打开“创建组织单元”对话框。



3. 从“父级”下拉菜单中，选择新组的上下文。

注意
您以后将无法更改父级。该组将继续嵌套在此上下文中。

4. 输入组名称并单击**“保存”**。

若要将用户添加到组

1. 在 Cyber Protect Cloud 中控台中，导航到**保护>数据丢失防护>组织地图**。
2. 在用户列表中，找到要添加的用户，然后选中用户行开头的复选框。
   “移动所选”和**“删除所选”**按钮会出现在用户列表上方。
3. 单击**“移动所选”**。
   将打开“移动用户”对话框。
4. 为所选用户选择一个新的父级，然后单击**“保存”**。

注意
一个用户只能属于一个组。

若要删除与用户关联的帐户

1. 在用户列表中找到该用户。
2. 单击用户行末尾的三个点，然后选择**“查看”**。
3. 在用户详细信息对话框中，找到**关联帐户**部分。
4. 找到您要删除的帐户，然后单击其旁边的三个点。
5. 从下拉列表中选择**删除**。

若要重命名用户组

1. 在 Cyber Protect Cloud 中控台中，导航到**保护>数据丢失防护>组织地图**。
2. 单击组名称旁边的三个点，然后单击**重命名**。

删除用户组

1. 在 Cyber Protect Cloud 中控台中，导航到**保护>数据丢失防护>组织地图**。
2. 单击组名称旁边的三个点，然后单击**删除**。
   该组中的所有用户都将移动到父实体。

已知问题和限制

- [DEVLOCK-4028] 在 Zoom 桌面代理程序中，无法控制群聊。
- [DEVLOCK-4016] 在创建草稿时，未为 GMX Web Mail 和 Web.de Mail 捕获友好名称和发件人 ID。
- [DEVLOCK-4447] 在创建草稿时，naver.com WebMail 没有“正当”对话框。
- [DEVLOCK-1033] DeviceLockDriver：IRP_MN_QUERY_DEVICE_RELATIONS 处理过程中死锁导致的潜在错误检查 DRIVER_POWER_STATE_FAILURE。

Endpoint Detection and Response (EDR)

注意
此功能是 “Advanced Security + XDR” 保护包的一部分，而该保护包又是网络安全保护服务的一部分。请注意，当您将 EDR 功能添加到保护计划中时，可能会收取额外费用。

EDR 会检测工作负载上的可疑活动，包括尚未注意到的攻击。EDR 随后会生成提供每个攻击的分步概述的事件，从而帮助您了解攻击是如何发生的以及如何防止它再次发生。通过轻松了解攻击中每个阶段的说明，调查攻击所花费的时间可以减少到几分钟。

从 C24.05 开始，可以使用 Extended Detection and Response (XDR) 来扩展 EDR 功能。使用 XDR 图表，通过将检测与 XDR 数据源（包括电子邮件和身份管理元数据）中的事件相关联，以获得 EDR 事件的附加丰富视图。有关详细信息，请参阅 "Extended Detection and Response (XDR)"（第 861 页）"Extended Detection and Response (XDR)"（第 861 页）。

为什么需要 Endpoint Detection and Response (EDR)

在当今网络威胁和恶意攻击不断扩张的世界中，预防不再能够提供 100% 的保护。一些攻击始终会穿透预防层，并成功入侵网络。传统的解决方案无法发现这种情况何时发生，从而攻击者可以在您的环境中不受限制地停留数天、数周或数月。

现有的 EDR 解决方案通过快速发现并解决攻击者，确实有助于防止出现这些“无声故障”。但是，它们通常需要高水平的安全专业知识或昂贵的安全运营中心 (SOC) 分析师，并且对事件的分析可能非常耗时。

“安克诺斯 Advanced Security + EDR” 功能克服了这些限制，方法是通过检测未注意到的攻击，并帮助您了解攻击是如何发生的以及如何防止它再次发生。反之，这又减少了调查攻击所花费的时间。

以下是您需要 EDR 的原因：

- **完全可见性**：了解发生的情况以及它是如何发生的，即使是未注意到的攻击。每个攻击的演变也都会逐步地直观地描绘出来（从最初的进入点到查看目标数据和/或泄露的数据），从而使您能够快速了解事件的范围和影响。有关详细信息，请参阅 "如何调查网络杀伤链中的事件"（第 817 页）。

- **最大程度地减少调查时间**:将事件调查时间从数小时缩短到仅几分钟。EDR 会以清晰易懂的人类语言详细描述攻击的每一步,从而有助于减少对费用昂贵的专家或其他人员的聘请需求。有关详细信息,请参阅 "调查事件"(第 816 页)。
- **检查工作负载上的已知威胁**:可以自动搜索工作负载,以查找恶意软件、漏洞和其他类型的全局事件(可能影响数据保护)造成的威胁。这些威胁称为危害事件 (IOC),并基于从网络安全保护运营中心 (CPOC) 收到的威胁数据。有关详细信息,请参阅 "检查工作负载上众所周知攻击的危害指标 (IOC)"(第 827 页)。
- **更快地响应事件**:通过访问所有破坏后活动和杀伤链的每个分解步骤,可以执行许多操作来修复每个攻击点。除此之外,还可以使用远程控制和取证备份(此功能在抢先体验版中不可用)、隔离工作负载和终止恶意软件进程来进行调查。还可以使用 Cyber Disaster Recovery Cloud 来恢复业务运营。有关详细信息,请参阅 "修复事件"(第 830 页)。
- **自信地报告安全态势**:在启用 EDR 后,可以消除网络攻击对您的业务可能造成的不安全感和影响的恐惧。此外,事件相关的信息会存储 180 天,可用于进行审核。

功能

Endpoint Detection and Response (EDR) 包括以下功能:

- 发生入侵时接收警报通知
- 在“事件”页面中管理事件
- 轻松了解攻击过程的可视化
- 建议和修复步骤
- 使用威胁源在工作负载上查找公开披露的攻击
- 在仪表板中快速概览
- 将安全事件存储 180 天

发生入侵时接收警报通知

EDR 会在发生事件时提供警报通知。这些警报会在 Cyber Protect 中控台的主菜单中亮显。然后,可以通过单击**调查事件**按钮来调查警报,该按钮会将您重定向到事件调查屏幕(也称为网络杀伤链)。

有关详细信息,请参阅 "查看事件"(第 797 页)。

在“事件”页面中管理事件

EDR 使您能够在“事件”页面(从 Cyber Protect 中控台中的**“保护”**菜单访问)中管理所有事件。可以根据要求在**“事件”**页面上对信息进行筛选,以快速轻松地了解事件的当前状态,包括其严重程度、受影响的工作负载和确定性级别。还可以直接导航到网络杀伤链,以逐节点查看攻击过程。

有关“事件”页面的详细信息,请参阅 "查看事件"(第 797 页)。

轻松了解攻击过程的可视化

EDR 会以易于阅读的格式提供攻击的可视化表示。这确保即使非安全人员也能理解任何攻击的目标和严重性。确实不需要安全运营中心 (SOC) 服务,也无需雇佣安全专家;EDR 详细描述了攻击发

生的具体情况，包括：

- 攻击者如何进入
- 攻击者如何隐藏其踪迹
- 造成哪些伤害
- 攻击如何传播

有关详细信息，请参阅 "如何调查网络杀伤链中的事件"(第 817 页)。

建议和修复步骤

EDR 会为解决工作负载上的攻击提供清晰且易于实施的建议。要快速解决攻击，请单击**修复整个事件**按钮以查看缓解事件的建议步骤并按照这些步骤操作。这些建议步骤使您能够快速恢复受攻击影响的操作。但是，如果您想要采取更精细的修复步骤，可以导航到每个节点并使用相关操作对其进行修复。

您还可以单击 **Copilot** 以启动 AI 辅助的 Copilot 聊天工具，以输入多个请求并接收所选事件的建议响应操作。

有关详细信息，请参阅 "修复事件"(第 830 页)。

使用威胁源在工作负载上查找公开披露的攻击

EDR 使您能够查看威胁源中针对工作负载的现有已知攻击。这些威胁源是根据从网络安全保护运营中心 (CPOC) 收到的威胁数据自动生成的；EDR 使您能够验证威胁是否影响工作负载，然后采取必要步骤来消除威胁。

有关详细信息，请参阅 "检查工作负载上众所周知攻击的危害指标 (IOC)"(第 827 页)。

在仪表板中快速概览

EDR 会在 Cyber Protect 中控台仪表板中提供一系列统计信息。可以查看：

- 当前威胁状态，包括需要调查的事件数量。
- 按严重性演变攻击，指示可能的攻击活动。
- 解决事件的效率。
- 用于攻击客户的最常见针对性策略。
- 工作负载的网络状态，即它处于隔离状态还是连接状态。

将安全事件存储 180 天

EDR 会收集工作负载和应用程序事件，并将其存储 180 天。将删除 180 天之前的事件(事件删除是基于存储时长而不是根据存储空间)。请注意，即使 EDR 处于关闭状态，也会保留以前为工作负载收集的所有事件，并可用于事件调查。

软件要求

Endpoint Detection and Response (EDR) 支持以下操作系统：

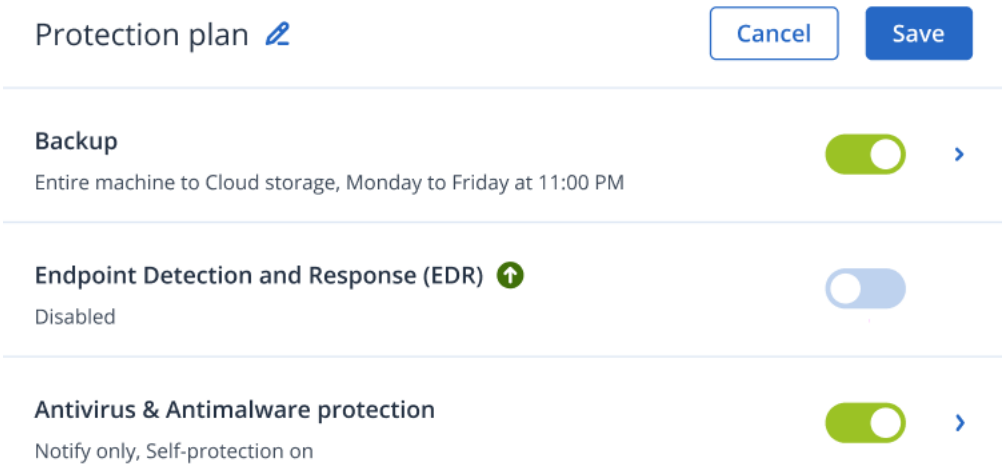
- Microsoft Windows 7 Service Pack 1 及更高版本
- Microsoft Windows Server 2008 R2 及更高版本
- macOS 版本 13、14

启用 Endpoint Detection and Response (EDR) 功能

可以在任何保护计划中启用 EDR。

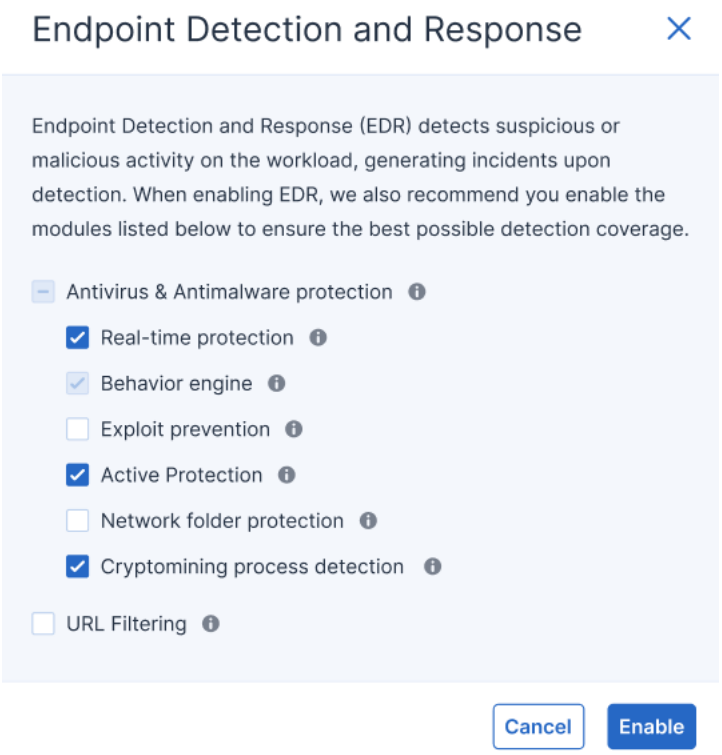
启用 EDR

1. 在 Cyber Protect 中控台中，转到**管理 > 保护计划**。
2. 从显示的列表中选择相关保护计划，然后在右侧边栏中单击**编辑**。
   或者，可以创建一个新的保护计划，并继续执行下一步。有关使用保护计划的更多信息，请参阅 "保护计划和模块"(第 192 页)。
3. 在保护计划侧边栏中，通过单击模块名称旁边的开关，可启用 **Endpoint Detection and Response (EDR)** 模块。



Advanced Security + EDR 包图标(如下所示) 会添加到实施保护计划所需的保护包列表中，具体取决于选择的其他包。

4. 在显示的对话框中，单击**启用**。请注意，可以在保护计划中启用 EDR，但仍可禁用任何防病毒和防恶意软件、Active Protection 和 URL 筛选器功能。



注意

如果在启用 EDR 时，保护计划中禁用了**行为引擎**或**防病毒和防恶意软件保护**，则也会禁用 **Endpoint Detection and Response (EDR)**。

如何使用 Endpoint Detection and Response (EDR)

EDR 使您能够检测尚未注意到的攻击，同时帮助您了解攻击是如何发生的以及如何防止它再次发生。通过轻松了解攻击中每个阶段的说明，调查攻击所花费的时间可以减少到几分钟。

下表描述了使用 EDR 时的一般工作流程。最初，您将查看任何新事件并确定其优先级、进一步调查网络杀伤链中的事件，然后采取相关修复操作。

步骤	如何使用 EDR
步骤 1：查看事件	在 EDR 事件列表中： • 了解组织的安全态势：需要调查多少事件？ • 了解哪些是最严重的事件，并根据事件的严重性确定其调查的优先级。 • 了解哪些事件是新的或正在发生。
步骤 2：调查事件	在 EDR 网络杀伤链中： • 了解攻击者的目标并查看所使用的攻击技术。 • 验证任何事件是真正恶意攻击的可能性。 • 验证威胁源是否影响工作负载。 • 查看已应用于事件的响应操作。

步骤	如何使用 EDR
步骤 3:修复事件	在相关 EDR 修复部分中: • 通过应用全局响应操作,快速轻松地修复整个事件。 • 修复事件中的个别攻击点。 • 应用操作以防止攻击(或将来的攻击)传播或影响尚未被攻击者锁定的工作负载。

查看事件

Endpoint Detection and Response (EDR) 会提供一个事件列表,其中包括工作负载上的预防(或恶意软件)和可疑检测。事件列表让您可以快速概览影响工作负载的任何攻击或威胁,包括尚未缓解的威胁。

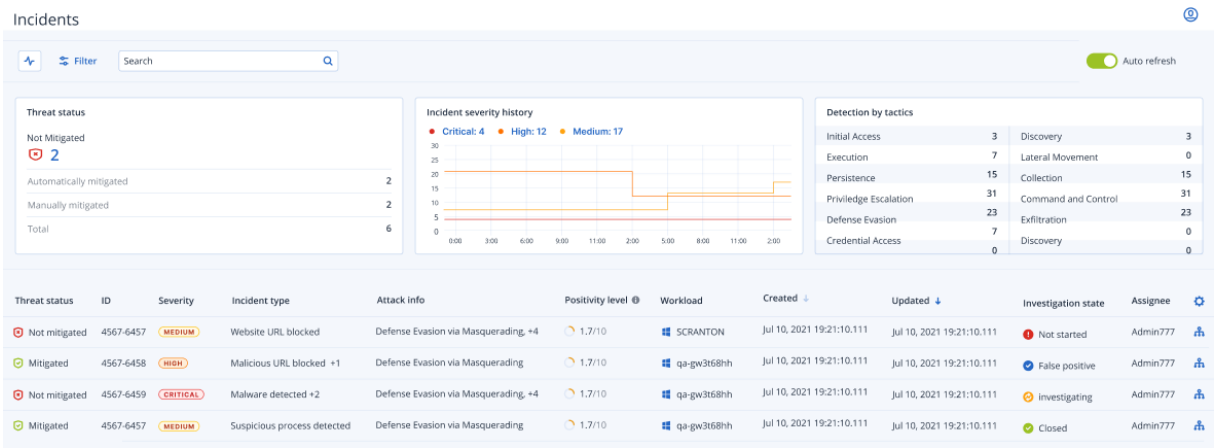
在事件列表中,可以快速确定:

- 组织的安全态势:需要调查多少事件?
- 哪些是最严重的事件,并根据事件的严重性确定其调查的优先级。
- 哪些事件是新的或正在发生。

注意
以合作伙伴管理员身份登录后,您可以在一个屏幕中查看所有 EDR 事件,该屏幕合并了所有客户的事件,而无需访问每个客户的单独事件视图。系统会显示一个附加的**"客户"**列,其中包括每个事件所属的客户名称。此外,**概览**仪表板上显示的小组件会显示所有客户的汇总指标数据。

从 Cyber Protect 中控台中的**保护**菜单访问如下所示的事件列表。有关查看事件列表中事件的更多信息,请参阅 " 查看当前未缓解的事件"(第 800 页)。要了解有关何时产生事件的更多信息,请参阅事件到底是什么? 。

注意
如果您的工作负载启用了托管检测和响应 (MDR),则会显示一个附加的 **MDR 票证**列。此列显示 MDR 供应商提供的票证号。



注意
必须打开 Cyber Protect 中控台,您才能收到事件通知。

事件到底是什么?

事件或安全事件可以视为至少包含一个预防或可疑检测点(或混合点)的*容器*,并包括单个攻击的所有相关事件和检测。这些安全事件还可以包括其他良性事件,可为发生的情况提供进一步的上下文。

这使您能够在单个事件中一起查看攻击事件,并了解攻击者执行的逻辑步骤。此外,它有助于缩短攻击的调查时间。

当 EDR 在保护计划中启用时,在以下情况下会产生安全事件:

- **预防层阻止某些内容:**系统会根据保护计划设置来自动解决这些事件。但是,可以调查恶意软件在遭停止之前到底做了哪些操作。例如,勒索软件在开始加密文件时遭停止;但在此之前,它可能已经盗取了凭据或安装了服务。
- **EDR 检测到可疑活动:**这些是应该调查并修复的检测。通过查看视觉上增强的网络杀伤链(有关详细信息,请参阅 "如何调查网络杀伤链中的事件"(第 817 页)),可以轻松应用相关的修复操作。

确定需要立即注意的事件的优先级

可以随时从 中控台中的**保护**菜单访问 Cyber Protect 中控台事件列表。事件列表会为您提供任何攻击或威胁的快速概览,从而使您能够确定需要注意的事件的优先级。

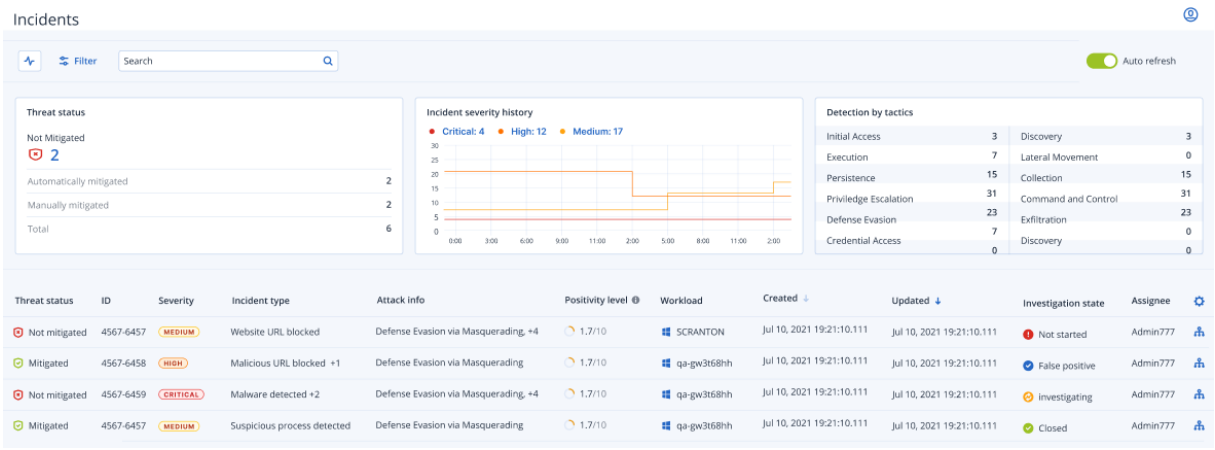
重要事项
为了确保工作负载一直受保护,请*始终*分析正在发生或未缓解的事件并确定其优先级。

如何分析需要立即注意的安全事件

事件列表使您能够分析列出的需要注意的事件,并确定其优先级。您可以:

- 查看当前未缓解的事件:通过事件列表,快速了解当前是否有任何攻击正在进行。如**威胁状态**列中所示,任何未缓解的事件都应该会立即看到(默认情况下,事件列表会进行过滤以显示这些事件)。
- 了解事件的范围和影响:根据您对新开启或正在进行的攻击的过滤,了解过滤事件的严重性以及对业务的影响。

在您有了最重要事件的精选列表后,就可以分析事件详细信息,以更好地了解特定事件,以及攻击者为实现其目标所使用的技术。有关详细信息,请参阅 "分析事件详细信息"(第 801 页)。

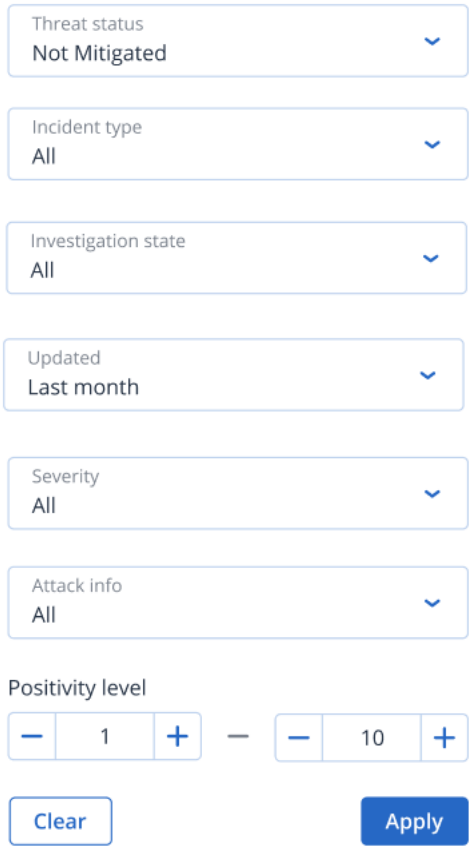


注意

默认情况下，事件列表会根据**已更新**列进行排序，该列表会详细说明事件上次更新的日期和时间以及事件中记录的新检测。请注意，可以随时更新任何现有事件，即使事件之前已解决。还可以根据您的要求过滤列表，以显示新开启或正在进行的攻击，如下面的步骤中所述。。

过滤事件列表

1. 在事件列表的顶部，单击**过滤器**以过滤显示的事件列表。例如，如果在**已创建**字段中选择开始和结束日期，则事件列表和小组件会显示在定义的时间段内创建的相关事件。



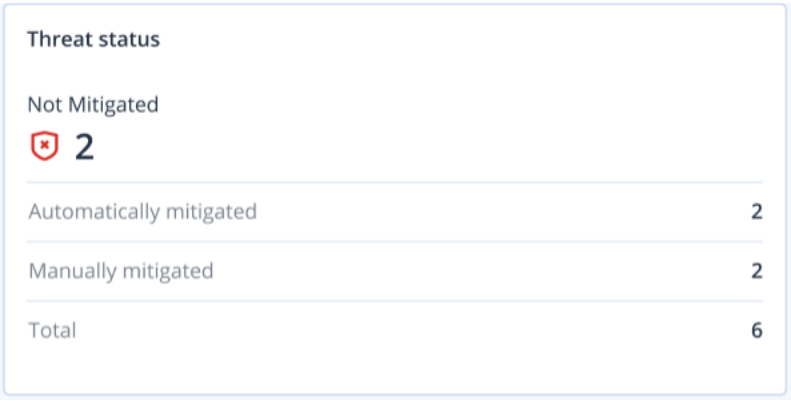
2. 完成操作后，单击**应用**。

查看当前未缓解的事件

可以在**威胁状态**列中查看事件的当前威胁状态，该列会显示事件是处于**已缓解**状态还是**未缓解**状态。EDR 会自动定义威胁状态；任何未得到缓解的事件都应尽快进行调查。

然后，可以通过应用过滤器来进一步调整显示的事件列表。例如，如果要根据威胁状态*和*特定严重级别过滤列表，请选择相关的过滤器选项。在已过滤出您感兴趣的事件后，就可以调查它们，如 "调查事件"（第 816 页）中所述。

还可以使用**威胁状态**小组件（如下所示），以快速概览当前威胁状态。请注意，此小组件中显示的数据反映了您应用的过滤器；请参阅 " 过滤事件列表"（第 799 页）。



了解事件的范围和影响

通过查看**严重性**、**攻击信息**和**确定性级别**列，可以快速了解事件的范围和影响。如上所述，在确定当前正在进行的事件后，可以过滤这些附加列以执行以下操作：

- 在**严重性**列中，查看哪些事件较严重。事件的严重程度可以是**严重**、**高**或**中**之一。
  - **严重**：存在恶意网络活动的风险严重，并有危及环境中关键主机的风险。
  - **高**：存在恶意网络活动的风险较高，并有严重危害环境的风险。
  - **中**：存在恶意网络活动的风险增加。

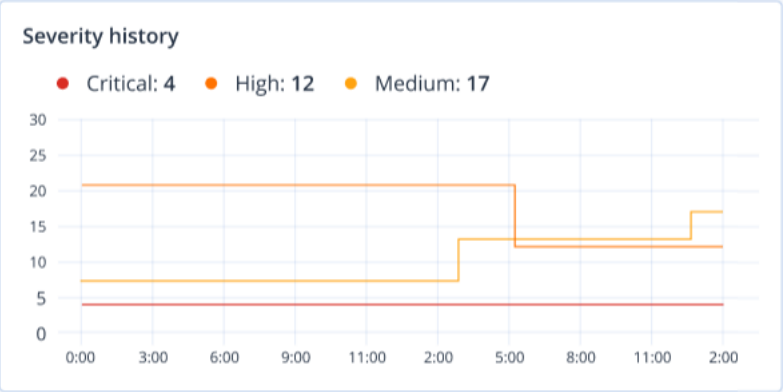
  注意
  在确定严重性时，EDR 算法会考虑工作负载类型以及攻击的每一步范围。例如，包含与凭证盗取相关步骤的事件会设置为**严重**。

- 了解**事件类型**列中创建事件的原因。事件类型可以包括以下任意一项或多项：
  - **检测到勒索软件**
  - **检测到恶意软件**
  - **检测到可疑进程**
  - **检测到恶意进程**
  - **可疑网址被屏蔽**
  - **恶意网址被阻止**
- 在**攻击信息**列中确定正在使用的攻击技术，并了解攻击是否有共同的主题或模式。

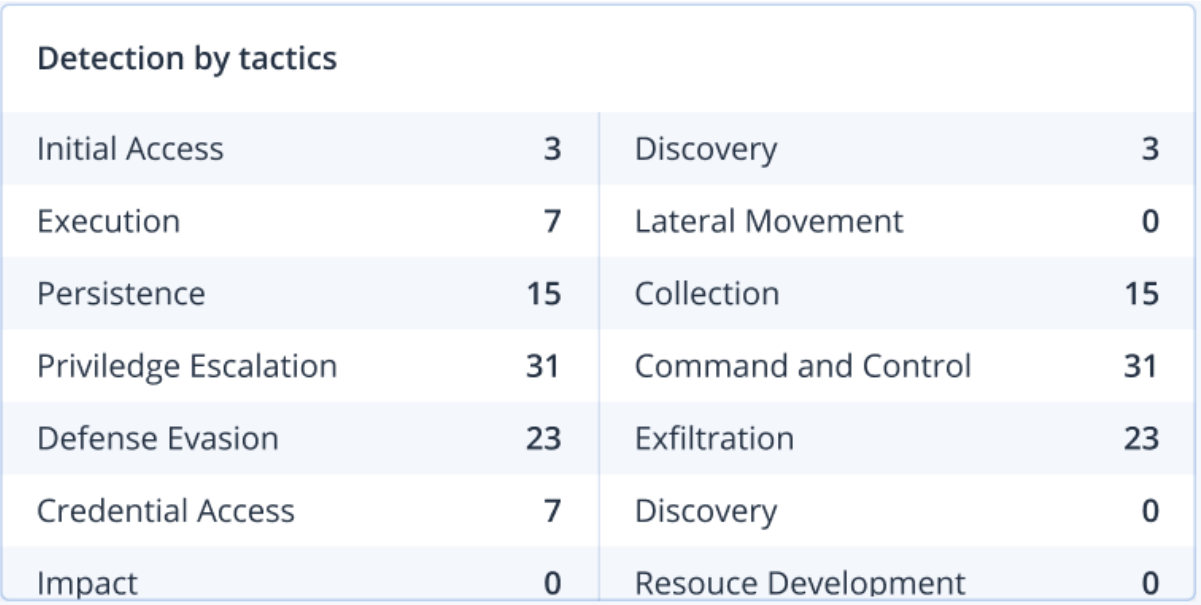
- 确定事件是真正恶意攻击的可能性;**确定性级别**列包含 1-10 之间的分数(分数越高,攻击越有可能是真正的恶意攻击)。

在发现需要立即注意的事件后,就可以对它们进行调查,如 "调查事件"(第 816 页) 中所述。

还可以使用**严重性历史记录**和**战术检测**小组件,来快速概览严重性和攻击技术。



战术检测小组件会显示使用的各种攻击技术,其中绿色值或红色值指示相较于上一指定时间范围是增加还是减少。此小组件会提供过滤事件中所有目标的汇总视图,以便可以快速了解对客户的影响。



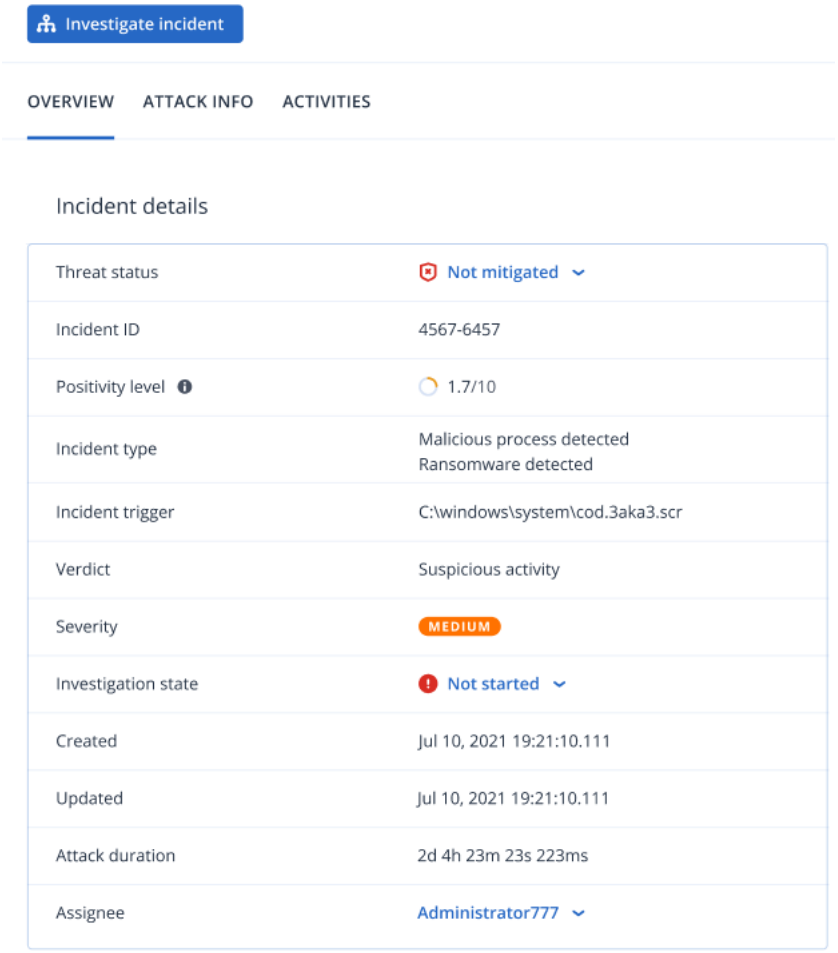
分析事件详细信息

在事件查看阶段,还可以分析 Endpoint Detection and Response (EDR) 事件列表中的每个事件的详细信息。这些详细信息使您能够深入了解整个事件,并了解事件发生的情况和时间。此外,还可以将事件指派给特定用户进行调查,并设置调查状态。

分析事件详细信息

1. 在 Cyber Protect 中控台中,转到**保护 > 事件**。事件列表即会显示。
2. 单击要查看的事件。选定事件的详细信息即会显示。

3. 在显示的**概述**选项卡中，可以查看事件和工作负载详细信息(包括当前威胁状态和严重性)。还可以定义**调查状态**(从**正在调查**、**未启动**(默认状态)、**误报**或**已关闭**中选择一个)，并选择接收事件指派的用户(在**被指派者**下拉列表中，选择相关用户)。



4. 单击**攻击信息**选项卡，可查看攻击的详细信息以及攻击中使用的技术。单击每个列出的攻击技术旁边的链接，可在 MITRE.org 上查看有关该技术的更多信息。
5. 单击**活动**选项卡，可查看在网络杀伤链中为缓解事件而执行的任何操作。有关详细信息，请参阅 "如何调查网络杀伤链中的事件"(第 817 页)。
   例如，如果在工作负载上运行过修补程序，则可以查看修补程序的启动者、所花费的时间以及在实施修补期间所发生的任何错误。
6. 单击**调查事件**以访问网络杀伤链，在其中可以逐节点调查事件。有关详细信息，请参阅 "如何调查网络杀伤链中的事件"(第 817 页)。

搜索入侵指标 (IoC) 和可疑活动

注意
此功能是抢先体验计划的一部分。部分功能和描述可能不完整。

若要在威胁升级为高影响事件之前检测并缓解威胁，请使用**事件搜索**功能。此搜索功能让您可以在启用了 Endpoint Detection and Response (EDR) 的所有工作负载中搜寻 IoC 和可疑活动。

使用**事件搜索**功能以：

- 对从所有工作负载收集的事件数据运行自定义查询以搜索哈希值。或者，可以获取指标来回答某些问题（例如，显示进程数异常高的工作负载）。
- 使用 EDR 终端提供的属性和来自其他集成的数据（例如操作系统活动、用户活动和网络活动）筛选查询。

可从中控台的**保护**菜单访问**事件搜索**功能。

注意
EDR 事件搜索结果的默认保留期为七天。

搜索事件

注意
此功能是抢先体验计划的一部分。部分功能和描述可能不完整。

您可以搜索所有受 EDR 保护的工作负载中的 Endpoint Detection and Response (EDR) 事件。

请注意，当您使用在合作伙伴租户**（所有客户）**级别的 Cyber Protect中控台时，可以搜索来自所有托管客户的事件。如果在客户租户级别工作，则可以搜索特定于所选客户的事件。

搜索事件

1. 在 Cyber Protect 中控台，转到**保护** > **事件搜索**。
2. 使用 Acronis XDR 查询语言 (XQL) 输入搜索查询，并定义日期范围。
   请注意，XQL 使用自动完成功能来帮助您构建查询。有关语法和可用查询选项的详细信息，请参阅"语法"（第 804 页）。
3. 单击输入字段右侧的箭头图标来执行查询。
   请注意，以下键盘操作也可用：
   - 按**Enter 键**将光标移至下一行。新行的开头还会添加“|”字符（这在编写多阶段查询时很有帮助）。
   - 按**Shift+Enter**将光标移至下一行。
   - 按**Ctrl+Enter**执行查询。
4. 根据需要优化搜索查询。例如，选择显示包含特定文件名的特定字段或事件。

Acronis XDR 查询语言 (XQL)

注意
此功能是抢先体验计划的一部分。部分功能和描述可能不完整。

使用 XQL 搜索 Endpoint Detection and Response (EDR) 事件，然后深入查找您要查找的事件。本部分列出了搜索 EDR 事件时您应该熟悉的各种 XQL 元素：

- 语法（包括示例查询）
- 事件类型和字段

有关使用**事件搜索**功能的更多信息，请参阅"搜索入侵指标 (IoC) 和可疑活动"（第 802 页）。

语法

操作	示例
选择数据源 选择查询要操作的数据源。此运算符必须是查询中的第一个运算符。	`eventType`

筛选数据
根据条件筛选数据，必须以`where`关键字开头。
请注意以下筛选选项：
• 字符串可以用单引号或双引号括起来。
• 可以使用`AND`和`OR`等逻辑运算符来组合筛选器。
`key = value AND key < value OR key = value`
• 可以在运算符周围添加括号：
`(key = value) AND (key < value OR key = value)`
• 使用`CONTAINS`进行部分字符串匹配：
`key CONTAINS 'value'`
• 使用`ICONTAINS`进行不区分大小写的部分字符串匹配：
`key ICONTAINS 'value'`
• 使用`IN`进行成员资格检查：
`key IN ('value1', 'value2')`
• 根据RE2标准使用正则表达式匹配：
`key MATCHES 'regex string'`
	`eventType | where field == 'value'`
	`eventType | where field != 'value'`
	`eventType | where field > 'value'`
	`eventType | where field < 'value'`
	`eventType | where field >= 'value'`
	`eventType | where field <= 'value'`
	`eventType | where field CONTAINS 'substring'`
	`eventType | where field NOT CONTAINS 'substring'`
	`eventType | where field ICONTAINS 'substring'`
	`eventType | where field NOT ICONTAINS 'substring'`
	`eventType | where field IN ('value1', 'value2')`
	`eventType | where field NOT IN ('value1', 'value2')`
	`eventType | where field MATCHES 'value1*'`
	`eventType | where field NOT MATCHES 'value1*'`

选择字段 指定从查询中选择并返回哪些字段。	`eventType | columns field1, field2, field3 ...`

排序
对查询结果进行排序，可以按升序或降序排序，若不指定排序方式，则默认按升序排序。
	`eventType | order field1, field2, field3 ...`
	`eventType | order field asc`
	`eventType | order field desc`

限制 限制查询的结果。	`eventType | limit 10` `eventType | limit 1000 | group [field1, field2] | limit 10`
组操作 对数据执行`group operation`。	`eventType | group [field]` `eventType | group [field1, field2, field3, ...]`

操作	示例
(可选)您以指定对聚合字段执行的聚合函数,或者只指定聚合函数,而不对特定字段执行 group operation。	eventType | group with [max(field1), min(field2), avg(field3)] eventType | group [field1, field2, field3, ...] with [max(field1), min(field2), avg(field3)] eventType | group [field1, field2, field3, ...] with [max(field1) as max_field, min(field2), avg(field3) as avg_field]
聚合 聚合查询结果来执行操作。 这些功能只能与group operation一起使用(见上文)。	min(field) max(field) avg(field) count() count(field) countdistinct(field)

示例查询

本节包含许多示例查询,用于说明如何将 XQL 语法规则应用于查询。

- 从 WinProcCreate 事件类型中选择字段:

```
WinProcCreate | columns host_name, parent_start, parent_gpid, parent_pid, parent_
user, proc_name
```

- 使用条件进行筛选,然后按proc_name对结果进行分组,并对parent_pid应用聚合函数min():

```
WinProcCreate | where host_name == 'BNi-Kub' AND parent_pid != -1 AND proc_name
CONTAINS '1' AND host_name IN ('Computer1') | group [proc_name] with [min(parent_
pid)]
```

- 使用筛选器选择数据,然后计算返回的行数并对其进行排序:

```
WinProcCreate | where host_name == 'BNi-Kub' | group with [count() as new_count] |
order new_count
```

- 使用正则表达式筛选器选择数据：

```
WinProcCreate | where host_name matches 'BNi.*'
```

- 使用复杂筛选器选择数据并限制结果：

```
WinProcCreate | where (host_name contains 'BNi-Kub') OR (host_name in
('Computer1', 'Computer2')) | limit 10
```

- 使用筛选器选择数据，然后计算返回的不同行数：

```
WinProcCreate | where host_name == 'BNi-Kub' | group with [countdistinct(*)]
```

- 使用筛选器选择数据、按字段排序并限制返回的行数：

```
WinProcCreate | where host_name == 'BNi-Kub' | order host_name | limit 10
```

事件类型和字段

本部分包括：

- 事件类型
- 示例数据类型
- 事件字段

事件类型

名称	描述	类型
WinProcCreate 有关可用字段的更多信息，请参阅 WinProcCreate。	Windows 进程创建事件	事件
WinProcTerminate 有关可用字段的更多信息，请参阅 WinProcTerminate。	Windows 进程终止事件	事件
WinNetAccess	Windows 网络访问事件	事

名称	描述	类型
有关可用字段的更多信息，请参阅 WinNetAccess。		件
WinRegAccess 有关可用字段的更多信息，请参阅 WinRegAccess。	Windows 注册表访问事件	事件
WinScriptExec 有关可用字段的更多信息，请参阅 WinScriptExec。	Windows 脚本执行事件(包括 PowerShell、VBS 等)	事件
WinFileAccess 有关可用字段的更多信息，请参阅 WinFileAccess。	Windows 文件访问事件(读/写)	事件
WinLogin 有关可用字段的更多信息，请参阅 WinLogin。	Windows 用户登录事件	事件
WinLogout 有关可用字段的更多信息，请参阅 WinLogout。	Windows 用户注销事件	事件
WinAgentDetection 有关可用字段的更多信息，请参阅 WinAgentDetection。	Windows 检测事件	检测

示例数据类型

数据类型	示例	描述
String	`WinProcCreate | where host_name == 'BNi-Kub'` `WinProcCreate | where host_name == "BNi-Kub"`	字符串必须用单引号或双引号括起来。
UUID	`WinProcCreate | where agent_id == '61f0c404-5cb3-11e7-907b-a6006ad3dba0'` `WinProcCreate | where agent_id == "61f0c404-5cb3-11e7-907b-a6006ad3dba0"`	UUID 是字符串值，必须用单引号或双引号括起来。 UUID 值必须符合 8-4-4-4-12 序列。
DateTime	`WinProcCreate | where event_time < '2022-11-01'` `WinProcCreate | where event_time < "2022-11-01"`	DateTime 是一个字符串值，必须用单引号或双引号括起来。 DateTime 必须采用 YYYY-MM-DD 格式。
Bool	`WinLogin | where is_admin == 1` `WinLogin | where is_admin == 0`	Boolean 值可以用 `1`、`0`、`true` 或 `false` 表示。

数据类型	示例	描述

	`WinLogin | where is_admin == true`
	
	`WinLogin | where is_admin == false`	

整数	`WinLogin | where proc_pid > 25`	一个整数值。

事件字段

事件类型	字段(数据类型)
WinProcCreate	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_prod (String) • proc_prod_desc (String) • proc_sha1 (String) • proc_sha256 (String) • proc_signatures (String)

事件类型	字段(数据类型)
	• proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinProcTerminate	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • term_args (String) • term_gpid (UUID) • term_integrity_level (String) • term_md5 (String) • term_name (String) • term_oname (String) • term_path (String) • term_pid (Int) • term_sha1 (String) • term_sha256 (String) • term_start (DateTime) • term_upn (String) • term_user (String)

事件类型	字段(数据类型)
	• term_user_domain (String) • timestamp (DateTime)
WinNetAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • net_dst_ip (String) • net_dst_port (Int) • net_host (String) • net_http_method (String) • net_http_url (String) • net_protocol (String) • net_src_ip (String) • net_src_port (Int) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String)

事件类型	字段(数据类型)
	• proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinRegAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String)

事件类型	字段(数据类型)
	• reg_key (String) • reg_operation (String) • reg_original_key (String) • reg_original_value_data (String) • reg_value_data (String) • reg_value_name (String) • reg_value_type (String) • resource_id (UUID) • timestamp (DateTime)
WinScriptExec	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime)

事件类型	字段(数据类型)
	• proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • script_data (String) • script_fragment (Bool) • script_size (Int) • script_type (String) • timestamp (DateTime)
WinFileAccess	• agent_id (UUID) • customer (String) • event_time (DateTime) • file_md5 (String) • file_name (String) • file_op (String) • file_path (String) • file_sha1 (String) • file_sha256 (String) • host_name (String) • id (UUID) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String)

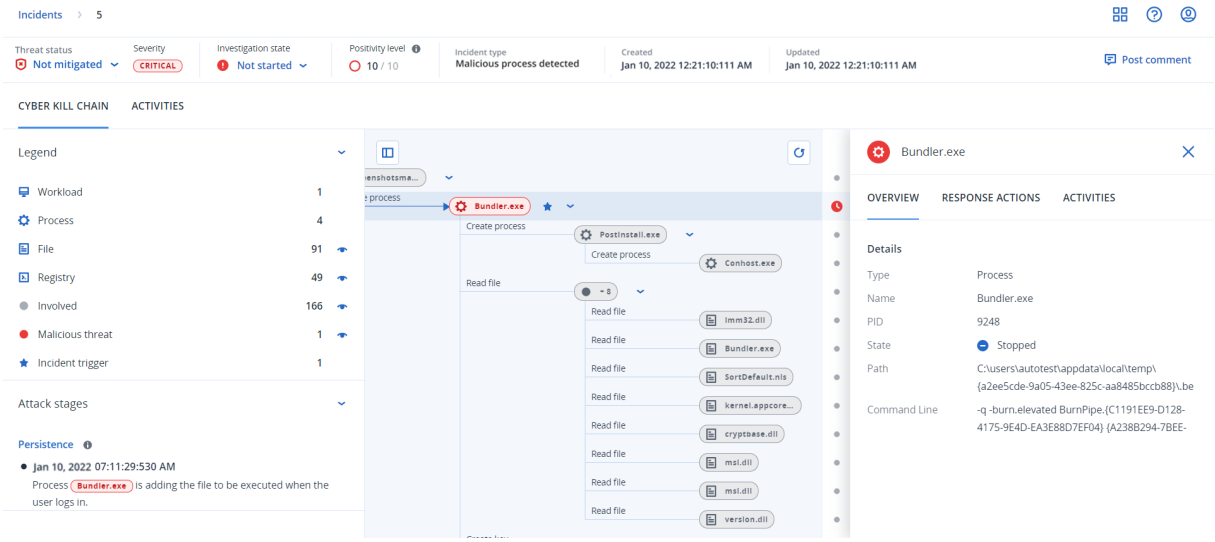
事件类型	字段(数据类型)
	• proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • timestamp (DateTime)
WinLogin	• agent_id (UUID) • customer (String) • domain (String) • event_time (DateTime) • host_name (String) • id (UUID) • is_admin (Bool) • login_time (DateTime) • name (String) • owner (String) • resource_id (UUID) • security_id (String) • timestamp (DateTime) • type (String)
WinLogout	• agent_id (UUID) • customer (String) • event_time (DateTime) • host_name (String) • id (UUID) • logout_time (DateTime) • resource_id (UUID) • security_id (String) • timestamp (DateTime)
WinAgentDetection	• agent_id (UUID) • customer (String) • detection_type (String) • event_time (DateTime) • file_md5 (String) • file_name (String)

事件类型	字段(数据类型)
	• file_path (String) • file_sha1 (String) • file_sha256 (String) • host_name (String) • id (UUID) • mitre_stid (Int) • mitre_tactics (Array(Int)) • mitre_tid (Int) • owner (String) • parent_args (String) • parent_gpid (UUID) • parent_integrity_level (String) • parent_md5 (String) • parent_name (String) • parent_oname (String) • parent_path (String) • parent_pid (Int) • parent_sha1 (String) • parent_sha256 (String) • parent_start (DateTime) • parent_upn (String) • parent_user (String) • parent_user_domain (String) • proc_args (String) • proc_gpid (UUID) • proc_integrity_level (String) • proc_md5 (String) • proc_name (String) • proc_oname (String) • proc_path (String) • proc_pid (Int) • proc_sha1 (String) • proc_sha256 (String) • proc_start (DateTime) • proc_upn (String) • proc_user (String) • proc_user_domain (String) • resource_id (UUID) • severity (String) • threat_name (String) • timestamp (DateTime)

事件类型	字段(数据类型)
	• url (String) • url_blocked (Bool) • url_cat (Array(String)) • url_list (String) • url_md5 (String)

调查事件

Endpoint Detection and Response (EDR) 使您能够调查整个事件，包括受攻击影响的所有攻击阶段和对象(进程、注册表、预定任务和域)。这些对象由易于理解的网络杀伤链中的节点表示，如下所示。使用网络杀伤链，可快速了解发生的具体情况以及何时发生。



将在网络杀伤链中查看攻击的每一步，这会为您详细说明事件发生的情况和原因。网络杀伤链使用易于理解的句子和图表，来帮助说明攻击的每一步，进而有助于最大程度地减少调查时间。

通过将攻击演变映射到 MITRE 框架，可以快速了解事件的范围和影响。这使您能够分析攻击的每一步中发生的情况，包括：

- 初始进入点
- 攻击如何执行
- 任何权限升级
- 规避检测技术
- 横向移动到其他工作负载
- 凭证盗取
- 渗出尝试

您还可以单击 **Copilot** 以启动 Copilot 聊天工具，使您可以输入多个请求并接收所选事件的建议响应操作。有关详细信息，请参阅 "如何调查网络杀伤链中的事件"(第 817 页)。

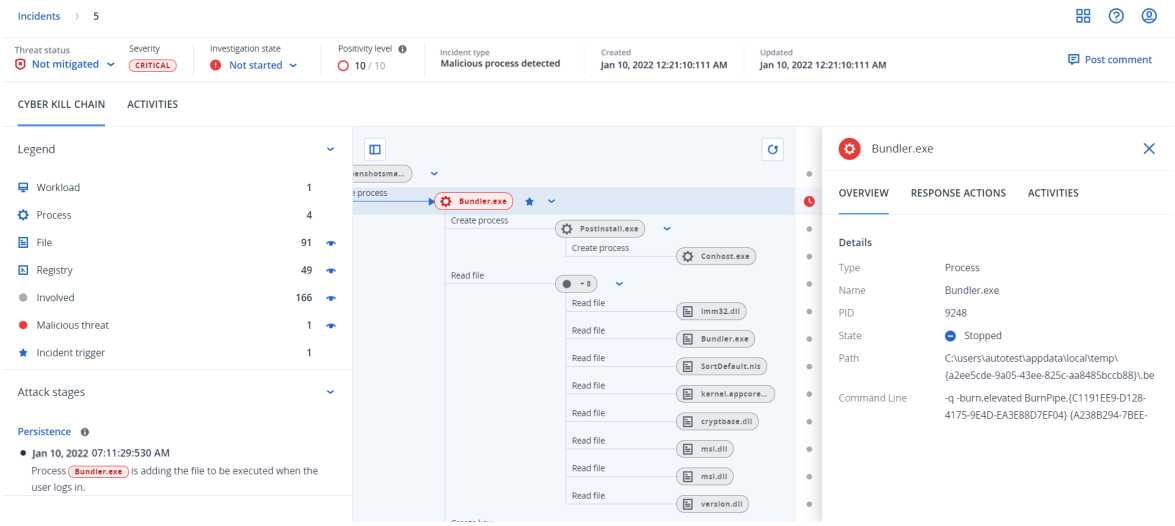
注意
受攻击影响的每个对象(无论是进程、注册表、预定任务还是域)都由网络杀伤链中的节点表示。

如何调查网络杀伤链中的事件

可以调查网络杀伤链中攻击的每一步。遵循网络杀伤链中易于理解的语句和图表,可了解攻击的每一步,这反过来有助于最大程度地减少调查时间。

开始调查网络杀伤链

1. 在 Cyber Protect 中控台中,转到**保护 > 事件**。
2. 在显示的事件列表中,单击要调查的事件最右侧列中的 。选定事件的网络杀伤链即会显示。



3. 在页面顶部的威胁状态栏中,查看事件摘要。威胁状态栏包括以下信息:
   - 当前威胁状态:威胁状态由系统自动定义。任何处于**未缓解**状态的事件都应尽快进行调查。

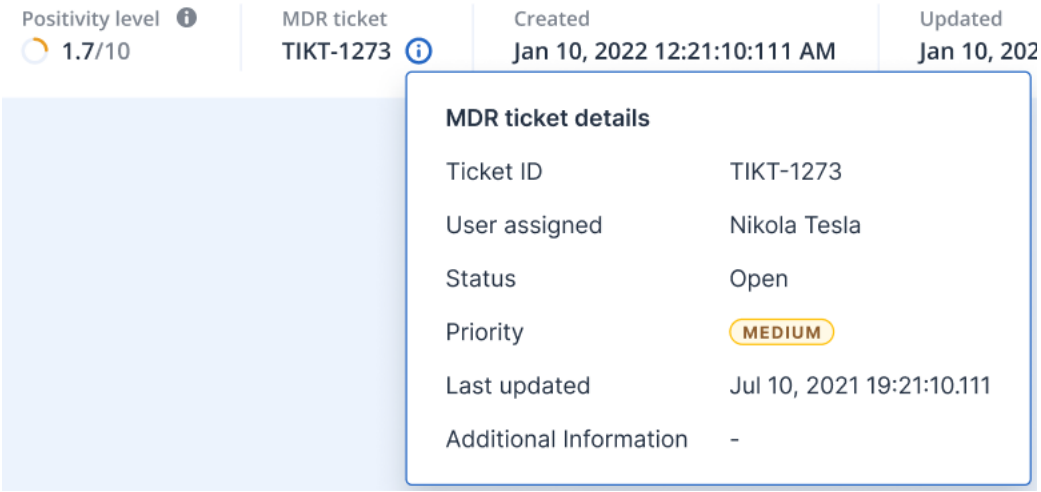
     重要事项
     当从备份恢复成功完成或所有检测都已通过停止进程、隔离或回滚操作成功修复时,事件会设置为**已缓解**。

     当从备份恢复未成功完成,或者至少有一个检测未通过停止进程、隔离或回滚操作成功修复时,事件会设置为**未缓解**。

     还可以手动将威胁状态设置为**已缓解**或**未缓解**。当选择任一状态时,系统会提示您输入注释。此注释将保存为调查活动的一部分,可以在**活动**选项卡中进行查看。请注意,如果发现事件的新检测或响应操作运行并成功完成,EDR 仍可以将威胁状态恢复为**已缓解**或**未缓解**。

   - 事件严重性:**严重**、**高**或**中**。有关详细信息,请参阅 "查看事件"(第 797 页)。
   - 当前调查状态:**正在调查**、**未启动**(默认状态)、**误报**或**已关闭**中的一个。当您开始调查事件时,应该更改该状态,以便其他同事会注意到对事件所做的任何更改。
   - 确定性级别:指示事件是真正恶意攻击的可能性,介于 1-10 之间。有关详细信息,请参阅 "查看事件"(第 797 页)。

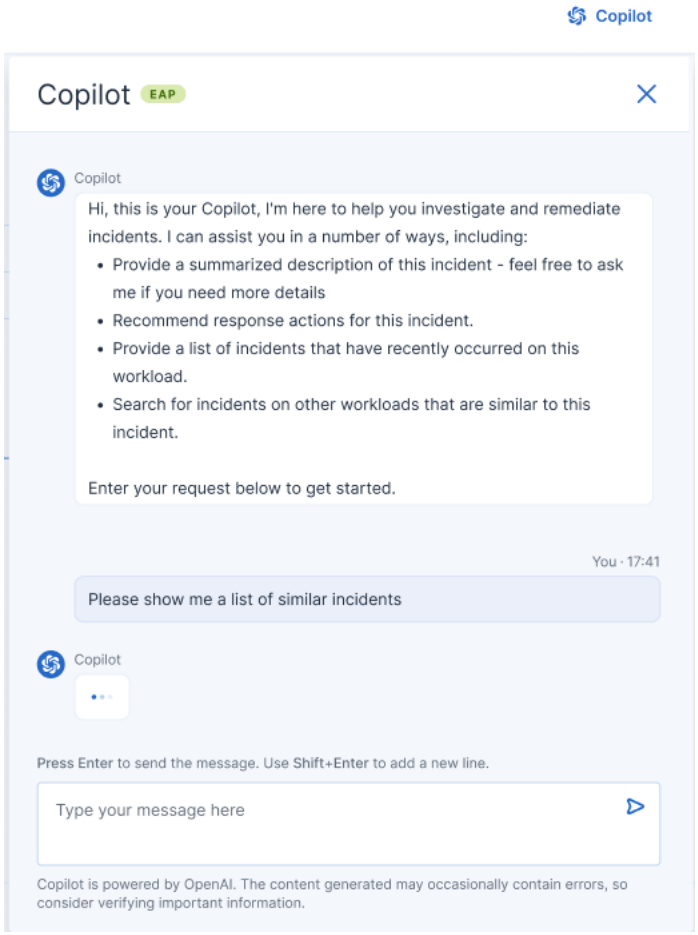
- 事件类型：**检测到勒索软件**、**检测到恶意软件**、**检测到可疑进程**、**检测到恶意进程**、**阻止可疑 URL** 和**阻止恶意 URL** 中的一项或多项。
- 如果在工作负载上启用了托管检测和响应 (MDR)，则会显示**MDR 票证**字段。可以查看为事件创建的 MDR 票证以及指派给事件的 MDR 安全分析师的详细信息。



- 创建和更新事件的时间：检测到事件的日期和时间，或上次使用事件内记录的新检测更新事件的时间。

4. 单击**图例**选项卡以查看组成杀伤链图的各个节点，并定义要查看的节点。有关更多信息，请参阅 "了解并自定义网络杀伤链视图"(第 819 页)。
5. 通过执行以下步骤来调查和修复事件。请注意，这是调查和修复事件的典型工作流，但可能因每个事件和您自己的要求而异。
   a. 在**攻击阶段**选项卡中，调查攻击的每个阶段。有关更多信息，请参阅 "如何导航攻击阶段"(第 821 页)。
   b. 单击 **纠正整个事件** 以应用纠正操作。有关详细信息，请参阅 "修复整个事件"(第 830 页)。您还可以按照 "各个网络杀伤链节点的响应操作"(第 834 页) 中的说明，纠正网络杀伤链中的单个节点。

      或者，单击 **Copilot** 以启动 AI 辅助的 Copilot 聊天工具。Copilot 根据事件提供响应选项和事件相关的上下文信息，例如有关攻击类型的详细信息。您可以选择相关的响应选项，然后按照屏幕上的说明操作。这些响应选项的说明如 "各个网络杀伤链节点的响应操作"(第 834 页) 所示。



重要事项
使用 Copilot 时，每个合作伙伴租户每月的请求限制为 1000 个。当达到此限制时，将显示错误消息，通知您已超出每月限制。

c. 在**活动**选项卡中，查看为缓解事件而执行的操作。有关更多信息，请参阅 "了解为缓解事件而执行的操作"(第 824 页)。

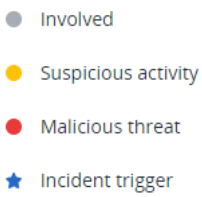
了解并自定义网络杀伤链视图

要了解在网络杀伤链中受影响的节点，请访问图例。图例会显示事件中涉及的所有节点，从而使您能够了解攻击者如何影响各个节点。还可以定义要在网络杀伤链中隐藏或显示的节点。

访问图例

1. 单击“图例”部分右侧的箭头图标。
   “图例”部分即会展开，如下所示。

2. 图例中使用了四种主要颜色，这使您能够快速了解网络杀伤链中每个节点的情况，如下所示。这些颜色编码的节点也会包括在攻击阶段中，如 "如何导航攻击阶段"(第 821 页) 中所述。



隐藏或显示网络杀伤链中的节点

1. 在展开的“图例”部分中，确保 显示在要在网络杀伤链中显示的节点旁边。如果显示的图标为 ，请单击该图标以将其更改为 。
2. 要隐藏网络杀伤链中的节点，请单击 。图标即会更改为 ，并且节点不会显示在网络杀伤链中。

调查事件的攻击阶段

通过事件的攻击阶段，可轻松了解对每个事件的解释。

每个攻击阶段都汇总了具体发生的情况以及针对的目标(在网络杀伤链中称为 *节点*) 。例如，如果下载的文件伪装成其他文件，则攻击阶段会指出这一点，并包括指向可以调查的网络杀伤链中相关节点的链接，以及指向相关 MITRE ATT&CK 技术的链接。

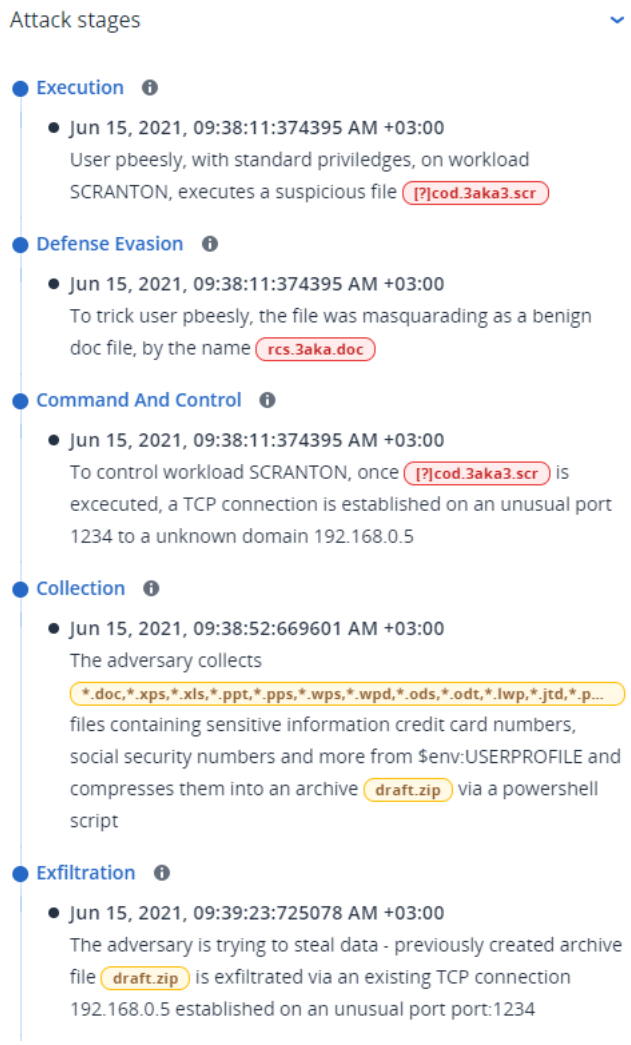
攻击的每个阶段都会为您提供解决三个关键问题所需的信息：

- 攻击者的目标是什么?
- 攻击者如何实现这一目标?
- 针对哪些节点?

更重要的是,提供的解释可确保显著减少调查事件所花费的时间,这是因为您不再需要从时间线或图形节点查看每个安全事件,然后尝试创建攻击的解释。

攻击阶段还包括有关包含敏感信息(如信用卡号和社会保障号码)的遭盗取文件的信息,如下面示例中的**收集**阶段所示。

有关详细信息,请参阅 "攻击阶段包含哪些信息? "(第 822 页)。



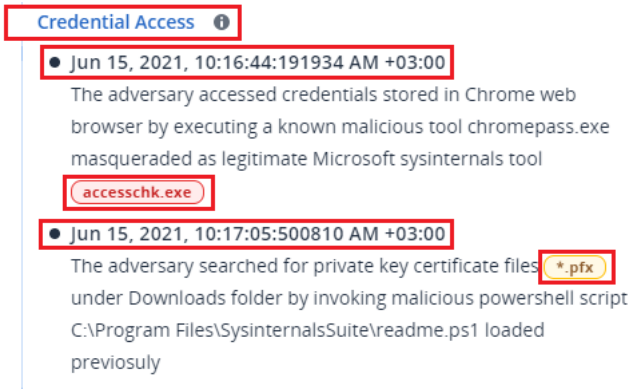
如何导航攻击阶段

攻击阶段会按时间顺序列出。向下滚动以查看事件的攻击阶段的完整列表。

要进一步调查特定攻击阶段,请单击攻击阶段中的任何位置,以导航到网络杀伤链图中的相关节点。有关导航网络杀伤链图和特定节点的详细信息,请参阅 "调查网络杀伤链中的各个节点"(第 823 页)。

攻击阶段包含哪些信息?

每个攻击阶段都以易于阅读的人类语言,提供易于理解的攻击解释。该解释由如下所示和下表所述的许多要素组成。



攻击阶段元素	描述
标题	描述攻击者试图执行的操作及其目标(在上例中,**凭据访问**),并提供指向已知 MITRE ATT&CK 技术的链接。单击该链接,可了解有关 MITRE ATT&CK 网站的详细信息。 **注意** 如果攻击阶段不是已知的 MITRE ATT&CK 技术,则不会链接标头文本。这与通用技术有关,例如在随机文件夹中检测到的文件。
时间戳	攻击阶段发生的时间。
技能	攻击者在技术上如何实现其目标,以及受影响的对象(注册表项、文件或预定任务)。 攻击技术的文本描述中包含的是指向网络杀伤链中每个受影响节点的颜色编码链接,如上图中所示。通过这些颜色编码链接,可以快速导航到受影响的节点,并调查确切发生的情况。攻击阶段使用的颜色的含义如下所示: ● Involved ● Suspicious activity ● Malicious threat ★ Incident trigger 通过查看上面的图例,我们可以看到"凭证访问"示例攻击阶段有指向恶意软件节点

攻击阶段元素	描述
	accesschk.exe 和可疑文件节点 *.pfx 的链接(单击这些链接，可跳转到网络杀伤链中的相应节点)。有关导航这些节点和可用操作的详细信息，请参阅 "调查网络杀伤链中的各个节点"(第 823 页)。 请注意，攻击阶段还包括指向文件节点的链接，这些文件节点有包含敏感信息(如受保护的运行状况信息 (PHI)、信用卡号和社会保障号码)的遭破坏文件的相关信息。

注意
每个攻击阶段都是单个检测事件。每个阶段中列出的内容(标头、时间戳、技术)是根据检测事件中的特定参数生成的，这些参数基于 Endpoint Detection and Response (EDR) 存储的攻击阶段模板。

调查网络杀伤链中的各个节点

除了查看攻击阶段之外，还可以导览网络杀伤链中的每个攻击节点。这使您能够深入到网络杀伤链中的特定节点，并根据需要调查和修复每个节点。

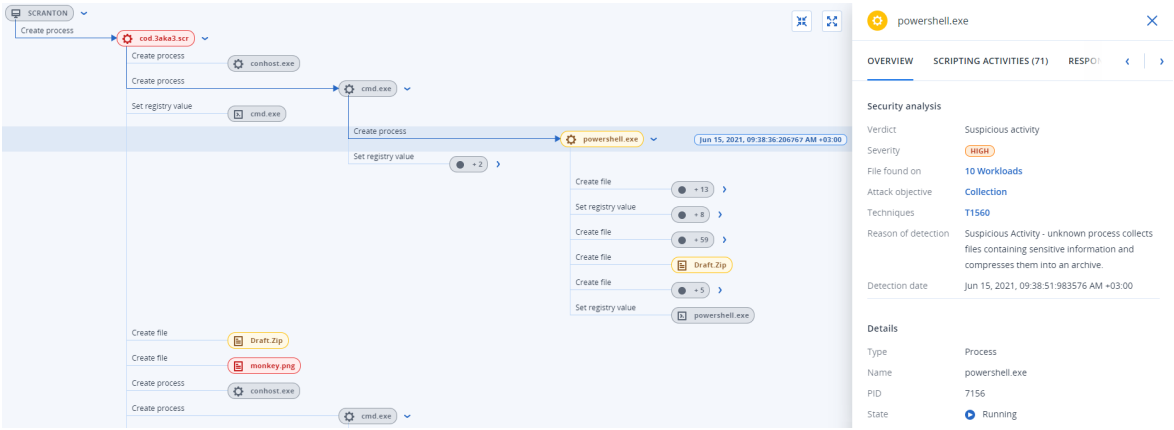
例如，可以确定某个事件是真正恶意攻击的可能性。根据调查，还可以将许多响应操作应用于节点，包括隔离工作负载或隔离可疑文件。

调查网络杀伤链中的各个节点

1. 在 Cyber Protect 中控台中，转到**保护 > 事件**。
2. 在显示的事件列表中，单击要调查的事件最右侧列中的 。选定事件的网络杀伤链即会显示。
3. 导航到相关节点，然后单击它以显示该节点的侧边栏。

   注意
   单击该节点以展开它，并显示关联的节点。

   例如。单击下面示例中的 **powershell.exe** 节点将打开该节点的侧边栏。还可以单击节点旁边的箭头图标以查看可能受 **powershell.exe** 节点影响的关联节点，包括文件和注册表值。反之，可以单击这些关联节点以进一步调查。



4. 调查侧边栏选项卡中包含的信息：
   - **概述**：包括两个主要部分，提供受攻击节点的安全摘要。
     - **安全分析**：提供受攻击节点的分析，包括 EDR 对威胁的裁决（如可疑活动）、根据 MITRE 攻击技术确定的攻击目标（单击相应链接可转到 MITRE 网站）、检测原因以及可能受攻击影响的工作负载数量（单击 **n 个工作负载**链接可查看受影响的工作负载）。

       注意
       n 个工作负载链接表示已在其他工作负载上*找到*特定的恶意或可疑对象。这并不意味着攻击发生在这些其他工作负载上，而是表明这些其他工作负载上存在侵入的迹象。攻击可能已经发生（并产生了另一个事件），或者攻击者正准备使用其攻击“工具包”来攻击这些其他工作负载。

     - **详细信息**：包括有关节点的详细信息，其中包括其类型、名称和当前状态、节点路径以及任何文件哈希和数字签名（如 MD5 和证书序列号）。
   - **脚本活动**：包括攻击中调用或加载的任何脚本的详细信息。单击  ，可将脚本复制到剪贴板以进一步调查。

     注意
     仅为运行命令或脚本（如 cmd 或 PowerShell 命令）的进程节点显示**脚本活动**选项卡。

   - **响应操作**：包括多个部分，提供其他调查、修复和预防操作，具体取决于节点类型。
     例如，对于工作负载节点，可以定义许多响应（包括取证备份和从备份恢复）。或者，对于恶意或可疑节点，可以停止或隔离节点、回滚攻击所做的更改，以及将节点添加到保护计划白名单或黑名单中。
     有关将响应操作应用于特定节点的详细信息，请参阅 "各个网络杀伤链节点的响应操作"（第 834 页）。
   - **活动**：按时间顺序显示应用于事件的操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"（第 824 页）。

了解为缓解事件而执行的操作

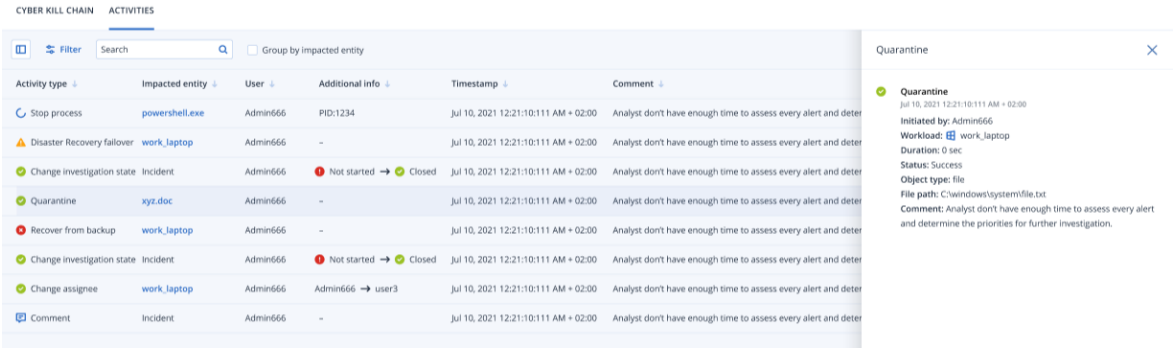
在已查看事件并调查攻击如何发生之后，通常将应用响应操作。在应用响应操作后，就可以在多个地方查看这些操作，以便更好地了解为缓解事件所执行的步骤。

注意
预防层创建的事件会自动应用在保护计划中配置的操作。对于检测点，需要定义相关响应操作，以用于缓解每个攻击情形。

要了解所执行的响应操作，可以查看应用于整个事件的所有响应操作，也可以查看应用于事件网络杀伤链中特定节点的操作。

查看应用于事件的所有响应操作

1. 在 Cyber Protect 中控台中，转到**保护 > 事件**。
2. 在显示的事件列表中，单击要调查的事件最右侧列中的 。选定事件的网络杀伤链即会显示。
3. 单击**活动**选项卡。
   已应用于事件的响应操作列表即会显示。

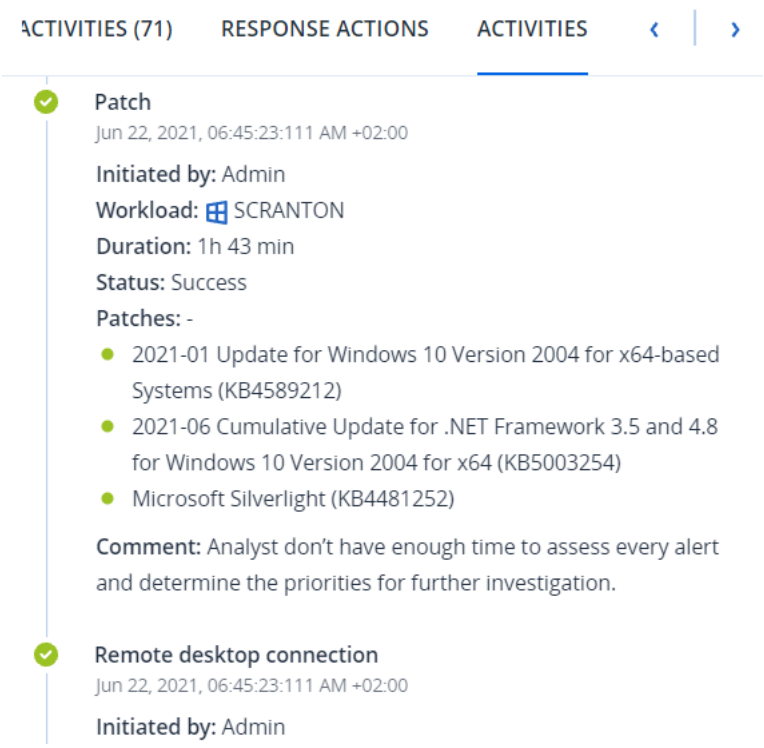


注意
如果响应操作是作为自动化工作流程的一部分启动的，则 **启动者** 字段将显示 **自动化工作流程**。有关详细信息，请参阅 "使用自动化工作流"(第 851 页)。

4. 可以对显示的列表执行许多操作：
   - 单击活动类型行，可显示有关选定活动的更多信息。信息会显示在侧边栏中(如步骤 3 中所示)，其中包括操作发起者、其状态、文件路径以及发起者添加的任何注释的相关详细信息。
   - 使用**搜索**框，来搜索特定操作。
   - 单击**过滤器**，以将过滤器应用于列表。
   - 选中**按受影响实体分组**复选框，以根据实体对相关操作进行分组。
   - 单击 以显示/隐藏已完成操作的列表。
     确保 显示在要显示的操作旁边。如果要在显示的列表中隐藏某个操作，请再次单击以将其更改为 。

查看应用于特定节点的响应操作

1. 在网络杀伤链中，单击某个节点可查看该节点的侧边栏。
2. 单击**活动**选项卡。



3. To get a complete understanding of what actions were applied and why, you may need to scroll through the applied response actions for the node.For example, for remote desktop connection actions, you can view who started the action and when, the duration of the action, and its overall status (if it succeeded, failed, or succeeded with errors).

注意
如果响应操作是作为自动化工作流程的一部分启动的，则 **启动者** 字段将显示 **自动化工作流程**。有关详细信息，请参阅 "使用自动化工作流"(第 851 页)。

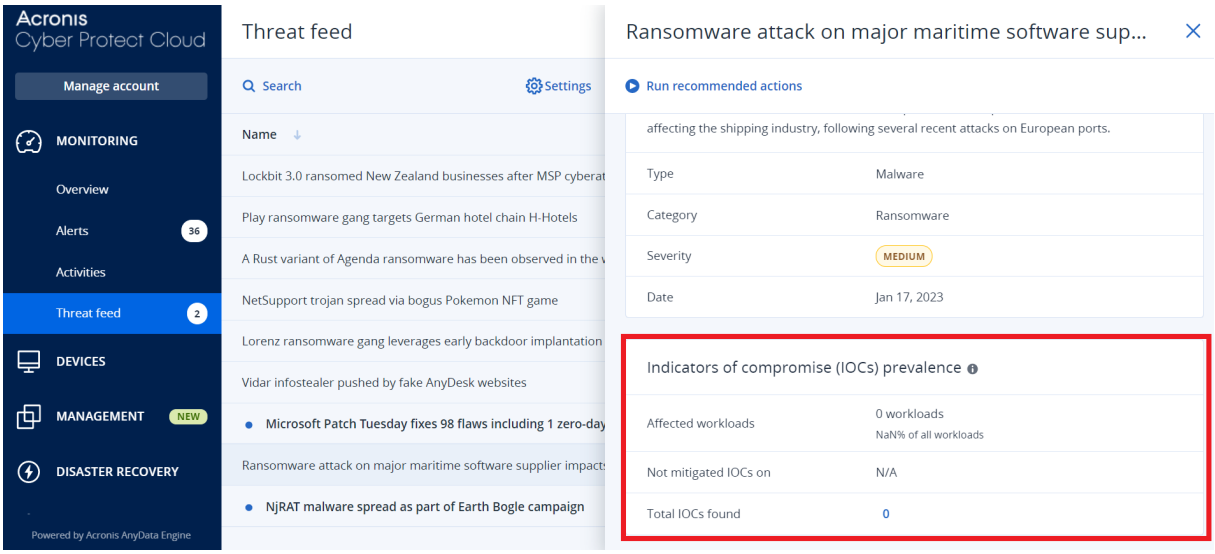
检查工作负载上众所周知攻击的危害指标 (IOC)

Endpoint Detection and Response (EDR) 使您能够查看威胁源中针对工作负载的现有已知攻击。这些威胁源是根据从网络安全保护运营中心 (CPOC) 收到的威胁数据自动生成的；EDR 使您能够验证威胁是否影响工作负载，然后采取必要步骤来消除威胁。

可以从 Cyber Protect 中控台中的**监视**菜单访问威胁源。有关详细信息，请参阅 "威胁源"(第 253 页)。

要查看特定的威胁详细信息并确认它们是否会影响工作负载，请单击威胁源。可以查看检测到的 IOC 数量和受影响的工作负载，并深入到包含 IOC 未缓解的工作负载。

注意
如果保护计划未启用 EDR，则不会显示如下所示的该附加威胁源功能。



定义威胁源设置

可以定义许多威胁源设置，以自动定位并缓解任何已知威胁。

定义威胁源设置

1. 在 Cyber Protect 中控台中，转到**监视 > 威胁源**。
2. 在显示的“威胁源”页面上，单击**设置**。
3. 在显示的对话框中，选择以下任一选项：

选项	描述
搜索危害指标(IOC)	单击该开关，可启用自动搜索工作负载上的 IOC。 启用此选项后，还会显示**对检测的操作**和**生成警报**选项。
对检测的操作	从下拉列表中，选择在工作负载上发现威胁时要对相关文件执行的操作： • **无操作** • **隔离** • **删除** • **隔离工作负载**
生成警报	选中该复选框，以在工作负载上发现 IOC 时生成警报。警报将显示在“警报”页面中。

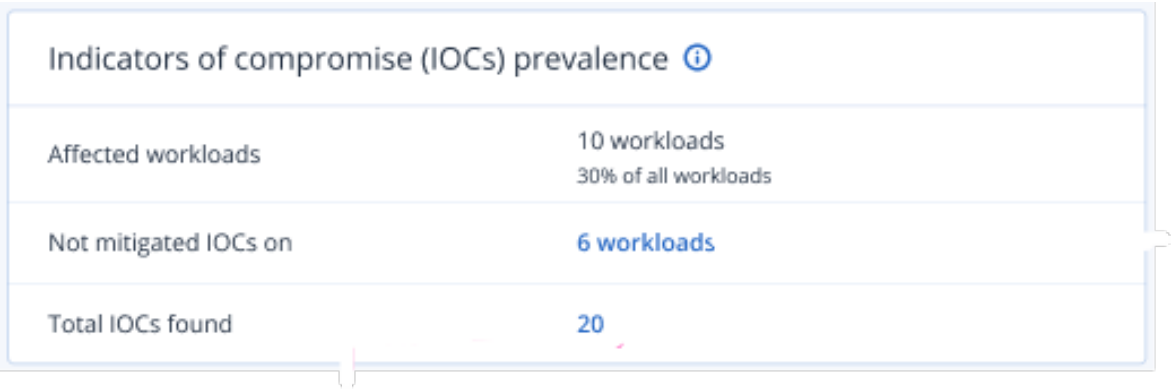
4. 单击**应用**。

查看并缓解受影响工作负载上的 IOC

在保护计划中启用 Endpoint Detection and Response (EDR) 后，可以查看正在影响保护计划中工作负载的任何已知威胁。还可以缓解未自动缓解的任何其余危害指标 (IOC)。有关如何自动缓解 IOC 的信息，请参阅 "定义威胁源设置"(第 828 页)。

查看并缓解受影响的工作负载

1. 在 Cyber Protect 中控台中，转到**监视 > 威胁源**。
2. 单击某个威胁，可显示该威胁的详细信息。
3. 在**危害指标(IOC)流行率**部分中，单击 ***n* 个工作负载**链接，以查看 IOC 未缓解的工作负载。



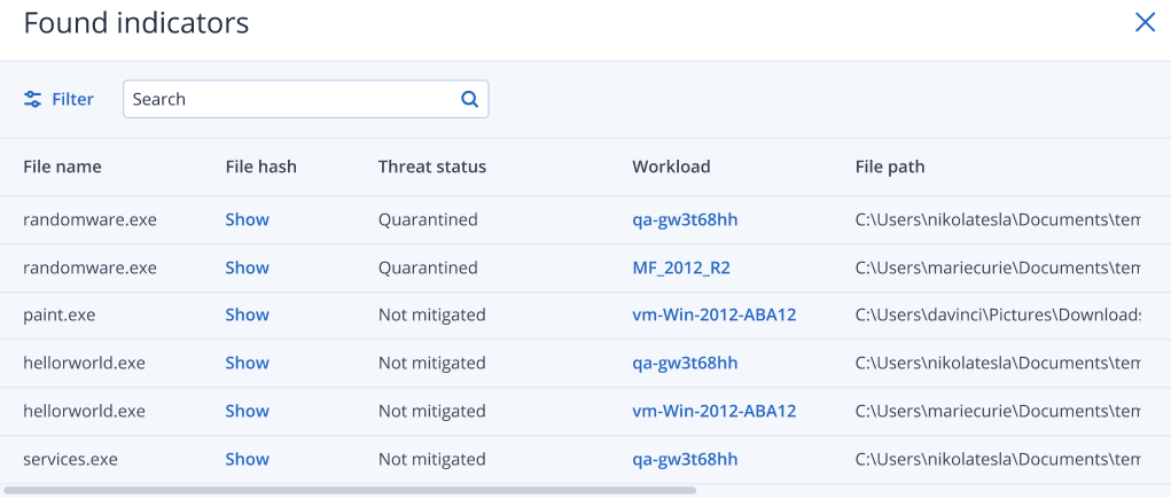
4. 在显示的“工作负载”页面中，单击相关工作负载并查看其详细信息。可以在工作负载上运行特定功能，包括定义要过滤的其他 URL(请参阅 "URL 过滤"(第 751 页))，以及阻止恶意进程(请参阅 "防病毒和反恶意软件保护设置"(第 732 页) 中的“排除”部分)。
例如，如果威胁源指示某个工作负载已受 IOC 影响，则请先定位并分析 IOC，如 "查看和分析发现的 IOC"(第 829 页) 中所述。然后，转到工作负载的保护计划并定义其他保护(例如，阻止恶意文件哈希或进程)。

查看和分析发现的 IOC

除了查看受已知威胁影响的任何工作负载，还可以查看和分析特定的危害指标 (IOC)。这使您能够查看受 IOC 影响的各个工作负载，并缓解 IOC。

查看和分析 IOC

1. 在 Cyber Protect 中控台中，转到**监视 > 威胁源**。
2. 单击某个威胁，可显示该威胁的详细信息。
3. 在**危害指标(IOC)流行率**部分中，单击**找到的 IOC 总数**链接。
“找到的指标”页面即会显示。



4. (可选)使用**过滤器**选项,可根据 IOC 的状态过滤 IOC 列表。还可以使用**搜索**选项来搜索特定 IOC。
5. 要查看受 IOC 影响的工作负载,请单击**工作负载**列中的链接。然后,可以对工作负载执行各种操作(例如,运行修补程序管理或修改保护计划)。
6. (可选)在**文件哈希**列中,单击**显示**可显示为特定 IOC 找到的文件哈希。在显示的对话框中,单击  可将 IOC 的文件哈希复制到文本编辑器。

修复事件

Endpoint Detection and Response (EDR) 使您能够修复整个事件或事件的个别攻击点。

通过修复整个事件,可以选择要对事件全局执行的修复。如果您需要更详细地管理事件,可以根据需要修复个别攻击点。例如,您可能想要隔离工作负载的网络,以停止横向移动或命令和控制 (C&C) 活动;这确保即使隔离了工作负载,所有 安克诺斯 Cyber Protect 技术仍能正常工作,并且可以启动调查。

EDR 会通过以下方式确保修复有效:

- 缓解 - 确保停止威胁。
- 恢复 - 确保服务立即恢复联机。
- 预防 - 确保在将来遭受的攻击中阻止某个攻击中使用的技术。

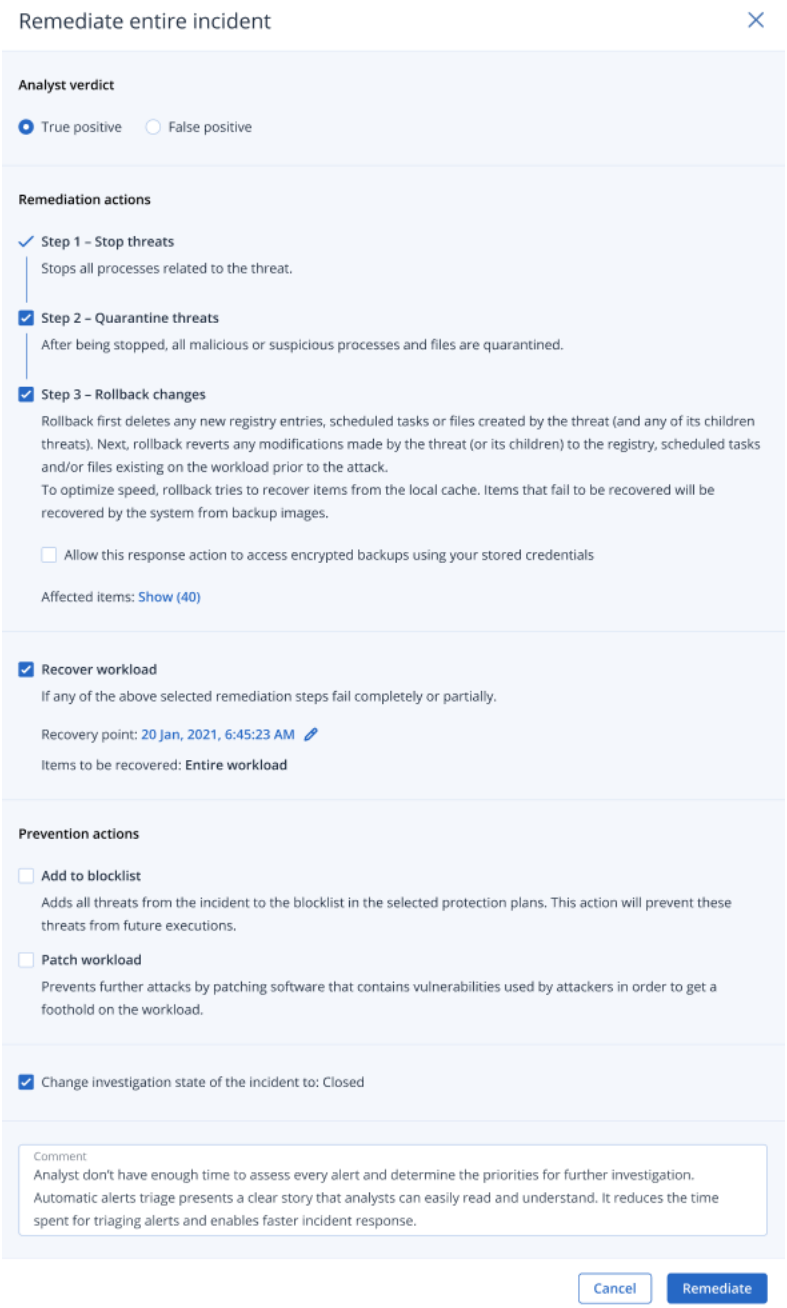
修复整个事件

通过修复整个事件,可以快速轻松地选择要对事件全局执行的修复。Endpoint Detection and Response (EDR) 会引导您逐步完成修复过程。

如果您需要更详细地管理网络和事件,请参阅 "各个网络杀伤链节点的响应操作"(第 834 页)。

修复整个事件

1. 在 Cyber Protect 中控台中,转到**保护 > 事件**。
2. 在显示的事件列表中,单击要调查的事件最右侧列中的  。选定事件的网络杀伤链即会显示。
3. 单击**修复整个事件**。“修复整个事件”对话框即会显示。



4. 在**分析裁决**部分中，请根据事件调查，选择以下选项之一：
   - **真正**：如果确定攻击是真正的攻击，则选择此选项。选中后，可以添加修复和预防操作，如以下步骤中所述。
   - **误报**：如果确定攻击不是真正的攻击，则选择此选项。在此模式下，可以定义如何防止这种情况再次发生（例如，将事件添加到保护计划白名单中）。

     注意
     在选择**误报**后，只能定义预防操作。有关详细信息，请参阅 "修复误报事件"（第 833 页）。

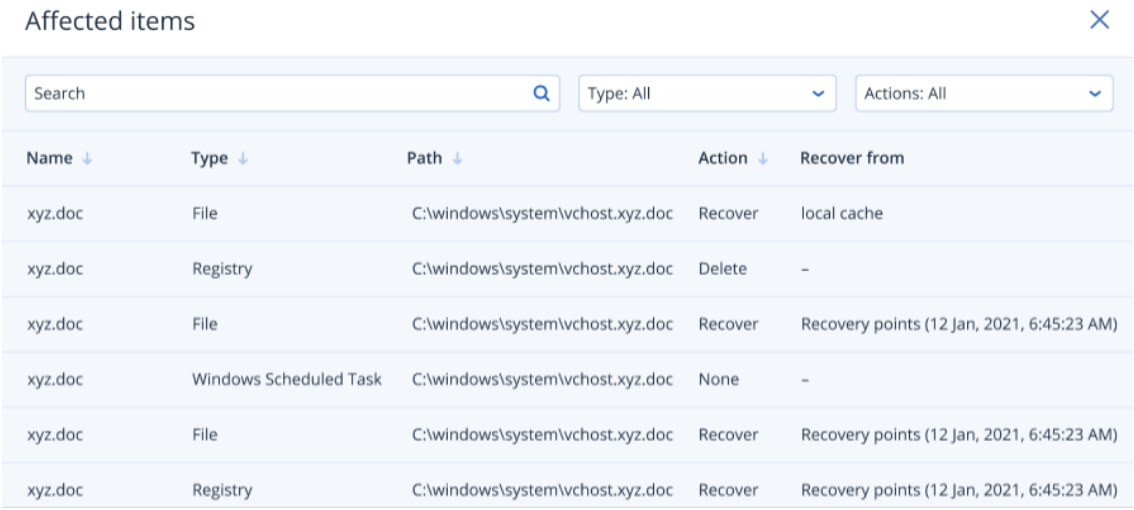
5. 在**修复操作**部分中，执行以下修复步骤。请注意，必须按顺序执行修复步骤；例如，在步骤 1 完成之前，不能选择步骤 2。

a. **步骤 1 - 停止威胁**：选中该复选框，可停止与威胁相关的所有进程。
b. **步骤 2 - 隔离威胁**：在停止威胁后，选中该复选框可隔离所有恶意和可疑的进程和文件。
c. **步骤 3 - 回滚更改**：在隔离威胁后，选中该复选框可删除由威胁（及其任何子威胁）创建的任何新注册表项、预定任务或文件。然后，回滚进程会恢复由威胁（或其子威胁）对攻击之前存在于工作负载上的注册表、预定任务和/或文件所做的任何修改。为了优化速度，回滚进程会尝试从本地缓存恢复项目。无法恢复的项目会由系统从备份映像恢复。

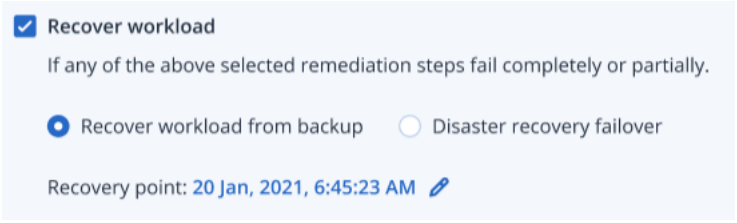
注意
回滚过程仅会从本地缓存中的项目恢复。在将来版本中，将可从备份存档回滚。

如果对相关备份的访问是加密的，请选中**允许此响应操作使用存储的凭据访问加密备份**复选框。EDR 访问存储的用户凭据以解密加密存档，并搜索相关文件。

还可以单击**受影响的项目**以查看受回滚影响的所有项目（文件、注册表或预定任务）、应用的操作（**删除**、**恢复**或**无**），以及是从本地缓存还是备份映像恢复项目。



d. **恢复工作负载**：如果以上任何修复步骤全部或部分失败，则选中该复选框可恢复工作负载。



选择以下恢复选项之一：

- **从备份中恢复工作负载**：使您能够从特定恢复点恢复工作负载。单击恢复点编辑图标，可从恢复备份列表中进行选择。
- **灾难恢复故障转移**：使您能够运行灾难恢复（如果已在保护计划中启用了此功能）。建议您对关键工作负载（如 AD 服务器或数据库服务器）使用此选项。有关详细信息，请参阅 "实施灾难恢复"（第 655 页）。

6. 在**预防操作**部分中，选择相关修复步骤：
   - **添加到黑名单**：选中该复选框，然后从显示的保护计划列表中选择相关保护计划。对于选定的保护计划，此预防操作可确保会阻止对事件执行所有检测。

- **修补工作负载**:选中该复选框可修补任何易受攻击的软件,并防止攻击者获取工作负载的访问权限。然后,可以选择要在修补完成后执行的相关操作(**不重新启动**、**重新启动**或**仅在需要时重新启动**),具体取决于用户是否已登录。
  还可以选中**备份正在进行时不重新启动**复选框,以确保在备份期间不会重新启动工作负载。

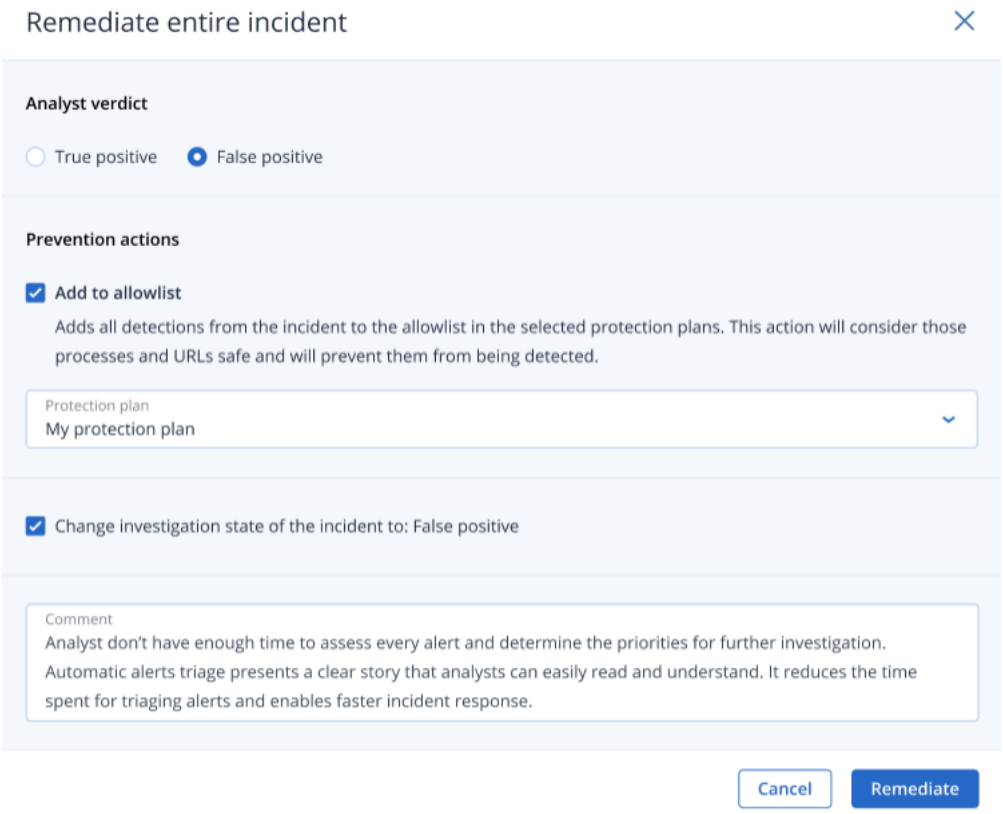
7. 选中**将事件的调查状态更改为:已解决**复选框。如果未选中,则调查状态仍会保持为其先前状态。
8. 单击**修复**。选择的修复操作即会逐步执行,同时每个修复步骤的进度会显示在"修复整个事件"对话框中。
   在单击后,该按钮会显示**转到活动**。单击**转到活动**以查看应用于事件的所有响应操作。有关详细信息,请参阅 "了解为缓解事件而执行的操作"(第 824 页)。

修复误报事件

如果您确定攻击不是真正的攻击(换句话说,是误报),则可以定义如何防止事件再次发生。例如,可以将事件添加到保护计划白名单中。

修复误报事件

1. 在选定事件的网络杀伤链中，单击**修复整个事件**。“修复整个事件”对话框即会显示。
2. 在**分析裁决**部分中，选择**误报**。



3. 在**预防操作**部分中，选中**添加到白名单**复选框。从显示的保护计划列表中，选择相关的保护计划。
   对于选定的保护计划，此预防操作可确保会阻止对事件的所有检测。
4. 选中**将事件的调查状态更改为:误报**复选框。
5. 单击**修复**。
   在单击后，该按钮会显示**转到活动**。单击**转到活动**以查看应用于事件的响应操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"(第 824 页)。

各个网络杀伤链节点的响应操作

如果需要更详细地管理事件，可以将各种响应操作应用于各个网络杀伤链节点。这些响应操作使您能够快速轻松地修复任何节点。

注意
要将全局响应操作应用于整个事件，请参阅 "修复整个事件"(第 830 页)。

响应操作分为以下类别，但并非所有节点都包括以下所有类别：

- **修复**：此类别中的操作使您能够立即对攻击作出响应，包括管理工作负载的网络隔离，以及删除和隔离文件、进程和注册表值。
- **调查**：此类别中的操作(仅适用于工作负载)使您能够运行取证备份或远程桌面连接，以便进行更深入的调查。

- **调查**:此类别中的操作(仅适用于工作负载)使您能够运行远程桌面连接,以便进行更深入的调查。
- **恢复**:此类别中的操作(仅适用于工作负载)使您能够通过运行从备份恢复或灾难恢复故障转移,来响应密集型攻击。
- **预防**:此类别中的操作使您能够通过将节点添加到保护计划白名单或黑名单中,来防止将来出现的威胁或误报。

注意

如果事件已关闭,则无法对节点应用响应操作。但是,可以通过更改调查状态为**正在调查**来重新打开已关闭的事件。在重新打开后,可以应用响应操作。

下表描述了网络杀伤链中的每个节点类型、每个节点的适用类别以及可用的响应操作。

节点	类别	响应操作
工作负载	修复	• 管理网络隔离 • 重新启动工作负载
	调查	• 取证备份 • 远程桌面连接
	调查	• 远程桌面连接
	恢复	• 从备份恢复 • 灾难恢复故障转移
	预防	• 修补
进程	修复	• 停止进程 • 隔离
	预防	• 添加到白名单 • 添加到黑名单
文件	修复	• 删除 • 隔离
	预防	• 添加到白名单 • 添加到黑名单

节点	类别	响应操作
登录	修复	• 删除
网络	预防	• 添加到白名单 • 添加到黑名单

定义受影响工作负载的响应操作

作为响应攻击的一部分，可以将以下操作应用于受影响的工作负载：

- **管理网络隔离**：使您能够管理工作负载的网络隔离，以停止横向移动或命令和控制 (C&C) 活动。有关详细信息，请参阅 "管理工作负载的网络隔离"(第 836 页)。
- **修补**：使您能够修补工作负载，以防止在将来可能遭受的攻击中利用漏洞。有关详细信息，请参阅 "修补工作负载"(第 839 页)。
- **重新启动工作负载**：使您能够立即重新启动工作负载，或根据预定义的超时时段重新启动工作负载。有关详细信息，请参阅 "重新启动工作负载"(第 840 页)。
- **法庭备份**：使您能够进行手动法庭备份以用于审计或进一步的调查。有关详细信息，请参阅 "在工作负载上运行手动取证备份"(第 841 页)。
- **远程桌面连接**：使您能够远程访问调查下的工作负载。有关详细信息，请参阅 "与工作负载的远程连接"(第 842 页)。
- **从备份恢复**：使您能够从备份或者特定文件或文件夹来恢复整台计算机。有关详细信息，请参阅 "从备份恢复"(第 843 页)。
- **灾难恢复故障转移**：使您能够运行 "实施灾难恢复"(第 655 页)。请注意，您的工作负载必须有 Advanced Disaster Recovery 的订购许可。有关详细信息，请参阅 "灾难恢复故障转移"(第 844 页)。

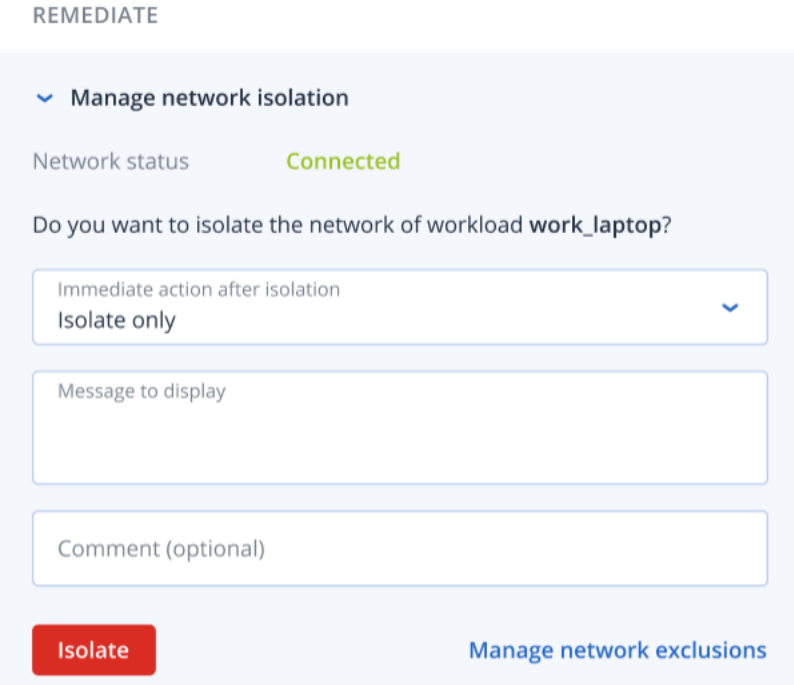
管理工作负载的网络隔离

EDR 使您能够管理工作负载的网络隔离，以停止横向移动或命令和控制 (C&C) 活动。根据您的要求，有许多隔离选项可供选择。请注意，即使隔离了工作负载，所有 安克诺斯 Cyber Protect 技术也能正常工作，从而确保可以充分开展调查。

将工作负载与网络隔离

1. 在网络杀伤链中，单击要修复的工作负载节点。
2. 在显示的侧边栏中，单击**响应操作**选项卡。

3. 在**修复**部分中，单击**管理网络隔离**。



注意

网络状态值指示工作负载当前是否已连接。如果该值显示为**已隔离**，则可以将隔离的工作负载重新连接到网络，如下面的步骤中所述。如果工作负载处于脱机状态，仍可以隔离工作负载；当工作负载恢复联机时，它会自动处于**隔离**状态。

4. 在**隔离后的即时操作**下拉列表中，选择以下选项之一：
   - **仅隔离**
   - **隔离并备份工作负载**
   - **隔离并备份具有取证数据的工作负载**
   - **隔离并关闭工作负载**

   有关定义备份工作负载的位置和加密选项的详细信息，请参阅 "管理工作负载和文件的备份和恢复"(第 353 页)。
5. [可选] 在**要显示的消息**字段中，添加要在最终用户访问隔离的工作负载时显示的消息。例如，可以通知用户工作负载现已隔离，并且工作负载内外的网络访问当前不可用。请注意，此消息也会显示为托盘监视器通知，并在用户关闭该消息之前一直显示。
6. [可选] 在**注释**字段中，添加注释。此注释在**活动**选项卡中可见(针对单个节点或整个事件)，并在您重新查看事件时可以帮助您(或您的同事)回忆执行该操作的原因。
7. 单击**管理网络排除**以添加端口、URL、主机名和 IP 地址，将可用于在隔离期间访问工作负载。有关详细信息，请参阅如何管理网络排除。
8. 单击**隔离**。

   工作负载即会被隔离。还可以在单个节点和整个事件的**活动**选项卡中查看此操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"(第 824 页)。

注意

工作负载也会在 Cyber Protect 中控台中的**工作负载**菜单下显示为**已隔离**。还可以从**工作负载 > 装有代理程序的工作负载**菜单隔离单个或多个工作负载；选择相关工作负载，然后在右侧边栏中选择**管理网络隔离**。在显示的对话框中，可以管理网络排除，然后单击**隔离**或**全部隔离**以隔离选定的工作负载。

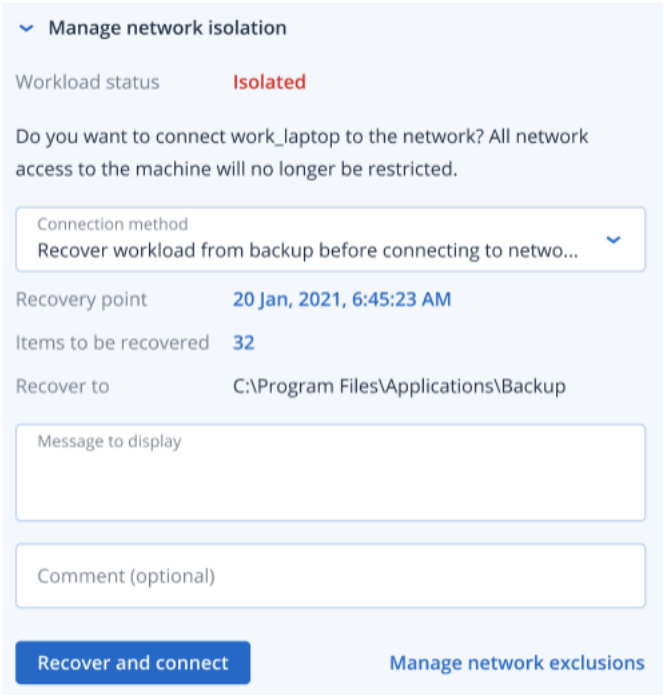
将隔离的工作负载重新连接到网络

1. 在网络杀伤链中，单击要重新连接的工作负载节点。

注意

如果隔离的工作负载当前处于脱机状态，仍可以将其重新连接到网络；当工作负载恢复联机时，它会自动处于**已连接**状态。

2. 在显示的侧边栏中，单击**响应操作**选项卡。
3. 在**修复**部分中，单击**管理网络隔离**。
4. 选择以下选项之一：
   - **立即连接到网络**：工作负载即会重新连接到网络。
   - **在连接到网络之前从备份中恢复工作负载**：选择要从中恢复工作负载的恢复点。
     a. 在**恢复点**字段中，单击**选择**。
     b. 在显示的侧边栏中，选择相关的恢复点。
     c. 单击**恢复 > 整个工作负载**，以恢复工作负载上的所有文件和文件夹。
     或
     单击**恢复 > 文件/文件夹**，以恢复工作负载上的特定文件和文件夹。然后，系统会提示您选择相关文件或文件夹。选中后，可以通过单击**要恢复的项目**字段中的相关值来查看项目列表。



注意
如果选择的恢复点已加密，则系统会提示您输入密码。

5. [可选] 选中**根据需要自动重新启动工作负载**复选框。仅当在步骤 4 中选择**恢复 > 整个工作负载**时，此选项才相关。
6. [可选] 在**要显示的消息**字段中，添加要在最终用户访问连接的工作负载时显示的消息。例如，可以通知用户备份已恢复到工作负载，并且工作负载内外的网络访问已恢复。
7. [可选] 在**注释**字段中，添加注释。此注释在**活动**选项卡中可见(针对单个节点或整个事件)，并在您重新查看事件时可以帮助您(或您的同事)回忆执行该操作的原因。
8. 如果在步骤 4 中选择了**立即连接到网络**，则单击**连接**。
   或
   如果在步骤 4 中选择了**在连接到网络之前从备份中恢复工作负载**，则单击**恢复并连接**。
   工作负载即会重新连接到网络，对工作负载的所有网络访问将不再受到限制。

注意
还可以从 Cyber Protect 中控台中的**工作负载 > 装有代理程序的工作负载**菜单连接一个或多个隔离的工作负载；选择相关工作负载，然后在右侧边栏中选择**管理网络隔离**。在显示的对话框中，单击**连接**或**全部连接**以将选定的工作负载重新连接到网络。

管理网络排除

注意
即使工作负载处于隔离状态时，所有 安克诺斯 Cyber Protect 技术都在工作，也可能存在需要建立额外网络连接的情况(例如，可能需要将文件从工作负载上传到共享目录)。在这些情况下，可以添加网络排除，但请确保在添加排除之前已消除了所有威胁。

1. 在**响应操作**选项卡的**修复**部分中，单击**管理网络排除**。
2. 在“网络排除”侧边栏中，添加相关排除。对于每个可用选项(端口、URL 地址和主机名/IP 地址)，请执行以下操作：
   a. 单击**添加**，然后输入相关的端口、URL 地址或主机名/IP 地址。
   b. 在**流量方向**下拉列表中，选择**传入和传出连接**、**仅传入连接**或**仅传出连接**之一。
   c. 单击**添加**。
3. 单击**保存**。

修补工作负载

EDR 会自动检测工作负载是否需要修补，并使您能够修补工作负载，以防止在将来可能遭受的攻击中利用漏洞。请注意，仅当合作伙伴的工作负载有 Advanced Management 的订购许可时，此功能才可用。

修补工作负载

1. 在网络杀伤链中，单击要修补的工作负载节点。
2. 在显示的侧边栏中，单击**响应操作**选项卡。

3. 在**修复**部分中，单击**修补**。
4. 在**要安装的修补程序**字段中，单击**选择**。在显示的对话框中，选择相关修补程序，然后单击**选择**。
5. 在**安装后选项**字段中，单击显示的链接。“安装后选项”对话框即会显示。
6. 选择是否希望计算机在完成安装修补程序后重新启动：

选项	描述
否	在完成安装修补程序后，计算机不会自动重新启动。
是	在完成安装修补程序后，计算机会自动重新启动。还可以计划重新启动。
如果需要	仅当应用修补程序需要重新启动时，才会重新启动计算机。

7. [可选] 选中**备份完成前不重新启动**复选框，以确保当前正在进行备份时不会重新启动工作负载。
8. 单击**保存**。
9. 在**响应操作**选项卡中，单击**修补**。
   选定的修补程序即会运行。还可以在单个节点和整个事件的**活动**选项卡中查看此操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"(第 824 页)。

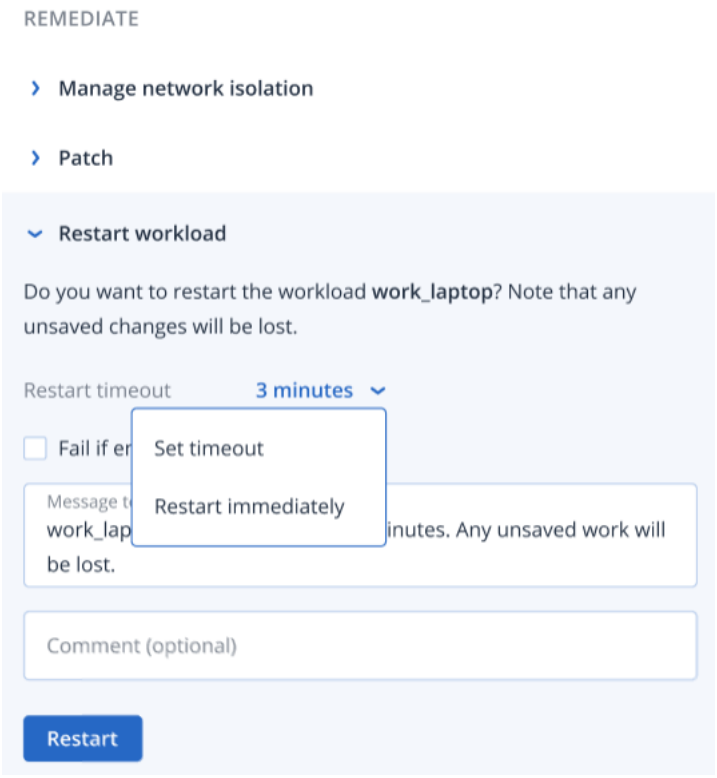
重新启动工作负载

作为修复响应攻击的一部分，EDR 使您能够立即重新启动工作负载，或根据预定义的超时时段重新启动工作负载。

重新启动工作负载

1. 在网络杀伤链中，单击要设置重新启动预定的工作负载节点。
2. 在显示的侧边栏中，单击**响应操作**选项卡。

3. 在**修复**部分中，单击**重新启动工作负载**。



4. 在**重新启动超时**字段中，单击显示的链接，然后选择以下选项之一：
   - **设置超时**：在“重新启动超时”对话框中，设置工作负载的重新启动时段，然后单击**保存**。
   - **立即重新启动**：选中该选项以立即重新启动工作负载。
5. [可选] 选中**最终用户登录时失效**复选框，以确保在用户登录时不会重新启动工作负载。
6. 在**要显示的消息**字段中，添加要在用户访问隔离的工作负载时显示的消息。
7. [可选] 在**注释**字段中，添加注释。此注释在**活动**选项卡中可见（针对单个节点或整个事件），并在您重新查看事件时可以帮助您（或您的同事）回忆执行该操作的原因。
8. 单击**重新启动**。
   工作负载设置为根据定义的预定重新启动。还可以在单个节点和整个事件的**活动**选项卡中查看此操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"（第 824 页）。

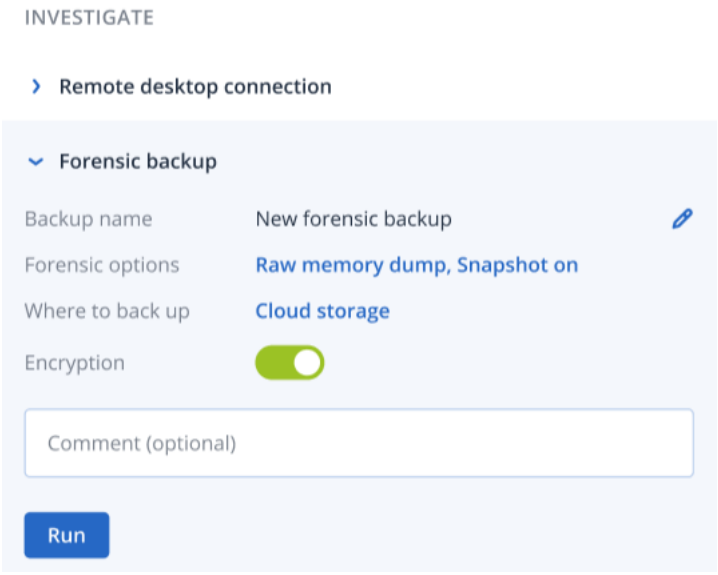
在工作负载上运行手动取证备份

作为攻击调查的一部分，EDR 使您能够运行手动取证备份，以进行审核或进一步调查。请注意，仅当合作伙伴的工作负载有 Advanced Backup 的订购许可时，此功能才可用。

运行取证备份

1. 在网络杀伤链中，单击要在其上运行取证备份的工作负载节点。
2. 在显示的侧边栏中，单击**响应操作**选项卡。

3. 在**调查**部分中，单击**取证备份**。



4. [可选] 在**备份名称**字段中，单击编辑图标可编辑备份名称。
5. 在**取证选项**字段中，单击显示的链接。在显示的"取证选项"对话框中，选择以下选项之一：
   - **收集原始内存转储**
   - **收集内核内存转储**

   还可以选中**正在运行的进程的快照**复选框，以添加有关备份开始时正在运行的进程的信息。此信息存储在备份映像中。

   单击**保存**，以关闭"取证选项"对话框。
6. 在**备份位置**字段中，单击显示的链接以定义备份的位置。
7. [可选] 单击**加密**选项以启用加密。在显示的对话框中，输入加密备份的密码，然后选择相关加密算法。
8. [可选] 在**注释**字段中，添加注释。此注释在**活动**选项卡中可见(针对单个节点或整个事件)，并在您重新查看事件时可以帮助您(或您的同事)回忆执行该操作的原因。
9. 单击**运行**。

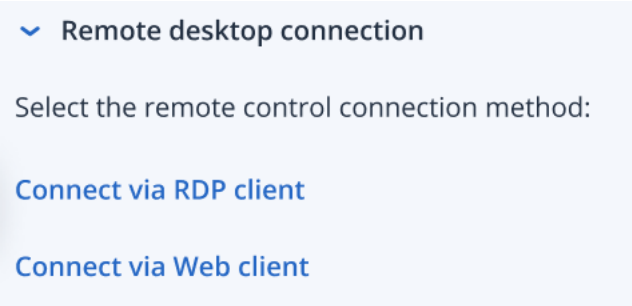
   取证备份即会开始。还可以在单个节点和整个事件的**活动**选项卡中查看此操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"(第 824 页)。

与工作负载的远程连接

作为攻击调查的一部分，EDR 使您能够远程访问正在调查的工作负载。

远程连接到工作负载

1. 在网络杀伤链中，单击要远程连接到的工作负载节点。
2. 在显示的侧边栏中，单击**响应操作**选项卡。
3. 在**调查**部分中，单击**远程桌面连接**。



4. 选择以下远程连接方法之一：
   - **通过 RDP 客户端连接**：此方法会提示您下载并安装远程桌面连接客户端。然后，可以从 中控台远程连接到工作负载。
   - **通过 Web 客户端连接**：此方法不需要在工作负载上安装 RDP 客户端。您将被重定向到登录屏幕，在该屏幕中必须输入远程计算机的凭据。

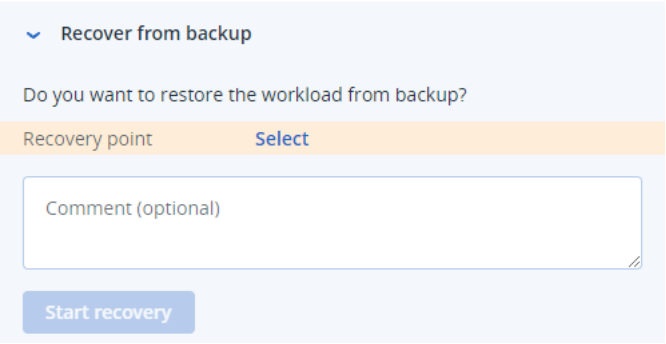
   在启动远程连接后，可以在单个节点和整个事件的**活动**选项卡中查看此操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"(第 824 页)。

从备份恢复

作为恢复响应攻击的一部分，EDR 使您能够从备份或者特定文件或文件夹恢复整台计算机。

从备份恢复工作负载

1. 在网络杀伤链中，单击要恢复的工作负载节点。
2. 在显示的侧边栏中，单击**响应操作**选项卡。
3. 在**恢复**部分中，单击**从备份恢复**。



4. 在**恢复点**字段中，单击**选择**，然后执行以下步骤：
   a. 在显示的侧边栏中，选择相关的恢复点。
   b. 单击**恢复 > 整个工作负载**，以恢复工作负载上的所有文件和文件夹。

      或

      单击**恢复 > 文件/文件夹**，以恢复工作负载上的特定文件和文件夹。然后，系统会提示您选择相关文件或文件夹。选中后，可以通过单击**要恢复的项目**字段中的相关值，来查看为恢复选择的项目。

      注意
      如果选择的恢复点已加密，则系统会提示您输入密码。

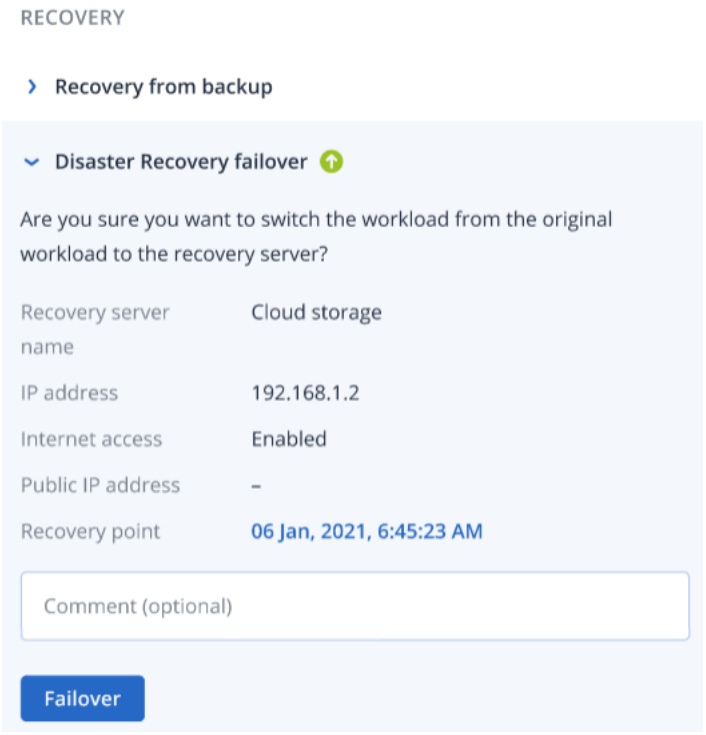
5. [可选] 选中**自动重新启动工作负载**复选框。仅当在步骤 4 中选择**恢复 > 整个工作负载**时，此选项才相关。
6. [可选] 在**注释**字段中，添加注释。此注释在**活动**选项卡中可见(针对单个节点或整个事件)，并在您重新查看事件时可以帮助您(或您的同事)回忆执行该操作的原因。
7. 单击**开始恢复**。
   恢复工作负载的过程即会开始。可以在单个节点和整个事件的**活动**选项卡中查看此操作的进度。有关详细信息，请参阅 "了解为缓解事件而执行的操作"(第 824 页)。

灾难恢复故障转移

作为恢复响应攻击的一部分，EDR 使您能够运行 "实施灾难恢复"(第 655 页)，这允许您将工作负载切换到恢复服务器。请注意，您的工作负载必须有 Advanced Disaster Recovery 的订购许可。

运行灾难恢复故障转移

1. 在网络杀伤链中，单击要恢复的工作负载节点。
2. 在显示的侧边栏中，单击**响应操作**选项卡。
3. 在**恢复**部分中，单击**灾难恢复故障转移**。



4. 在**恢复点**字段中，执行以下步骤：
   a. 单击当前的恢复点日期以选择恢复点。
   b. 在显示的侧边栏中，选择相关的恢复点。

注意
如果您有 Advanced Disaster Recovery 订购许可，则可以选择在灾难恢复中创建的相关恢复服务器(脱机 VM)。如果您没有订购许可，则系统会提示您配置灾难恢复。

5. [可选] 在**注释**字段中，添加注释。此注释在**活动**选项卡中可见（针对单个节点或整个事件），并在您重新查看事件时可以帮助您（或您的同事）回忆执行该操作的原因。
6. 单击**故障转移**。
   工作负载即会切换到恢复服务器。可以在单个节点和整个事件的**活动**选项卡中查看此操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"（第 824 页）。

定义可疑进程的响应操作

作为修复响应攻击的一部分，可以将以下操作应用于可疑进程：

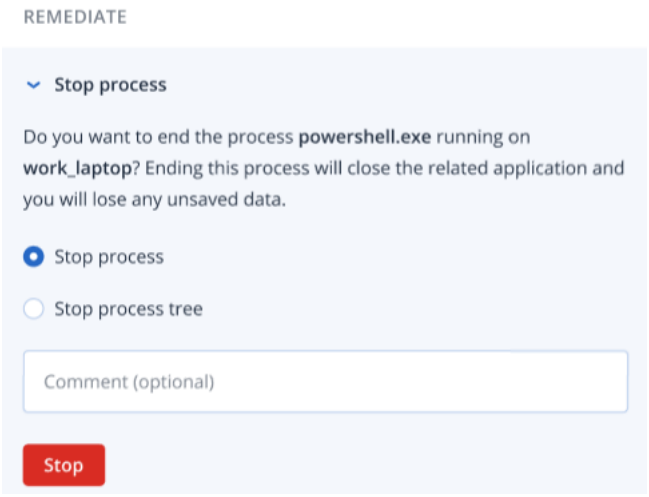
- 停止进程（见下文）
- 隔离进程（见下文）
- 回滚进程所做的更改（见下文）
- 将进程添加到保护计划白名单或黑名单（请参阅 "将进程、文件或网络添加到保护计划黑名单或白名单或从其中移除"（第 849 页））

停止可疑进程

1. 在网络杀伤链中，单击要修复的进程节点。

   注意
   Windows 关键进程或非运行进程无法停止，并且在网络杀伤链中处于禁用状态。

2. 在显示的侧边栏中，单击**响应操作**选项卡。
3. 在**修复**部分中，单击**停止进程**。



4. 请选择下列任一选项：
   - **停止进程**（停止特定进程）
   - **停止进程树**（停止特定进程和所有子进程）
5. [可选] 添加注释。此注释在**活动**选项卡中可见（针对单个节点或整个事件），并在您重新查看事件时可以帮助您（或您的同事）回忆执行该操作的原因。

6. 单击**停止**。进程即会被停止。

注意
相关应用程序将关闭，所有未保存的数据都会丢失。

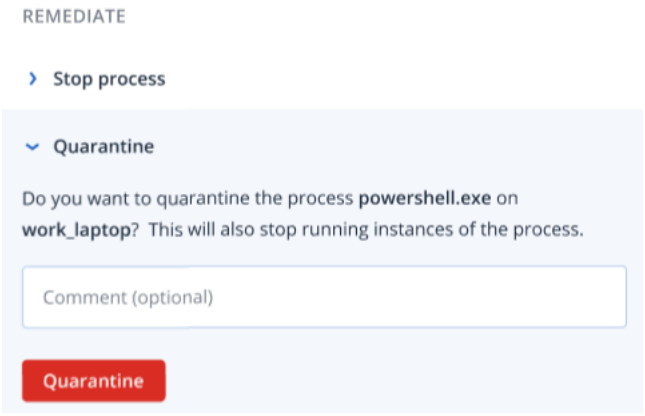
还可以在单个节点和整个事件的**活动**选项卡中查看此操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"(第 824 页)。

隔离可疑进程

1. 在网络杀伤链中，单击要隔离的进程节点。

注意
Windows 关键进程无法隔离，并且在网络杀伤链中处于禁用状态。

2. 在显示的侧边栏中，单击**响应操作**选项卡。
3. 在**修复**部分中，单击**隔离**。



4. [可选]添加注释。此注释在**活动**选项卡中可见(针对单个节点或整个事件)，并在您重新查看事件时可以帮助您(或您的同事)回忆执行该操作的原因。
5. 单击**隔离**。进程即会被停止，然后隔离。

注意
该进程会添加到防恶意软件保护下的“隔离区”部分中，并可在其中进行管理。

还可以在单个节点和整个事件的**活动**选项卡中查看此操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"(第 824 页)。

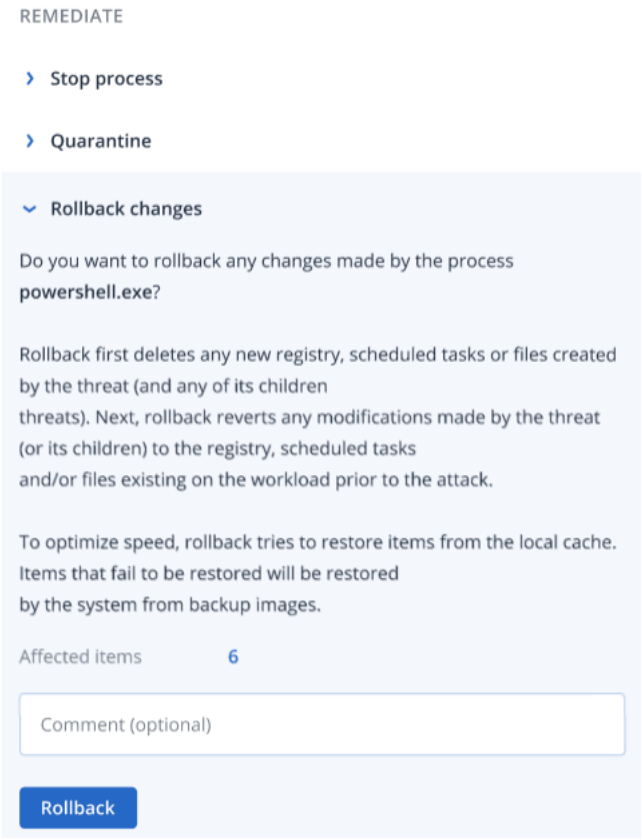
回滚更改

1. 在网络杀伤链中，单击要回滚更改的进程节点。

注意
此操作仅适用于检测节点(显示为红色或黄色节点)。

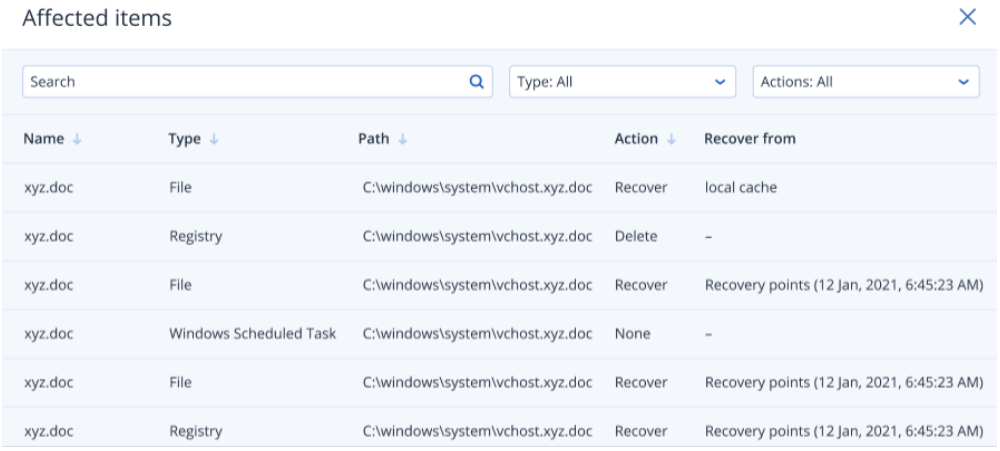
2. 在显示的侧边栏中，单击**响应操作**选项卡。

3. 在**修复**部分中，单击**回滚更改**。



注意
回滚过程仅会从本地缓存中的项目恢复。在将来版本中，将可从备份存档回滚。

4. 要查看受回滚更改影响的项目，请单击**受影响的项目**链接。出现的对话框会显示回滚将恢复的所有项目(文件、注册表、预定任务)以及执行的操作(**删除**、**恢复**或**无**)。此外，还可以看到恢复的项目将从本地缓存还是备份恢复点进行恢复。



5. [可选]添加注释。此注释在**活动**选项卡中可见(针对单个节点或整个事件)，并在您重新查看事件时可以帮助您(或您的同事)回忆执行该操作的原因。

6. 单击**回滚**。在以下步骤中，回滚功能将恢复进程所做的任何注册表、文件或预定任务更改：
   a. 将删除威胁（及其子威胁）创建的任何新条目（注册表、预定任务、文件）。
   b. 将恢复威胁（或其子威胁）对攻击之前存在于工作负载上的注册表、预定任务和/或文件所做的任何修改。
   c. 回滚会尝试从本地缓存恢复项目。对于无法恢复的项目，EDR 将自动从干净的备份映像恢复它们。

   还可以在单个节点和整个事件的**活动**选项卡中查看回滚操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"（第 824 页）。

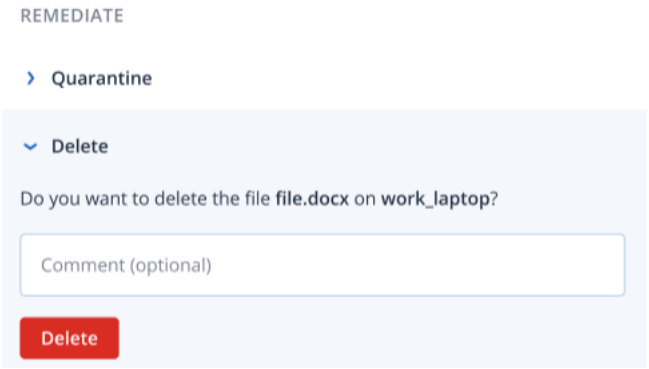
定义可疑文件的响应操作

作为修复响应攻击的一部分，可以将以下操作应用于可疑文件：

- 删除文件（见下文）
- 隔离文件（见下文）
- 将文件添加到保护计划白名单或黑名单（请参阅 "将进程、文件或网络添加到保护计划黑名单或白名单或从其中移除"（第 849 页））

删除可疑文件

1. 在网络杀伤链中，单击要修复的文件节点。
2. 在显示的侧边栏中，单击**响应操作**选项卡。
3. 在**修复**部分中，单击**删除**。

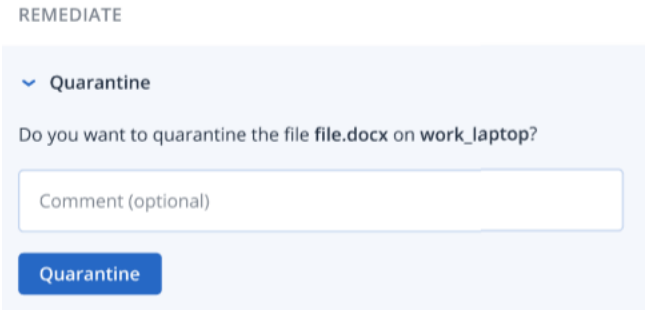


4. [可选] 添加注释。此注释在**活动**选项卡中可见（针对单个节点或整个事件），并在您重新查看事件时可以帮助您（或您的同事）回忆执行该操作的原因。
5. 单击**删除**。
   文件即会被删除。还可以在单个节点和整个事件的**活动**选项卡中查看此操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"（第 824 页）。

隔离可疑文件

1. 在网络杀伤链中，单击要修复的文件节点。
2. 在显示的侧边栏中，转到**响应操作**。

3. 在**修复**部分中，单击**隔离**。



4. [可选] 添加注释。此注释在**活动**选项卡中可见（针对单个节点或整个事件），并在您重新查看事件时可以帮助您（或您的同事）回忆执行该操作的原因。
5. 单击**隔离**。
   文件即会被隔离。还可以在单个节点和整个事件的**活动**选项卡中查看此操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"（第 824 页）。

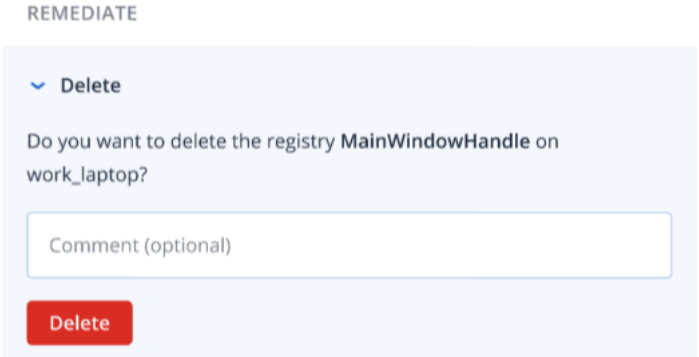
定义可疑注册表项的响应操作

作为修复响应攻击的一部分，可以删除可疑注册表项。

此选项可用于注册表网络杀伤链节点。

删除可疑注册表项

1. 在网络杀伤链中，单击要修复的节点。
2. 在显示的侧边栏中，单击**响应操作**选项卡。
3. 在**修复**部分中，单击**删除**。



4. [可选] 添加注释。此注释在**活动**选项卡中可见（针对单个节点或整个事件），并在您重新查看事件时可以帮助您（或您的同事）回忆执行该操作的原因。
5. 单击**删除**。
   注册表项即会被删除。还可以在单个节点和整个事件的**活动**选项卡中查看此操作。有关详细信息，请参阅 "了解为缓解事件而执行的操作"（第 824 页）。

将进程、文件或网络添加到保护计划黑名单或白名单或从其中移除

作为预防响应攻击的一部分，可以将节点添加到保护计划白名单或黑名单中。

如果您认为某个节点是安全的并希望将来阻止对其进行任何检测，可以将该节点添加到白名单。将一个节点添加到黑名单，可在将来阻止运行该节点。

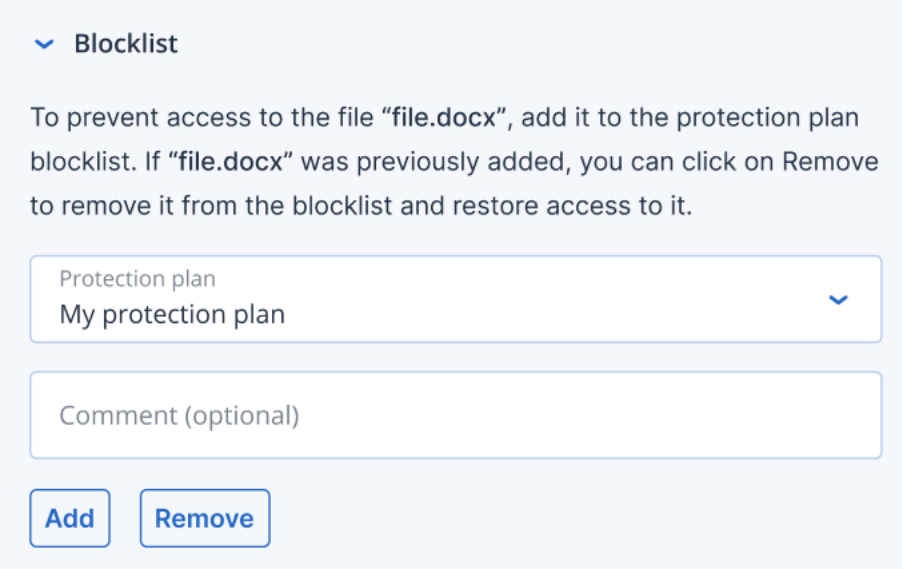
您还可以从白名单表或黑名单中删除节点，以允许或阻止将来对该节点的任何访问。

此选项可用于以下网络杀伤链节点：

- 进程
- 文件
- 网络

若要在保护计划阻止列表中添加或删除进程、文件或网络

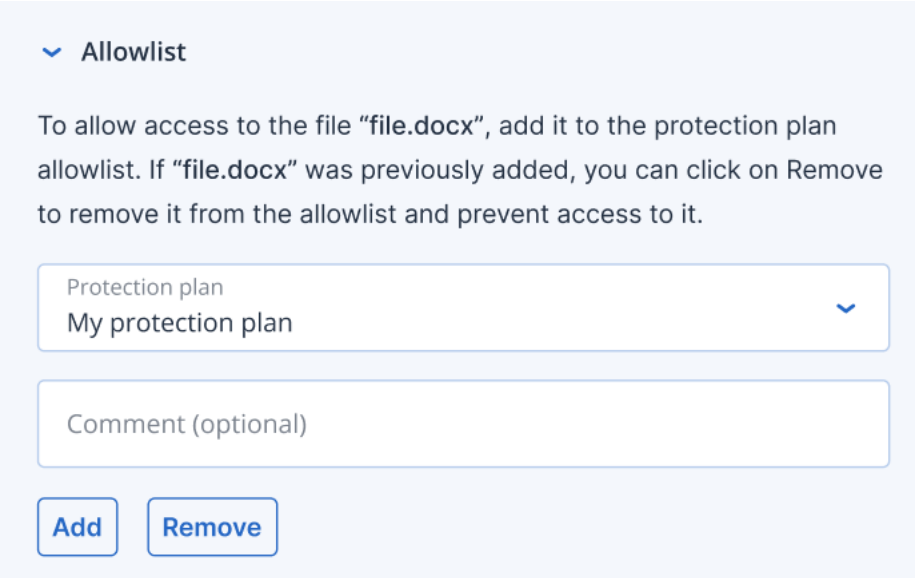
1. 在网络攻击链中，点击您想要修复的进程、文件或网络节点。
2. 在显示的侧边栏中，单击**响应操作**选项卡。
3. 在**"阻止"**部分中，单击**"黑名单"**旁边的箭头图标。



4. 选择要应用此操作的相关保护计划。
5. [可选] 添加注释。此注释在**活动**选项卡中可见(针对单个节点或整个事件)，并在您重新查看事件时可以帮助您(或您的同事)回忆执行该操作的原因。
6. 单击**添加**。
   该操作已实施，并且该进程、文件或网络将被阻止在将来启动。
   或者，如果进程、文件或网络之前已添加到黑名单，而您现在想要将其从黑名单中删除，请单击**删除**。这将允许将来访问该节点。
   还可以在单个节点和整个事件的**"活动"**选项卡中查看添加或删除操作。有关更多信息，请参阅 "了解为缓解事件而执行的操作"(第 824 页)。

在保护计划白名单中添加或删除进程、文件或网络

1. 在网络攻击链中，点击您想要修复的进程、文件或网络节点。
2. 在显示的侧边栏中，单击**响应操作**选项卡。
3. 在**"阻止"**部分中，单击**"白名单"**旁边的箭头图标。



4. 选择要应用此操作的相关保护计划。
5. [可选] 添加注释。此注释在**活动**选项卡中可见(针对单个节点或整个事件),并在您重新查看事件时可以帮助您(或您的同事)回忆执行该操作的原因。
6. 单击**添加**。
   该操作已实施,并且该进程、文件或网络将被阻止在将来检测。
   或者,如果进程、文件或网络之前已添加到白名单,而您现在想要将其从白名单中删除,请单击**删除**。这将阻止任何将来对该节点的访问。
   还可以在单个节点和整个事件的**“活动”**选项卡中查看添加或删除操作。有关更多信息,请参阅 "了解为缓解事件而执行的操作"(第 824 页)。

使用自动化工作流

您可以使用 Acronis 自动化工作流来应用一组预定义操作,这些操作可以自动修复 Endpoint Detection and Response (EDR) 和 Extended Detection and Response (XDR) 中的安全事件。这些工作流程或操作手册可帮助您简化安全操作,以提高响应时间,同时减少管理和响应安全事件的操作负担。

有六个预定义的 EDR 工作流,每个工作流都可根据需要进行配置。有关详细信息,请参阅 "Endpoint Detection and Response (EDR)"(第 851 页)。

若要访问自动化工作流程,请转到**管理 > 工作流程**。工作流程列表显示当前已启用或已禁用的工作流程、上次执行时间和状态。

Endpoint Detection and Response (EDR)

有六个默认 EDR 工作流程,您可以根据自己的需求进行配置:

- 隔离威胁(创建 EDR 事件时)
- 隔离威胁(更新 EDR 事件时)
- 隔离工作负载(创建 EDR 事件时)
- 隔离工作负载(更新 EDR 事件时)

- 需要注意的恶意软件事件
- 需要注意的事件

下表描述了每个工作流程适用的默认触发器、条件和操作。有关修改这些条件和操作的详细信息，请参阅 "配置自动化 Endpoint Detection and Response (EDR) 工作流"(第 854 页) 。

工作流程	触发器	条件	操作
隔离威胁	已创建 EDR 事件	威胁状态 = "未减轻" 和 事件状态 = 未启动 和 严重程度 = "高" 和 事件类型 = “已检测到处理” OR “已检测到恶意软件”	1. 停止进程。 2. 隔离进程。 3. 添加注释。默认注释文本为“<工作流程名称> - 已隔离高严重程度威胁”。 4. 关闭事件。
隔离威胁	已更新 EDR 事件		

工作流程	触发器	条件	操作
隔离工作负载	已创建 EDR 事件	威胁状态 = "未减轻" 和 事件状态 = 未启动 和 严重程度 = "严重" 和 判决 = “恶意” 和 积极程度 > 9 和 事件类型 = “已检测到处理” OR “已检测到恶意软件”	1. 停止进程。 2. 隔离进程。 3. 隔离工作负载。 4. 添加注释。默认注释文本为“<工作流程名称> - 严重恶意软件检测后，工作负载 <工作负载名称> 已隔离”。 5. 向所选的 Cyber Protect 中控台用户发送电子邮件。
隔离工作负载	已更新 EDR 事件		
需要注意的恶意软件事件	已创建 EDR 事件	威胁状态 = "未减轻" 和 事件状态 = 未启动 和 事件年龄 > 8 小时 和 严重程度 = ”高“ OR ”严重“ 和 判决 = “恶意” 和 事件类型 = “恶意软件检测”	1. 停止进程。 2. 隔离进程。 3. 添加注释。默认注释文本为 “<工作流程名称} - 由于 8 小时未进行调查，因此隔离严重程度为高/严重

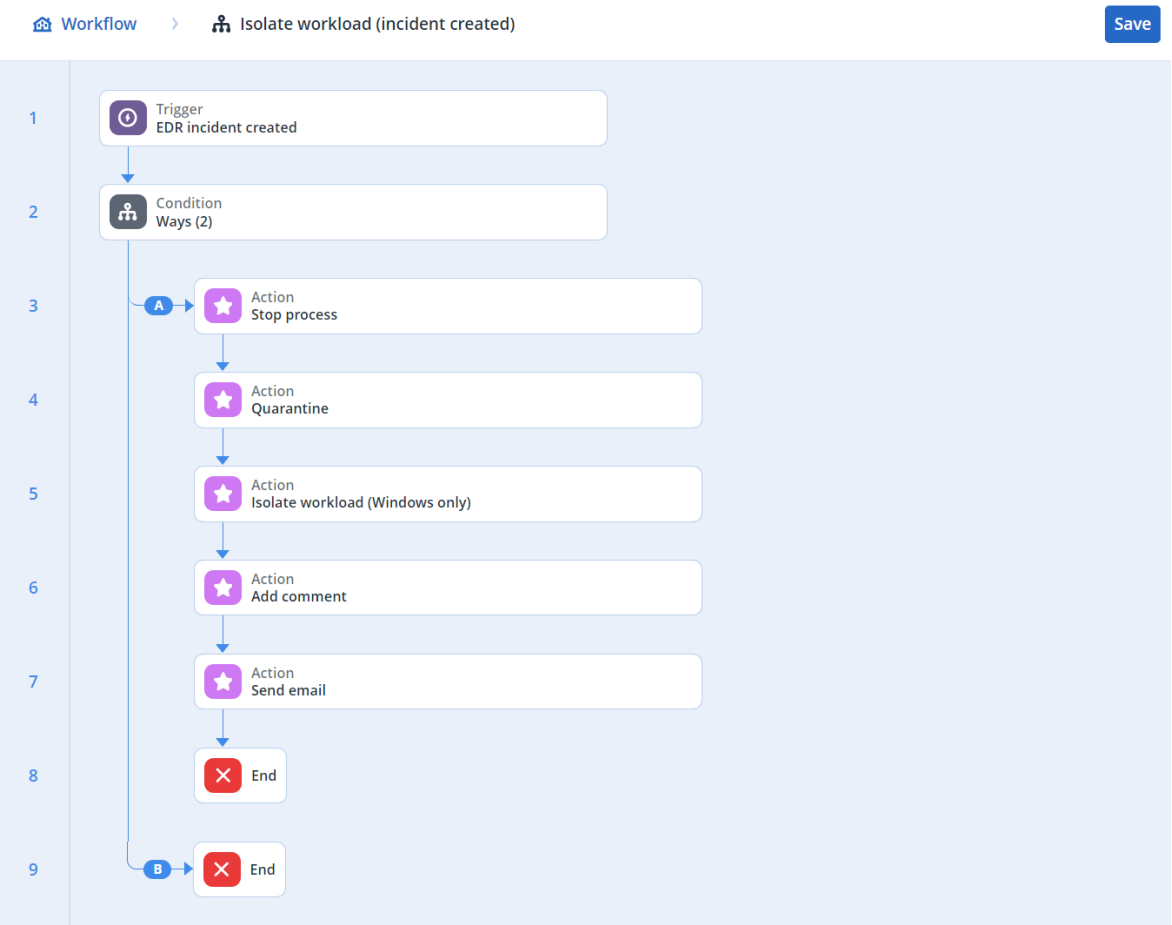
工作流程	触发器	条件	操作
			的威胁”。 4. 向所选的 Cyber Protect 中控台用户发送电子邮件。
需要注意的事件	已创建 EDR 事件	威胁状态 = "未减轻" 和 事件状态 = 未启动 和 事件发生时间 > 24 小时 和 严重程度 = ”高“ OR ”严重“ 和 判决 = “恶意”	1. 停止进程。 2. 隔离进程。 3. 添加注释。默认注释文本为“<工作流程名称} - 由于未进行 24 小时的调查，因此高/关键严重性威胁被隔离”。 4. 向所选的 Cyber Protect 中控台用户发送电子邮件。

配置自动化 Endpoint Detection and Response (EDR) 工作流

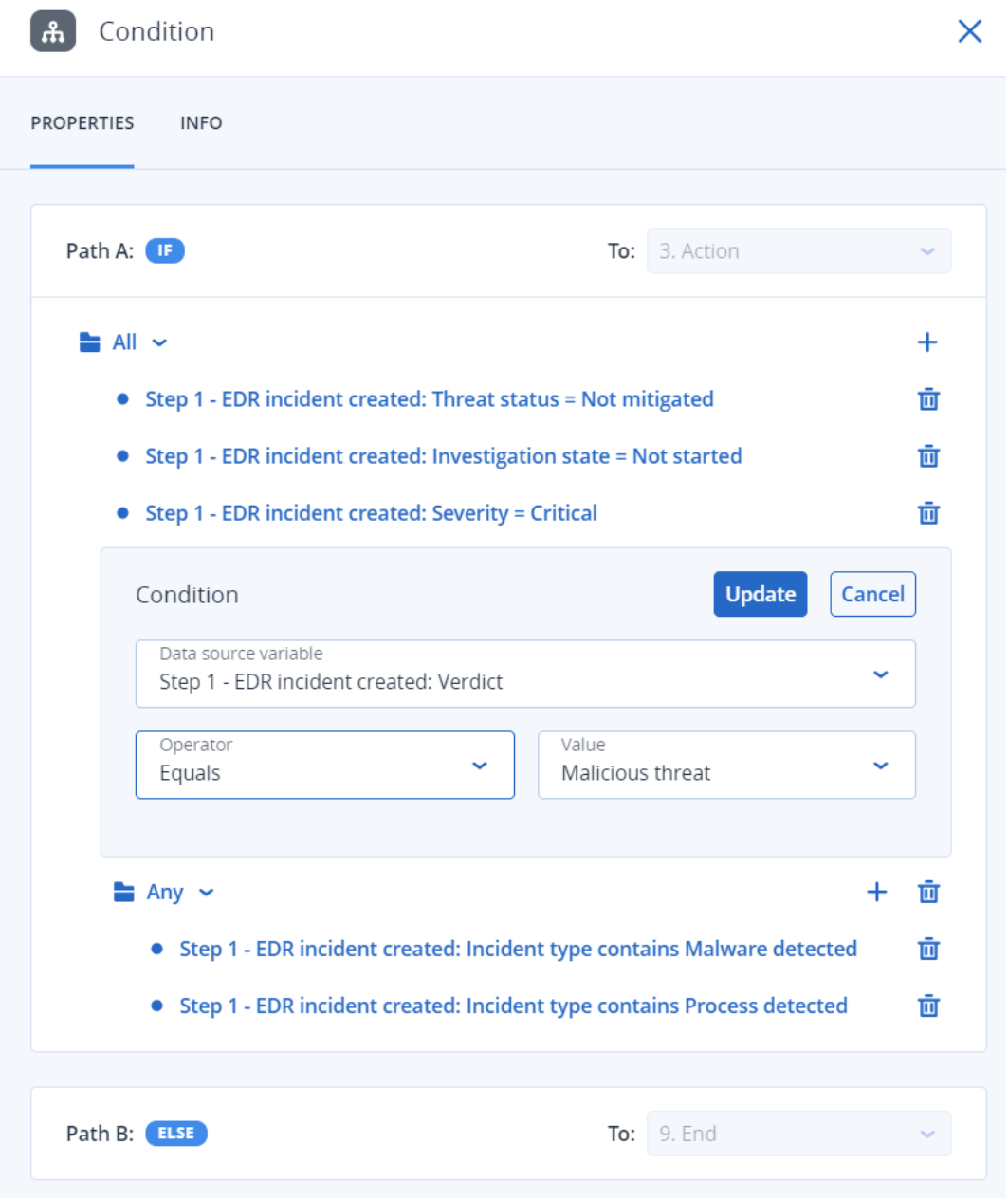
您可以根据自己的需求配置预定义的 EDR 工作流程。

若要配置 EDR 工作流程

1. 在 Cyber Protect 中控台中，转到**管理 > 工作流**。
2. 在最右侧的列中，单击要配置的工作流的行中的省略号图标 (...)，然后选择 **打开**。
   或者，单击相关工作流程，在显示的窗格中，单击 **打开**。
   将显示工作流程的条件和操作。



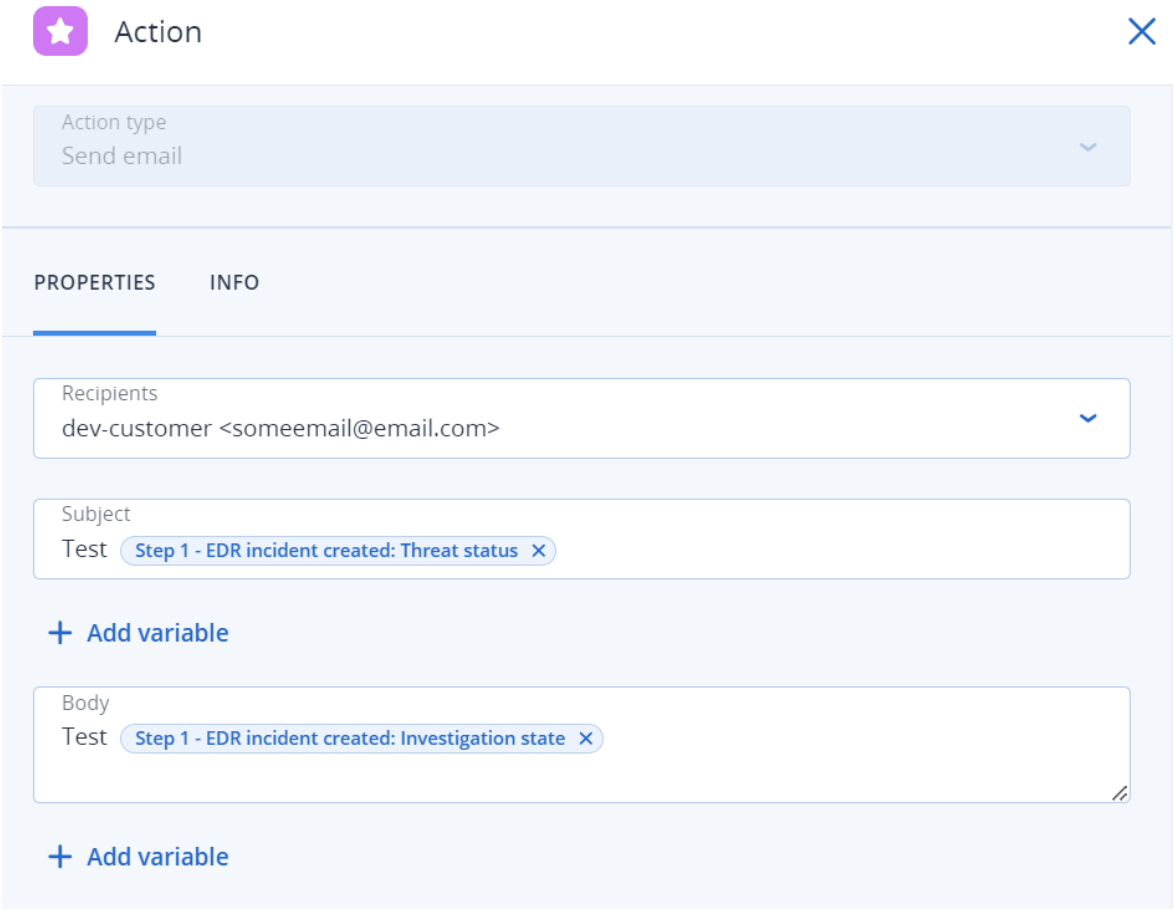
3. 若要查看和修改工作流程的任何条件，请单击**条件**块。



条件块定义了一组必须作为工作流的一部分执行的条件，由两种块类型组成：

- **全部**：应满足此块中的所有条件，才能继续工作流程的下一步。
- **任一**：必须满足此块中的至少一个条件，才能继续工作流程的下一步。

4. 若要修改条件，请单击条件并修改相关值。完成后，请单击**更新**。
   请注意，您也可以通过单击其旁边的垃圾桶图标来删除条件。
5. 若要修改操作，请单击要修改的操作。
6. 在显示的窗格中，进行相关更改。
   例如，单击操作**发送电子邮件**，然后修改所选收件人、电子邮件正文和主题，以便将其作为此工作流的一部分发送。



7. [可选] 修改附加操作。
8. 单击**保存**。

   若工作流程先前未启用且处于**草稿**状态，请单击**保存并启用**以启用它。或者，单击**保存**以将工作流程保持为**已禁用**。

   请注意，您可以从主工作流程屏幕单击相关工作流程并选择 **启用** 或 **禁用**，以便根据需要启用和禁用工作流程。

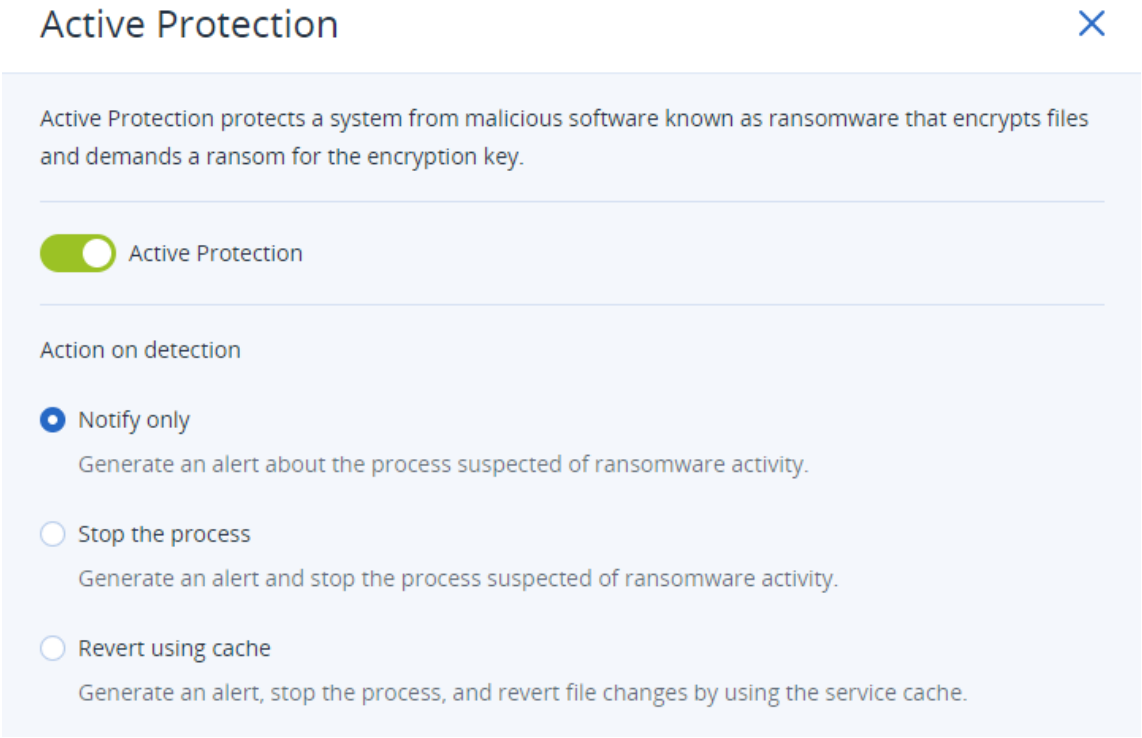
启用 Endpoint Detection and Response (EDR) 的监控模式

Cyber Protection 中的监控模式使您能够在生产环境中使用 EDR。反过来，这使您可以在完全部署 EDR 之前检查任何误报，并进行必要的排除。

在监控模式下，没有任何内容被阻止或停止，已创建事件，但没有响应被初始化。

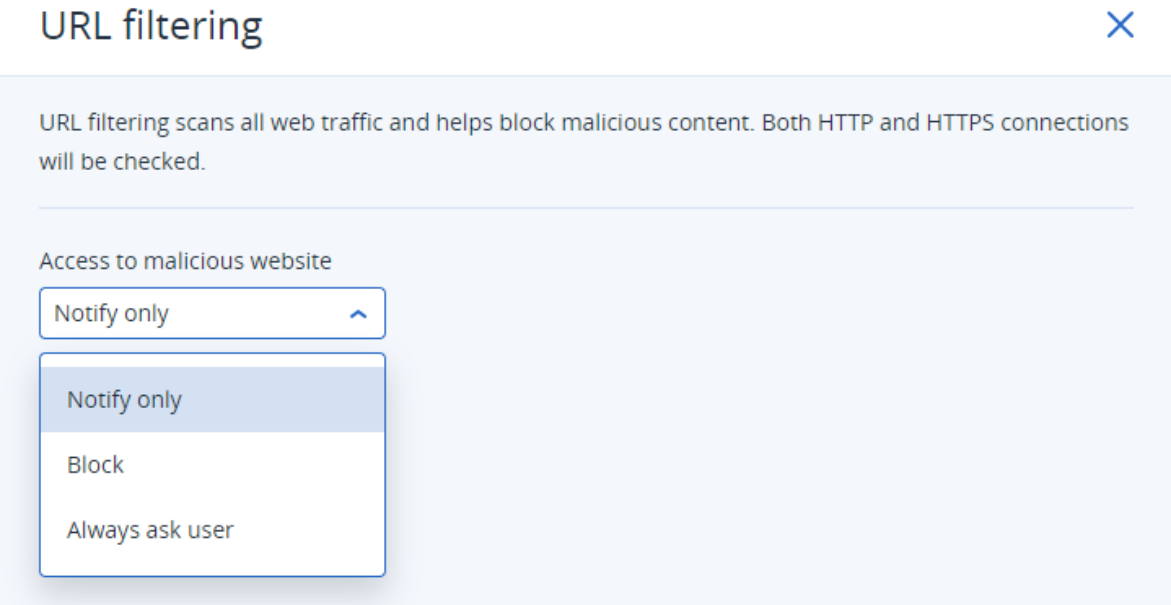
启用 EDR 的监控模式

1. 在相关的保护计划中，确保启用了 EDR。有关更多信息，请参见"启用 Endpoint Detection and Response (EDR) 功能"(第 795 页)。
2. 展开**防病毒 & 防恶意软件保护**模块，然后定义以下内容：
   - 点击**Active Protection**，并在**检测到的操作**部分，选择**仅通知**。然后点击**完成**。有关更多信息，请参见"Active Protection"(第 733 页)。



- 点击**行为引擎**，并在**检测到的操作**部分中，选择**仅通知**。然后点击**完成**。有关更多信息，请参见"行为引擎"(第 737 页)。
- 点击**防止利用**，并在**检测到的操作**部分，选择**仅通知**。然后点击**完成**。有关更多信息，请参见"漏洞利用预防"(第 737 页)。
- 点击**实时保护**，并在**检测到的动作**部分中，选择**仅通知**。然后点击**完成**。有关更多信息，请参见"实时保护"(第 739 页)。
- 点击**预定扫描**，并在**检测到的操作**部分，选择**仅通知**。然后点击**完成**。有关更多信息，请参见"预定扫描"(第 739 页)。

3. 展开**URL 过滤**模块，并在**访问恶意网站**下拉列表中，选择**仅通知**。然后点击**完成**。有关更多信息，请参见"URL 过滤"(第 751 页)。



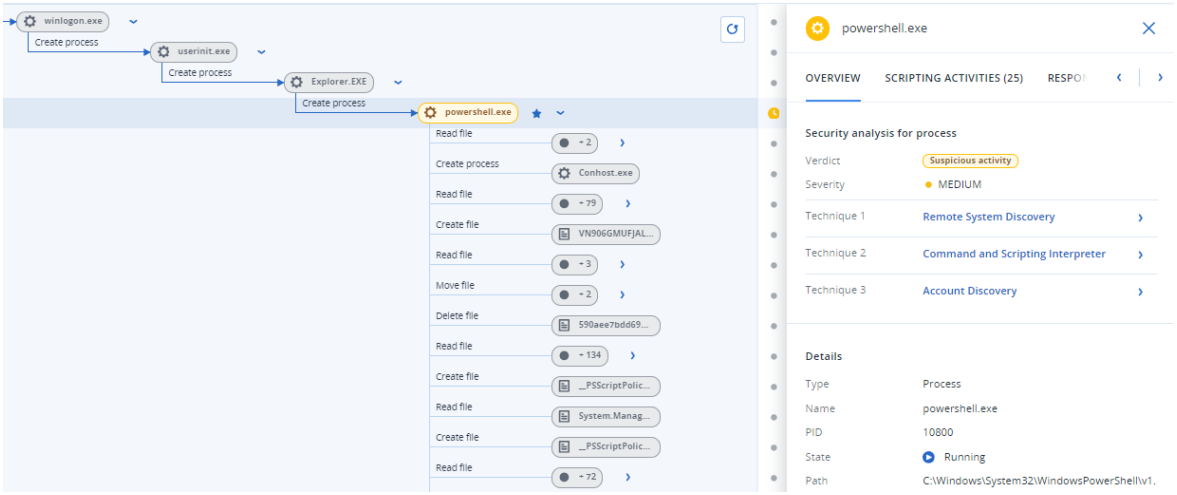
如何测试 Endpoint Detection and Response (EDR) 是否正常工作

为了确保 EDR 已部署并正常工作，可以运行许多触发 EDR 检测的命令。

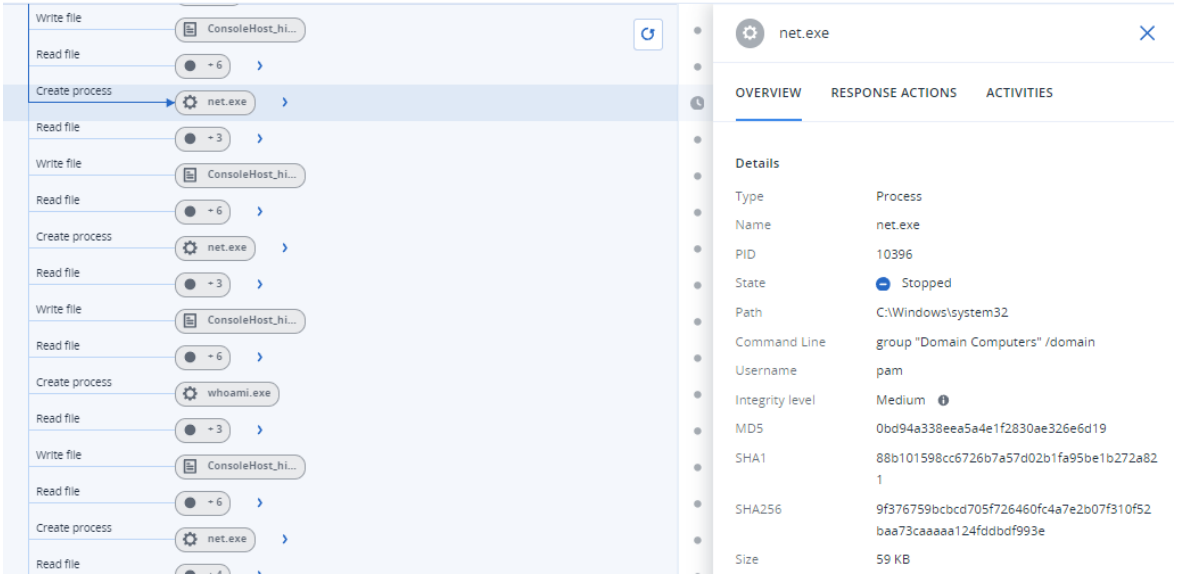
注意
在 EDR 已部署后，如果发生任何可疑活动，您应该会立即看到事件。如果连续几天没有触发新的事件，则可以通过以下步骤来检查 EDR 是否正常工作。

测试 EDR 是否已部署并正常工作

1. 登录到加入域的相关 Active Directory 用户帐户。
2. 在 Windows PowerShell 中运行以下两个命令：
   - `net group "Domain Computers" /domain`
   - `net user administrator /domain`
3. 在 Cyber Protect 中控台中，转到**保护 > 事件**以查看生成的事件。
   还可以单击触发的**中等**严重性类型事件以将其显示在 EDR 网络杀伤链中，并确认您在上一步中执行的 PowerShell 命令，如下面的示例所示。



4. 在 Windows PowerShell 中运行以下命令：
   - `c:\>whoami`
   - `c:\>net localgroup`
   - `c:\>net localgroup administrators`
   - `c:\>powershell -command start-process cmd -verb runas`
   - `c:\WINDOWS\system32>net user administrator /active:yes`
   - `c:\>powershell -command Get-Hotfix`
5. 在 EDR 网络杀伤链中，单击可执行节点（例如，**net.exe** 或 **whoami.exe**），以显示在命令行中执行的确切 PowerShell 命令。在下面的示例中，这些命令显示在**概述**选项卡的**详细信息**部分中。



6. 在确认生成 EDR 事件后，手动将事件的**威胁状态**设置为**已缓解**，并将**调查状态**设置为**已关闭**。有关详细信息，请参阅 "如何调查网络杀伤链中的事件"（第 817 页）。还可以为事件输入注释，以表明这是一个测试事件。

Extended Detection and Response (XDR)

注意
此功能是 Advanced Security + XDR 保护包的一部分，而后者又是 Cyber Protection 服务的一部分。请注意，您必须在保护计划中启用 Endpoint Detection and Response (EDR) 功能，才能使 XDR 正常运行。

XDR 使用 EDR 进行事件关联并识别终端上的高级攻击，然后通过识别终端、电子邮件、身份等方面的高级威胁来扩展该功能。

通过在多个 XDR 集成（包括 Perception Point 和 Microsoft Entra ID）中使用 XDR 图表，您还可以使用针对每种类型的集成可用的特定操作来响应事件，例如阻止电子邮件发件人或暂停用户。

XDR 与工作站、服务器、虚拟机和网络托管服务器兼容。

为什么需要 Extended Detection and Response (XDR)

以前，提供安全服务的 MSP 必须在保护不足、不完整或昂贵而复杂的解决方案之间做出选择。XDR 通过扩展和丰富 "Endpoint Detection and Response (EDR)"（第 792 页）提供的功能来克服这些限制，并能够识别终端、电子邮件、身份等方面的高级威胁。

随着*攻击面不断增长*（远程位置的多个客户、本地和基于云的工作负载混合以及私有云和公共云）、*安全基础设施漏洞*（由于为不同客户部署了大量安全工具、警报让技术人员应接不暇以及缺乏安全人才），以及*网络威胁不断演变*（例如攻击者利用基于人工智能的工具查找和利用零日漏洞和勒索软件生成器），显然，需要一种通过简化补救步骤来阻止现代网络威胁的解决方案。

以下是您需要 XDR 的原因：

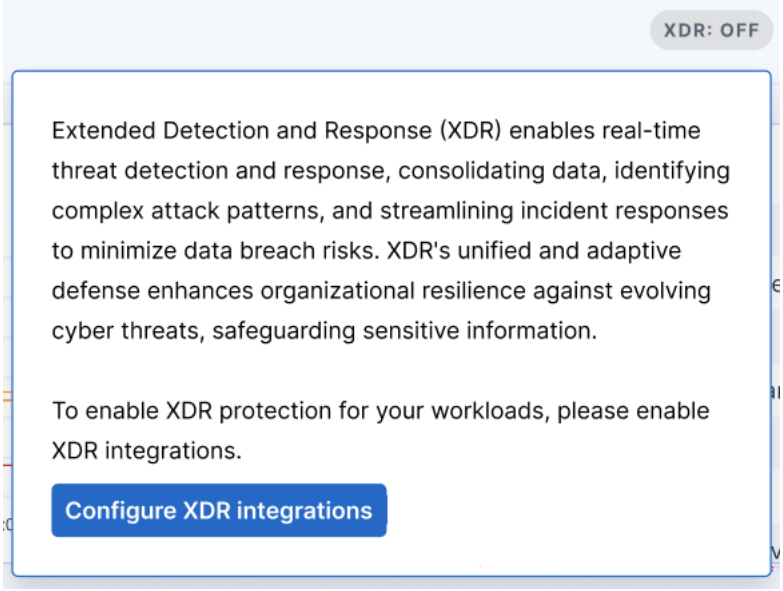
- **扩展保护**：通过覆盖终端、电子邮件、Microsoft Entra ID 和 Microsoft 365 应用程序（如 SharePoint、OneDrive 和 Teams）的广泛可视性，保护客户环境免受易受攻击表面上的复杂威胁。增强的可视性意味着检测速度比 EDR 提供的更快。
- **本地集成**：轻松集成网络安全、数据保护和终端管理平台。XDR 旨在保护易受攻击的面，从而实现无与伦比的业务连续性。
- **高效且具有增强的补救措施**：轻松启动、管理、扩展和交付安全服务。此外，XDR 还包括基于 AI 的事件分析和一键响应，可轻松进行调查和补救，AI 辅助和自动补救措施可防范多阶段和高级网络威胁。主动安全还使技术人员能够在攻击者利用潜在问题之前识别和补救它们。

启用 Extended Detection and Response (XDR)

重要事项
为了使 XDR 能够发挥作用，必须首先在相关保护计划中启用 Endpoint Detection and Response (EDR) 选项。这可确保为客户租户显示 **XDR：开/关**选项开关。如果未显示此选项开关，请联系您的合作伙伴管理员。

若要启用 XDR

1. 确保在保护计划中启用了 EDR。有关更多信息，请参阅 "启用 Endpoint Detection and Response (EDR) 功能"(第 795 页) 。
2. 转到**“保护”** > **“事件”**。
3. 点击屏幕右上角的 XDR: OFF 。
4. 系统会提示您配置 XDR 集成，这是 XDR 保护您的工作负载所必需的。单击**配置 XDR 集成**。



如果已经配置了现有的 XDR 集成并想要添加其他集成，请单击**添加 XDR 集成**。

将自动将您重定向到管理门户，您可以在其中选择和配置相关的 XDR 集成。有关更多信息，请参阅与第三方系统集成。

有关与 Microsoft Entra ID 集成的更多信息，请参阅这些集成步骤。

有关与 Perception Point 集成的更多信息，请参阅这些集成步骤。

当至少配置了一个 XDR 配置时，XDR 选项开关为启用 XDR: ON ，您可以开始使用 XDR。

使用 XDR 图表

XDR 图表通过将检测与来自 XDR 数据源(包括电子邮件和身份管理元数据) 的事件关联起来，为查看 EDR(Endpoint Detection and Response) 事件增加了另一个丰富的视角。

图中显示的节点类型取决于 XDR 集成。例如，当与电子邮件和身份管理集成时，该图将显示电子邮件节点、电子邮件文件附件节点和用户身份节点。有关 XDR 图中显示的各种节点图标的更多信息，请参阅"XDR 图形图标"(第 866 页) 。

使用 XDR 图表以：

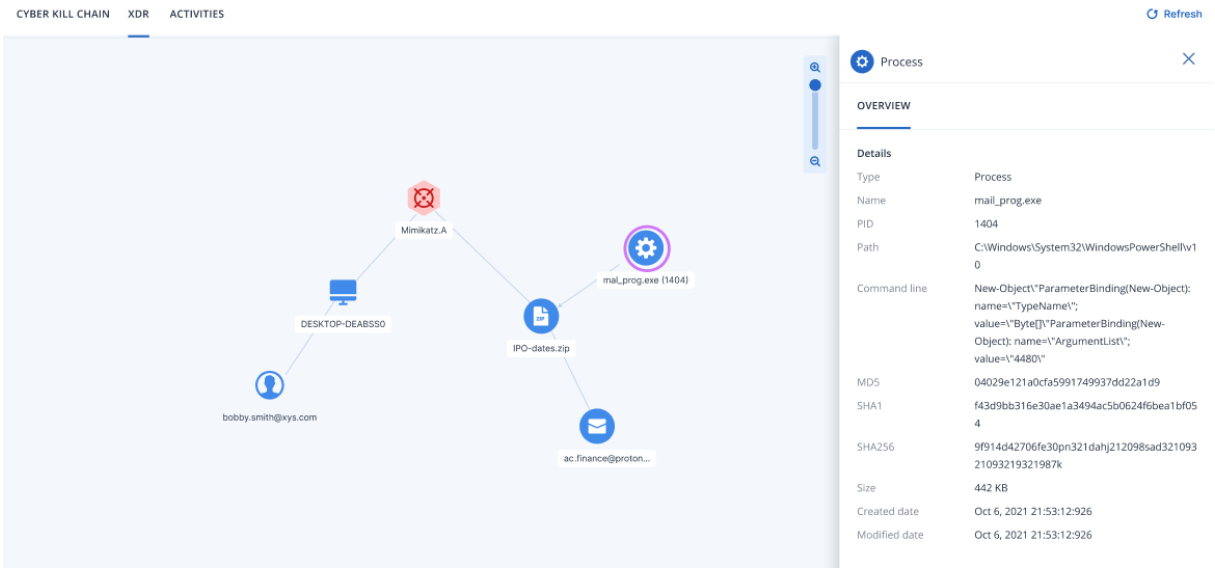
- 调查单个节点
- 将响应操作应用于节点
- 查看集成错误

若要访问 XDR 图表，请转到**“保护”**>**“事件”**，单击相关事件，然后单击**“XDR”**选项卡。

若要刷新 XDR 图表的内容，请点击 Refresh 。

注意

仅当启用 XDR 时才会显示 **XDR** 选项卡。有关详细信息，请参阅 "启用 Extended Detection and Response (XDR)"(第 861 页) 。

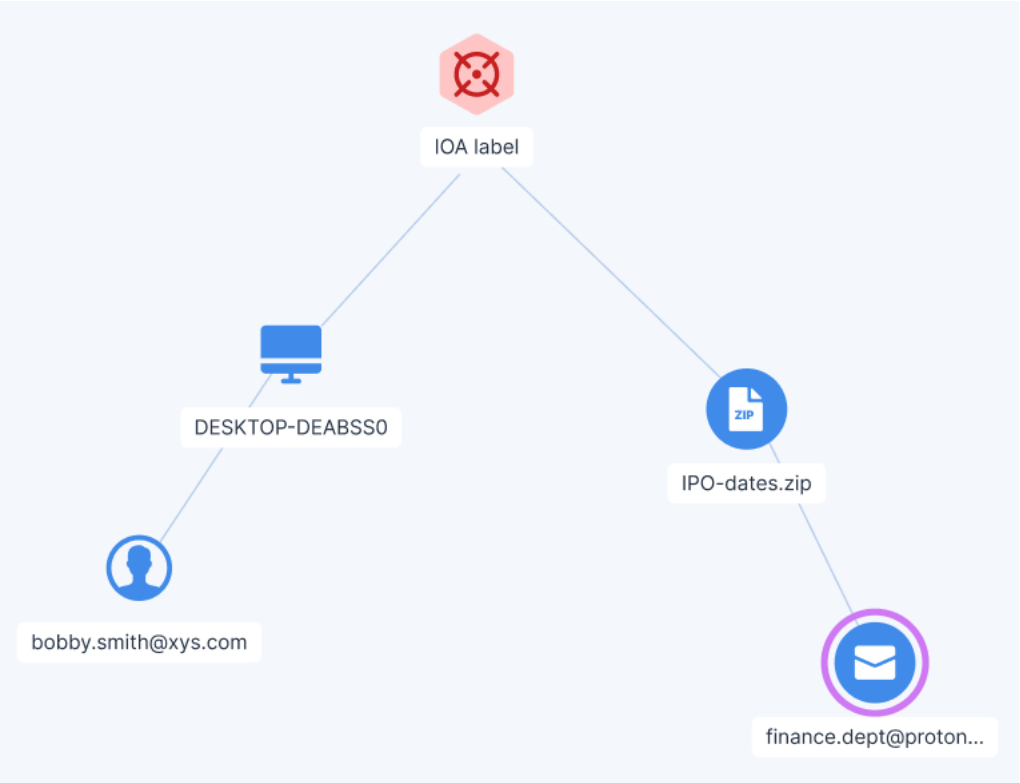


如何分析 XDR 图

XDR(Extended Detection and Response) 为 EDR(Endpoint Detection and Response) 事件添加了更多详细信息，例如验证威胁是来自电子邮件附件还是电子邮件中的链接，以及是哪个用户登录并负打开恶意附件的责任。通过分析 XDR 图表，您可以了解有关事件发生情况的更多背景信息，以及是否需要采取超出 EDR 功能的措施，例如阻止某用户帐户和/或阻止某电子邮件发件人。

查看下面显示的 XDR 图中显示的节点，您可以看到从下载到 **DESKTOP-DEABSS0** 的电子邮件附件中的 zip 文件中提取了恶意威胁。发件人的电子邮件地址是 **finance.dept@proton.me**，登录并打开 zip 文件的用户是 **bobby.smith@xys.com**。

通过单击桌面图标，您可以在**"概览"**选项卡中查看工作负载是否是登录用户的正常工作负载。如果用户使用他们以前从未使用过的操作系统或 IP 地址登录，则事件很可能是恶意的。然后，您可以对受感染设备上的用户应用所需的响应操作，以确保他们无法访问敏感数据和 IT 资源。



还有额外的 XDR 图形元素可以帮助您准确了解发生的情况。

例如，与 Perception Point 集成的 XDR 包括以下内容：

- 当恶意文件是电子邮件的直接附件时，会显示一条线将恶意文件节点和电子邮件节点连接起来。
- 当恶意节点是 URL 节点时，会显示一条线将恶意 URL 节点与电子邮件节点连接起来。
- 当从 zip 存档附件（或其他类型的压缩存档）中提取恶意文件时，会为 zip 存档创建一个文件节点，并显示一条线将恶意文件节点与附件节点连接起来。

调查单个节点

您可以查看任何 XDR 图形节点的详细信息。这样就可以深入了解图形中的特定节点，并根据需要调查和对每个节点应用响应操作。

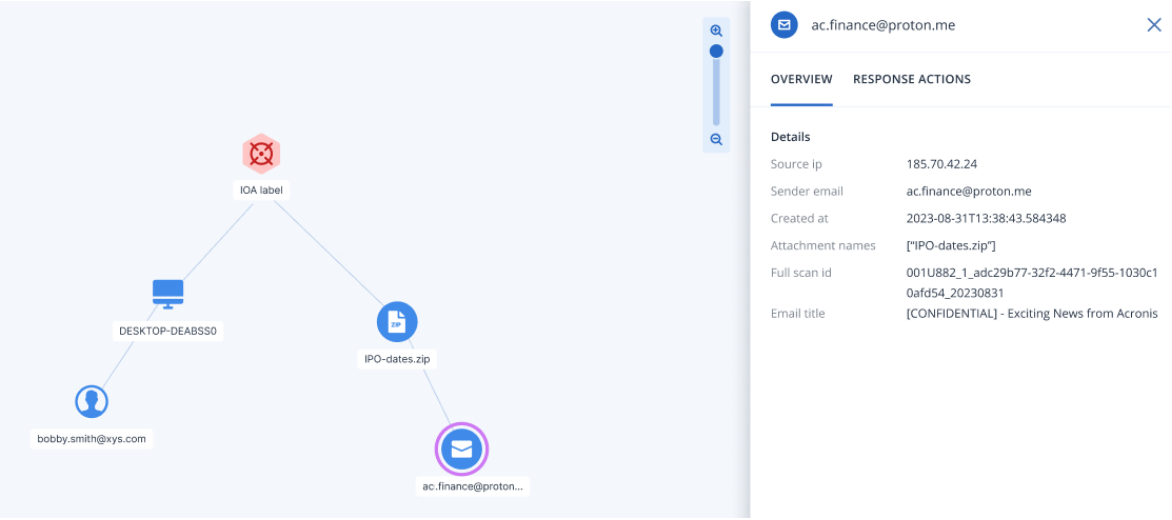
显示的节点将根据实施的 XDR 集成而有所不同。节点详细信息显示在**“概览”**选项卡中，该节点可用的响应操作则显示在**“响应操作”**选项卡中。

注意
对于危害指标 (IoC) 和攻击指标 (IoA) 节点，没有可用的响应操作。

若要调查单个节点

1. 在 Cyber Protect 中控台中，转到**保护 > 事件**。
2. 在显示的事件列表中，单击要调查的事件最右侧列中的 。
3. 单击 **XDR** 选项卡。

4. 导航到相关节点，然后单击它以显示该节点的侧边栏。
   例如。单击下面示例中的电子邮件节点将打开该节点的侧边栏。



5. 调查侧边栏选项卡中包含的信息：
   - **概述**：此选项卡包含有关所选节点的详细信息，具体取决于节点类型。
     - 攻击指标 (IoA) 节点：包括检测时间戳、检测严重性、检测描述、MITRE 策略和技术以及威胁名称。
     - 入侵指标 (IoC) 节点：每个 IoC 节点类型（进程、文件或 URL）都有自己的一组字段，这些字段也用于 Endpoint Detection and Response (EDR)。有关详细信息，请参阅 "调查网络杀伤链中的各个节点"（第 823 页）。
     - 集成节点：根据集成，会包含所选节点的详细信息。例如，电子邮件节点包含有关发件人 IP 地址、姓名和所用客户端的详细信息，以及每个附件的名称、格式和大小。
   - **响应操作**：此选项卡列出了可用的各种响应操作，具体因集成而异。例如，电子邮件节点将显示阻止发件人的电子邮件为恶意邮件以及删除附件的选项。有关更多信息，请参阅"应用响应操作"（第 865 页）。

应用响应操作

您可以对单个 XDR 图形节点应用各种响应操作。这些响应操作使您能够快速轻松地修复任何节点。

若要应用响应操作

1. 在 Cyber Protect 中控台中，转到**保护 > 事件**。
2. 在显示的事件列表中，单击要调查的事件最右侧列中的  。
3. 单击 **XDR** 选项卡。
4. 导航到相关节点，然后单击它以显示该节点的侧边栏。
   请注意，如果节点是分组身份、电子邮件或协作节点类型（由节点上的标签编号表示），则应用于此节点的响应操作将应用于组节点中的所有子节点。
5. 单击**响应操作**选项卡。
6. 单击**"执行"**以执行所需的响应操作。
   例如，Perception Point 集成支持阻止名单发件人响应操作。

对于 Microsoft Entra ID 集成，可以终止用户会话、强制密码重置和暂停用户响应操作。

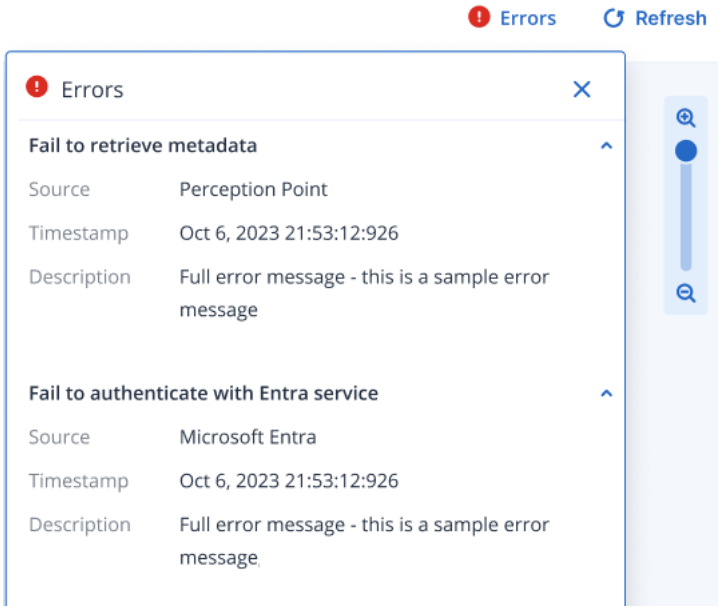
注意
点击**执行**后，会暂时禁用其他响应操作。操作完成后，将启用其他响应操作。

7. (可选) 单击**"活动"**选项卡以查看应用于节点的所有响应操作。请注意，针对 XDR 事件执行的响应操作会与 Endpoint Detection and Response (EDR) 事件一起显示。有关更多信息，请参阅 "了解为缓解事件而执行的操作"(第 824 页)。

查看 XDR 集成错误

如果在与第三方 XDR 解决方案集成期间发生错误，则会显示"错误"对话框。此对话框会显示集成错误，包括无法连接到集成源或集成配置不正确。

当您访问 XDR 图表时，如果出现错误，则会自动显示"错误"对话框。若要在其他任何时间访问此对话框，请单击 XDR 图表右上角的**错误**。请注意，如果当前没有 XDR 图表错误，则不会显示**"错误"**按钮。



XDR 图形图标

下表列出了 XDR 图表中当前可用的各种图标。

请注意，节点可以"分组"以包含多个相同类型的单个节点。代表节点的图标会显示一个数字，表示分组节点内的节点数。

例如， 

表示事件中有超过 100 个进程。如果分组的节点数少于 100，则会显示其实际数量。

图标	描述
	危害指标 (IoC) 指示通用或注入的进程。

图标	描述
	该图标标有进程名称，例如 **processname.exe**。
	泄露指标 (IoC) 指示通用文件、文档、可执行文件或脚本文件。 该图标标有文件名，例如 **filename.dll**。
	泄露指标 (IoC) 指示一个 URL。 该图标上标有 URL，例如 **abc.com**。
	攻击指标 (IoA)。 该图标标有 IoA 名称，例如 **Minikatz**。
	工作负载 该图标标有工作负载名称，例如 **DESKTOP-D123**。
	身份(用户) 该图标标有用户的帐户 ID，例如 **david.smith@b.com**。
	电子邮件图标表示通用电子邮件、附件或 URL。 该图标上标有发件人的电子邮件地址，例如 **david.smith@b.com**。

管理软件

评估漏洞和管理修补程序

漏洞评估 (VA) 是一个对系统中发现的漏洞进行识别、量化并确定优先级的过程。在漏洞评估模块中，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。

具有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 868 页)。
- macOS。有关详细信息，请参阅 "支持的 Apple 和第三方产品"(第 870 页)。
- Linux (CentOS 7/Virtuozzo/安克诺斯 Cyber Infrastructure) 计算机。有关详细信息，请参阅 "支持的 Linux 产品"(第 870 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。

具有 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 868 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计算机上已安装的保护代理程序。
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. 在获取发现的漏洞列表后，可以处理它并确定必须修复哪些找到的漏洞。

可以在**监控** > **概述** > **漏洞/现有漏洞**小组件中，监视漏洞评估扫描的结果。

支持的 Microsoft 和第三方产品

支持针对以下适用于 Windows 操作系统的 Microsoft 产品和第三方产品进行漏洞评估和修补程序管理。

支持的 Microsoft 产品

桌面操作系统

- Windows 11
- Windows 10
- Windows 8.1

- Windows 8
- Windows 7 (Enterprise, Professional, Ultimate)

服务器操作系统

- Windows Server 2022
- 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 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2013
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Server 2016

Windows 支持的第三方产品

Cyber Protect 支持漏洞评估和修补管理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，例如以下所示：

- Microsoft Teams
- Zoom
- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

有关 Windows 支持的第三方产品的完整列表，请参阅 第三方产品支持的修补管理列表 (62853)。

支持的 Apple 和第三方产品

支持以下适用于 macOS 的 Apple 产品和第三方产品进行漏洞评估：

支持的 Apple 产品

macOS

- macOS 10.13.x 及更高版本

macOS 内置应用程序

- Safari、iTunes 等。

支持的 macOS 第三方产品

- Microsoft Office(Word、Excel、PowerPoint、Outlook、OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Skype
- Thunderbird
- VLC media player

支持的 Linux 产品

支持以下 Linux 发行版和版本进行 VA：

- Virtuozzo 7.x
- CentOS 7.x
- CentOS 8.x

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”。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 VA 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**（有关支持的适用于 Windows 操作系统的第三方产品的详细信息，请参阅修补程序管理支持的第三方产品列表 (62853)）
- macOS 计算机：
  - **Apple 产品**
  - **macOS 第三方产品**
- Linux 计算机：
  - **扫描 Linux 程序包**

预定

根据要在选定计算机上执行的漏洞评估扫描来定义预定：

现场	描述
使用以下事件预定任务运行	此设置定义任务将何时运行。 以下值可用： • **按时间预定** - 这是默认设置。任务将根据指定的时间运行。 • **用户登录系统时** - 默认情况下，任何用户登录都会触发任务。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，任何用户注销都会触发任务。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。
预定类型	如果在**使用以下事件预定任务运行**中选择了**按时间预定**，则该字段会显示。 以下值可用： • **月** – 选择运行任务的月份和月份中的特定周或特定天。 • **每日** - 这是默认设置。选择任务将在星期几运行。 • **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。
启动时间	如果在**使用以下事件预定任务运行**中选择了**按时间预定**，则该字段会显示。 选择任务将运行的确切时间。

现场	描述
在日期范围内运行	如果在**使用以下事件预定任务运行**中选择了**按时间预定**，则该字段会显示。 设置配置的预定将有效的日期范围。
指定登录到操作系统将启动任务的用户帐户	如果在**使用以下事件预定任务运行**中选择了**用户登录系统时**，则该字段会显示。 以下值可用： • **任何用户** - 如果希望任何用户的登录触发任务，请使用此选项。 • **以下用户** - 如果仅希望特定用户帐户的登录触发任务，请使用此选项。
指定从操作系统注销将启动任务的用户帐户	如果在**使用以下事件预定任务运行**中选择了**用户注销系统时**，则该字段会显示。 以下值可用： • **任何用户** - 如果希望任何用户的注销触发任务，请使用此选项。 • **以下用户** - 如果仅希望特定用户帐户的注销触发任务，请使用此选项。
开始条件	定义为了任务能够运行而必须同时满足的所有条件。 防恶意软件扫描的开始条件类似于“开始条件”中所述的**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 10:00 点，延迟时间为 60 分钟，则任务将在上午 10:00 点到上午 11:00 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。

为 Windows 计算机配置漏洞评估

1. 在 Cyber Protect 中控台中，创建保护计划，然后启用**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 870 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**监控** > **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 Cyber Protect 中控台中，创建保护计划，然后启用**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 870 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**监控** > **概述** > **漏洞/现有漏洞**小组件。

macOS 设备的漏洞评估

可以扫描 macOS 设备以查找操作系统级别和应用程序级别的漏洞。

为 macOS 设备配置漏洞评估

1. 在 Cyber Protect 中控台中，创建保护计划，然后启用**漏洞评估**模块。
2. 指定漏洞评估设置：
   - **扫描内容** – 选择 **Apple 产品**、**macOS 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 870 页)。
3. 将计划指派给 macOS 设备。

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。

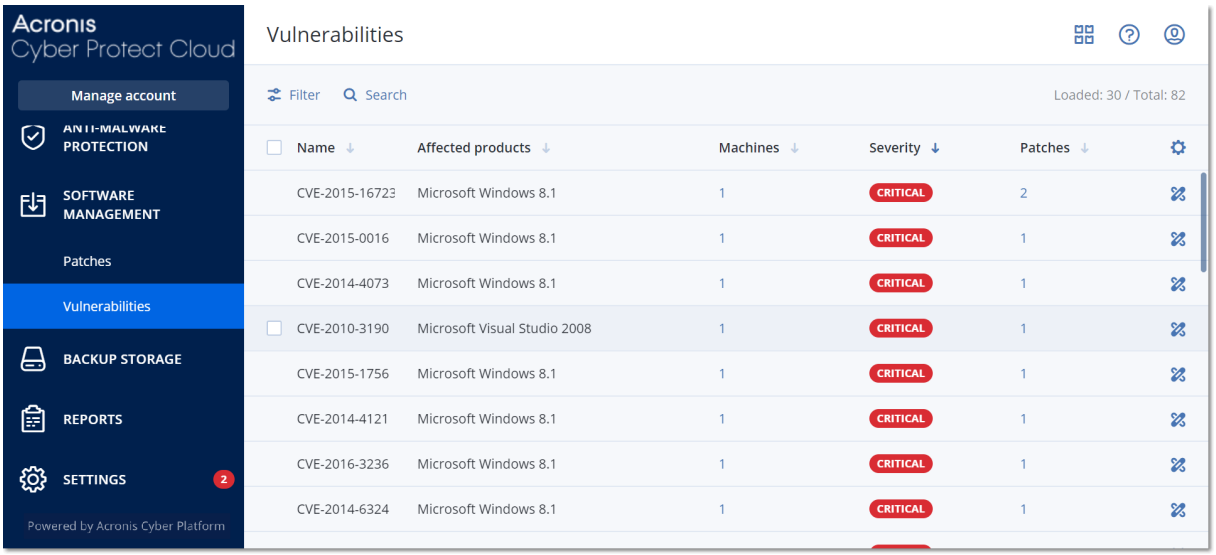
要监控漏洞评估的结果，请查看**监控** > **概述** > **漏洞/现有漏洞**小组件。

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要安装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修补程序的漏洞。

名称	描述
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 Cyber Protect 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. 选择要在选定计算机上安装的修补程序，然后单击**下一步**。
4. 选择要安装修补程序的计算机。
5. 选择重新启动选项。

a. 选择是否希望计算机在完成安装修补程序后重新启动。

选项	描述
否	在完成安装修补程序后，计算机不会自动重新启动。
如果需要	仅当应用修补程序需要重新启动时，才会重新启动计算机。
是	在完成安装修补程序后，计算机会自动重新启动。还可以指定重新启动延迟。

b. [可选] 如果要在计算机备份过程中延迟计算机重新启动，请选择**备份完成之前，请勿重新启动**。

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

注意
此功能的可用性取决于为您的帐户启用的服务配额。

有关支持的适用于 Windows 操作系统的第三方产品的详细信息，请参阅修补程序管理支持的第三方产品列表 (62853)。

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
- 手动或按预定安装修补程序
- 根据不同的条件精确定义要安装的修补程序：严重性、类别和批准状态
- 执行更新前备份以防止更新可能失败
- 定义修补程序安装后的重新启动操作

注意
要使用 Windows 更新，修补程序管理功能要求在工作负载上启用 Windows 更新。

Cyber Protection 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。

修补程序管理工作流

修补程序管理工作流包括配置和应用保护计划、运行漏洞评估扫描、配置修补程序设置、批准修补程序以及最后安装已批准修补程序的步骤。工作流的具体步骤如下所示。

1. 配置已启用**漏洞评估**和**修补程序管理**模块的保护计划。
2. 配置漏洞评估设置。有关这些设置的详细信息，请参阅 "漏洞评估设置"(第 870 页)。
3. 配置修补程序管理设置。有关这些设置的详细信息，请参阅 "在保护计划中的修补程序管理设置"(第 876 页)。
4. 将保护计划应用于一台或多台计算机。
5. 等待漏洞评估扫描完成。扫描将根据保护计划中配置的预定自动启动。或者，可以根据需要通过单击保护计划的**漏洞评估**模块中的**立即运行**图标，来手动启动扫描。
6. 批准修补程序。可以定义自动修补程序批准的设置，其中包括在测试计算机上自动安装修补程序。有关详细信息，请参阅 "自动修补程序批准"(第 882 页)。或者，可以通过将修补程序的批准状态设置为**已批准**，来手动批准修补程序。有关详细信息，请参阅 "手动批准修补程序"(第 885 页)。
7. 安装修补程序。批准的修补程序可以根据保护计划中配置的预定自动安装。或者，可以根据需要手动安装修补程序。有关详细信息，请参阅 "手动安装修补程序"(第 886 页)。

可以在**监控** > **概述** > **修补程序安装历史记录**小组件中，监视修补程序安装的结果。

在保护计划中的修补程序管理设置

在保护计划的**修补程序管理**模块中，可以配置以下修补程序管理设置：

- 要为 Microsoft 和适用于 Windows OS 的第三方产品安装哪些更新。
- 何时运行自动修补程序安装。
- 是否运行更新前备份。

有关创建保护计划并启用**修补程序管理**模块的更多信息，请参阅 "创建保护计划"(第 192 页)。

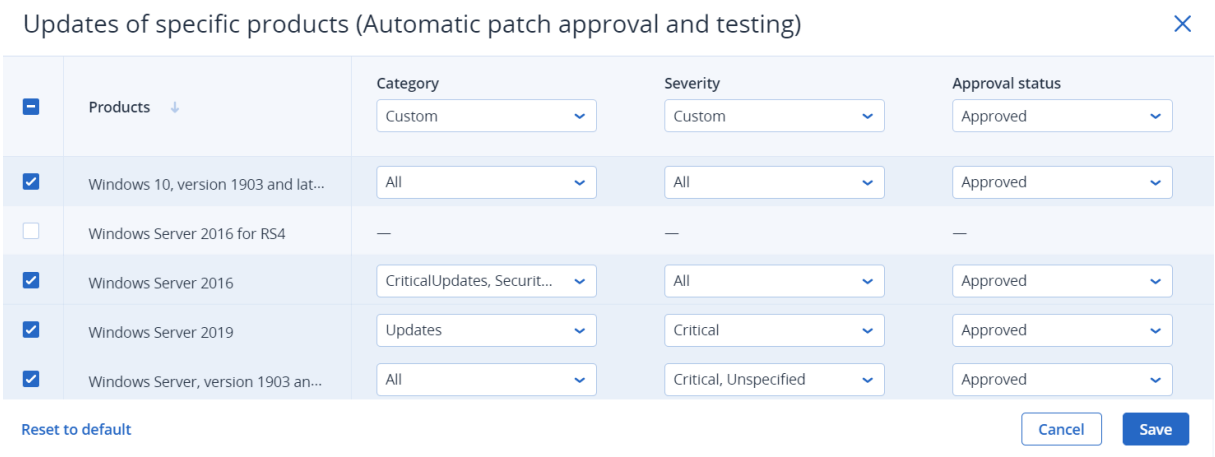
注意
此功能的可用性取决于为您的帐户启用的服务配额。

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。

选择安装选项：

选项	描述
所有更新	如果要安装所有已批准的更新，请使用此选项。
仅安全和重要更新	如果要安装所有已批准的安全和关键更新，请使用此选项。
特定产品的更新(自动修补程序批准和测试)	如果要为不同的产品定义自定义设置，请使用此选项。 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。 若要配置修补程序的自动测试批准和测试，请选择此选项。



对于 Microsoft 产品，修补程序分发使用 Windows API 服务。修补程序和更新不会在内部或分发代理程序上下载或存储。相反，将从 Microsoft CDN 下载它们。因此，即使指派了“更新程序”角色，代理程序也无法下载和分发修补程序。

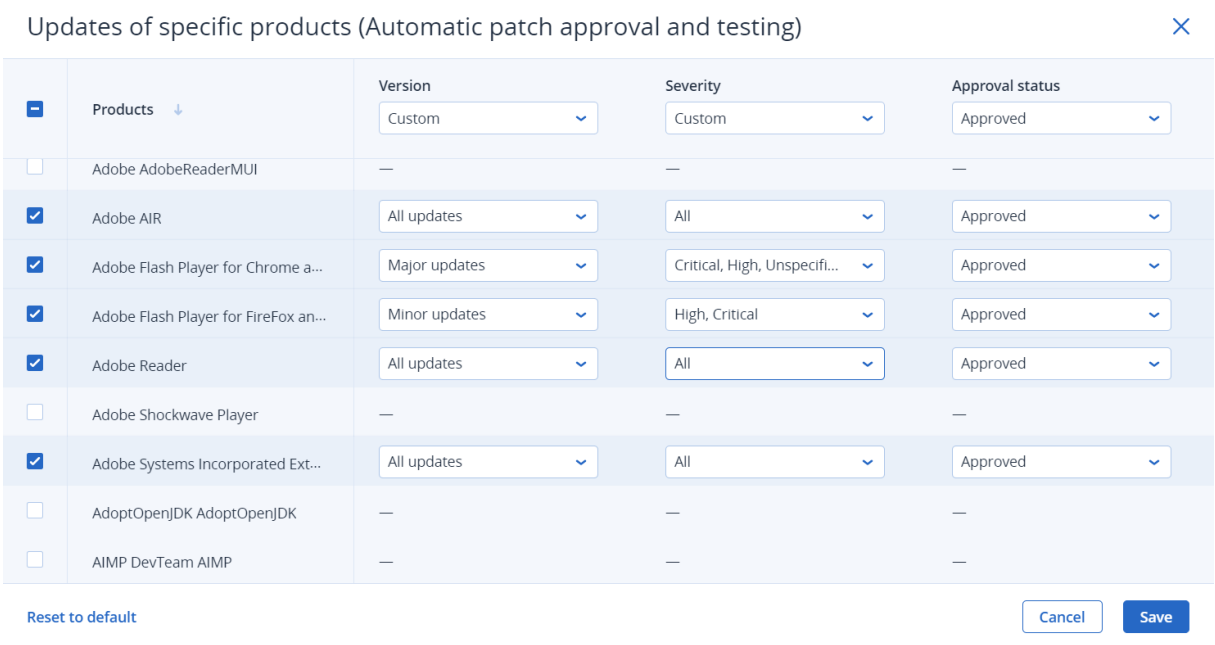
Windows 第三方产品

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。

选择安装选项：

选项	描述
所有更新	如果要安装所有已批准的更新，请使用此选项。*
仅主要更新	如果要安装所有已批准的主要更新，请使用此选项。
仅小幅更新	如果要安装已批准的小幅更新，请使用此选项。
特定产品的更新(自动修补程序批准和测试)	如果要为不同的产品定义自定义设置，请使用此选项。 如果要更新特定产品，那么可以按类别、严重性或批准状态为每个产品定义要安装的更新。 若要配置修补程序的自动测试批准和测试，请选择此选项。
仅为检测到漏洞的应用程序安装最新版本	如果要仅为检测到漏洞的应用程序安装最新更新，请选中此复选框。*

* 此选项需要 Cyber Protect 代理程序版本 23.11.36772 或更高版本。



对于 Windows 第三方产品，修补程序将直接从内部 安克诺斯 数据库分发到托管工作负载。如果“更新程序”角色已指派给代理程序，则该代理程序将用于下载和分发修补程序。

预定

定义在选定计算机上安装更新所依据的预定和条件。

现场	描述
使用以下事件预定任务运行	此设置定义任务将何时运行。 以下值可用： • **按时间预定** - 这是默认设置。任务将根据指定的时间运行。 • **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。
预定类型	如果在**使用以下事件预定任务运行**中选择了**按时间预定**，则该字段会显示。 以下值可用： • **月** – 选择运行任务的月份和月份中的特定周或特定天。 • **每日** - 这是默认设置。选择任务将在星期几运行。

现场	描述
	• **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。
启动时间	如果在**使用以下事件预定任务运行**中选择了**按时间预定**，则该字段会显示 选择任务将运行的确切时间。
配置修补程序的维护窗口	如果在**使用以下事件预定任务运行**中选择了**按时间预定**，则该字段会显示。 如果希望修补程序安装仅在您将指定的时间间隔期间运行，则选择此设置。如果修补程序安装进程在为修补程序定义的维护时段结束时还未完成，则将自动停止。
在日期范围内运行	如果在**使用以下事件预定任务运行**中选择了**按时间预定**，则该字段会显示。 设置配置的预定将有效的日期范围。
指定登录到操作系统将启动任务的用户帐户	如果在**使用以下事件预定任务运行**中选择了**用户登录系统时**，则该字段会显示。 以下值可用： • **任何用户** - 如果希望任何用户的登录触发任务，请使用此选项。 • **以下用户** - 如果仅希望特定用户帐户的登录触发任务，请使用此选项。
指定从操作系统注销将启动任务的用户帐户	如果在**使用以下事件预定任务运行**中选择了**用户注销系统时**，则该字段会显示。 以下值可用： • **任何用户** - 如果希望任何用户的注销触发任务，请使用此选项。 • **以下用户** - 如果仅希望特定用户帐户的注销触发任务，请使用此选项。
开始条件	定义为了任务能够运行而必须同时满足的所有条件。 防恶意软件扫描的开始条件类似于“开始条件”中所述的**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 10:00 点，延迟时间为 60 分钟，则任务将在上午 10:00 点到上午 11:00 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。
更新后重新启动	定义是否在更新安装完成后自动重新启动计算机。

现场	描述
	以下值可用： • **从不** - 在更新之后，从不进行重新启动。 • **如果需要** - 仅当应用更新需要，才会进行重新启动。 • **始终** - 在更新之后，始终进行重新启动。可以指定重新启动延迟。
备份完成之前，请勿重新启动	如果选择此选项，而且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。

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。它让您可以针对以下情况有预防措施：安装更新失败并且您需要返回到以前状态。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。

查看可用修补程序的列表

在漏洞评估扫描完成后，可以在**软件管理 > 修补程序**中查看有关可用修补程序的信息。

要查看有关特定修补程序的详细信息，请在修补程序列表中单击相应修补程序。

下表描述了可以在屏幕上查看的修补程序的信息。

现场	描述
批准状态	批准状态主要用于自动批准场景。 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 • **待批准** - 修补程序状态不清楚，应进行验证
许可协议	• 同意 • 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
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

受影响的产品	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。
发布日期	修补程序的发布日期
上次报告	上次报告修补程序的日期
首次安装	首次在计算机上成功安装修补程序的日期
Microsoft 知识库	如果修补程序适用于 Microsoft 产品，则该字段会显示知识库文章 ID
计算机	受影响的计算机数量
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

配置列表中的修补程序生命周期

可以通过在**修补程序**屏幕上配置列表中的修补程序生命周期，来使修补程序列表保持处于最新状态。此设置定义检测到的可用修补程序将在修补程序列表中可见的时长。在修补程序成功安装在所有指示它丢失的计算机上或列表中的生命周期结束后，该修补程序会从列表中删除。

配置列表中的修补程序生命周期

1. 在 Cyber Protect 中控台中，转到**软件管理** > **修补程序**。
2. 单击**设置**。
3. 在**列表中的生命周期**中，选择适当选项。

选项	描述
永远	修补程序将始终保留在列表中。
7 天	在修补程序首次安装 7 天后，该修补程序将从列表中删除。 例如，让我们假定您有两台必须安装修补程序的计算机。其中一台处于联机状态，另一台处于脱机状态。修补程序已安装在第一台计算机上。7 天后，该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	在修补程序首次安装 30 天后，该修补程序将从列表中删除。

自动修补程序批准

自动修补程序批准使在计算机上安装更新的过程更简单。通过使用自动修补程序批准，安装修补程序就不会因手动修补程序批准过程而延迟。重要更新和修补程序的安装速度更快，从而提高系统的可靠性。

可以在测试场景中使用自动修补程序批准，来自动安装修补程序。如果修补程序成功安装在测试计算机上，那么这些修补程序也会自动安装在生产计算机上。有关此场景的详细信息，请参阅 "自动修补程序批准和测试使用案例"(第 883 页)。

还可以在场景中使用自动修补程序批准以在生产环境中自动安装修补程序，从而跳过测试阶段。有关此场景的详细信息，请参阅 "自动修补程序批准(不测试)使用案例"(第 885 页)。

配置自动修补程序批准

可以配置自动修补程序批准，并确保安装修补程序不会因手动修补程序批准过程而延迟。

配置自动修补程序批准

1. 在 Cyber Protect 中控台中，转到**软件管理** > **修补程序**。
2. 单击**设置**。
3. 启用**自动修补程序批准**。
4. 配置自动修补程序批准的设置。

a. 选择自动修补程序批准选项。

选项	描述
自动修补程序批准和测试	当成功安装修补程序后经过选定天数时，修补程序的批准状态将更改为**已批准**。如果要通过先在测试计算机上安装修补程序来测试它们、确保一切都按预期工作，然后在生产环境中安装修补程序，建议您使用此设置。
自动修补程序批准(不测试)	当找到修补程序后经过选定天数时，修补程序的批准状态将更改为**已批准**。

b. 选择满足自动修补程序批准选项中条件后必须经过的天数。在此期间过后，修补程序的批准状态将自动从**待批准**更改为**已批准**。

5. 选择**自动接受许可协议**。
6. 单击**应用**。

自动修补程序批准和测试使用案例

如果您想要在将新修补程序安装在生产计算机上之前先在测试计算机上测试它们，可以配置两个保护计划 - 一个计划用于安装修补程序以供测试之用，一个计划用于在生产计算机上安装测试过的修补程序。这样，您将确保安装在生产环境中的修补程序是安全的，而且生产计算机在修补程序安装之后正常工作。

使用案例包括以下阶段：

1. 配置自动修补程序批准的设置。选择**自动修补程序批准和测试**选项。有关详细信息，请参阅 "配置自动修补程序批准"(第 882 页)。
2. 准备保护计划用于测试目的(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**待批准**。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。有关详细信息，请参阅 "配置测试修补保护计划"(第 883 页)。
3. 配置用于生产环境的保护计划(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**。有关详细信息，请参阅 "配置生产修补保护计划"(第 884 页)。
4. 运行“测试修补”计划并检查结果。将没有问题的计算机的批准状态保留为**待批准**，但将错误运行的计算机的批准状态更改为**已拒绝**。根据在**自动修补程序批准**中设置的天数，修补程序的批准状态将自动从**待批准**更改为**已批准**。当您运行生产修补计划时，仅**已批准**的修补程序将安装在生产计算机上。有关详细信息，请参阅 "运行测试修补保护计划并拒绝不安全的修补程序"(第 885 页)。
5. 运行生产修补计划。

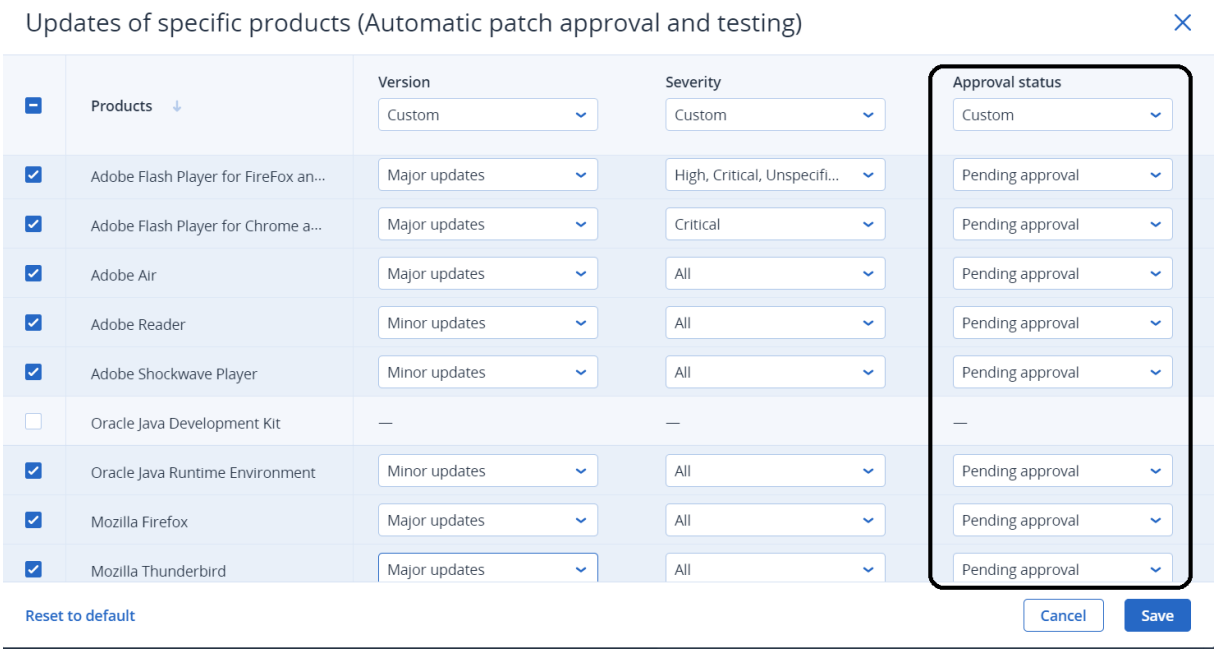
配置测试修补保护计划

可以为测试环境中的计算机配置具有修补程序安装设置的保护计划。

配置测试修补保护计划

1. 在 Cyber Protect 中控台中，转到**管理** > **保护计划**。
2. 单击**创建计划**。
3. 启用**修补程序管理**模块。
4. 为 Microsoft 和第三方产品、预定以及更新前备份定义要安装的更新。有关这些设置的更多详细信息，请参阅 "在保护计划中的修补程序管理设置"(第 876 页)。

重要事项
对于要更新的所有产品，请选择**待批准**批准状态。因此，代理程序会仅将**待批准**修补程序安装在测试环境中的选定计算机上。



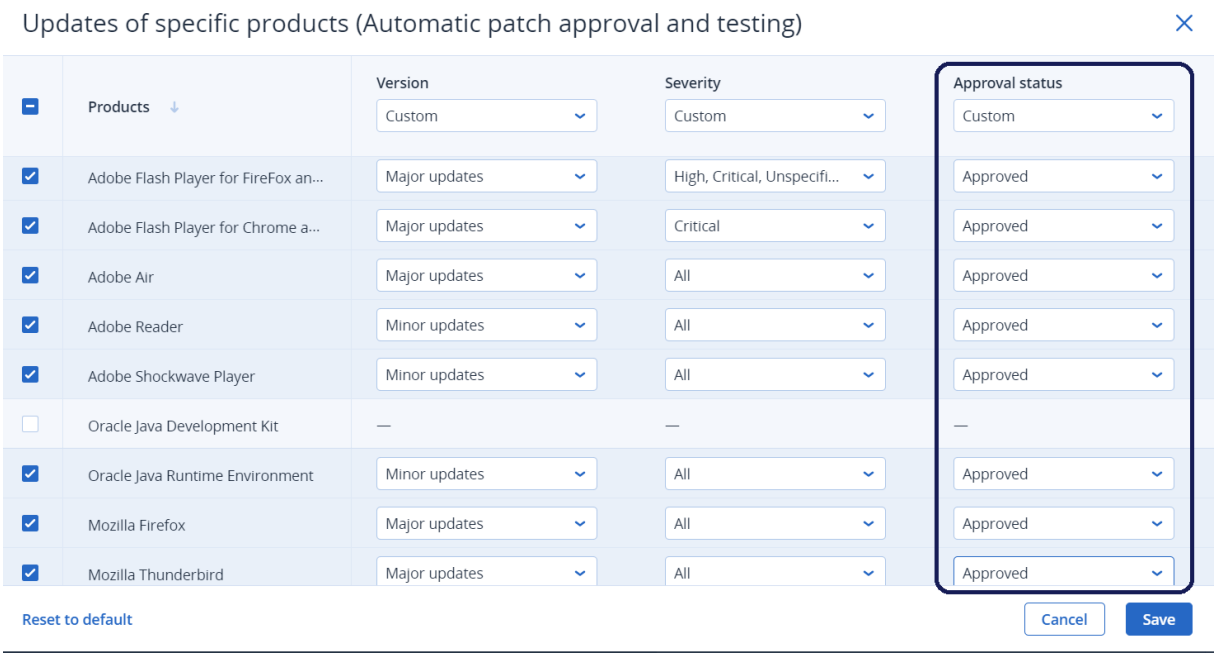
配置生产修补保护计划

可以为生产环境中的计算机配置具有修补程序安装设置的保护计划。

配置生产修补保护计划

1. 在 Cyber Protect 中控台中，转到**管理** > **保护计划**。
2. 单击**创建计划**。
3. 启用**修补程序管理**模块。
4. 为 Microsoft 和第三方产品、预定以及更新前备份定义要安装的更新。有关这些设置的更多详细信息，请参阅 "在保护计划中的修补程序管理设置"(第 876 页)。

重要事项
对于要更新的所有产品，请将**批准状态**设置为**已批准**。因此，代理程序会仅将**已批准**修补程序安装在生产环境中的选定计算机上。



运行测试修补保护计划并拒绝不安全的修补程序

在修补程序安装在测试环境中的计算机上后，可以检查是否一切运行正常。可以将没有问题的计算机的批准状态保留为**待批准**，但将错误运行的计算机的批准状态更改为**已拒绝**。

运行测试修补保护计划并拒绝不安全的修补程序

1. 运行测试修补保护计划(按预定或手动)。
2. 根据结果，查看哪些已安装的修补程序是安全的。
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**设置为**已拒绝**。

自动修补程序批准(不测试)使用案例

如果您想尽快在生产计算机上自动安装新修补程序，而不先在测试计算机上安装它们，则可以仅配置一个保护计划。

使用案例包括以下阶段：

1. 配置自动修补程序批准的设置。选择**自动修补程序批准(不测试)**选项。有关详细信息，请参阅 "配置自动修补程序批准"(第 882 页)。
2. 配置用于生产环境的保护计划(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**。有关详细信息，请参阅 "配置生产修补保护计划"(第 884 页)。
3. 运行生产修补计划。

手动批准修补程序

可以手动批准修补程序，并通过跳过测试阶段来加快其安装速度。

先决条件

- 已将启用**修补程序管理**模块的保护计划应用于至少一台 Windows 计算机。
- 存在仍未安装在已应用保护计划的计算机上的修补程序。

手动批准修补程序

1. 在 Cyber Protect 中控台中，转到**软件管理** > **修补程序**。
2. 选择要安装的修补程序，然后接受它们的许可协议。
3. 将修补程序的**批准状态**设置为**已批准**。

   修补程序的批准状态已设置为**已批准**。修补程序将根据保护计划中定义的预定自动安装在计算机上。如果要立即安装修补程序，请按照 "手动安装修补程序"(第 886 页) 中所述的步骤进行操作。

手动安装修补程序

当您不打算等待预定的修补程序安装时间时，可以根据需要手动安装修补程序。

可以从三个屏幕启动手动安装修补程序：**修补程序**、**漏洞**和**所有设备**。

手动安装修补程序

从修补程序

1. 在 Cyber Protect 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. 在**安装修补程序**向导中，选择要安装的修补程序，然后单击**安装**。
4. 选择要安装修补程序的计算机。
5. 选择重新启动选项。
   a. 选择是否希望计算机在完成安装修补程序后重新启动。

选项	描述
否	在完成安装修补程序后，计算机不会自动重新启动。
如果需要	仅当应用修补程序需要重新启动时，才会重新启动计算机。
是	在完成安装修补程序后，计算机会自动重新启动。还可以指定重新启动延迟。

   b. [可选] 如果要在计算机备份过程中延迟计算机重新启动，请选择**备份完成之前，请勿重新启动**。
6. 单击**安装修补程序**。

从漏洞

1. 在 Cyber Protect 中控台中，转到**软件管理** > **漏洞**。
2. 执行修补过程，如 "管理发现的漏洞"(第 873 页) 中所述。

从所有设备

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 选择要安装修补程序的计算机。
3. 单击**修补**。
4. 选择要安装的修补程序，然后单击**下一步**。
5. 选择重新启动选项。
   a. 选择是否希望计算机在完成安装修补程序后重新启动。

选项	描述
否	在完成安装修补程序后，计算机不会自动重新启动。
如果需要	仅当应用修补程序需要重新启动时，才会重新启动计算机。
是	在完成安装修补程序后，计算机会自动重新启动。还可以指定重新启动延迟。

   b. [可选] 如果要在计算机备份过程中延迟计算机重新启动，请选择**备份完成之前，请勿重新启动**。
6. 单击**安装修补程序**。

使用软件存储库和软件包

注意
此功能需要 Advanced Management 包。

软件包

软件包是 .msi 或 .exe 文件，您可以使用它们在工作负载上远程部署(安装或卸载)软件。

软件包由软件版本和一些自定义设置(如语言和架构类型)定义。

软件存储库

软件存储库是存储软件包的仓库。

有两个软件存储库：**库**和**我的程序包**。

库

库存储库包含 40 个最常用的软件应用程序。此存储库的内容是预定义的，并由系统维护。您无法编辑或删除此存储库中的软件包。此外，您无法直接从此处部署软件包。若要部署软件包，您必须首先将其添加到**我的包**存储库。

我的软件包

我的包存储库包含您可以部署并包括在软件部署计划中的所有软件包。初始情况下，即使**库**存储库中有程序包，此存储库也是空的。您可以通过以下方式将程序包添加到**我的包**：

- 通过从 **Library** 存储库添加程序包。有关详细信息，请参阅 "从库中添加软件包"(第 889 页)。
- 通过手动上传软件包。有关详细信息，请参阅 "上传软件包"(第 890 页)。

将软件包添加到**我的包**后，您可以使用快速部署操作或将其包含在软件部署计划中进行部署。有关详细信息，请参阅 "正在安装软件"(第 892 页)、"正在卸载软件"(第 894 页) 和 "创建软件部署计划"(第 895 页)。

浏览软件存储库

注意
此功能需要 Advanced Management 包。

可以在软件存储库中搜索特定的软件包，并查看有关此软件包的详细信息。

若要搜索软件包

在库中

1. 在 Cyber Protect 中控台中，转到**软件管理** > **库**。
   在**库**屏幕上，可以看到包含 40 个最常用的软件应用程序的列表，以及每个应用程序的以下信息：

现场	描述
名称	软件的名称。
最新版本	存储库中可用的应用程序的最新版本。
供应商	软件供应商的名称。
许可证类型	许可证类型：专有或开源。

2. [可选] 若要按名称搜索软件包，请单击**搜索**，然后输入名称。
   根据在字段中输入的文本，程序包列表会进行动态筛选。
3. [可选] 若要筛选包的列表，请单击**筛选**，指定值，然后单击**应用**。
   以下表格提供有关此页面可用筛选器的更多详细信息。

过滤器	描述
供应商	如果您知道软件供应商的名称，并且只想查看该供应商的软件，请使用此筛选器。
许可证类型	如果要根据许可证类型(专有或开源)筛选结果，请使用此筛选器。
最新发布期	若要筛选结果并仅查看在指定期间发布的软件包，请使用此筛选器。

4. 若要查看包的所有详细信息，请单击列表中的相应行。

在我的包中

1. 在 Cyber Protect 中控台中，转到**软件管理 > 我的包**。
   在 **我的包** 屏幕上，可以看到可在受控工作负载上部署的程序包以及每个程序包的以下信息：

现场	描述
名称	软件的名称。
版本	软件的版本。
供应商	软件供应商的名称。
数字签名检查	数字签名检查的状态。
操作系统	可部署该软件包的操作系统。
上次编辑者	上次编辑包的用户名。
系统类型	将部署软件包的操作系统的体系结构类型。
包大小	软件包的大小。

2. [可选] 若要按名称搜索软件包，请单击**搜索**，然后输入名称。
   根据在字段中输入的文本，程序包列表会进行动态筛选。
3. [可选] 若要筛选包的列表，请单击**筛选**，指定值，然后单击**应用**。
   以下表格提供有关此页面可用筛选器的更多详细信息。

过滤器	描述
供应商	如果您知道软件供应商的名称，并且只想查看该供应商的软件，请使用此筛选器。
上次编辑者	若要筛选结果并仅查看特定用户编辑的包，请使用此筛选器。
系统类型	如果要根据系统架构类型筛选结果，请使用此筛选器。
语言	如果想要根据软件语言来筛选结果，请使用此筛选器。
发布期	若要筛选结果并仅查看在指定期间发布的软件包，请使用此筛选器。

4. 若要查看包的所有详细信息，请单击列表中的相应行。

从库中添加软件包

注意
此功能需要 Advanced Management 包。

库存储库包含 40 个最常用的软件应用程序。若要能够从库中部署包，首先必须将其添加到您的包。

将库中的程序包添加到"我的程序包"

1. 在 Cyber Protect 中控台中，转到**软件管理** > **库**。
2. 在要添加至您的包的软件包的行上，单击**添加**。
3. 在**添加到我的包**向导中，选择软件设置。

设置	描述
版本	软件的版本。
语言	软件的语言。
架构类型	将部署软件包的操作系统的体系结构类型。

4. 选择**我接受 EULA 条款和条件**，然后单击**添加**。
   已将该包添加到您的包。可以在"**我的包**"页面上看到它。

上传软件包

注意
此功能需要 Advanced Management 包。

在**我的包**页面，可以上传以下格式的软件包：.msi 或 .exe。

若要上传软件包

1. 在 Cyber Protect 中控台中，转到**软件管理** > **我的包**。
2. 单击**添加包**。
3. 在**一般信息**选项卡中，输入软件设置，然后单击**下一步**。

现场	描述
软件名称	软件名称。此字段为必填字段。
供应商/发行商	软件供应商的名称。此字段为必填字段。
软件描述	软件的其他描述。此字段为可选字段。
许可证类型	软件的许可证类型。 • **专有**。专有许可证由软件供应商拥有和控制。这是默认值。 • **开源**。这些是开源软件的许可证，可供公众免费分发。

4. 在**上传包**选项卡上，执行以下操作：
   a. 单击**上传**，选择要上传的软件包，然后单击**打开**。
   b. 配置软件包设置，然后单击**下一步**。

设置	描述
版本	软件版本。此字段为必填字段。
架构类型	将部署软件包的操作系统的体系结构类型。此字段为必填字段。

设置	描述
语言	软件的语言。此字段为可选字段。
发布日期	软件发布日期。此字段为必填字段。

5. 在**安装/卸载命令**选项卡中，执行以下操作：
   a. [可选] 在**安装选项**部分的**命令参数**字段中，输入安装命令参数。
   b. [可选] 在**重新启动返回代码**和**成功返回代码**字段中，指定指示安装进程结果的返回代码。
   c. 在 **卸载选项** 部分，选择卸载方法：

卸载方法	描述
命令行	若选择此方法，则必须提供正确的静默卸载命令和参数。否则，卸载可能会停止响应。
软件或供应商名称	若选择此方法，系统将使用您提供的软件名称、供应商名称或 RegEx 模式来自动定位和运行卸载命令。 如果不确定应用程序的卸载命令，请使用此方法。

   d. [若选择 **软件或供应商名称**] 请在 **软件名称** 字段中输入软件名称。
   e. [若选择 **软件或供应商名称**] 请在 **供应商名称** 字段中输入软件供应商的名称。
   f. [如果选择 **命令行**] 在 **卸载路径** 字段中，输入卸载路径和命令。
   卸载路径是计算机上包含软件程序卸载可执行文件的目录路径。卸载路径对于确保软件能够从系统中干净完全地删除是必不可少的。
   g. 在**命令参数**字段中，输入卸载命令参数。
   h. [可选] 在**重新启动返回代码**中，输入返回代码。
   i. [可选] 在**成功返回代码**字段中，输入返回代码。
   j. 单击**下一步**。
6. 在**摘要**选项卡上，查看软件包的详细信息，选择**我已查看软件包详细信息，并确认要将其添加到我的软件包**和**我接受 EULA 的条款和条件**，然后单击**下一步**。
7. 在 **数字签名检查** 选项卡中：
   - 若要对软件包执行数字签名检查，请选择**启用数字签名检查**。

     注意
     我们建议您始终执行数字签名检查。这可确保要上传的自定义包符合标准且已进行数字签名，并可将部署未经验证或篡改的软件的风险降至最低。

   - 若要跳过检查，请清除**启用数字签名检查**。
8. 单击**添加包**。

编辑软件包

注意
此功能需要 Advanced Management 包。

您只能编辑手动上传的软件包。

若要编辑软件包

1. 在 Cyber Protect 中控台中，转到**软件管理** > **我的包**。
2. 若要编辑包，请单击 **...** 图标，然后单击 **编辑**。
3. 在**编辑程序包**向导中编辑设置，然后单击**保存**。

删除软件包

注意
此功能需要 Advanced Management 包。

您可以删除不再需要的软件包。

若要删除软件包

1. 在 Cyber Protect 中控台中，转到**软件管理** > **我的包**。
2. 若要编辑包，请单击 **...** 图标，然后单击 **删除**。
3. 在确认窗口中，单击**删除**。

如果包是手动上传的，则将永久删除该包。如果包是从库中添加的，则将仅从您的包中删除该包。

正在安装软件

注意
此功能需要 Advanced Management 包。

您可以在受控工作负载上进行远程安装，而无需创建软件部署计划。此操作支持同时最多 15 个软件包和最多 150 个目标工作负载。

若要安装软件包

从我的包

1. 在 Cyber Protect 中控台中，转到**软件管理** > **我的包**。
2. 选择要安装的软件，然后单击**安装**。
3. 在**部署软件**窗口中，单击**添加工作负载**。
4. 选择要在其上安装包的工作负载，然后单击**添加**。
5. [可选] 若要选择部署后操作，请单击**部署后操作**字段，选择选项，然后单击**完成**。

选项	描述
永不重新启动	如果不希望在安装或卸载软件后重新启动工作负载，请选择此选项。
在必要时重新启动	如果仅在软件需要时才希望在安装或卸载软件后重新启动工作负载，请选择此选项。

选项	描述
始终重新启动	如果希望始终在安装或卸载软件后重新启动工作负载，请选择此选项。
备份完成之前，请勿重新启动	若要确保在重新启动工作负载前已完成目标工作负载的任何备份，请选择此选项。 若选择了**始终重启**或**必要时重启**，则可使用此选项。
重新启动延迟	选择目标工作负载操作系统重新启动前必须经过的时间段的下拉字段。 若选择了**始终重启**或**必要时重启**，则可使用此选项。

6. 单击**立即安装**。

注意
将不会被部署未通过数字签名检查的软件包。

从所有设备

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 单击工作负载，然后单击**部署软件**。
3. 在**部署软件**窗口中，**操作**字段中选择**安装**。
4. 单击**选择软件**，选择要安装的软件，然后单击**完成**。
5. [可选] 若要选择部署后操作，请单击**部署后操作**字段，选择选项，然后单击**完成**。

选项	描述
永不重新启动	如果不希望在安装或卸载软件后重新启动工作负载，请选择此选项。
在必要时重新启动	如果仅在软件需要时才希望在安装或卸载软件后重新启动工作负载，请选择此选项。
始终重新启动	如果希望始终在安装或卸载软件后重新启动工作负载，请选择此选项。
备份完成之前，请勿重新启动	若要确保在重新启动工作负载前已完成目标工作负载的任何备份，请选择此选项。 若选择了**始终重启**或**必要时重启**，则可使用此选项。
重新启动延迟	选择目标工作负载操作系统重新启动前必须经过的时间段的下拉字段。 若选择了**始终重启**或**必要时重启**，则可使用此选项。

6. 单击**立即部署**。

正在卸载软件

注意
此功能需要 Advanced Management 包。

您可以在受控工作负载上远程卸载软件，而无需创建软件部署计划。

若要卸载软件包

从我的包

1. 在 Cyber Protect 中控台中，转到**软件管理** > **我的包**。
2. 点击要安装的修补程序，然后单击**卸载**。
3. 在**部署软件**窗口中，单击**添加工作负载**。
4. 选择要在其上安装包的一个或多个工作负载，然后单击**添加**。
5. [可选] 若要选择部署后操作，请单击**部署后操作**字段，选择选项，然后单击**完成**。

选项	描述
永不重新启动	如果不希望在安装或卸载软件后重新启动工作负载，请选择此选项。
在必要时重新启动	如果仅在软件需要时才希望在安装或卸载软件后重新启动工作负载，请选择此选项。
始终重新启动	如果希望始终在安装或卸载软件后重新启动工作负载，请选择此选项。
备份完成之前，请勿重新启动	若要确保在重新启动工作负载前已完成目标工作负载的任何备份，请选择此选项。 若选择了**始终重启**或**必要时重启**，则可使用此选项。
重新启动延迟	选择目标工作负载操作系统重新启动前必须经过的时间段的下拉字段。 若选择了**始终重启**或**必要时重启**，则可使用此选项。

6. 单击**立即卸载**。

从所有设备

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 单击工作负载，然后单击**部署软件**。
3. 在**部署软件**窗口中，**操作**字段中选择**卸载**。
4. 单击**选择软件**，选择要卸载的软件，然后单击**完成**。

5. [可选]若要选择部署后操作，请单击**部署后操作**字段，选择选项，然后单击**完成**。

选项	描述
永不重新启动	如果不希望在安装或卸载软件后重新启动工作负载，请选择此选项。
在必要时重新启动	如果仅在软件需要时才希望在安装或卸载软件后重新启动工作负载，请选择此选项。
始终重新启动	如果希望始终在安装或卸载软件后重新启动工作负载，请选择此选项。
备份完成之前，请勿重新启动	若要确保在重新启动工作负载前已完成目标工作负载的任何备份，请选择此选项。 若选择了**始终重启**或**必要时重启**，则可使用此选项。
重新启动延迟	选择目标工作负载操作系统重新启动前必须经过的时间段的下拉字段。 若选择了**始终重启**或**必要时重启**，则可使用此选项。

6. 单击**立即部署**。

软件部署计划

注意
此功能需要 Advanced Management 包。

使用软件部署计划，您可以自动执行软件部署过程，并确保受控工作负载上的软件分发一致。该功能包括以下功能：

- 软件的远程安装或卸载。
- 预定软件的自动安装或卸载。
- 安装后操作。

创建软件部署计划

注意
此功能需要 Advanced Management 包。

您可以创建软件部署计划，然后将其指派给一个或多个工作负载。右此，您可以确保在受控工作负载上分发和安装经批准的软件，同时卸载组织中已过时或未经批准的软件。

当在应用于工作负载的保护计划中启用 Active Protection 时，软件部署将受到防恶意软件引擎的保护。在工作负载上安装软件包之前，系统将自动运行防恶意软件扫描。这种主动防御层可保护免受恶意注入，确保软件部署不会在系统中引入漏洞。这在安全性至关重要的环境中尤其有价值，可降低停机和昂贵的事件响应的风险。

注意
单一软件部署计划仅支持部署操作之一:安装或卸载。这意味着您必须创建单独的计划 - 一个用于软件安装,另一个用于软件卸载。

若要创建软件部署计划

从软件部署计划

1. 在 Cyber Protect 中控台中,转到**管理** > **软件部署计划**。
2. 使用两个选项之一创建计划:
   - 如果列表中没有软件部署计划,则单击**创建**。
   - 如果列表中有软件部署计划,则单击**创建计划**。
3. [可选] 要为计划添加工作负载,请执行以下操作:
   a. 单击**添加工作负载**。
   b. 选择工作负载,然后单击**添加**。
4. 要更改计划的默认名称,请单击铅笔图标、输入计划的名称,然后单击**继续**.
5. 在**操作**字段中,选择计划将安装还是卸载软件。
6. 在**软件**字段中,单击**选择软件**,从列表中选择一个或多个应用程序,然后单击**完成**。
7. 若要配置部署后操作,请执行以下操作:
   a. 单击**部署后操作**字段。
   b. 在**安装后重启字段**中,配置系统是否在软件安装或卸载后重新启动工作负载。

值	描述
永不重新启动	如果不希望在安装或卸载软件后重新启动工作负载,请选择此选项。
在必要时重新启动	如果仅在软件需要时才希望在安装或卸载软件后重新启动工作负载,请选择此选项。
始终重新启动	如果希望始终在安装或卸载软件后重新启动工作负载,请选择此选项。

   c. [如果选择了 **始终重启** 或 **必要时重启**] 请在 **重启延迟** 字段中配置系统在重启工作负载前必须等待的时间。
   d. [可选] [如果选择了 **始终重启** 或 **必要时重启**] 为确保在备份工作负载时不会重启工作负载,请选择 **在备份完成前不要重启**。
   e. 单击**完成**。
8. 若要创建计划执行的预定程序,请执行以下操作:
   a. 单击**预定**字段。
   b. 在**预定**屏幕的**使用下列事件预定任务运行**字段中,选择将启动计划的事件。

选项	描述
运行一次	如果选择此选项,必须配置计划将运行的日期和时间。

选项	描述
按时间预定	如果选择此选项，可以配置每小时、每天或每月运行的计划。 若要此预定仅在特定时间段内生效，请勾选**在日期范围内运行**复选框，然后配置预定计划将运行的时间段(以天为单位)。
用户登录系统时	若选择此选项，则计划将在特定用户或任何用户登录至目标工作负载时运行。
用户注销系统时	若选择此选项，则计划将在特定用户或任何用户从目标工作负载注销时运行。
系统启动时	若选择此选项，则目标工作负载启动时将运行计划。
系统关闭时	若选择此选项，则目标工作负载关闭时将运行计划。
系统联机时	若选择此选项，则目标工作负载联机时将运行计划。

c. 在**启动条件**部分，选择所有必须同时满足的条件，以启动计划。

条件	描述
仅当工作负载联机时运行	该条件会在目标工作负载连接到 Internet 时得到满足。
用户空闲时	当计算机正在运行屏幕保护程序或计算机已锁定时，就会满足此条件。
用户已注销	如果选择此条件，则可以推迟预定的计划，直到目标工作负载的用户注销为止。
适合时间间隔	若选择此条件，则必须定义计划可运行的时间间隔。
节省电池电量	如果选择此条件时，可以确保计划不会因电池电量不足而中断。可使用以下选项： • **不在使用电池时启动** 仅当计算机连接到电源时，该计划才会启动。 • **如果电池电量高于以下值，则在使用电池时启动** 如果计算机连接到电源或者电池电量高于指定值，则该计划会启动。
请勿在使用按流量计费的连接时启动	若选择此条件，则当目标工作负载通过按使用量计费的连接访问 Internet 时，计划将不会运行。
不在连接到以下 Wi-Fi 网络时启动	若选择此条件，如果目标工作负载已连接至任何指定的无线网络，则计划将不会运行。 若要使用此条件，则必须指定禁止网络的 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，则当设备连接到以下任何网络时，计划将不会启动：John's iPhone、phone_wifi 或 my_PHONE_wifi。

条件	描述
检查设备 IP 地址	如果选择此条件，则目标工作负载的任何 IP 地址在指定的 IP 地址范围之内或之外，则计划将不会运行。 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** 仅支持 IPv4 地址。
如果启动条件不满足，仍运行任务	使用此选项，以设置计划将运行的时间间隔，而无需考虑任何其他条件。该计划将在其他条件满足时或这一期限结束时启动，取决于哪种情况先发生。 如果您为预定选择了**仅运行一次**选项，则无法使用此选项。

d. 单击**完成**。

9. 单击**创建**。

从所有设备

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 单击要应用软件部署计划的工作负载。
3. 单击**保护**，然后单击**添加计划**。
4. 单击**创建计划**，然后选择**软件部署**。
5. [可选] 要更改计划的默认名称，请单击铅笔图标、输入计划的名称，然后单击**继续**.
6. 在**操作**字段中，选择计划将安装还是卸载软件。
7. 在**软件**字段中，单击**选择软件**，从列表中选择一个或多个应用程序，然后单击**完成**。
8. 若要配置部署后操作，请执行以下操作：
   a. 单击**部署后操作**字段。
   b. 在**安装后重启字段**中，配置系统是否在软件安装或卸载后重新启动工作负载。

值	描述
永不重新启动	如果不希望在安装或卸载软件后重新启动工作负载，请选择此选项。
始终重新启动	如果希望始终在安装或卸载软件后重新启动工作负载，请选择此选项。
在必要时重新启动	如果仅在软件需要时才希望在安装或卸载软件后重新启动工作负载，请选择此选项。

   c. [如果选择了 **始终重启** 或 **需要重启**] 请在 **重启延迟** 字段中，配置系统在重新启动工作负载前必须等待的时间。
   d. [可选] [如果选择了 **始终重启** 或 **必要时重启**] 为确保在备份工作负载时不会重启工作负载，请选择 **在备份完成前不要重启**。
   e. 单击**完成**。
9. 若要创建计划执行的预定程序，请执行以下操作：

a. 单击**预定**字段。

b. 在**预定**屏幕的**使用下列事件预定任务运行**字段中，选择将启动计划的事件。

选项	描述
运行一次	如果选择此选项，必须配置计划将运行的日期和时间。
按时间预定	如果选择此选项，可以配置每小时、每天或每月运行的计划。 若要此预定仅在特定时间段内生效，请勾选**在日期范围内运行**复选框，然后配置预定计划将运行的时间段(以天为单位)。
用户登录系统时	若选择此选项，则计划将在特定用户或任何用户登录至目标工作负载时运行。
用户注销系统时	若选择此选项，则计划将在特定用户或任何用户从目标工作负载注销时运行。
系统启动时	若选择此选项，则目标工作负载启动时将运行计划。
系统关闭时	若选择此选项，则目标工作负载关闭时将运行计划。
系统联机时	若选择此选项，则目标工作负载联机时将运行计划。

c. 在**启动条件**部分，选择所有必须同时满足的条件，以启动计划。

条件	描述
仅当工作负载联机时运行	该条件会在目标工作负载连接到 Internet 时得到满足。
用户空闲时	当计算机正在运行屏幕保护程序或计算机已锁定时，就会满足此条件。
用户已注销	如果选择此条件，则可以推迟预定的计划，直到目标工作负载的用户注销为止。
适合时间间隔	若选择此条件，则必须定义计划可运行的时间间隔。
节省电池电量	如果选择此条件时，可以确保计划不会因电池电量不足而中断。可使用以下选项： • **不在使用电池时启动** 仅当计算机连接到电源时，该计划才会启动。 • **如果电池电量高于以下值，则在使用电池时启动** 如果计算机连接到电源或者电池电量高于指定值，则该计划会启动。
请勿在使用按流量计费的连接时启动	若选择此条件，则当目标工作负载通过按使用量计费的连接访问 Internet 时，计划将不会运行。
不在连接到以下 Wi-Fi 网络时启动	若选择此条件，如果目标工作负载已连接至任何指定的无线网络，则计划将不会运行。

条件	描述
	若要使用此条件，则必须指定禁止网络的 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，则当设备连接到以下任何网络时，计划将不会启动：John's iPhone、phone_wifi 或 my_PHONE_wifi。
检查设备 IP 地址	如果选择此条件，则目标工作负载的任何 IP 地址在指定的 IP 地址范围之内或之外，则计划将不会运行。 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** 仅支持 IPv4 地址。
如果启动条件不满足，仍运行任务	使用此选项，以设置计划将运行的时间间隔，而无需考虑任何其他条件。该计划将在其他条件满足时或这一期限结束时启动，取决于哪种情况先发生。 如果您为预定选择了**仅运行一次**选项，则无法使用此选项。

d. 单击**完成**。

10. 单击**创建**。

将工作负载添加到软件部署计划

注意
此功能需要 Advanced Management 包。

可以在创建软件部署计划后，将工作负载添加到计划。

先决条件

已为您的用户帐户启用双重身份验证。

将工作负载添加到软件部署计划

从软件部署计划

1. 在 Cyber Protect 中控台中，转到**管理** > **软件部署计划**。
2. 单击软件部署计划。
3. 根据计划是否已应用于任何工作负载，执行以下操作：
   - 如果计划尚未应用于任何工作负载，则单击**添加工作负载**。
   - 如果计划已应用于任何工作负载，则单击**管理工作负载**。
4. 从列表中选择一个工作负载，然后单击**添加**。
5. 单击**保存**。
6. 单击**确认**，以将所需的服务配额应用于工作负载。

从所有设备

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 单击要应用软件部署计划的工作负载。
3. 单击**保护**，然后单击**添加计划**。
4. 在**从下面的列表中选择计划**中，选择**软件部署**以仅查看软件部署计划。
5. 单击**应用**。
6. 单击**确认**，以将所需的服务配额应用于工作负载。

从软件部署计划中删除工作负载

注意
此功能需要 Advanced Management 包。

可以删除添加到软件部署计划的工作负载。

先决条件

已为您的用户帐户启用双重身份验证。

若要从软件部署计划中删除工作负载

1. 在 Cyber Protect 中控台中，转到**管理** > **软件部署计划**。
2. 单击软件部署计划。
3. 单击**管理工作负载**。
4. 选择一个或多个要从软件部署计划中删除的工作负载，然后单击**删除**。
5. 单击**完成**。
6. 单击**保存**。

使用软件部署计划的其他操作

注意
此功能需要 Advanced Management 包。

在**软件部署划屏幕**中，可以对软件部署执行以下附加操作：查看详细信息、编辑、查看活动、查看警报、重命名、克隆、导出和删除。

查看详细信息

先决条件

已为您的用户帐户启用双重身份验证。

若要查看软件部署计划的详细信息

1. 在**软件部署计划**屏幕中，单击软件部署计划的**更多操作**图标。
2. 单击**查看详细信息**。

编辑

先决条件

已为您的用户帐户启用双重身份验证。

若要编辑软件部署计划

1. 在**软件部署计划**屏幕中，单击软件部署计划的**更多操作**图标。
2. 单击**编辑**。

活动

若要查看与件部署计划相关的活动

1. 在**软件部署计划**屏幕中，单击软件部署计划的**更多操作**图标。
2. 单击**活动**。
3. 单击某个活动，可查看有关它的更多详细信息。

警告

查看警报

1. 在**软件部署计划**屏幕中，单击软件部署计划的**更多操作**图标。
2. 单击**警告**。

重命名

先决条件

已为您的用户帐户启用双重身份验证。

若要重命名软件部署计划

1. 在**软件部署计划**屏幕中，单击软件部署计划的**更多操作**图标。
2. 单击**重命名**。
3. 输入计划的新名称，然后单击**继续**。

克隆

先决条件

已为您的用户帐户启用双重身份验证。

若要克隆软件部署计划

1. 在**软件部署计划**屏幕中，单击软件部署计划的**更多操作**图标。
2. 单击**克隆**。
3. 单击**创建**。

导出

先决条件

已为您的用户帐户启用双重身份验证。

若要导出软件部署计划

1. 在**软件部署计划**屏幕中，单击软件部署计划的**更多操作**图标。
2. 单击**导出**。
   计划配置以 JSON 格式导出到本地计算机。

删除

先决条件

已为您的用户帐户启用双重身份验证。

若要删除软件部署计划

1. 在**软件部署计划**屏幕中，单击软件部署计划的**更多操作**图标。
2. 单击**删除**。
3. 选择**我确认**，然后单击**删除**。

软件部署计划的兼容性问题

在某些情况下，对工作负载应用软件部署计划可能会导致出现兼容性问题。您可能会发现以下兼容性问题：

- 不兼容的操作系统 - 当软件与工作负载的操作系统不兼容时，将出现此问题。
- 代理程序不受支持 - 当工作负载上的保护代理程序版本过时且不支持软件部署功能时，会出现此问题。

如果软件部署计划应用于多达 150 个单独选定的工作负载，则系统会提示您在保存计划之前解决现有冲突。要解决冲突，请消除其根本原因或从计划中删除受影响的工作负载。如果在未解决冲突的情况下保存计划，将针对不兼容的工作负载自动禁用该计划，并显示警报。

如果软件部署计划应用于 150 多个工作负载或设备组，则会先保存该计划，然后检查兼容性。该计划会针对不兼容的工作负载自动禁用，并会显示警报。

管理软件和硬件清查

软件库存记录

软件清查功能可用于已启用高级包或有(旧版) Cyber Protect 许可证的设备。该功能让您可以查看安装在所有 Windows 和 macOS 设备上的所有软件应用程序。

要获取软件清查数据，可以在设备上运行自动或手动扫描。

可以将软件清查数据用于以下用途：

- 浏览和比较有关公司设备上安装的所有应用程序的信息
- 确定是否需要更新应用程序
- 确定是否需要删除未使用的应用程序
- 确保多个公司设备上的软件版本相同
- 监控两次连续扫描之间软件状态的变化。

启用软件清查扫描

如果在设备上启用软件清查扫描，则系统会每隔 12 小时自动收集一次软件数据。

软件清查扫描功能默认会为具有所需许可证的所有设备启用，但可以根据需要更改设置。

注意
客户租户可以启用或禁用软件清查扫描。单位租户只可以查看软件清查扫描设置，但无法更改设置。

启用软件清查扫描

1. 在 Cyber Protect 中控台中，转到**设置**。
2. 单击**保护**。
3. 单击**清查扫描**。
4. 通过单击模块名称旁边的开关，即可启用**软件清查扫描**模块。

禁用软件清查扫描

1. 在 Cyber Protect 中控台中，转到**设置**。
2. 单击**保护**。
3. 单击**清查扫描**。
4. 通过单击模块名称旁边的开关，即可禁用**软件清查扫描**模块。

手动运行软件清查扫描

可以从**软件清查**屏幕手动运行软件清查，也可以从**清查**屏幕中的**软件**选项卡手动运行软件清查。

先决条件

- 设备使用的是 Windows 和 macOS 操作系统。
- 设备有所需的(旧版) Cyber Protect 许可证或已激活 Advanced Management 包。

从软件清查屏幕运行软件清查扫描

1. 在 Cyber Protect 中控台中，转到**软件管理**。
2. 单击**软件清查**。
3. 在**分组依据:**下拉字段中，选择**设备**。
4. 查找要扫描的设备，然后单击**立即扫描**。

从清查屏幕中的软件选项卡运行软件清查扫描

1. 在 Cyber Protect 中控台中，转到**设备**。
2. 单击要扫描的设备，然后单击**清查**。
3. 在**软件**选项卡中，单击**立即扫描**。

浏览软件清查

可以查看和浏览所有公司设备上可用的所有软件应用程序的数据。

先决条件

- 设备使用的是 Windows 和 macOS 操作系统。
- 设备有所需的(旧版) Cyber Protect 许可证或已激活 Advanced Management 包。
- 设备上的软件清查扫描已成功完成。

查看所有 Windows 和 macOS 公司设备上可用的所有软件应用程序

1. 在 Cyber Protect 中控台中，转到**软件管理**。
2. 单击**软件清查**。

   默认情况下，数据按设备分组。下表描述了在**软件清查**屏幕中可见的数据。

列	描述
名称	应用程序的名称。
版本	应用程序的版本。
状态	应用程序的状态。 • **新增**。 • **已更新**。 • **已删除**。 • **无更改**。
供应商	应用程序的供应商。

列	描述
安装日期	应用程序的安装日期和时间。
上次运行	仅适用于 macOS 设备。应用程序的上次活动日期和时间。
位置	应用程序的安装目录。
用户	安装应用程序的用户。
系统类型	仅适用于 Windows 设备。应用程序的位类型。 • **X86** 适用于 32 位应用程序。 • **X64** 适用于 64 位应用程序。

3. 要按应用程序对数据进行分组，请在**分组依据:** 下拉字段中选择**应用程序**。
4. 要缩小屏幕上所显示信息的范围，请使用一个过滤器或一组过滤器。
   a. 单击**过滤器**。
   b. 选择一个过滤器或一组多个过滤器。
      下表描述了**软件清查**屏幕中的过滤器。

过滤器	描述
设备名称	设备名称。可以多选。如果要比较特定设备上的软件，请使用此过滤器。
应用程序	应用程序名称。可以多选。如果要比较特定设备或所有设备上特定应用程序的数据，请使用此过滤器。
供应商	应用程序的供应商。可以多选。如果要查看特定设备或所有设备上特定供应商的所有应用程序，请使用此过滤器。
状态	应用程序状态。可以多选。如果要查看特定设备或所有设备上处于选中状态的所有应用程序，请使用此过滤器。
安装日期	应用程序的安装日期。如果要查看特定设备或所有设备上于特定日期安装的所有应用程序，请使用此过滤器。
扫描日期	软件清查扫描的日期。如果要查看有关特定设备或所有设备上于相应日期扫描的软件的信息，请使用此过滤器。

   c. 单击**应用**。
5. 要浏览整个软件清查列表，请使用屏幕左下方的分页。

- 单击要打开的页码的编号。
- 在下拉字段中，选择要打开的页面的页码。

查看单个设备的软件清查

可以查看单个设备上安装的所有软件应用程序的列表，以及有关应用程序的详细信息，例如状态、版本、供应商、安装日期、上次运行和位置。

先决条件

- 设备使用的是 Windows 和 macOS 操作系统。
- 设备有所需的（旧版）Cyber Protect 许可证或已激活 Advanced Management 包。
- 设备上的软件清查扫描已成功完成。

从软件清查屏幕查看单个设备的软件清查

1. 在 Cyber Protect 中控台中，转到**软件管理**。
2. 单击**软件清查**。
3. 在**分组依据：**下拉字段中，选择**设备**。
4. 使用以下选项之一查找要检查的设备。
   - 使用**过滤器**查找设备：
     a. 单击**过滤器**。
     b. 在**设备名称**字段中，选择要查看的设备的名称。
     c. 单击**应用**。
   - 使用动态**搜索**查找设备：
     a. 单击**搜索**。
     b. 键入完整设备名称或部分设备名称。

从设备屏幕查看单个设备的软件清查

1. 在 Cyber Protect 中控台中，转到**设备**。
2. 单击要查看的设备，然后单击**清查**。
3. 单击**软件**选项卡。

硬件清查

通过使用硬件清查功能，可以查看以下位置上可用的所有硬件组件：

- 具有支持硬件清查功能的许可证的物理 Windows 和 macOS 设备。
- 在以下虚拟化平台上运行的虚拟 Windows 和 macOS 计算机：VMware、Hyper-V、Citrix、Parallels、Oracle、Nutanix、Virtuozzo 和 Virtuozzo Hybrid Infrastructure。有关受支持的虚拟化平台版本的详细信息，请参阅 "所支持的虚拟化平台"（第 30 页）。

注意
Cyber Protect 旧版本不支持虚拟机的硬件清查功能。

仅安装有保护代理程序的设备才支持硬件清查功能。

要获取硬件清查数据，可以在设备上运行自动或手动扫描。

可以将硬件清查数据用于以下用途：

- 发现组织的所有硬件资产
- 浏览贵组织中所有设备的硬件清查
- 比较多个公司设备上的硬件组件
- 查看有关硬件组件的详细信息。

启用硬件清查扫描

如果在物理设备和虚拟机上启用硬件清查扫描，则系统会每隔 12 小时自动收集一次硬件数据。

硬件清查扫描功能默认处于启用状态，但可以根据需要更改该设置。

注意
客户租户可以启用或禁用硬件清查扫描。单位租户只可以查看硬件清查扫描设置，但无法更改设置。

启用硬件清查扫描

1. 在 Cyber Protect 中控台中，转到**设置**。
2. 单击**保护**。
3. 单击**清查扫描**。
4. 通过单击模块名称旁边的开关，即可启用**硬件清查扫描**模块。

禁用硬件清查扫描

1. 在 Cyber Protect 中控台中，转到**设置**。
2. 单击**保护**。
3. 单击**清查扫描**。
4. 通过单击模块名称旁边的开关，即可禁用**硬件清查扫描**模块。

手动运行硬件清查扫描

可以针对单个设备手动运行硬件清查扫描，然后查看该设备的硬件组件的当前数据。

注意
仅当虚拟机的当前日期和时间与 UTC 中的当前日期和时间相对应时，才支持对虚拟机进行硬件清查扫描。为了确保虚拟机使用正确的时间设置，请禁用虚拟机的**时间同步**选项、设置当前日期、时间和时区，然后重新启动 **安克诺斯 Agent Core Service** 和 **安克诺斯 Managed Machine Service**。

先决条件

- （对于所有设备）设备使用 Windows 或 macOS 操作系统。
- （对于所有设备）设备有支持硬件清查功能的许可证。请注意，（旧版）Cyber Protect 版本不支持虚拟机的硬件清查功能。
- （对于所有设备）保护代理程序已安装在设备上。

- (对于虚拟机)计算机在受支持的虚拟化平台之一上运行。有关详细信息,请参阅 "硬件清查"(第 907 页)。

在单个设备上运行硬件清查扫描

1. 在 Cyber Protect 中控台中,转到**设备**。
2. 单击要扫描的设备,然后单击**清查**。
3. 在**硬件**选项卡中,单击**立即扫描**。

浏览硬件清查

可以查看和浏览所有公司设备上可用的所有硬件组件的数据。

先决条件

- (对于所有设备)设备使用 Windows 或 macOS 操作系统。
- (对于所有设备)设备的许可证支持硬件清查功能。请注意,Cyber Protect 旧版本不支持虚拟机的硬件清查功能。
- (对于所有设备)保护代理程序已安装在设备上。
- (对于所有设备)设备上的硬件清查扫描已成功完成。
- (对于虚拟机)计算机在受支持的虚拟化平台之一上运行。有关详细信息,请参阅 "硬件清查"(第 907 页)。

查看 Windows 和 macOS 公司设备上可用的所有硬件组件

1. 在 Cyber Protect 中控台中,转到**设备**。
2. 在**视图:**下拉字段中,选择**硬件**。

注意
该视图是一组列,这些列确定屏幕上可见的数据。预定义的视图为**标准**和**硬件**视图。可以创建和保存自定义视图,这些视图包含各组不同的列,并且更方便满足您的需求。

下表描述了在**硬件**视图中可见的数据。

列	描述
名称	设备名称。
硬件扫描状态	硬件扫描的状态。 • **已完成**。 • **未启动**。 • **不支持**。针对不支持硬件清查功能的工作负载(即虚拟机、移动设备、Linux 设备)显示状态。 • **更新代理程序**。如果设备上安装了过时版本的代理程序时,会显示该状态。单击此操作将重定向到"设置">"代理程序"页面,其中管理员可以执行代理程序更新。

列	描述
	• **升级配额**。单击它会打开一个对话框，其中管理员可以将当前许可证切换为其他可用于租户许可证的许可证
处理器	设备所有处理器的型号。
处理器核心	设备所有处理器的核心数。
磁盘存储	设备已使用的存储，以及所有磁盘的总存储。
内存	设备的总 RAM 容量。
扫描日期	上次硬件清查扫描的日期和时间。
主板	设备的主板。
主板序列号	主板的序列号。
BIOS 版本	系统 BIOS 的版本。
组织	设备所属的组织。
所有者	设备的所有者。
域	设备的域。
操作系统	设备的操作系统。
操作系统版本	设备操作系统的版本。

3. 要在表中添加列，请单击相应列选项图标，然后选择要在表中可见的列。
4. 要缩小屏幕上所显示信息的范围，请使用一个或多个过滤器。
   a. 单击**搜索**。
   b. 单击相应箭头，然后单击**硬件**。
   c. 选择一个过滤器或一组多个过滤器。
      下表描述了**硬件**过滤器。

过滤器	描述
处理器型号	可以多选。如果要查看具有指定处理器型号的设备的硬件数据，请使用此过滤器。
处理器核心	如果要查看具有指定处理器核心数量的设备的硬件数据，请使用此过滤器。
磁盘总大小	如果要查看具有指定总存储大小的设备的硬件数据，请使用此过滤器。
内存容量	如果要查看具有指定 RAM 容量的设备的硬件数据，请使用此过滤器。

   d. 单击**应用**。

5. 要按升序对数据进行排序，请单击列名。

查看单个设备的硬件

可以查看有关特定设备的主板、处理器、内存、图形卡、存储驱动器、网络和系统的详细信息。

先决条件

- （对于所有设备）设备使用 Windows 或 macOS 操作系统。
- （对于所有设备）设备的许可证支持硬件清查功能。请注意，Cyber Protect 旧版本不支持虚拟机的硬件清查功能。
- （对于所有设备）保护代理程序已安装在设备上。
- （对于所有设备）设备上的硬件清查扫描已成功完成。
- （对于虚拟机）计算机在受支持的虚拟化平台之一上运行。有关详细信息，请参阅 "硬件清查"（第 907 页）。

查看有关特定设备的硬件的详细信息

1. 在 Cyber Protect 中控台中，转到**设备** -> **所有设备**。
2. 在**视图:** 下拉字段中，选择**硬件**。
3. 使用以下所述方法之一查找要检查的设备。
   - 使用**过滤器**查找设备：
     a. 单击**过滤器**。
     b. 选择一个或一组多个过滤器参数来查找设备。
     c. 单击**应用**。
   - 使用**搜索**查找设备：
     a. 单击**搜索**。
     b. 键入完整设备名称或部分设备名称，然后单击 **Enter**。
4. 选择列出相应设备的行，然后单击**清查**。
5. 单击**硬件**选项卡。
   以下硬件数据可用。

硬件组件	显示的信息
主板	设备主板的名称、制造商、型号和序列号。
处理器	每个设备处理器的制造商、型号、最大时钟速度和核心数量。
内存	设备内存的容量、制造商和序列号。
图形卡	设备 GPU 的制造商和型号。
存储驱动器	设备存储驱动器的型号、媒体类型、可用空间和大小。

硬件组件	显示的信息
网络	设备网络适配器的 Mac 地址、IP 地址和类型。
系统	系统的产品 ID、原始安装日期、系统启动时间、系统制造商、系统型号、BIOS 版本、启动设备、系统区域设置和时区。

连接到工作负载以实现远程桌面或远程协助

远程桌面和协助功能是一种便捷方式，可用于连接到组织中的工作负载以实现远程控制或远程协助。从 2022 年 12 月开始，该功能支持 NEAR、RDP 和 Apple 屏幕共享协议。有关详细信息，请参阅 "远程连接协议"(第 917 页)。

可以使用远程桌面功能来执行以下任务。

- 在“仅查看”模式下，使用 NEAR 连接到远程 Windows、macOS 和 Linux 工作负载。
- 使用 RDP 连接到远程 Windows 工作负载。
- 在“仅查看”或“隔离”模式下，使用 Apple 屏幕共享连接到远程 macOS 工作负载。
- 连接到托管工作负载，并使用云远程连接来远程控制它们。
- 连接到非托管工作负载，并使用直接远程连接来远程控制它们。
- 使用 安克诺斯 Quick Assist 连接到非托管远程工作负载。
- 使用不同的身份验证方法连接到远程工作负载：使用远程工作负载凭据、通过请求观察或控制权限，或使用访问代码(适用于 Quick Assist)。
- 在多视图中，同时观察多个监视器。
- 记录远程会话(通过 NEAR 连接时)。
- 查看会话历史记录报告。

有关标准和 Advanced Management 包中所包含功能的详细信息，请参阅 "支持的远程桌面和协助功能"(第 914 页)。

可以使用远程协助功能来执行以下任务。

- 在控制模式下，使用 NEAR 连接到远程 Windows、macOS 和 Linux 工作负载。
- 在“控制”模式下，使用 Apple 屏幕共享连接到远程 macOS 工作负载。
- 通过使用云远程连接，为工作负载提供远程协助。
- 在本地和远程工作负载之间传输文件。
- 对远程工作负载执行基本管理操作：重新启动、关机、睡眠、清空回收站和注销远程用户。
- 通过定期对远程工作负载的桌面拍摄屏幕截图来监视它。

有关标准保护和 Advanced Management 中所包含功能的详细信息，请参阅 "支持的远程桌面和协助功能"(第 914 页)。

重要事项

要为托管工作负载激活完整的远程桌面和协助功能，必须配置远程管理计划并将其应用于工作负载。尽管只能对工作负载应用一个远程管理计划，但根据需要，可以配置不同的远程管理计划并将其应用于不同的工作负载。

例如，可以创建一个仅已启用 RDP 协议的远程管理计划，并将其应用于某些工作负载。这样，就可以远程连接到这些工作负载，而无需为每个工作负载激活 Advanced Management 许可证，也无需支付任何额外费用。

另一方面，可以创建另一个已启用 NEAR 和 Apple 屏幕共享协议的远程管理计划。在这种情况下，将为每个工作负载激活 Advanced Management 许可证，您将为应用此远程管理计划的每个工作负载付费。

有关远程管理计划及其使用的详细信息，请参阅 "远程管理计划"(第 920 页)。

注意

远程桌面和协助功能需要满足以下条件：

- 在管理(主机) 工作负载上一次性安装 Connect Client。当首次对目标工作负载尝试执行远程操作(远程控制或远程协助) 时，系统会建议您下载该客户端。或者，可以从 保护 中控台的**下载**窗口下载 Connect Client。有关可以配置的设置的详细信息，请参阅 "配置 Connect Client 设置"(第 947 页)。
- 在托管工作负载上安装 Connect Agent。从版本 15.0.31266 开始，Connect Agent 是 保护 代理程序包含的模块。
- 对于 macOS 远程工作负载，应将所需系统权限授予 Connect Agent。有关详细信息，请参阅 "在 macOS 中安装保护代理程序"(第 76 页)。
- 在非托管工作负载上运行 安克诺斯 Quick Assist 应用程序。可以从网站下载 安克诺斯 Quick Assist。

有关每个远程桌面和协助组件支持的平台的详细信息，请参阅 "支持的平台"(第 916 页)。

支持的远程桌面和协助功能

下表提供了有关对 2022 年 12 月引入的远程桌面和协助功能的受支持功能的更改的详细信息。

功能	标准保护 2022 年 12 月之前	Advanced Management 2022 年 12 月之前	标准保护 2022 年 12 月之后	Advanced Management 2022 年 12 月之后
通过 RDP 远程协助(适用于 Windows)	是	否	否	否
与用户共享远程连接	否	是	否	否
远程连接				

功能	标准保护 2022 年 12 月之前	Advanced Management 2022 年 12 月之前	标准保护 2022 年 12 月之后	Advanced Management 2022 年 12 月之后
远程操作	否	否	是	是
为 Windows/macOS/Linux 选择要连接的会话	否	否	否	是
通过 RDP 和 Apple 屏幕共享直接连接	否	否	否	是
多窗口控制	否	否	否	是
连接模式:控制/仅查看/隔离	否	否	否	是
远程连接支持的常用凭据	否	否	是	是
每个技术人员的并发连接				
通过 RDP	是	是	是	是
通过 NEAR	否	否	否	是
文件传输和共享				
从 Windows 到 Windows/macOS/Linux	否	否	否	是
从 macOS 到 Windows/macOS/Linux	否	否	否	是
从 Linux 到 Windows/macOS/Linux	否	否	否	是
通过 Quick Assist 应用程序连接				
从 Windows 到 Windows/macOS/Linux	否	否	否	是
从 macOS 到 Windows/macOS/Linux	否	否	否	是
从 Linux 到 Windows/macOS/Linux	否	否	否	是
通过协议远程连接				
通过 NEAR 远程连接				
从 Windows 到 Windows/macOS/Linux	否	否	否	是

功能	标准保护 2022 年 12 月之前	Advanced Management 2022 年 12 月之前	标准保护 2022 年 12 月之后	Advanced Management 2022 年 12 月之后
从 macOS 到 Windows/macOS/Linux	否	否	否	是
从 Linux 到 Windows/macOS/Linux	否	否	否	是
通过 RDP 远程连接(桌面客户端)				
从 Windows 到 Windows	是	是	是	是
从 macOS 到 Windows	是	是	是	是
从 Linux 到 Windows	否	否	是	是
通过 RDP 远程连接(Web 客户端)				
从 Windows 到 Windows	是	是	是	是
从 macOS 到 Windows	是	是	是	是
从 Linux 到 Windows	否	否	是	是
通过 Apple 屏幕共享远程连接				
从 Windows/macOS/Linux 到 macOS	否	否	否	是
会话管理				
会话录制	否	否	否	是
报告和监视				
会话历史记录和搜索	否	否	否	是
屏幕截图传输	否	否	否	是
通过剪贴板进行文件交换	否	否	否	是

支持的平台

下表列出了远程桌面和协助功能的每个组件支持的操作系统。

远程桌面组件	支持的平台
Connect Client	• Windows 7 或更高版本 • macOS 10.13 或更高版本 • Linux:

远程桌面组件	支持的平台
	openSUSE 8 Debian 9, 10 Ubuntu 18.0-20.10 Red Hat Enterprise Linux 8 CentOS 8 Fedora 31-33 SUSE Linux Enterprise Server 15 SP2 Linux Mint 20 Manjaro 20
Connect Agent	• Windows 7 或更高版本 • Windows Server 2008 R2 或更高版本 • macOS 10.13 或更高版本 • Linux： Red Hat Enterprise Linux 8、8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) -19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1
安克诺斯 Quick Assist	• Windows 7 或更高版本 • Windows Server 2008 R2 或更高版本 • macOS 10.13 或更高版本 • Linux： Red Hat Enterprise Linux 8、8.1 Fedora 30 Ubuntu 18.4 LTS (Bionic Beaver) -19.04 (Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1

远程连接协议

远程桌面功能使用以下协议进行远程连接。

NEAR

NEAR 是一种由 Acronis 开发的高度安全的协议，有以下特点。

- ### H.264

  NEAR 实现了三种质量模式：**平滑**、**平衡**和**锐利**。在**平滑**模式下，NEAR 在 macOS 和 Windows 上使用硬件 H.264 编码来对桌面图片进行编码；如果硬件编码器不可用，则返回到软件编码器。图片大小目前限制为全高清分辨率 (1920x1080)。

- ### 自适应编解码器

  在**平衡**和**锐利**质量模式下，NEAR 使用自适应编解码器；与 H.264 使用的“视频”模式相比，该编解码器可提供 32 位的全画质。

  在**平衡**模式下，图像质量会根据当前网络条件自动调整，并保持当前帧速率。

  在**锐利**模式下，图片是全质量的；但如果网络、处理器或视频卡过载，则图片的帧速率可能会降低。

  当 OpenCL 在 Windows 和 macOS 的图形驱动程序中可用时，自适应编解码器会在其上使用 OpenCL。

- ### 声音传输

  NEAR 能够捕获远程计算机的声音并将其传输给主机。有关在 Windows、macOS 和 Linux 上启用远程声音重定向的详细信息，请参阅 "远程声音重定向"(第 919 页)。

- ### 不同的登录选项

  可以使用以下方法登录到远程工作负载。

  访问代码：登录到远程工作负载的用户运行 Quick Assist 并告知您访问代码。使用此方法，将始终连接到当前登录用户的会话。

  工作负载凭据：使用在工作负载中注册的管理员凭据登录到远程工作负载。

  请求观察或控制权限：登录到远程工作负载的用户会被要求允许或拒绝连接。

- ### 安全

  在 NEAR 中，您的数据始终是使用 AES 加密进行双向加密的。

RDP

远程桌面协议 (RDP) 是由 Microsoft 开发的专有协议，可允许通过网络连接来连接到远程 Windows 计算机。

Apple 屏幕共享

Apple 屏幕共享是 Apple 公司推出的 VNC 客户端，作为 macOS 10.5 版及更高版本的一部分。

远程声音重定向

Connect Client 通过 NEAR 连接协议支持音频流。有关 NEAR 的详细信息，请参阅 "远程连接协议"(第 917 页)。

重定向远程 Windows 工作负载的声音

对于 Windows 工作负载，远程声音应该会自动传输。确保有声音输出设备(扬声器或耳机)连接到远程工作负载。

重定向远程 macOS 工作负载的声音

要支持重定向 macOS 工作负载的声音，请确保：

- 工作负载已装有 保护 代理程序。
- 工作负载已装有声音捕获驱动程序。
- 工作负载使用 NEAR 协议进行远程连接。

注意
对于 macOS 10.15 Catalina，必须将麦克风权限授予 Connect Agent。有关将麦克风权限授予 Connect Agent 的详细信息，请参阅 "为 Connect Agent 授予所需的系统权限"(第 71 页)。

该代理程序使用以下声音捕获驱动程序：Soundflower 或 Blackhole。

Blackhole WiKi 页面上描述了最新版本的安装过程：https://github.com/ExistentialAudio/BlackHole/wiki/Installation。

注意
当前，Connect Client 仅支持 2 通道版本的 Blackhole。

或者，如果在工作负载上安装 Homebrew，则可以通过运行以下命令来安装 Blackhole：

```
brew install --cask blackhole-2ch
```

注意
当重定向远程 macOS 工作负载的声音时，已登录到远程工作负载的用户不会听到声音。

重定向远程 Linux 工作负载的声音

远程声音重定向应该会在大多数 Linux 发行版中自动工作。如果远程声音重定向默认不起作用，则通过运行以下命令来安装 PulseAudio 驱动程序：

```
sudo apt-get install pulseaudio
```

连接到远程工作负载以实现远程桌面或远程协助

远程桌面和协助功能提供了几种方法，可用于建立与您的工作负载的远程直接连接或云连接。

通过局域网 (LAN) 中的 TCP/IP，在 Connect Client 和未装有代理程序的远程工作负载之间建立直接连接。它们不需要访问 Internet。

通过 Cloud，在 Connect Client 和工作负载上的代理程序或 Quick Assist 之间建立云连接。

下表提供了有关云连接选项的详细信息。

云连接	云连接选项	视图模式	支持的远程操作	适用于
通过 NEAR	从 Connect Client 至 Connect Agent 从 Connect Client 至 Quick Assist	控制 仅查看	远程桌面 远程协助	托管工作负载
通过 RDP	从 Connect Client 至 Connect Agent 从 Web 客户端到 Connect Agent	控制	远程桌面	托管工作负载
通过 Apple 屏幕共享	从 Connect Client 至 Connect Agent	控制 仅查看 隔离	远程桌面 远程协助	托管工作负载

下表提供了有关直接连接选项的详细信息。

直接连接	直接连接选项	支持的远程操作	适用于
通过 RDP	从 Connect Client 到 RDP 服务器	远程桌面	非托管工作负载
通过 Apple 屏幕共享	从 Connect Client 到 Apple 屏幕共享服务器	远程桌面 远程协助	非托管工作负载

远程管理计划

远程管理计划是您在 保护 代理程序上应用的计划，可用于在托管工作负载上启用和配置远程桌面和协助功能。

如果在工作负载上未应用远程管理计划，则远程桌面和协助功能将仅限于远程操作（重新启动、关机、睡眠、清空回收站和注销远程用户）。

注意

可以在远程管理计划中配置的设置的可用性取决于应用于租户的服务包。要访问所有设置，请激活 Advanced Management 包。有关标准和 Advanced Management 包中所包含功能的详细信息，请参阅 "支持的远程桌面和协助功能"（第 914 页）。

创建远程管理计划

可以创建远程管理计划，然后将其指派给工作负载，以配置托管工作负载上的远程桌面和协助功能。

注意
远程管理计划设置的可用性取决于指派给租户的服务配额。如果使用的是标准功能，则只能配置通过 RDP 连接。

先决条件

已为您的用户帐户启用双重身份验证。

创建远程管理计划

从远程管理计划

1. 在 Cyber Protect 中控台中，转到**管理** > **远程管理计划**。
2. 使用两个选项之一创建远程管理计划。
   - 如果列表中没有远程管理计划，则单击**创建**。
   - 如果列表中有远程管理计划，则单击**创建计划**。
3. [可选] 要更改计划的默认名称，请单击铅笔图标、输入计划的名称，然后单击**继续**.
4. 单击**连接协议**，然后为远程连接启用要在此远程管理计划中可用的协议：NEAR、RDP 或 Apple 屏幕共享。
5. [可选] 对于 NEAR 协议，在**安全设置**部分中，选中或取消选中复选框以启用或禁用相应设置，然后单击**完成**。

设置	描述	适用于
当用户与中控台会话断开连接时锁定工作负载	如果选择此设置，则与中控台会话断开连接时，将锁定远程工作负载。	Windows、macOS
一次只允许一个用户使用 NEAR 连接或传输文件	如果选择此设置，则当与工作负载的远程连接处于活动状态时，无法使用 NEAR 连接，也无法传输文件。	Windows、macOS、Linux
允许工作负载的管理员连接到任何非管理员用户会话	如果选择此设置，则允许管理员连接到工作负载上的任何标准用户会话。 如果同时取消选中**允许工作负载的管理员连接到任何非管理员用户会话**和**允许创建系统会话**，则只能连接到远程 macOS 工作负载上的活动管理员会话。	Windows、macOS

设置	描述	适用于
允许创建系统会话	如果选择此设置，则当建立远程连接时，管理员将在新会话中进行连接，而不是在现有的其中一个活动会话中进行连接。	macOS
允许剪贴板同步	如果选择此设置，则可以在剪贴板和远程工作负载的剪贴板之间传输数据。例如，您将能够从远程工作负载上的文件中复制一些文本，并将其粘贴到您工作负载上的文件中，反之亦然。	Windows、macOS、Linux

6. 单击**安全设置**、选中或取消选中复选框以启用或禁用相应设置，然后单击**完成**。

设置	描述
显示是否远程控制工作负载	如果选择此设置，则当存在与工作负载的活动远程桌面连接时，远程工作负载的桌面上会显示通知。
要求用户提供权限以对工作负载拍摄屏幕截图	如果选择此设置，则当管理员请求从工作负载传输屏幕截图时，远程工作负载的用户会收到通知。

7. 单击**工作负载管理**、选择要在远程工作负载上可用的功能，然后单击**完成**。

设置	描述	可用于
文件传输	支持本地和远程工作负载之间的文件传输。	Windows、macOS、Linux
屏幕截图传输	支持将远程工作负载的桌面屏幕截图传输给 Cyber Protect 中控台。	Windows、macOS、Linux

8. 单击**显示设置**、选中或取消选中复选框以启用或禁用相应设置，然后单击**完成**。

注意
显示设置仅适用于通过 NEAR 连接。

设置	描述	可用于
使用桌面重复数据删除进行桌面捕获	桌面复制是 Windows 上的屏幕捕获方法之一。在某些环境中，它可能不稳定。如果不使用桌面重复数据删除，将	Windows

设置	描述	可用于
	改用基本方法 (BitBlt):它的速度较慢,但更稳定。	
使用 OpenCL 加速	OpenCL 加速可以通过在图形处理单元 (GPU) 上运行一些计算,来提高负责**平衡**质量模式的自适应编解码器的速度。这需要在远程 Linux 上安装 OpenCL 驱动程序。 如果 OpenCL 在您的图形驱动程序中可用,则自适应编解码器会在 macOS 和 Windows 上使用 OpenCL。	Linux
使用硬件 H.264 编码	NEAR 支持三种质量模式:**平滑**、**平衡**和**锐利**。 **平滑**模式使用硬件 H.264 编码来对桌面图片进行编码。 **平衡**模式使用自适应编解码器;与 H.264 使用的"视频"模式相比,该编解码器可提供 32 位的全画质。图像质量会根据当前网络条件自动调整,并保持当前帧速率。 **锐利**模式使用自适应编解码器;与 H.264 使用的"视频"模式相比,该编解码器可提供 32 位的全画质。图像质量始终是全画质,但如果网络或处理器/视频卡过载,则图像质量可能会随每秒帧数的降低而下降。	Windows、macOS

9. 如果您希望在工作负载的详细信息中显示上次登录到工作负载的用户的相关信息,请单击**工具箱**、选择**显示上次登录的用户**,然后单击**完成**。
   有关上次登录用户的详细信息,请参阅 "查找上次登录用户"(第 327 页)。
10. [可选] 要为计划添加工作负载,请执行以下操作:
    a. 单击**添加工作负载**。
    b. 选择工作负载,然后单击**添加**。
    c. 如果有要解决的兼容性问题,则按照 "解决远程管理计划的兼容性问题"(第 930 页) 中所述的步骤操作。
11. 单击**创建**。

从所有设备

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 单击要应用远程管理计划的工作负载。
3. 单击**保护**，然后单击**添加计划**。
4. 单击**创建计划**，然后选择**远程管理**。
5. [可选] 要更改计划的默认名称，请单击铅笔图标、输入计划的名称，然后单击**继续**.
6. 单击**连接协议**，然后为远程连接启用要在此远程管理计划中可用的协议：NEAR、RDP 或 Apple 屏幕共享。
7. [可选] 对于 NEAR 协议，在**安全设置**部分中，选中或取消选中复选框以启用或禁用相应设置，然后单击**完成**。

设置	描述	适用于
当用户与中控台会话断开连接时锁定工作负载	如果选择此设置，则与中控台会话断开连接时，将锁定远程工作负载。	Windows、macOS
一次只允许一个用户使用 NEAR 连接或传输文件	如果选择此设置，则当与工作负载的远程连接处于活动状态时，无法使用 NEAR 连接，也无法传输文件。	Windows、macOS、Linux
允许工作负载的管理员连接到任何非管理员用户会话	如果选择此设置，则允许管理员连接到工作负载上的任何标准用户会话。 如果同时取消选中**允许工作负载的管理员连接到任何非管理员用户会话**和**允许创建系统会话**，则只能连接到远程 macOS 工作负载上的活动管理员会话。	Windows、macOS
允许创建系统会话	如果选择此设置，则当建立远程连接时，管理员将在新会话中进行连接，而不是在现有的其中一个活动会话中进行连接。	macOS
允许剪贴板同步	如果选择此设置，则可以在剪贴板和远程工作负载的剪贴板之间传输数据。例如，您将能够从远程工作负载上的文件中复制一些文本，并将其粘贴到您工作负载上的文件中，反之亦然。	Windows、macOS、Linux

8. 单击**安全设置**、选中或取消选中复选框以启用或禁用相应设置，然后单击**完成**。

设置	描述
显示是否远程控制工作负载	如果选择此设置，则当存在与工作负载的活动远程桌面连接时，远程工作负载的桌面上会显示通知。
要求用户提供权限以对工作负载拍摄屏幕截图	如果选择此设置，则当管理员请求从工作负载传输屏幕截图时，远程工作负载的用户会收到通知。

9. 单击**工作负载管理**、选择要在远程工作负载上可用的功能，然后单击**完成**。

设置	描述	可用于
文件传输	支持本地和远程工作负载之间的文件传输。	Windows、macOS、Linux
屏幕截图传输	支持将远程工作负载的桌面屏幕截图传输给 Cyber Protect 中控台。	Windows、macOS、Linux

10. 单击**显示设置**、选中或取消选中复选框以启用或禁用相应设置，然后单击**完成**。

注意
显示设置仅适用于通过 NEAR 连接。

设置	描述	可用于
使用桌面重复数据删除进行桌面捕获	桌面复制是 Windows 上的屏幕捕获方法之一。在某些环境中，它可能不稳定。如果不使用桌面重复数据删除，将改用基本方法 (BitBlt)：它的速度较慢，但更稳定。	Windows
使用 OpenCL 加速	OpenCL 加速可以通过在图形处理单元 (GPU) 上运行一些计算，来提高负责**平衡**质量模式的自适应编解码器的速度。这需要在远程 Linux 上安装 OpenCL 驱动程序。 如果 OpenCL 在您的图形驱动程序中可用，则自适应编解码器会在 macOS 和 Windows 上使用 OpenCL。	Linux
使用硬件 H.264 编码	NEAR 支持三种质量模式：**平滑**、**平衡**和**锐利**。 **平滑**模式使用硬件 H.264 编	Windows、macOS

设置	描述	可用于
	码来对桌面图片进行编码。 **平衡**模式使用自适应编解码器;与 H.264 使用的“视频”模式相比,该编解码器可提供 32 位的全画质。图像质量会根据当前网络条件自动调整,并保持当前帧速率。 **锐利**模式使用自适应编解码器;与 H.264 使用的“视频”模式相比,该编解码器可提供 32 位的全画质。图像质量始终是全画质,但如果网络或处理器/视频卡过载,则图像质量可能会随每秒帧数的降低而下降。	

11. 如果您希望在工作负载的详细信息中显示上次登录到工作负载的用户的相关信息,请单击**工具箱**、选择**显示上次登录的用户**,然后单击**完成**。
    有关上次登录用户的详细信息,请参阅 "查找上次登录用户"(第 327 页)。
12. 单击**创建**。

将工作负载添加到远程管理计划

根据需要,可以在创建计划后为远程管理计划添加工作负载。

先决条件

已为您的用户帐户启用双重身份验证。

将工作负载添加到远程管理计划

从远程管理计划

1. 在 Cyber Protect 中控台中,转到**管理** > **远程管理计划**。
2. 单击远程管理计划。
3. 根据计划是否已应用于任何工作负载,执行以下操作:
   - 如果计划尚未应用于任何工作负载,则单击**添加工作负载**。
   - 如果计划已应用于任何工作负载,则单击**管理工作负载**。
4. 从列表中选择一个工作负载,然后单击**添加**。
5. 单击**保存**。
6. 单击**确认**,以将所需的服务配额应用于工作负载。

从所有设备

1. 在 Cyber Protect 中控台中,转到**设备** > **所有设备**。
2. 单击要应用远程管理计划的工作负载。

3. 单击**保护**，然后单击**添加计划**。
4. 在**从下面的列表中选择计划**中，选择**远程管理**以仅查看远程管理计划。
5. 单击**应用**。
6. 单击**确认**，以将所需的服务配额应用于工作负载。

从远程管理计划中删除工作负载

根据需要，可以从远程管理计划中删除工作负载。

先决条件

已为您的用户帐户启用双重身份验证。

从远程管理计划中删除工作负载

1. 在 Cyber Protect 中控台中，转到**管理** > **远程管理计划**。
2. 单击远程管理计划。
3. 单击**管理工作负载**。
4. 选择一个或多个要从远程管理计划中删除的工作负载，然后单击**删除**。
5. 单击**完成**。
6. 单击**保存**。

现有远程管理计划的附加措施

在**远程管理计划**屏幕中，可以对远程管理计划执行以下附加操作：查看详细信息、编辑、查看活动、查看警报、重命名、启用、禁用、克隆、导出、删除、设为收藏、设为默认，和删除。

查看详细信息

先决条件

已为您的用户帐户启用双重身份验证。

查看远程管理计划的详细信息

1. 在**远程管理计划**屏幕中，单击远程管理计划的**更多操作**图标。
2. 单击**查看详细信息**。

编辑

先决条件

已为您的用户帐户启用双重身份验证。

编辑计划

1. 在**远程管理计划**屏幕中，单击远程管理计划的**更多操作**图标。
2. 单击**编辑**。

活动

查看与远程管理计划相关的活动

1. 在**远程管理计划**屏幕中，单击远程管理计划的**更多操作**图标。
2. 单击**活动**。
3. 单击某个活动，可查看有关它的更多详细信息。

警告

查看警报

1. 在**远程管理计划**屏幕中，单击远程管理计划的**更多操作**图标。
2. 单击**警告**。

重命名

先决条件

已为您的用户帐户启用双重身份验证。

重命名远程管理计划

1. 在**远程管理计划**屏幕中，单击远程管理计划的**更多操作**图标。
2. 单击**重命名**。
3. 输入计划的新名称，然后单击**继续**。

启用

先决条件

已为您的用户帐户启用双重身份验证。

启用远程管理计划

1. 在**远程管理计划**屏幕中，单击远程管理计划的**更多操作**图标。
2. 单击**启用**。

禁用

先决条件

已为您的用户帐户启用双重身份验证。

禁用远程管理计划

1. 在**远程管理计划**屏幕中，单击远程管理计划的**更多操作**图标。
2. 单击**禁用**。

克隆

先决条件

已为您的用户帐户启用双重身份验证。

若要克隆一个远程管理计划

1. 在**远程管理计划**屏幕中，单击远程管理计划的**更多操作**图标。
2. 单击**克隆**。

3. 单击**创建**。

导出

先决条件

已为您的用户帐户启用双重身份验证。

若要导出远程管理计划

1. 在**远程管理计划**屏幕中，单击远程管理计划的**更多操作**图标。
2. 单击**导出**。
   计划配置以 JSON 格式导出到本地计算机。

设置为默认值

先决条件

已为您的用户帐户启用双重身份验证。

将远程管理计划设置为默认

1. 在**远程管理计划**屏幕中，单击远程管理计划的**更多操作**图标。
2. 单击**"设为默认值"**。
3. 在确认窗口中，单击**"设置"**。
   在**远程管理计划**屏幕上，计划名称旁边会出现**默认**标签。

设为收藏

先决条件

已为您的用户帐户启用双重身份验证。

将远程管理计划设置为收藏

1. 在**远程管理计划**屏幕中，单击远程管理计划的**更多操作**图标。
2. 单击**添加到收藏夹**。
   在**远程管理计划**屏幕上，计划名称旁边会出现一个星形图标。

删除

先决条件

已为您的用户帐户启用双重身份验证。

删除远程管理计划

1. 在**远程管理计划**屏幕中，单击远程管理计划的**更多操作**图标。
2. 单击**删除**。
3. 选择**我确认**，然后单击**删除**。

远程管理计划的兼容性问题

在某些情况下，对工作负载应用远程管理计划可能会导致出现兼容性问题。您可能会发现以下兼容性问题：

- 计划冲突 - 由于只能将一个远程管理计划应用于工作负载，因此当另一个远程管理计划已应用于该工作负载时，就会出现此问题。
- 操作系统不兼容 - 当工作负载的操作系统不受支持时，会出现此问题。
- 代理程序不受支持 - 当工作负载上的保护代理程序版本过时且不支持远程桌面功能时，会出现此问题。
- 配额不足 - 当租户中的服务配额不足以指派给选定工作负载时，会出现此问题。

如果远程管理计划应用于多达 150 个单独选定的工作负载，则系统会提示您先解决现有冲突，然后再保存计划。要解决冲突，请消除冲突的根本原因或从计划中删除受影响的工作负载。有关详细信息，请参阅 "解决远程管理计划的兼容性问题"(第 930 页)。如果在未解决冲突的情况下保存计划，则会为不兼容的工作负载自动禁用该计划，并显示警报。

如果远程管理计划应用于 150 多个工作负载或设备组，则会先保存该计划，然后检查兼容性。该计划会针对不兼容的工作负载自动禁用，并会显示警报。

解决远程管理计划的兼容性问题

根据兼容性问题的原因，可以在创建新远程管理计划的过程中执行不同的操作来解决兼容性问题。

注意
通过从计划中删除工作负载来解决兼容性问题时，无法删除属于设备组的工作负载。

解决兼容性问题

1. 单击**查看问题**。
2. [通过从新计划中删除工作负载来解决现有远程管理计划的兼容性问题]
   a. 在**冲突计划**选项卡上，选择要删除的工作负载。
   b. 单击**从计划中删除工作负载**。
   c. 单击**删除**，然后单击**关闭**。
3. [通过禁用已应用于工作负载的计划来解决远程管理计划的兼容性问题]
   a. 单击**禁用已应用的计划**。
   b. 单击**禁用**，然后单击**关闭**。
4. [解决操作系统不兼容的兼容性问题]
   a. 在**不兼容操作系统**选项卡上，选择要删除的工作负载。
   b. 单击**从计划中删除工作负载**。
   c. 单击**删除**，然后单击**关闭**。
5. [通过从计划中删除工作负载来解决代理程序不受支持的兼容性问题]
   a. 在**不支持的代理程序**选项卡上，选择要删除的工作负载。
   b. 单击**从计划中删除工作负载**。

c. 单击**删除**，然后单击**关闭**。

6. [通过更新代理程序版本来解决代理程序不受支持的兼容性问题] 单击**转到代理程序列表**。

注意
此选项仅适用于客户管理员。

7. [通过从计划中删除工作负载来解决配额不足的兼容性问题]
   a. 在**配额不足**选项卡上，选择要删除的工作负载。
   b. 单击**从计划中删除工作负载**。
   c. 单击**删除**，然后单击**关闭**。
8. [通过增加租户的配额来解决配额不足的兼容性问题]

注意
此选项仅适用于合作伙伴管理员。

   a. 在**配额不足**选项卡上，单击**转到管理门户**。
   b. 增加客户的服务配额。

工作负载凭据

可以添加远程工作负载的管理或非管理员凭据(用户名和密码，或 VNC 密码)、将它们保存在云凭据存储中，然后在连接到您管理的工作负载时使用它们来进行自动身份验证。通过这种方式，就可以将这些凭据保存在凭据存储中一次、将它们指派给多个工作负载，然后 Connect Client 会在您每次要远程连接到工作负载时使用这些凭据，而无需每次在连接的身份验证步骤中手动输入这些凭据。

注意
存储在凭据存储中的凭据不会在不同租户级别之间共享。它们仅在同一租户级别上为同一客户租户或合作伙伴租户共享。

这意味着，如果客户租户有多个管理员，则他们将在凭据存储中看到并共享凭据，而任何其他合作伙伴管理员或其他租户的客户管理员将无法查看或使用这些凭据。

添加凭据

可以添加凭据，然后将它们用于与多个工作负载的远程连接。

为工作负载添加凭据并将其保存在凭据存储中

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 单击要为其添加凭据的工作负载。
3. 通过以下方式之一访问**"设置"**菜单：
   - 单击**"远程桌面"**，然后单击**"设置"**。
   - 单击**"管理"**，然后单击**"设置"**。
4. 单击**添加凭据**。

5. 在**凭据存储**中，单击**添加凭据**。
6. 输入凭据。

现场	描述
凭据名称	将在凭据存储中可见的凭据的标识符。
用户名	将用于与目标工作负载远程连接的用户名。
密码	将用于与目标工作负载远程连接的密码。
VNC 密码	此字段仅适用于 Apple 屏幕共享。

7. 单击**保存**。

为工作负载指派凭据

在添加凭据后，当连接到要管理的工作负载时，可以使用这些凭据来自动进行身份验证。

将保存用于自动身份验证的凭据指派给工作负载

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 通过以下方式之一访问**"设置"**菜单：
   - 单击**"远程桌面"**，然后单击**"设置"**。
   - 单击**"管理"**，然后单击**"设置"**。
3. 在受支持协议（NEAR、RDP 或 Apple 屏幕共享）的选项卡上，单击**添加凭据**。
4. 在**凭据存储**中，从列表中选择凭据，然后单击**选择凭据**。

删除凭据

可以删除不再需要的凭据。

从凭据存储中删除凭据

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 通过以下方式之一访问**"设置"**菜单：
   - 单击**"远程桌面"**，然后单击**"设置"**。
   - 单击**"管理"**，然后单击**"设置"**。
3. 在受支持协议（NEAR、RDP 或 Apple 屏幕共享）的选项卡上，单击**删除**。
4. 在确认窗口中，单击**删除**。

取消指派工作负载中的凭据

可以取消指派工作负载中的凭据，但仍会将它们保留在凭据存储中。

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 通过以下方式之一访问**"设置"**菜单：
   - 单击**"远程桌面"**，然后单击**"设置"**。
   - 单击**"管理"**，然后单击**"设置"**。

3. 在受支持协议(NEAR、RDP 或 Apple 屏幕共享)的选项卡上,单击**取消指派**。
4. 在确认窗口中,单击**取消指派**。

使用托管工作负载

托管工作负载是装有 保护 代理程序的工作负载。

可以对远程托管工作负载执行以下操作:

- 在"控制"或"仅查看"模式下使用 NEAR 连接以实现远程协助或远程桌面
- 在控制模式下使用 RDP 连接以实现远程桌面
- 在"控制"、"仅查看"或"隔离"模式下使用 Apple 屏幕共享连接以实现远程协助或远程桌面
- 通过 Web 客户端连接以实现远程桌面
- 重新启动、关闭、睡眠、清空回收站、从远程工作负载中注销远程用户
- 在您的工作负载和远程工作负载之间传输文件
- 通过拍摄屏幕截图监视它们

注意
与托管工作负载的远程桌面连接需要在工作负载上安装 保护 代理程序并应用远程管理计划。

配置 RDP 设置

可以配置将自动应用于与托管工作负载的远程控制 RDP 连接的设置。

配置工作负载的 RDP 设置

1. 在 Cyber Protect 中控台中,转到**设备** > **装有代理程序的计算机**。
2. 通过以下方式之一访问**"设置"**菜单:
   - 单击**"远程桌面"**,然后单击**"设置"**。
   - 单击**"管理"**,然后单击**"设置"**。

3. 在 **RDP** 选项卡上，配置设置。

设置	描述
音频播放	此设置可启用或禁用本地工作负载上远程工作负载声音的重定向。
音频录制	此设置可确定是否要将音频录制(对着麦克风讲话)传输给远程工作负载。
重定向打印机	如果选择此设置，则您工作负载中的打印机将在远程工作负载上可用。
重定向文件	此设置可定义是否会将本地工作负载中的文件共享给远程工作负载。
色深	此设置可确定 RDP 将传输的图片中的颜色数。更高的值需要更高的带宽。 **增强色**：16 位 **真彩色**： • 24 位，适用于通过 Web 客户端进行的 RDP 连接 • 32 位，适用于通过 Connect Client 进行的 RDP 连接

4. 单击“关闭”按钮。

连接到托管工作负载以实现远程桌面或远程协助

注意
可以用于远程连接的连接协议的可用性取决于远程管理计划配置和远程工作负载的操作系统。

先决条件

- 已启用相应连接协议的远程管理计划已应用于托管工作负载。
- 所需的服务配额已指派给工作负载。(当将远程管理计划应用于工作负载时，会自动获得服务配额。)
- [对于 Apple 屏幕共享连接] Apple 屏幕共享在 macOS 工作负载上处于启用状态。
- 在 安克诺斯 Cyber Protect Cloud 中，已为您的用户帐户启用双重身份验证。

远程连接到托管工作负载以实现远程桌面或远程协助

1. 在 Cyber Protect 中控台中，转到**设备** > **装有代理程序的计算机**。
2. 单击要连接到的工作负载。
3. 单击**远程桌面**。
   默认情况下，选择 NEAR 作为连接协议。
4. [可选] 在**连接协议**下拉列表中，选择您要使用的连接协议。
5. 单击您要使用的查看模式。

协议	远程连接到	视图模式	支持的远程操作
NEAR	Windows	**控制** - 在此模式下，您将能够观察远程工作负载并在其上	远程

协议	远程连接到	视图模式	支持的远程操作
	Linux macOS	执行操作。 **仅查看** - 在此模式下，您将只能查看远程工作负载。	桌面远程协助
RDP	Windows	**控制** - 在此模式下，您将能够查看远程工作负载并在其上执行操作。 **注意** 如果 RDP 在工作负载的操作系统设置中处于禁用状态，则一个弹出窗口将显示。使用此窗口可为当前会话的工作负载启用 RDP，或者一般情况下： • 如果要仅为当前会话的此工作负载启用 RDP，则选择**会话结束后禁用它**，然后单击**允许**。 • 如果要为此工作负载启用 RDP，则单击**允许**。	远程桌面
Apple 屏幕共享	macOS	**控制** - 在此模式下，您将能够观察远程工作负载并在其上执行操作。 **仅查看** - 在此模式下，您将只能查看远程工作负载。 **隔离** - 仅适用于 macOS 工作负载。如果在隔离模式下连接到远程工作负载，则远程工作负载的显示会暗淡，并且远程用户将无法看到您在工作负载上的操作。	远程桌面 远程协助

6. 根据工作负载上是否已装有 Connect Client，执行以下操作之一：
   - 如果 Connect Client 未安装，则下载并安装它，然后在出现的确认弹出窗口中选择**允许**。
   - 如果 Connect Client 已安装，则在出现的确认弹出窗口中选择**打开 Connect Client**。
7. 在**身份验证**窗口中，选择一个身份验证选项，然后提供所需的凭据。

注意
如果已为工作负载指派了凭据，则将自动完成身份验证，并跳过此步骤。有关详细信息，请参阅 "为工作负载指派凭据"(第 932 页)。

身份验证选项	描述
使用远程工作负载凭据	在提供远程工作负载的管理员用户的用户名和密码后，将允许您建立远程连接。 此选项适用于 NEAR、RDP 和 Apple 屏幕共享。 可以使用此选项来验证身份，以实现远程桌面和远程协助。
请求观察权限	在远程工作负载上已登录的用户允许观察后，将允许您在观察模式下建立远程连接。 此选项适用于 NEAR 和 Apple 屏幕共享。

身份验证选项	描述
	可以使用此选项来验证身份，以实现远程协助。
请求控制权限	在远程工作负载上已登录的用户允许控制后，将允许您在控制模式下建立远程连接。 此选项适用于 NEAR 和 Apple 屏幕共享。 可以使用此选项来验证身份，以实现远程协助。

8. 单击**连接**，然后单击要显示的会话(如果工作负载上有多个用户会话可用)。

   Connect Client 将打开一个新的查看器窗口，在其中可以查看远程工作负载的桌面。查看器有一个工具栏，其中包含可以在远程连接建立后对远程工作负载执行的其他操作。有关详细信息，请参阅 "使用查看器窗口中的工具栏"(第 944 页)。

通过 Web 客户端连接到托管工作负载

可以通过 Web 客户端建立与托管工作负载的远程桌面连接。

先决条件

- 标准服务配额已指派给工作负载。
- 已启用 RDP 的远程管理计划将应用于托管工作负载。
- 已在托管工作负载上启用 RDP。
- 您的浏览器支持 HTML5。
- 在 安克诺斯 Cyber Protect Cloud 中，已为您的用户帐户启用双重身份验证。

通过 Web 客户端远程连接到工作负载

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 单击要远程连接的工作负载，然后依次单击**远程桌面** > **通过 Web 客户端连接**。
3. 输入用于访问工作负载的登录名和密码，然后单击**连接**。

注意
如果已为工作负载指派了凭据，则将自动完成身份验证，并跳过此步骤。有关详细信息，请参阅 "为工作负载指派凭据"(第 932 页)。

传输文件

可以轻松地在本地工作负载和托管工作负载之间传输文件。

先决条件

- 启用了 NEAR 协议和文件传输的远程管理计划已应用于工作负载。
- “Advanced Management” 配额已应用于工作负载。
- 在 安克诺斯 Cyber Protect Cloud 中，已为您的用户帐户启用双重身份验证。

在您的工作负载和托管工作负载之间远程传输文件

1. 在 Cyber Protect 中控台中，转到**设备** > **装有代理程序的计算机**。
2. 单击要与其传输文件的工作负载。
3. 单击**"管理"**，然后单击**"传输文件"**。
4. 根据工作负载上是否已装有 Connect Client，执行以下操作之一：
   - 如果 Connect Client 未安装，则下载并安装它，然后在出现的确认弹出窗口中单击**允许**。
   - 如果 Connect Client 已安装，则在出现的确认弹出窗口中选择**打开 Connect Client**。
5. 在**身份验证**窗口中，选择一个身份验证选项，然后提供所需的凭据。

身份验证选项	描述
使用远程工作负载凭据	在提供远程工作负载的管理员用户的用户名和密码后，将允许您建立远程连接。
请求传输文件权限	在远程工作负载上已登录的用户允许传输文件后，将允许您传输文件。

6. 在**文件传输**窗口中，浏览文件并将其拖放到所需的目的位置。

注意
本地工作负载的文件列在左侧窗格中，远程工作负载的文件列在右侧窗格中。
当文件传输开始时，它会列在**任务**窗格中。

7. [可选] 如果要从**任务**窗格中删除已完成的任务，请单击**清除已完成的任务**。
8. 所有传输完成后，关闭窗口。

在工作负载之间共享剪贴板内容

您可以通过 NEAR 将工作负载的剪贴板内容发送到远程工作负载，或从远程工作负载获取剪贴板内容。例如，您可能希望从远程工作负载上的文件中复制一些文本，并将其粘贴到本地工作负载上的文档中，或者反向操作。

发送剪贴板

先决条件

已为您的用户帐户启用双重身份验证。

将来自工作负载的剪贴板内容发送至远程工作负载

1. 通过 NEAR 启动对受控工作负载的远程控制会话。
   有关详细信息，请参阅 "连接到托管工作负载以实现远程桌面或远程协助"(第 934 页)。
2. [可选] 若要自动同步剪贴板和远程工作负载的剪贴板内容，请在**查看器**工具栏中，单击 **其他** 图标，然后选择 **剪贴板自动同步**。
3. 若要将剪贴簿上的内容与远程工作负载的剪贴簿共享，请执行以下操作。
   - 如果已禁用 **剪贴板自动同步**，请执行相应步骤：
     a. 在本地工作负载上，复制要发送的文本或图像。
     b. 在远程工作负载的 **查看器** 工具栏中，单击 **其他** 图标。

c. 单击**发送剪贴板**。

d. 打开要粘贴内容的文件，然后将其粘贴。

- 如果启用了**剪贴板自动同步**，则根据要共享的内容执行相应的步骤。

选项	操作
如果您想要共享本地剪贴板中的一个或多个文件	a. 在本地工作负载上，复制要发送的文件。 b. 打开远程工作负载的**查看器**窗口。 c. 在弹出的警报中，单击**发送到远程计算机**。 d. 将内容粘贴到远程工作负载。
如果您想要从本地剪贴板中的文件共享文本	a. 在本地工作负载上，复制您要发送的文本。 b. 打开远程工作负载的**查看器**窗口。 c. 打开要将内容粘贴到其中的文件。 d. 将内容粘贴到文件。

获取剪贴板

先决条件

已为您的用户帐户启用双重身份验证。

若要从远程工作负载获取剪贴板内容到您的工作负载

1. 通过 NEAR 启动对受控工作负载的远程控制会话。
   有关详细信息，请参阅 "连接到托管工作负载以实现远程桌面或远程协助"(第 934 页) 。
2. 若要自动同步剪贴板和远程工作负载的剪贴板内容，请在**查看器**工具栏中，单击 **其他** 图标，然后选择 **剪贴板自动同步**。
3. 若要将远程工作负载的剪贴板内容复制到本地剪贴板，请执行以下操作。
   - 如果已禁用**剪贴板自动同步**，请执行相应步骤。
     a. 在远程工作负载上，复制要共享的文本或图像。
     b. 在远程工作负载的 **查看器** 工具栏中，单击 **其他** 图标。
     c. 单击**获取剪贴板**。
     d. 在本地工作负载上，打开要粘贴内容的文件。
     e. 将内容粘贴到文件。
   - 如果启用了**剪贴板自动同步**，则根据要获取的内容执行相应的步骤。

选项	操作
若要将远程工作负载的一个或多个文件从剪贴板复制到本地剪贴板	a. 在远程工作负载上，复制要获取的文件。 b. 在弹出的警报中单击 **接收剪贴板**。 c. 将内容粘贴到本地工作负载。

选项	操作
若要将远程工作负载的剪贴板上的文本复制到本地剪贴板	a. 在远程工作负载上，复制您要获取的文本。 b. 在本地工作负载上，将内容粘贴到文件中。

对托管工作负载执行控制操作

可以通过对远程工作负载执行以下基本控制操作来管理它：清空回收站、睡眠、重新启动、关闭和注销远程用户。

先决条件

- 标准服务配额已应用于工作负载。
- 在 安克诺斯 Cyber Protect Cloud 中，已为您的用户帐户启用双重身份验证。

清空回收站

清空远程工作负载上的回收站

1. 在 Cyber Protect 中控台中，转到**设备** > **装有代理程序的计算机**。
2. 单击要对其执行此操作的工作负载。
3. 单击**管理**，然后单击**清空回收站**。
4. 选择要对其执行此操作的用户会话，然后单击**清空回收站**。

睡眠

使远程工作负载进入睡眠状态

1. 在 Cyber Protect 中控台中，转到**设备** > **装有代理程序的计算机**。
2. 单击要对其执行此操作的工作负载。
3. 单击**管理**，然后单击**睡眠**。

重新启动

重新启动远程工作负载

1. 在 Cyber Protect 中控台中，转到**设备** > **装有代理程序的计算机**。
2. 单击要对其执行此操作的工作负载。
3. 单击**管理**，然后单击**重新启动**。
   - 对于 Windows 工作负载，选择是否允许用户(当前已本地登录到工作负载)在重新启动工作负载之前保存更改、选择用户，然后再次单击**重新启动**。
   - 对于 macOS 工作负载，选择是否允许用户(当前已本地登录到工作负载)在重新启动工作负载之前保存更改，然后再次单击**重新启动**。
   - 对于 Linux 工作负载，单击**重新启动**。

关机

关闭远程工作负载

1. 在 Cyber Protect 中控台中，转到**设备** > **装有代理程序的计算机**。
2. 单击要对其执行此操作的工作负载。
3. 单击**管理**，然后单击**关机**。
   - 对于 Windows 工作负载，选择是否允许用户（当前已本地登录到工作负载）在关闭工作负载之前保存更改、选择用户，然后再次单击**关闭**。
   - 对于 macOS 工作负载，选择是否允许用户（当前已本地登录到工作负载）在关闭工作负载之前保存更改，然后再次单击**关闭**。
   - 对于 Linux 工作负载，再次单击**关机**。

注销远程用户

注销远程工作负载的用户

1. 在 Cyber Protect 中控台中，转到**设备** > **装有代理程序的计算机**。
2. 单击要对其执行此操作的工作负载。
3. 单击**管理**，然后单击**注销远程用户**。
4. 选择要注销的用户，然后单击**注销**。

通过屏幕截图传输监视工作负载

可以使用屏幕截图传输功能来监视工作负载的状态。

先决条件

- 启用了屏幕截图传输功能的远程管理计划已应用于工作负载。
- 保护代理程序版本是最新的，支持屏幕截图传输功能。
- “Advanced Management” 服务配额已应用于工作负载。
- 该工作负载处于联机状态。
- 在 安克诺斯 Cyber Protect Cloud 中，已为您的用户帐户启用双重身份验证。

通过屏幕截图传输监视工作负载

通过屏幕截图传输监视工作负载

1. 在 Cyber Protect 中控台中，转到**设备** > **屏幕截图传输**。
2. 单击要监视的工作负载。
3. 选择用户会话。
4. 选择显示。
5. 选择要对桌面拍摄新屏幕截图的刷新率。
6. 选择图像质量。
7. 要下载屏幕截图，请单击下载图标。

对工作负载拍摄屏幕截图

对托管工作负载拍摄屏幕截图

1. 在 Cyber Protect 中控台中，转到**设备** > **装有代理程序的计算机**。
2. 单击要拍摄屏幕截图的工作负载。
3. 单击**管理**，然后单击**拍摄桌面屏幕截图**。

   屏幕截图传输屏幕即会打开，其中包含预选的工作负载。根据应用于工作负载的远程管理计划的设置，您会看到屏幕截图，或者您会在远程工作负载的用户批准请求后看到屏幕截图。

同时观察多个托管工作负载

可以在一个窗口中同时观察多个远程工作负载的桌面。

注意
在窗口中可以同时看到的桌面数量取决于显示器的尺寸。

先决条件

- NEAR/Apple 屏幕共享在应用于工作负载的远程管理计划中处于启用状态。
- “Advanced Management” 服务配额已应用于工作负载。
- 在 安克诺斯 Cyber Protect Cloud 中，已为您的用户帐户启用双重身份验证。

同时观察多个工作负载

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 选择要观察的工作负载。
3. 单击**多视图**。
4. 根据工作负载上是否已装有 Connect Client，执行以下操作之一：
   - 如果 Connect Client 未安装，则下载并安装它，然后在出现的确认弹出窗口中选择**允许**。
   - 如果 Connect Client 已安装，则在出现的确认弹出窗口中选择**打开 Connect Client**。
5. 在**身份验证**窗口中，选择一个身份验证选项，然后提供所需的凭据。

身份验证选项	描述
使用远程工作负载凭据	在远程工作负载上提供管理员用户的用户名和密码后，将允许您建立远程连接。
请求观察权限	在远程工作负载上已登录的用户允许观察后，将允许您在观察模式下建立远程连接。

6. 如果要在连接到步骤 2 中选定的所有远程工作负载时使用相同的身份验证方法和凭据，请选择**在其他计算机上使用**。
7. 单击**连接**。

   在多视图窗口的工具栏中，可以选择要连接到工作负载的视图模式。此操作会为该工作负载打开一个单独的查看器窗口。

注意

如果任何选定的工作负载处于脱机状态，或装有过时版本的代理程序，则它不会显示在多视图窗口中。

所有与远程工作负载的多视图连接都处于**仅查看**模式。

使用非托管工作负载

非托管工作负载是未装有 保护 代理程序的工作负载。

可以对非托管远程工作负载执行以下操作：

- 使用 安克诺斯 Quick Assist 连接以实现远程协助
- 使用 IP 地址连接以实现远程桌面或远程协助
- 使用 Quick Assist 在您的工作负载和远程工作负载之间传输文件

注意

使用 Quick Assist 远程连接到非托管工作负载时，请确保：

- 已为客户租户激活 Advanced Management 包。
- Quick Assist 应用程序正在要连接的远程工作负载上运行。

通过 安克诺斯 Quick Assist 连接到非托管工作负载

可以使用“Quick Assist”功能以按需远程连接到非托管工作负载，并提供一次性协助。

先决条件

- Advanced Management 包已指派给客户租户。
- 在 安克诺斯 Cyber Protect Cloud 中，已为您的用户帐户启用双重身份验证。
- 远程用户已提供来自 Quick Assist 的工作负载 ID 和访问代码。
- 远程用户已下载并运行 安克诺斯 Quick Assist。

使用 Quick Assist 连接到工作负载以实现远程协助

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 单击 **Quick Assist**。
3. 在 **Quick Assist** 窗口中，输入最终用户已为您提供的工作负载 ID，然后选择**连接**。
4. 单击**连接**。
5. 根据工作负载上是否已装有 Connect Client，执行以下操作之一：
   - 如果 Connect Client 未安装，则下载并安装它，然后在出现的确认弹出窗口中选择**允许**。
   - 如果 Connect Client 已安装，则在出现的确认弹出窗口中选择**打开 Connect Client**。
6. 在**身份验证**窗口中，输入访问代码。
7. Connect Client 将打开一个新的查看器窗口，在其中可以查看远程工作负载的桌面。查看器有一个工具栏，其中包含可以在远程连接建立后对远程工作负载执行的其他操作。有关详细信息，请参阅 "使用查看器窗口中的工具栏"(第 944 页) 。

通过 IP 地址连接到非托管工作负载

如果 LAN 中有一个非托管工作负载，则可以使用其 IP 地址连接到该工作负载以实现远程控制或远程协助。此连接不需要 Internet 访问。

先决条件

- Advanced Management 包已指派给客户租户。
- 在 安克诺斯 Cyber Protect Cloud 中，已为您的用户帐户启用双重身份验证。

使用 IP 地址连接到工作负载以实现远程桌面或远程协助

1. 在 Cyber Protect 中控台中，转到**所有设备**。
2. 单击 **Quick Assist**。
3. 单击**通过 IP 地址**选项卡。
4. 输入工作负载的 IP 地址和端口。
5. 根据远程工作负载的操作系统，选择连接协议：RDP(Windows 工作负载) 或 Apple 屏幕共享(适用于 macOS 工作负载) 。

   注意
   通过 RDP 连接支持远程桌面操作，通过 Apple 屏幕共享连接同时支持远程桌面和远程协助操作。

6. 单击**连接**。
7. 在**身份验证**窗口中，提供所需的凭据。

对于 Apple 屏幕共享连接，Connect Client 将打开一个新的查看器窗口，在其中可以查看远程工作负载的桌面。查看器有一个工具栏，其中包含可以在远程连接建立后对远程工作负载执行的其他操作。有关详细信息，请参阅 "使用查看器窗口中的工具栏"(第 944 页)。

通过 安克诺斯 Quick Assist 传输文件

可以使用“Quick Assist”功能，以在您的工作负载和非托管工作负载之间传输文件。

先决条件

- Advanced Management 包已指派给客户租户。
- 在 安克诺斯 Cyber Protect Cloud 中，已为您的用户帐户启用双重身份验证。
- 远程用户已下载并运行 安克诺斯 Quick Assist。
- 远程用户已提供了从 Quick Assist 获取的计算机 ID 和访问代码。

使用 Quick Assist 将文件传输到工作负载

1. 在 Cyber Protect 中控台中，转到**设备** > **所有设备**。
2. 单击 **Quick Assist**。
3. 在 **Quick Assist** 窗口中，输入最终用户为您提供的工作负载 ID，然后选择**文件传输**。

4. 单击**连接**。
5. 根据工作负载上是否已装有 Connect Client，执行以下操作之一：
   - 如果 Connect Client 未安装，则下载并安装它，然后在出现的确认弹出窗口中选择**允许**。
   - 如果 Connect Client 已安装，则在出现的确认弹出窗口中选择**打开 Connect Client**。
6. 在**身份验证**窗口中，输入访问代码。
7. 在**文件传输**窗口中，浏览文件并将其拖放到所需的目的位置。

注意
本地工作负载的文件列在左侧窗格中，远程工作负载的文件列在右侧窗格中。
当文件传输开始时，它会列在**任务**窗格中。

8. [可选] 如果要从**任务**窗格中删除已完成的任务，请单击**清除已完成的任务**。
9. 所有传输完成后，关闭窗口。

使用查看器窗口中的工具栏

连接到远程工作负载后，可以使用查看器窗口的工具栏来快速执行不同的操作。

图标	描述
	**实际大小** 缩放远程工作负载的桌面，以使远程桌面的一个像素对应于查看器窗口上的一个像素。
	**缩放以适合** 缩放远程工作负载桌面以适合查看器窗口。
	**锁定**和**解锁屏幕** 在远程工作负载的显示器上显示占位符，以便远程用户不会看到您的操作。
	**拍摄屏幕截图** 将远程服务器的桌面图像保存到本地文件。
	**选择显示** 选择要查看的远程工作负载显示和所需分辨率。 适用于与 macOS 的 Apple 屏幕共享连接，以及与任何操作系统的 NEAR 连接。 如果远程计算机有多个显示器，则可为多个显示器选择以下显示模式： • **组合的** - 所有远程显示器都在单个窗口中显示。 • **分开的** - 每个远程显示器在单独的窗口中显示。 如果有多个显示器连接到本地工作负载，则此模式非常方便。在

图标	描述
	这种情况下，例如，您可以安排在每个本地显示器上查看一个远程显示器。 如果关闭任何远程工作负载显示，远程连接将会结束。若要查看远程工作负载显示，必须再次重新连接。 仅适用于 NEAR 连接
	**图像质量** 通过 Apple 屏幕共享连接，将远程屏幕图像质量从黑白调整为可能的最高质量。
	**NEAR 图像质量** 调整 NEAR 连接的质量/性能比。滑块的左侧(平滑)使性能优先于图像质量，右侧(锐利)表示远程桌面屏幕的最佳质量，但性能可能较差。
	**发送 Ctrl+Alt+Del** 向远程工作负载发送“Ctrl + Alt + Delete”序列。 适用于 Windows 和 Linux 工作负载。
	**文件传输** 打开“文件管理器”窗口，以在远程和本地工作负载之间交换文件。适用于 NEAR 连接。
	**固定工具栏** 关闭查看器工具栏的自动隐藏。 适用于 Windows 工作负载。
	**全屏** 切换到全屏模式并缩放远程工作负载，以完全填满本地屏幕。 适用于 Windows 工作负载。
	**关闭** 关闭查看器窗口并结束远程控制会话。 适用于 Windows 工作负载。

根据连接类型，单击**其他**图标时可能会有其他选项可用。

选项	描述
开始记录/停止记录	记录当前远程桌面会话。 会话录制在本地工作负载上保存为 .crec 文件。您可以使用 安克诺斯 Connect Client 打开 .crec 文件。

选项	描述
	适用于 NEAR 连接
剪贴板自动同步	启用此选项后，客户端会自动同步本地剪贴板和远程工作负载的剪贴板。 适用于 NEAR 连接
发送剪贴板	**发送剪贴板**会用本地剪贴板的内容替换远程工作负载的剪贴板内容。 如果启用了**剪贴板自动同步**，则将禁用此选项。 有关详细信息，请参阅 "在工作负载之间共享剪贴板内容"(第 937 页)。 适用于 NEAR 连接
获取剪贴板	**获取剪贴板**将远程工作负载的剪贴板内容传输到本地工作负载的剪贴板。 如果启用了**剪贴板自动同步**，则将禁用此选项。 有关详细信息，请参阅 "在工作负载之间共享剪贴板内容"(第 937 页)。 适用于 NEAR 连接
智能键盘/原始键/所有快捷键的原始键	更改当前连接的键盘输入模式。 **智能键盘** - 客户端将本地键入符号的 Unicode 代码传输给远程计算机 **原始键** - 客户端使用您按下的键盘按钮的原始代码。 **所有快捷键的原始键** - 客户端禁用本地系统快捷键，以便它们也会传输给远程操作系统。
鼠标悬停时的键盘焦点	启用后，当本地鼠标光标放置在查看器窗口上时，客户端仅捕获键盘输入。 禁用后，客户端会在其窗口处于活动状态时捕获键盘。
显示连接信息/隐藏连接信息	选择**显示连接信息**后，远程桌面屏幕上会出现一个小信息面板，以显示有关当前连接的最基本信息。
远程声音	使客户端能够将声音从远程计算机重定向到本地计算机。 适用于 NEAR 连接
首选项	配置 Connect Client 的设置。有关详细信息，请参阅 "配置 Connect Client 设置"(第 947 页)。

录制和播放远程会话

可以通过 安克诺斯 Connect Client 中的 NEAR 记录远程会话。

若要记录远程会话

1. 在 Connect Client 的查看器工具栏中，单击**"其他"**，然后选择**"开始录制"**。
2. 选择录制的名称和位置。

   默认情况下，该文件将以当前日期和时间命名，并位于当前用户主目录的 **Documents** 文件夹中。当录制处于活动状态时，在**查看器**工具栏中，您将在远程屏幕和录制计时器的右上角看到一个闪烁的红色圆圈。
3. 要停止录制，请单击**"其他"**，然后单击**"停止录制"**。在 Mac 上，您还可以单击工具栏上的**"停止"**。

   由 安克诺斯 Connect Client 创建的所有 .crec 文件在默认情况下将使用 安克诺斯 Connect Client 打开。

若要播放录音

1. 找到录音文件。
2. 打开它。

   已打开 安克诺斯 Connect Client 的录音播放器。请注意，无法浏览录音。若要查找录音中的某个时刻，请等待播放器到达该时刻。
3. [可选] 要调整播放速度，请使用播放控制部分中的**<<**和**>>**图标。

   记录存储为在连接期间往返于远程服务器的一系列事件。这可确保以最小的文件大小获得最佳的录制质量。然而，这也意味着无法浏览录音。目前还无法将录制内容转换为视频格式。

配置 Connect Client 设置

在工作负载上完成安装 Connect Client 后，可以根据您的偏好配置其设置。

配置 Connect Client 的设置

1. 在"开始"菜单中，找到 **Connect Client**，然后启动它。
2. 在**常规**选项卡上，配置设置。

选项	描述
写入详细日志	选择此选项，可允许 Connect Client 写入详细日志。如果禁用此选项，则该客户端仅会将常规信息写入日志文件。
代理设置	选择是使用默认系统代理，还是配置自定义 SOCKSS 代理。

3. 在**查看器**选项卡上，配置设置。

选项	描述
关闭查看器时请求确认	如果希望 Connect Client 在您尝试关闭查看器窗口时显示确认消息，以防止意外关闭，则选择此选项。
最小化时	选择最小化时是否暂停查看器活动，以减少 CPU 负载。

选项	描述
最大化时	选择最大化时是否启用全屏模式。
剪贴板传输	启用在复制或粘贴文本和图像时，在查看器窗口中显示剪贴板传输指示器。
键盘模式	启用在鼠标和键盘事件发送给远程计算机时，在查看器窗口标题中显示输入模式指示器。
剪贴板	选择**自动同步剪贴板**，以启用自动剪贴板同步(如果可用)。
发送键盘事件	选择是在 Connect Client 窗口处于活动状态时获取本地键盘输入，还是仅在本地鼠标指针位于其上时获取本地键盘输入。
查看器背景色	更改查看器窗口背景色。
自动重新连接	如果希望 在连接中断时自动重新建立连接，请选择**启用自动重新连接**。
H.264	可以禁用硬件解码器。
空闲时关闭	选择其后关闭查看器窗口的空闲状态时间间隔。

4. 在**键盘**选项卡上，配置设置。

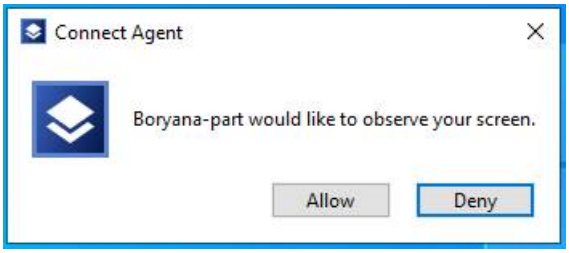
选项	描述
修改器映射	使用弹出菜单更改修改器键的行为。分别为 NEAR、Apple 屏幕共享和 RDP 连接存储这些设置。
输入模式	对于每种类型的连接(在窗格的标题中选择)，选择默认的键盘输入模式。

5. 单击**确定**。

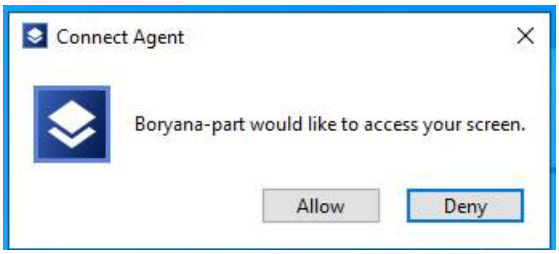
远程桌面通知程序

在以下情况下，Connect Agent 会在远程工作负载的桌面上显示操作对话框(通知程序)：

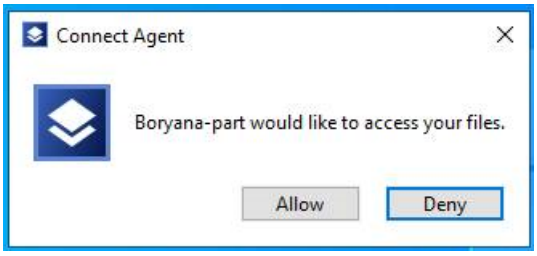
- 当您试图通过请求观察权限来远程连接到工作负载时。本地登录到远程工作负载的用户可以允许或拒绝请求。



- 当您试图通过请求控制权限来远程连接到工作负载时。本地登录到远程工作负载的用户可以允许或拒绝请求。



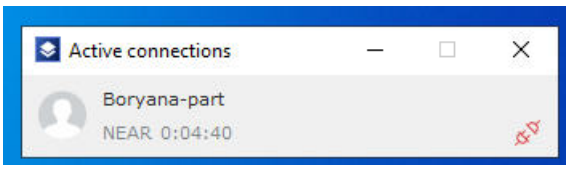
- 当您试图通过请求传输文件的权限来在您的工作负载和远程工作负载之间交换文件时。本地登录到远程工作负载的用户可以允许或拒绝请求。



当您与工作负载建立远程桌面连接时，登录到该工作负载的用户将查看包含以下信息的不同连接通知程序：

- 远程连接的用户的名称
- 用于建立远程连接的连接协议
- 远程连接的持续时间

本地登录到远程工作负载的用户可以随时通过单击**断开连接**图标或**关闭**图标来结束连接。



监视工作负载的运行状况和性能

可以监视组织中工作负载的系统参数和运行状况。如果某个参数超出正常范围，您会立即收到通知，并能够快速解决该问题。还可以配置自定义警报和自动响应操作。这些操作将自动执行，以解决工作负载行为中的异常。

注意
监视功能需要在工作负载上安装 保护 代理程序 15.0.35324 版或更高版本。

监视计划

要开始监视托管工作负载的性能、硬件、软件、系统和安全参数，请对这些工作负载应用监视计划。监视计划由不同的监视器组成，可以启用和配置这些监视器。有些监视器支持基于异常的监视类型。有关监视计划的详细信息，请参阅 "监视计划"(第 976 页)。有关可以在监视计划中配置的可用监视器的详细信息，请参阅 "可配置的监视器"(第 951 页)。

如果代理程序由于某种原因而无法从工作负载收集数据，则系统会生成警报。

监视类型

必须为计划中启用的每个监视器配置监视类型。监视类型确定监视器将用于估测工作负载的正常行为和偏差的算法。有两种监视类型：基于阈值和基于异常。某些监视器仅支持基于阈值的监视类型。

基于阈值的监视跟踪参数值是高于还是低于配置的阈值。通过使用这种监视类型，您负责为工作负载定义正确的阈值。系统根据这些静态阈值确定正常行为，而不考虑可能导致出现该行为的其他特定条件。因此，相较于基于异常的监视，基于阈值的监视可能不太准确。

基于异常的监视使用机器学习来创建工作负载的正常行为模式，以及检测异常行为。有关详细信息，请参阅 "基于异常的监视"(第 950 页)。

基于异常的监视

基于异常的监视使用机器学习模型来创建工作负载的正常行为模式，以及检测工作负载行为中的异常(时间序列数据中的意外峰值)。在激活此监视类型后，系统会创建一个模型，然后开始训练自身，并根据从工作负载中收集到的数据来调整特定工作负载的模型。这意味着在训练期开始时，数据可能并不完全准确。创建一个可靠模型需要至少对模型训练三周。随着系统收集更多数据并分析历史数据集，它会逐渐优化模型，并为工作负载的每个指标创建动态的上限阈值和下限阈值。由于系统会监视参数的值及其上下文，因此该监视类型相较于基于阈值的监视更灵活。例如，特定工作负载在一天中的特定时间内有更大的负载可能是正常的。基于阈值的监视类型会错误地将该情况解释为异常行为，并触发警报。

可以重置工作负载的机器学习模型。在这种情况下，系统将删除已应用于工作负载的监视器的所有数据和模型。有关详细信息，请参阅 "重置机器学习模型"(第 984 页)。

支持监视的平台

以下操作系统支持监视功能。

支持的 Windows 版本	支持的 macOS 版本
• Windows 7 SP1 • Windows 8, 8.1 • Windows 10 • Windows 11 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• macOS 10.14 (Mojave) • macOS 10.15 (Catalina) • macOS 11.x (Big Sur) • macOS 12.x (Monterey) • macOS 13.x (Ventura)

可配置的监视器

监视功能支持以下监视器，分为六类：硬件、性能、软件、系统、安全和自定义。

监视器	描述	支持的操作系统	数据收集频率	支持基于异常的监视	标准保护或 Advanced Management 中的可用性
硬件					
磁盘空间	监视工作负载的特定驱动器上的可用空间。	Windows macOS	1 分钟	是	标准保护
CPU 温度	监视 CPU 温度。	Windows macOS	30 秒	是	Advanced Management
GPU 温度	监视 GPU 温度。	Windows macOS	30 秒	是	Advanced Management
硬件更改	监视硬件更改，如在工作负载上添加、删除或替换硬件。	Windows macOS	24 小时	否	标准保护
性能					
CPU 使用情况	监视总体 CPU 使用情况(按工作负载上的所有 CPU)。	Windows macOS	30 秒	是	Advanced Management

监视器	描述	支持的操作系统	数据收集频率	支持基于异常的监视	标准保护或 Advanced Management 中的可用性
内存使用情况	监视总体内存使用情况(按工作负载上的所有内存插槽)。	Windows macOS	30 秒	是	Advanced Management
磁盘传输速率	监视工作负载上每个物理磁盘的读写速度。	Windows macOS	30 秒	是	Advanced Management
网络使用情况	监视工作负载的每个网络适配器的传入和传出流量。	Windows macOS	30 秒	是	Advanced Management
CPU 使用率(按进程)	监视特定进程的 CPU 使用情况。	Windows macOS	30 秒	否	Advanced Management
内存使用率(按进程)	监视选定进程的内存使用情况。	Windows macOS	30 秒	否	Advanced Management
磁盘传输速率(按进程)	监视选定进程的读写速度。	Windows macOS	30 秒	否	Advanced Management
网络使用率(按进程)	监视选定进程的传入和传出流量。	Windows macOS	30 秒	否	Advanced Management
软件					
Windows 服务状态	监视选定 Windows 服务的状态(正在运行或已停止)。	Windows	30 秒	否	Advanced Management
进程状态	监视选定进程的状态(正在运行或已停止)。	Windows macOS	30 秒	否	Advanced Management
安装的软件	监视软件应用程序的安装、更新或删除。	Windows macOS	24 小时	否	Advanced Management
系统					
上次系统重新启动	监视工作负载何时重新启动。	Windows macOS	1 小时	否	标准保护
Windows 事件日志	监视 Windows 事件日志中的特定业务关键型事件。	Windows	10 分钟	否	Advanced Management
文件和文件夹大小	监视选定文件或文件夹的总大小。	Windows macOS	10 分钟	否	标准保护

监视器	描述	支持的操作系统	数据收集频率	支持基于异常的监视	标准保护或 Advanced Management 中的可用性
安全					
Windows Update 状态	监视工作负载的 Windows Update 状态以及最新更新是否已安装。	Windows	15 分钟	否	Advanced Management
防火墙状态	监视工作负载上安装的内置防火墙或第三方防火墙的状态。	Windows macOS	5 分钟	否	Advanced Management
防恶意软件软件状态	监视工作负载上安装的内置防恶意软件或第三方防恶意软件的状态。	Windows macOS	5 分钟	否	Advanced Management
失败的登录	监视工作负载上失败的登录尝试。	Windows	1 小时	否	Advanced Management
自动运行状态	监视可移动存储媒体的“自动运行”功能是否已启用。	Windows	1 小时	否	Advanced Management
自定义					
自定义	通过运行脚本监视自定义对象。	Windows macOS	自定义	否	Advanced Management

磁盘空间监视器的设置

磁盘空间监视工作负载的特定驱动器上的可用空间。

注意
在计算空间时，监视器对 Windows 和 macOS 工作负载都使用二进制字节(每 KB 为 1024 字节、每 MB 为 1024 KB 和每 GB 为 1024 MB)。

可以为监视器配置以下设置。

设置	描述
基于阈值的监视	
驱动器	要监视的驱动器。 以下值可用。 • **系统驱动器** -这是默认值。 • **任何驱动器**

设置	描述
运算符	运算符是一个条件函数，用于定义如何根据指标衡量性能。 以下值可用。 • **小于** -这是默认值。 • **小于或等于**
磁盘可用空间阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时，系统会生成警报。 输入一个介于 1 到 100 (%) 之间的整数值。默认值为 20。
包括可移动驱动器	如果**驱动器**值为**任何驱动器**，则此设置可用。 如果要添加可移动驱动器（如 USB 闪存驱动器）进行监视，请选择此设置。默认情况下，该设置处于禁用状态。
时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 60（分钟）之间的整数值。默认值为 30。
基于异常的监视	
驱动器	要监视的驱动器。 以下值可用。 • **系统驱动器** -这是默认值。 • **任何驱动器**
模型训练期	在此期间，系统将根据从代理程序收集到的数据训练机器学习模型，然后创建工作负载的正常行为模式。模型训练期越长，系统将创建的长期行为模式就越准确。我们建议最短模型训练期为 21 天。 输入一个整数值（天）。默认值为 21。
在训练期间接收异常警报	如果选择此设置，则您会在模型训练期间收到有关异常的警报。由于模型仍在进行训练，可能不够准确，因此这些警报可能是误报。 默认情况下，该设置处于选中状态。
灵敏度级别	如果异常值在特定范围内，则灵敏度级别可用作异常的初步过滤器。该过滤器独立于异常检测算法运行。其目的是阻止异常检测算法处理在指定范围内的异常。 在训练期间： 1. 使用在训练期间收集到的数据来训练该算法。 2. 该算法对训练数据进行异常检测。 3. 应用基于平均值和标准偏差的过滤过程。 4. 过滤在指定间隔内的任何异常。 5. 在其余异常数据点中，异常级别最低的异常处于选中状态。该级别（介于 0 和 1 之间的浮点数）记录在模型中。

设置	描述
	在预测期间： 1. 该算法根据推断数据预测异常。 2. 根据灵敏度级别，基于平均值和标准偏差过滤预测的异常。 3. 根据以下原则对其余异常进一步过滤：高于阈值水平的值被视为异常，而低于阈值水平的值被视为正常行为。 以下值可用。 • **低** - 低水平等于平均值和标准偏差值。 • **正常** - 这是默认值。正常水平等于平均值和标准偏差值的两倍。 • **高** - 高水平等于平均值和标准偏差值的三倍。
异常持续时间	仅当异常行为持续一段指定时间时，系统才会为检测到的异常生成警报。 默认值为 30 分钟。

CPU 温度监视器的设置

CPU 温度监视工作负载的 CPU 温度。

可以为监视器配置以下设置。

设置	描述
基于阈值的监视	
CPU 温度已超过(°C)	受监视指标的最大值。如果超过该值，系统会生成警报。 输入一个整数值 (C°)。默认值为 80。
时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟) 之间的整数值。默认值为 5。
基于异常的监视	
模型训练期	在此期间，系统将根据从代理程序收集到的数据训练机器学习模型，然后创建工作负载的正常行为模式。模型训练期越长，系统将创建的长期行为模式就越准确。我们建议最短模型训练期为 21 天。 输入一个整数值(天) 。默认值为 21。
灵敏度级别	如果异常值在特定范围内，则灵敏度级别可用作异常的初步过滤器。该过滤器独立于异常检测算法运行。其目的是阻止异常检测算法处理在指定范围内的异常。 在训练期间： 1. 使用在训练期间收集到的数据来训练该算法。

设置	描述
	2. 该算法对训练数据进行异常检测。 3. 应用基于平均值和标准偏差的过滤过程。 4. 过滤在指定间隔内的任何异常。 5. 在其余异常数据点中，异常级别最低的异常处于选中状态。该级别(介于 0 和 1 之间的浮点数)记录在模型中。 在预测期间： 1. 该算法根据推断数据预测异常。 2. 根据灵敏度级别，基于平均值和标准偏差过滤预测的异常。 3. 根据以下原则对其余异常进一步过滤：高于阈值水平的值被视为异常，而低于阈值水平的值被视为正常行为。 以下值可用。 • **低** - 低水平等于平均值和标准偏差值。 • **正常** - 这是默认值。正常水平等于平均值和标准偏差值的两倍。 • **高** - 高水平等于平均值和标准偏差值的三倍。
异常持续时间	仅当异常行为持续一段指定时间时，系统才会为检测到的异常生成警报。 输入一个介于 1 到 60(分钟)之间的整数值。默认值为 15。

GPU 温度监视器的设置

GPU 温度监视工作负载的 GPU 温度。

可以为监视器配置以下设置。

设置	描述
基于阈值的监视	
GPU 温度已超过	受监视指标的最大值。如果超过该值，系统会检测到异常。 输入一个整数值 (C°)。默认值为 80。
时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟)之间的整数值。默认值为 5。
基于异常的监视	
模型训练期	在此期间，系统将根据从代理程序收集到的数据训练机器学习模型，然后创建工作负载的正常行为模式。模型训练期越长，系统将创建的长期行为模式就越准确。我们建议最短模型训练期为 21 天。 输入一个整数值(天)。默认值为 21。

设置	描述
灵敏度级别	如果异常值在特定范围内，则灵敏度级别可用作异常的初步过滤器。该过滤器独立于异常检测算法运行。其目的是阻止异常检测算法处理在指定范围内的异常。 在训练期间： 1. 使用在训练期间收集到的数据来训练该算法。 2. 该算法对训练数据进行异常检测。 3. 应用基于平均值和标准偏差的过滤过程。 4. 过滤在指定间隔内的任何异常。 5. 在其余异常数据点中，异常级别最低的异常处于选中状态。该级别(介于 0 和 1 之间的浮点数)记录在模型中。 在预测期间： 1. 该算法根据推断数据预测异常。 2. 根据灵敏度级别，基于平均值和标准偏差过滤预测的异常。 3. 根据以下原则对其余异常进一步过滤：高于阈值水平的值被视为异常，而低于阈值水平的值被视为正常行为。 以下值可用。 • **低** - 低水平等于平均值和标准偏差值。 • **正常** - 这是默认值。正常水平等于平均值和标准偏差值的两倍。 • **高** - 高水平等于平均值和标准偏差值的三倍。
异常持续时间	仅当异常行为持续一段指定时间时，系统才会为检测到的异常生成警报。 输入一个介于 1 到 60(分钟)之间的整数值。默认值为 15。

硬件更改监视器的设置

硬件更改监视硬件更改，例如在工作负载上添加、删除或替换硬件。

可以为监视器配置以下设置。

设置	描述
硬件组件	选择要监视其更改的一个或多个硬件组件。 以下值可用。 • **全部** - 这是默认值。 • **主板** • **CPU** • **RAM** • **磁盘** • **GPU** • **网络适配器**

设置	描述
要监视的内容	指定要监视选定硬件组件的更改。可以从列表中选择多个项目。 以下值可用。 • **任何更改** -这是默认值。 • **新增组件** • **已替换组件** • **已删除组件**

CPU 使用率监视器的设置

CPU 使用率监视工作负载的总 CPU 使用情况(处理器使用率)。如果工作负载有多个 CPU,则总 CPU 使用情况将是每个 CPU 的 CPU 使用情况之和。

可以为监视器配置以下设置。

设置	描述
基于阈值的监视	
运算符	运算符是一个条件函数,用于定义如何根据指标衡量性能。 以下值可用。 • **大于** -这是默认值。 • **大于或等于** • **小于** • **小于或等于**
CPU 使用率阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时,系统会生成警报。 输入一个介于 1 到 100 (%) 之间的整数值。默认值为 90。
时间段	仅当指标值在指定时间段内超出正常水平时,系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟)之间的整数值。默认值为 5。
基于异常的监视	
模型训练期	在此期间,系统将根据从代理程序收集到的数据训练机器学习模型,然后创建工作负载的正常行为模式。模型训练期越长,系统将创建的长期行为模式就越准确。我们建议最短模型训练期为 21 天。 输入一个整数值(天)。默认值为 21。
在训练期间接收异常警报	如果选择此设置,则您会在模型训练期间收到有关异常的警报。由于模型仍在进行训练,可能不够准确,因此这些警报可能是误报。 默认情况下,该设置处于选中状态。

设置	描述
灵敏度级别	如果异常值在特定范围内，则灵敏度级别可用作异常的初步过滤器。该过滤器独立于异常检测算法运行。其目的是阻止异常检测算法处理在指定范围内的异常。 在训练期间： 1. 使用在训练期间收集到的数据来训练该算法。 2. 该算法对训练数据进行异常检测。 3. 应用基于平均值和标准偏差的过滤过程。 4. 过滤在指定间隔内的任何异常。 5. 在其余异常数据点中，异常级别最低的异常处于选中状态。该级别(介于 0 和 1 之间的浮点数)记录在模型中。 在预测期间： 1. 该算法根据推断数据预测异常。 2. 根据灵敏度级别，基于平均值和标准偏差过滤预测的异常。 3. 根据以下原则对其余异常进一步过滤：高于阈值水平的值被视为异常，而低于阈值水平的值被视为正常行为。 以下值可用。 • **低** - 低水平等于平均值和标准偏差值。 • **正常** - 这是默认值。正常水平等于平均值和标准偏差值的两倍。 • **高** - 高水平等于平均值和标准偏差值的三倍。
异常持续时间	仅当异常行为持续一段指定时间时，系统才会为检测到的异常生成警报。 输入一个介于 1 到 60(分钟)之间的整数值。默认值为 15。

内存使用率监视器的设置

内存使用率监视工作负载的所有内存模块的总内存使用情况。

可以为监视器配置以下设置。

设置	描述
基于阈值的监视	
运算符	运算符是一个条件函数，用于定义如何根据指标衡量性能。 以下值可用。 • **大于** -这是默认值。 • **大于或等于** • **小于** • **小于或等于**
内存使用率阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时，系统会生成警报。 输入一个介于 1 到 100 (%) 之间的整数值。默认值为 90。

设置	描述
时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟)之间的整数值。默认值为 5。
基于异常的监视	
模型训练期	在此期间，系统将根据从代理程序收集到的数据训练机器学习模型，然后创建工作负载的正常行为模式。模型训练期越长，系统将创建的长期行为模式就越准确。我们建议最短模型训练期为 21 天。 输入一个整数值(天)。默认值为 21。
在训练期间接收异常警报	如果选择此设置，则您会在模型训练期间收到有关异常的警报。由于模型仍在进行训练，可能不够准确，因此这些警报可能是误报。 默认情况下，该设置处于选中状态。
灵敏度级别	如果异常值在特定范围内，则灵敏度级别可用作异常的初步过滤器。该过滤器独立于异常检测算法运行。其目的是阻止异常检测算法处理在指定范围内的异常。 在训练期间： 1. 使用在训练期间收集到的数据来训练该算法。 2. 该算法对训练数据进行异常检测。 3. 应用基于平均值和标准偏差的过滤过程。 4. 过滤在指定间隔内的任何异常。 5. 在其余异常数据点中，异常级别最低的异常处于选中状态。该级别(介于 0 和 1 之间的浮点数)记录在模型中。 在预测期间： 1. 该算法根据推断数据预测异常。 2. 根据灵敏度级别，基于平均值和标准偏差过滤预测的异常。 3. 根据以下原则对其余异常进一步过滤：高于阈值水平的值被视为异常，而低于阈值水平的值被视为正常行为。 以下值可用。 • **低** - 低水平等于平均值和标准偏差值。 • **正常** - 这是默认值。正常水平等于平均值和标准偏差值的两倍。 • **高** - 高水平等于平均值和标准偏差值的三倍。
异常持续时间	仅当异常行为持续一段指定时间时，系统才会为检测到的异常生成警报。 输入一个介于 1 到 60(分钟)之间的整数值。默认值为 30 分钟。

磁盘传输速率监视器的设置

磁盘传输速率监视工作负载上每个物理磁盘的读写速度。

可以为监视器配置以下设置。

设置	描述
基于阈值的监视	
要监视的内容	选择要监视的速度。 以下值可用。 • **读取速度和写入速度**。这是默认值。 • **读取速度** • **写入速度**
读取速度运算符	运算符是一个条件函数，用于定义如何根据指标衡量性能。 以下值可用。 • **大于**。这是默认值。 • **大于或等于** • **小于** • **小于或等于**
读取速度阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时，系统会生成警报。 输入一个整数值 (kb/s)。默认值为 0 kb/s。
读取速度时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟) 之间的整数值。默认值为 5。
写入速度运算符	运算符是一个条件函数，用于定义如何根据指标衡量性能。 以下值可用。 • **大于** -这是默认值。 • **大于或等于** • **小于** • **小于或等于**
写入速度阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时，系统会生成警报。 输入一个整数值 (kb/s)。默认值为 0 kb/s。
写入速度时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟) 之间的整数值。默认值为 5。
基于异常的监视	
模型训练期	在此期间，系统将根据从代理程序收集到的数据训练机器学习模型，然后创建工作负载的正常行为模式。模型训练期越长，系统将创建的长期行为模式就越准确。我们建议最短模型训练期为 21 天。

设置	描述
	输入一个整数值(天)。默认值为 21。
在训练期间接收异常警报	如果选择此设置,则您会在模型训练期间收到有关异常的警报。由于模型仍在进行训练,可能不够准确,因此这些警报可能是误报。 默认情况下,该设置处于选中状态。
要监视的内容	选择要监视的速度。 以下值可用。 • **读取速度和写入速度**。这是默认值。 • **读取速度** • **写入速度**
灵敏度级别	如果异常值在特定范围内,则灵敏度级别可用作异常的初步过滤器。该过滤器独立于异常检测算法运行。其目的是阻止异常检测算法处理在指定范围内的异常。 在训练期间: 1. 使用在训练期间收集到的数据来训练该算法。 2. 该算法对训练数据进行异常检测。 3. 应用基于平均值和标准偏差的过滤过程。 4. 过滤在指定间隔内的任何异常。 5. 在其余异常数据点中,异常级别最低的异常处于选中状态。该级别(介于 0 和 1 之间的浮点数)记录在模型中。 在预测期间: 1. 该算法根据推断数据预测异常。 2. 根据灵敏度级别,基于平均值和标准偏差过滤预测的异常。 3. 根据以下原则对其余异常进一步过滤:高于阈值水平的值被视为异常,而低于阈值水平的值被视为正常行为。 以下值可用。 • **低** - 低水平等于平均值和标准偏差值。 • **正常** - 这是默认值。正常水平等于平均值和标准偏差值的两倍。 • **高** - 高水平等于平均值和标准偏差值的三倍。
异常持续时间(读取速度)	仅当异常行为持续一段指定时间时,系统才会为检测到的异常生成警报。 输入一个介于 1 到 60(分钟)之间的整数值。 默认值为 25。
异常持续时间(写入速度)	仅当异常行为持续一段指定时间时,系统才会为检测到的异常生成警报。 输入一个介于 1 到 60(分钟)之间的整数值。 默认值为 25。

网络使用率监视器的设置

网络使用率监视工作负载的每个网络适配器的传入和传出流量。

可以为监视器配置以下设置。

设置	描述
基于阈值的监视	
流量方向	要监视的流量方向。 以下值可用。 • **传入和传出流量**。这是默认值。 • **传入流量** • **传出流量**
传入流量运算符	运算符是一个条件函数，用于定义如何根据指标衡量性能。 以下值可用。 • **大于** -这是默认值。 • **大于或等于** • **小于** • **小于或等于**
传入流量阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时，系统会生成警报。 输入一个整数值 (kb/s)。默认值为 0 kb/s。
传入流量时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟) 之间的整数值。默认值为 5。
传出流量运算符	运算符是一个条件函数，用于定义如何根据指标衡量性能。 以下值可用。 • **大于** -这是默认值。 • **大于或等于** • **小于** • **小于或等于**
传出流量阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时，系统会生成警报。 输入一个整数值 (kb/s)。默认值为 0 kb/s。
传出流量时间段	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时，系统会生成警报。

设置	描述
	输入一个介于 1 到 60(分钟) 之间的整数值。默认值为 5。
基于异常的监视	
模型训练期	在此期间，系统将根据从代理程序收集到的数据训练机器学习模型，然后创建工作负载的正常行为模式。模型训练期越长，系统将创建的长期行为模式就越准确。我们建议最短模型训练期为 21 天。 输入一个整数值(天) 。默认值为 21。
在训练期间接收异常警报	如果选择此设置，则您会在模型训练期间收到有关异常的警报。由于模型仍在进行训练，可能不够准确，因此这些警报可能是误报。 默认情况下，该设置处于选中状态。
流量方向	• **传入和传出流量**。这是默认值。 • **传入流量** • **传出流量**
灵敏度级别	如果异常值在特定范围内，则灵敏度级别可用作异常的初步过滤器。该过滤器独立于异常检测算法运行。其目的是阻止异常检测算法处理在指定范围内的异常。 在训练期间： 1. 使用在训练期间收集到的数据来训练该算法。 2. 该算法对训练数据进行异常检测。 3. 应用基于平均值和标准偏差的过滤过程。 4. 过滤在指定间隔内的任何异常。 5. 在其余异常数据点中，异常级别最低的异常处于选中状态。该级别(介于 0 和 1 之间的浮点数) 记录在模型中。 在预测期间： 1. 该算法根据推断数据预测异常。 2. 根据灵敏度级别，基于平均值和标准偏差过滤预测的异常。 3. 根据以下原则对其余异常进一步过滤：高于阈值水平的值被视为异常，而低于阈值水平的值被视为正常行为。 以下值可用。 • **低** - 低水平等于平均值和标准偏差值。 • **正常** - 这是默认值。正常水平等于平均值和标准偏差值的两倍。 • **高** - 高水平等于平均值和标准偏差值的三倍。
异常持续时间(传入)	仅当异常行为持续一段指定时间时，系统才会为检测到的异常生成警报。 输入一个介于 1 到 60(分钟) 之间的整数值。 默认值为 25。
异常持续时间(传	仅当异常行为持续一段指定时间时，系统才会为检测到的异常生成警报。 输入一个介于 1 到 60(分钟) 之间的整数值。

设置	描述
出)	默认值为 25。

CPU 使用率(按进程)监视器的设置

CPU 使用率(按进程) 监视选定进程的 CPU 使用情况。如果同一进程有多个实例,则系统将监视所有进程实例的总使用情况,并在满足条件时生成警报。

可以为监视器配置以下设置。

设置	描述
进程名称	要监视的进程的名称。输入不带扩展名的进程名称。
运算符	运算符是一个条件函数,用于定义如何根据指标衡量性能。 以下值可用。 • **大于** -这是默认值。 • **大于或等于** • **小于** • **小于或等于**
阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时,系统会生成警报。 输入一个介于 1 到 100 (%) 之间的整数值。默认值为 90。
时间段	仅当指标值在指定时间段内超出正常水平时,系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟)之间的整数值。默认值为 5。

内存使用率(按进程)监视器的设置

内存使用率(按进程) 监视选定进程的内存使用情况。如果同一进程有多个实例,则系统将监视所有进程实例的总使用情况,并在满足条件时生成警报。

注意
代理程序会使用总进程工作集(专用和共享),来估算进程的内存使用量大小。这就是小组件显示的大小可能与 Windows 任务管理器(专用工作集)中所示内存使用量大小不同的原因。

可以为监视器配置以下设置。

设置	描述
进程名称	要监视的进程的名称。输入不带扩展名的进程名称。
运算符	运算符是一个条件函数,用于定义如何根据指标衡量性能。

设置	描述
	以下值可用。 • **大于** -这是默认值。 • **大于或等于** • **小于** • **小于或等于**
阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时，系统会生成警报。 输入一个整数值 (kb)。默认值为“1”。
时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟) 之间的整数值。默认值为 5。

磁盘传输速率(按进程) 监视器的设置

磁盘传输速率(按进程) 监视选定进程的读写速度。如果同一进程有多个实例，则系统将监视所有进程实例的总使用情况，并在满足条件时生成警报。

可以为监视器配置以下设置。

设置	描述
进程名称	要监视的进程的名称。输入不带扩展名的进程名称。
要监视的内容	要监视的速度。 以下值可用。 • **读取速度和写入速度**。这是默认值。 • **读取速度** • **写入速度**
读取速度运算符	运算符是一个条件函数，用于定义如何根据指标衡量性能。 以下值可用。 • **大于** -这是默认值。 • **大于或等于** • **小于** • **小于或等于**
读取速度阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时，系统会生成警报。 输入一个整数值 (kb/s)。默认值为 0 kb/s。
读取速度时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。

设置	描述
	输入一个介于 1 到 60(分钟) 之间的整数值。默认值为 5。
写入速度运算符	运算符是一个条件函数，用于定义如何根据指标衡量性能。 以下值可用。 • **大于** -这是默认值。 • **大于或等于** • **小于** • **小于或等于**
写入速度阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时，系统会生成警报。 输入一个整数值 (kb/s)。默认值为 0 kb/s。
写入速度时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟) 之间的整数值。默认值为 5。

网络使用率(按进程) 监视器的设置

网络使用率(按进程) 监视选定进程的传入和传出流量。如果同一进程有多个实例，则系统将监视所有进程实例的总使用情况，并在所有实例满足条件时生成警报。

可以为监视器配置以下设置。

设置	描述
进程名称	要监视的进程的名称。输入不带扩展名的进程名称。
流量方向	要监视的流量方向。 以下值可用。 • **传入流量和传出流量**。这是默认值。 • **传入流量** • **传出流量**
传入流量运算符	运算符是一个条件函数，用于定义如何根据指标衡量性能。 以下值可用。 • **大于** -这是默认值。 • **大于或等于** • **小于** • **小于或等于**
传入流量阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时，系统会生成警报。

设置	描述
	输入一个整数值 (kb/s)。默认值为 0 kb/s。
传入流量时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟) 之间的整数值。默认值为 5。
传出流量运算符	运算符是一个条件函数，用于定义如何根据指标衡量性能。 以下值可用。 • **大于** -这是默认值。 • **大于或等于** • **小于** • **小于或等于**
传出流量阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时，系统会生成警报。 输入一个整数值 (kb/s)。默认值为 0 kb/s。
传出流量时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟) 之间的整数值。默认值为 5。

Windows 服务状态监视器的设置

Windows 服务状态监视选定 Windows 服务是正在运行还是已停止。

可以为监视器配置以下设置。

设置	描述
服务名称	要监视的 Windows 服务的名称。 可以从 Windows 服务列表中选择服务名称。在工作负载上成功完成软件清查扫描后，租户的所有代理程序会填入该列表。也可以添加不在列表中的服务名称。如果未在工作负载上执行软件清查扫描，则这是唯一可用的选项。
服务状态	如果服务处于选定状态，则系统会生成一个事件。 以下值可用。 • **正在运行** • **已停止** - 这是默认值。
时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟) 之间的整数值。默认值为“1”。

进程状态监视器的设置

进程状态监视选定进程是正在运行还是已停止。如果同一进程有多个实例，则系统将监视该进程的每个实例，并在该进程的所有实例满足条件时生成警报。

可以为监视器配置以下设置。

设置	描述
进程名称	要监视的进程的名称。输入不带扩展名的可执行文件的名称。
进程状态	如果进程处于选定状态，则系统会生成一个事件。 以下值可用。 • **正在运行** • **已停止** - 这是默认值。
时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 60(分钟) 之间的整数值。默认值为“1”。

已安装软件监视器的设置

已安装软件监视工作负载上软件应用程序的安装、更新或删除。

可以为监视器配置以下设置。

设置	描述
要监视的软件	指定要监视的软件。 以下值可用。 • **任何软件** -这是默认值。 • **特定软件**
软件名称	如果为**要监视的软件**选择**特定软件**值，则此设置可用。 输入一个或多个软件应用程序的名称。 可以从 Windows 服务列表中选择一个软件应用程序名称。在工作负载上成功完成软件清查扫描后，租户的所有代理程序会填入该列表。也可以添加不在列表中的软件应用程序名称。如果未在工作负载上执行软件清查扫描，则这是唯一可用的选项。
安装状态	指定是否要监视已安装软件、未安装软件或已更新软件。 以下值可用。 • **已安装** - 这是默认值。如果选择此值，则监视器将在工作负载上安装新的软件应用程序时生成警报。

设置	描述
	• **已更新** - 如果选择此值，则监视器将在更新软件应用程序时生成警报。 • **未安装** - 如果选择此值，当软件应用程序被卸载或在工作负载上不可用时，监视器将生成警报。

上次系统重新启动监视器的设置

上次系统重新启动监视工作负载上次何时重新启动。

可以为监视器配置以下设置。

设置	描述
工作负载未重新启动时长	自上次重新启动工作负载以来的时长(天数)。如果工作负载未重新启动的时间比您指定的时间长，则系统将生成警报。 输入一个介于 1 到 180(天)之间的整数值。默认值为 30。

Windows 事件日志监视器的设置

Windows 事件日志监视 Windows 事件日志中的特定业务关键事件。

可以为监视器配置以下设置。

设置	描述
事件日志名称	从 Windows 事件查看器中可用的 Windows 事件日志列表中选择某个事件日志。 以下值可用。 • **任何** -这是默认值。 • **应用程序** • **安全** • **系统**
事件源	事件源名称 可以从收集自租户的所有代理程序的事件源列表中选择值，也可以手动输入新的源名称。 如果已为租户禁用软件清查扫描，则事件源列表将为空。
匹配模式	在此字段中，可以使用**任何**或**全部**运算符来指定是否要连接**事件 ID**、**事件类型**和**事件描述**设置。 以下值可用。 • **任何** -这是默认值。仅当匹配任何选定条件时，才会生成警报 • **全部** - 当匹配所有选定条件时，会生成警报。
事件	输入一个或多个用逗号分隔的事件 ID。如果系统在事件日志中发现您在此字段中输

设置	描述
ID	入的任何事件代码，则会生成警报。
事件类型	选择要监视的一个或多个事件类型。 以下值可用。 • **任何** - 这是默认值。 • **错误** • **警告** • **信息** • **成功审核** • **失败审核**
事件描述	事件描述中要搜索的特定关键字或短语。输入的每个关键字或短语都必须用引号括起来，并且必须用逗号分隔。如果系统发现您输入的任何关键字或短语，它会生成警报。
出现的次数	在系统生成警报的时间段内，事件在日志中必须出现的最小次数。 输入一个介于 1 到 1000 之间的整数值。
时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个整数值，然后选择单位：分钟或小时。默认值为 60 分钟。

文件和文件夹大小监视器的设置

文件和文件夹大小监视选定文件和文件夹的总大小。

可以为监视器配置以下设置。

设置	描述
要监视的文件或文件夹	要监视的文件或文件夹的路径。也可以指定要排除监视的文件或文件夹。 可以使用以下通配符字符。 • * - 用于替代文件或文件夹名称中的零个或多个字符 • ? - 用于仅替代文件或文件夹名称中的一个字符 对于 Windows 工作负载： • 完整路径应从驱动器号开始，后跟 :\ 分隔符。 • 可以使用斜杠或反斜杠作为路径分隔符字符。 • 文件或文件夹名称不得以空格或句点结尾。 对于 macOS 工作负载： • 完整路径应从根目录开始。 • 可以使用斜杠作为路径分隔符字符。 • 文件或文件夹名称不得以空格或句点结尾。

设置	描述
	对于排除过滤器，指定特定位置不是强制性的。在受监视文件夹中，将排除没有特定位置的输入文件。
运算符	运算符是一个条件函数，用于定义如何根据指标衡量性能。 以下值可用。 • **大于** -这是默认值。 • **小于**
阈值	阈值和**运算符**值确定受监视指标的正常性能。当受监视指标的值超出正常水平时，系统会生成警报。 输入一个整数值 (MB)。
时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 10 到 60(分钟) 之间的整数值。默认值为 10。

Windows Update 状态监视器的设置

Windows Update 状态监视工作负载的 Windows Update 状态以及最新更新是否已安装。

如果启用此监视器，则系统会在以下情况下生成警报。

- Windows Update 在工作负载上已禁用。
- Windows Update 在工作负载上已启用，但最新更新未安装。

防火墙状态监视器的设置

防火墙状态监视工作负载上安装的内置或第三方防火墙。

如果启用此监视器，则系统会在以下情况下生成警报。

- 内置操作系统防火墙(Windows Defender 防火墙或 macOS 防火墙) 已禁用，且没有第三方防火墙正在运行。
- 已为公用网络禁用 Windows Defender 防火墙。
- 已为专用网络禁用 Windows Defender 防火墙。
- 已为域网络禁用 Windows Defender 防火墙。

失败登录监视器的设置

失败登录监视工作负载上失败的登录尝试。

可以为监视器配置以下设置。

设置	描述
失败登录尝试	该阈值确定受监视指标的正常性能的边界。当超过该阈值时，即表示该值超

设置	描述
阈值	出正常范围。 输入一个整数值。默认值为 60。
时间段	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。 输入一个介于 1 到 24 之间的整数值，并选择单位：小时或天。默认值为 12。

防恶意软件软件状态监视器的设置

防恶意软件软件状态监视工作负载上安装的内置或第三方防恶意软件软件。

如果启用此监视器，则系统会在识别出以下情况之一时生成警报。

- 工作负载上未安装防恶意软件软件。
- 防恶意软件软件已安装，但未在运行。
- 防恶意软件软件已安装并在运行，但恶意软件定义并非最新。

注意
针对 Windows 和 Windows Server 操作系统检查此条件。

操作系统	支持的防恶意软件软件
Windows	• 安克诺斯 Cyber Protect • Windows Defender • Symantec Endpoint Security • Norton 360 • Norton AntiVirus • SentinelOne • Trend Micro Endpoint Security with Apex One • Trend Micro Worry-Free Business • McAfee Endpoint Security • McAfee Endpoint Protection for SMB • FireEye Endpoint Security • F-Secure SAFE • F-Secure Client Security • CrowdStrike Falcon • Kaspersky Endpoint Security Cloud • BitDefender Antivirus • Sophos Intercept X Endpoint • Avast Business Antivirus • AVG Antivirus Business Edition • AVG Internet Security Business Edition • Panda Endpoint Protection

操作系统	支持的防恶意软件软件
	• Tencent PC Manager • Webroot Business Endpoint Protection • ESET Endpoint Security • Avira Antivirus • Comodo Internet Security • Comodo Business Antivirus • K7 Business Security • K7 Total Security • Vipre Endpoint Protection • Total AV
Windows Server	• 安克诺斯 Cyber Protect • Windows Defender • ESET Endpoint Security **注意** 该监视器可能会与其他防恶意软件应用程序一起使用，但这一点并不能保证。
macOS	• 安克诺斯 Cyber Protect • F-Secure Safe • BitDefender Anti-virus for Mac • Sophos Home • Sophos Endpoint Protection • Avast Security for Mac • AVG AntiVirus for Mac • Webroot SecureAnywhere • ESET Cybersecurity • Avira Antivirus for Mac • Comodo Antivirus for Mac • K7 Antivirus for Mac • Vipre Advanced Security • Total AV for Mac **注意** 该监视器可能会与其他防恶意软件应用程序一起使用，但这一点并不能保证。

“自动运行”功能状态监视器的设置

“自动运行”功能状态监视是否已为可移动媒体启用“自动运行”功能。

出于安全原因，建议您在工作负载上禁用可移动媒体的“自动运行”功能。如果该功能已启用，则系统将生成警报。

自定义监视器的设置

自定义通过正在运行的脚本监视自定义对象。

可以为监视器配置以下设置。

设置	描述
要运行的脚本	脚本存储库中预定义脚本的列表。
预定	脚本运行的时间，以及要运行脚本应满足的附加条件(可选)。 以下值可用。 • **按时间预定** - 脚本将在指定的确切时间、天、周或月运行。这是默认值。 **预定类型** - **每小时**、**每日**或**每月**。 **在日期范围内运行** - 运行脚本的时间范围。 • **用户登录系统时** - 脚本将在用户登录到工作负载时运行。 • **用户注销系统时** - 脚本将在用户注销工作负载时运行。 • **系统启动时** - 脚本将在工作负载的操作系统启动时运行。 • **系统关闭时** - 脚本将在工作负载关闭时运行。 • **系统联机时** - 脚本将在工作负载联机可用时运行。 **启动条件** - 仅当满足条件时，才会在指定时间或根据指定事件执行任务。如果选择了多个条件，则必须同时满足所有条件才能启动任务。 默认情况下，**阻止睡眠或休眠模式启动预定任务**条件处于选中状态。 **如果不满足启动条件，请务必在以下时间过后运行任务** - 默认情况下，此条件处于启用状态。默认值为 1 小时。
执行脚本的帐户	将运行脚本的帐户。 以下值可用。 • **系统帐户** - 这是默认值。 • **当前登录的帐户**
最长持续时间	脚本可以在工作负载上运行的最长时间。 如果脚本在此期间未完成，则操作会失败。 输入一个介于 1 到 1440(分钟)之间的整数值。默认值为 3 分钟。
PowerShell 执行策略	PowerShell 执行策略。 以下值可用。 • **Undefined** • **AllSigned** • **Bypass** - 这是默认值。 • **RemoteSigned** • **Restricted**

设置	描述
	• **Unrestricted** 有关这些值的详细信息，请参阅 Microsoft 文档。

监视计划

监视计划是应用于托管工作负载以启用和配置监视功能的计划。

如果没有对工作负载应用监视计划，则监视功能将不可用于该工作负载。

注意
可以在监视计划中配置的设置的可用性取决于应用于租户的服务包。要访问所有设置，请激活 Advanced Management 包。

创建监视计划

可以创建一个监视计划，然后为该监视计划添加工作负载以配置对托管工作负载的监视功能。

先决条件

工作负载上安装的相应版本的代理程序支持监视功能。

创建监视计划

从监视计划

1. 在 保护 中控台中，转到**管理** > **监视计划**。
2. 使用两个选项之一创建监视计划。
   - 如果列表中没有监视计划，则单击**创建**。
   - 如果列表中有监视计划，则单击**创建计划**。
3. 在**创建监视计划**窗口中，根据是否已为租户启用 “Advanced Management” 包，执行以下操作：
   - 如果租户正在使用“标准”保护，则以下四个监视器会自动添加到监视计划：磁盘空间、硬件更改、上次系统重新启动以及文件和文件夹大小。
   - 如果已为租户启用 “Advanced Management” 包，则选择其中一个模板选项，然后单击**下一步**。

选项	描述
建议	选择此选项，可创建具有默认监视配置的监视计划。
自定义	使用此选项，可从头开始创建监视计划。
4. [可选] 要更改计划的默认名称，请单击铅笔图标、输入计划的名称，然后单击**确定**。
5. [可选] 要为计划添加监视器，请单击**添加监视器**、单击列表中的监视器，然后单击**添加**。

注意
监视器的设置将自动填充默认值。
可以为监视计划最多添加同类型的三个监视器，总共最多添加 30 个监视器。

6. [可选] 在监视器参数屏幕中，更改监视器和警报的默认设置，然后单击**完成**。

注意
可以为每个监视器配置不同的设置。有关详细信息，请参阅 "可配置的监视器"(第 951 页) 和 "配置监视警报"(第 985 页) 。

7. [可选] 要删除监视器，请单击垃圾桶图标，然后单击**删除**。
8. [可选] 要为计划添加工作负载，请执行以下操作：
   a. 单击**添加工作负载**。
   b. 选择工作负载，然后单击**添加**。
   c. 如果有要解决的兼容性问题，则按照 "解决监视计划的兼容性问题"(第 983 页) 中所述的步骤操作。
9. 单击**创建**。

从所有设备

1. 在 保护 中控台中，转到**设备** > **所有设备**。
2. 单击要应用监视计划的工作负载。
3. 单击**保护**。
4. 根据是否已将监视计划应用于工作负载，执行以下操作：
   - 如果监视计划已应用于工作负载，则单击**创建计划**，然后选择**监视**。
   - 如果监视计划未应用于工作负载，则单击**添加计划**、单击**创建计划**，然后选择**监视**。
5. 在**创建监视计划**窗口中，选择其中一个模板选项，然后单击**下一步**。

选项	描述
建议	选择此选项，可创建具有默认监视配置的监视计划。
自定义	使用此选项，可从头开始创建监视计划。

6. [可选] 要更改计划的默认名称，请单击铅笔图标、输入计划的名称，然后单击**确定**。
7. [可选] 如果要更改监视器和警报的默认设置，请配置新值，然后单击**完成**。

注意
可以为监视计划最多添加同类型的三个监视器，总共最多添加 30 个监视器。

8. [可选] 在监视器参数屏幕中，更改监视器和警报的默认设置，然后单击**完成**。

注意
可以为每个监视器配置不同的设置。有关详细信息，请参阅 "可配置的监视器"(第 951 页) 和 "配置监视警报"(第 985 页) 。

9. [可选] 要删除监视器，请单击垃圾桶图标，然后单击**删除**。
10. 单击**创建**。

将工作负载添加到监视计划

根据需要，可以在创建计划后为监视计划添加工作负载。

先决条件

- 已为您的用户帐户启用双重身份验证。
- 工作负载上安装的相应版本的代理程序支持监视功能。
- 至少有一个监视计划可用。

将工作负载添加到监视计划

从监视计划

1. 在 保护 中控台中，转到**管理** > **监视计划**。
2. 单击相应监视计划。
3. 根据计划是否已应用于任何工作负载，执行以下操作：
   - 如果计划尚未应用于任何工作负载，则单击**添加工作负载**。
   - 如果计划已应用于任何工作负载，则单击**管理工作负载**。
4. 从列表中选择一个工作负载，然后单击**添加**。
5. 单击**保存**。
6. 如果需要，请单击**确认**以将所需的服务配额应用于工作负载。

从所有设备

1. 在 保护 中控台中，转到**设备** > **所有设备**。
2. 单击要应用监视计划的工作负载。
3. 单击**保护**。
4. 查找要添加工作负载的监视计划，然后单击**应用**。
5. 如果需要，请单击**确认**以将所需的服务配额应用于工作负载。

吊销监视计划

可以从已应用监视计划的工作负载中吊销该计划。

先决条件

至少一个监视计划已应用于工作负载。

吊销监视计划

1. 在 保护 中控台中，转到**设备** > **所有设备**。
2. 单击工作负载，然后单击**保护**。
3. 单击要吊销的监视计划的**更多操作**图标，然后单击**吊销**。

配置自动响应操作

对警报事件的自动响应操作是自动触发以响应检测到事件的预定义操作或措施。这些操作旨在缓解潜在威胁并最大限度地减少损害。

可以对警报事件配置一个或多个自动响应操作。每个监视器的最大自动响应操作数可以是 20。

配置自动响应操作

1. 在 保护 中控台中，转到**管理 > 监视计划**。
2. 选择要为其配置自动响应操作的监视计划。
3. 选择要为其配置自动响应操作的监视器；或者，如果尚未添加监视器，请单击**添加监视器**、单击列表中的监视器、单击**添加**，然后选择监视器。
4. 单击**自动响应操作**旁边的链接。
5. 在**自动响应操作**窗口中，添加一个或多个将在触发警报时自动执行的响应操作。
6. 配置每个响应操作。例如，如果已添加响应操作**启动 Windows 服务**，请执行以下操作：
   a. 在 **Windows 服务**的旁边，请单击**指定**。
   b. 在**服务**字段中，选择要作为响应操作启动的服务。
   c. 单击**完成**。
7. 在所有已添加的响应操作列表中，使用上下箭头或拖放操作来设置响应操作的顺序。
8. 配置在上一个响应操作失败时如何处理后续响应操作。请选择下列任一选项：
   a. **继续执行下一个响应操作**。
   b. **请勿继续执行下一个响应操作**。
9. 单击**完成**。
   您即会在监视计划的**自动响应操作**设置旁边看到配置的操作数。可以编辑或删除这些操作，也可以稍后随时添加新操作。

下表列出并描述了在监视器设置中可用的所有自动响应操作。

自动响应操作	描述	支持的操作系统
运行脚本	如果添加此操作，则可以： 1. 选择要在工作负载上运行的特定脚本。 2. 指定要在其下执行脚本的帐户。 3. 指定运行的最长持续时间。 4. 指定 PowerShell 执行策略。 5. 运行脚本。 要执行此操作，您需要有工作负载的 “Advanced Management” 包许可证（如果尚未指派）。 当满足条件时，系统将使用指定的参数运行选定的远程脚本。	Windows、macOS

自动响应操作	描述	支持的操作系统
重新启动工作负载	如果添加此操作，则系统将在满足条件时远程重新启动工作负载。	Windows、macOS
停止进程	如果添加此操作，则可以通过手动输入进程名称来指定要停止的进程。 当满足条件时，系统将停止该进程。	Windows、macOS
启动 Windows 服务	如果添加此操作，则可以从代理程序填充的服务的动态列表中选择要启动的 Windows 服务。 当满足条件时，系统将启动该服务。	Windows
停止 Windows 服务	如果添加此操作，则可以从代理程序填充的服务的动态列表中选择要停止的 Windows 服务。 当满足条件时，系统将停止该服务。	Windows
启用 Windows Update	如果添加此操作，则系统将在满足条件时启用 Windows Update。 此操作仅适用于 Windows Update 状态监视器。	Windows
禁用可移动驱动器上的“自动运行”	如果添加此操作，则系统将在满足条件时为工作负载禁用可移动存储媒体上的“自动运行”功能。 此操作仅适用于“自动运行”功能状态监视器。	Windows

监测计划的附加行动

在**监视计划**屏幕中，可以对监视计划执行以下附加操作：查看详细信息、编辑、查看活动、查看警报、重命名、启用、禁用、克隆、导出、删除、设为收藏、设为默认，和删除。

查看详细信息

查看监视计划的详细信息

1. 在**监视计划**屏幕中，单击监视计划的**更多操作**图标。
2. 单击**查看详细信息**。
3. [可选] 如果要查看计划中启用的监视器的详细信息，则单击监视器名称。

编辑

先决条件

已为您的用户帐户启用双重身份验证。

编辑计划

1. 在**监视计划**屏幕中，单击监视计划的**更多操作**图标。
2. 单击**编辑**。
3. [可选] 要从计划中删除监视器，请单击监视器名称右侧的回收站图标。
4. [可选] 要启用或禁用计划中的监视器，请使用监视器名称旁边的开关。
5. [可选] 要编辑监视器参数，请执行以下操作。
   a. 单击监视器名称。
   b. 单击监视器参数的概述。
   c. 在**监视器参数**屏幕中，配置参数，然后单击**完成**。

      注意
      可以为每个监视器配置不同的设置。有关详细信息，请参阅 "可配置的监视器"(第 951 页) 和 "配置监视警报"(第 985 页)。

   d. 关闭屏幕并确认更改。
6. [可选] 要添加监视器，请单击**添加监视器**，然后根据需要按照上一步中所述编辑参数。
7. 单击**保存**。

活动

查看与监视计划相关的活动

1. 在**监视计划**屏幕中，单击监视计划的**更多操作**图标。
2. 单击**活动**。
3. 单击某个活动，可查看有关它的更多详细信息。

警告

查看警报

1. 在**监视计划**屏幕中，单击监视计划的**更多操作**图标。
2. 单击**警告**。

重命名

先决条件

已为您的用户帐户启用双重身份验证。

重命名监视计划

1. 在**监视计划**屏幕中，单击监视计划的**更多操作**图标。
2. 单击**重命名**。
3. 输入计划的新名称，然后单击**确定**。

启用

先决条件

- 已为您的用户帐户启用双重身份验证。
- 监视计划至少已应用于一个工作负载。

启用监视计划

1. 在**监视计划**屏幕中，单击监视计划的**更多操作**图标。
2. 单击**启用**。

禁用

先决条件

已为您的用户帐户启用双重身份验证。

禁用监视计划

1. 在**监视计划**屏幕中，单击监视计划的**更多操作**图标。
2. 单击**禁用**。

克隆

先决条件

已为您的用户帐户启用双重身份验证。

若要克隆监控计划

1. 在**监视计划**屏幕中，单击监视计划的**更多操作**图标。
2. 单击**克隆**。
3. 单击**创建**。

导出

先决条件

已为您的用户帐户启用双重身份验证。

若要导出监控计划

1. 在**监视计划**屏幕中，单击监视计划的**更多操作**图标。
2. 单击**导出**。

   计划配置以 JSON 格式导出到本地计算机。

删除

先决条件

已为您的用户帐户启用双重身份验证。

删除监视计划

1. 在**监视计划**屏幕中，单击监视计划的**更多操作**图标。
2. 单击**删除**。
3. 选择**我确认**，然后单击**删除**。

设置为默认值

先决条件

已为您的用户帐户启用双重身份验证。

将监视计划设置为默认计划

1. 在**监视计划**屏幕中，单击监视计划的**更多操作**图标。
2. 单击**"设为默认值"**。
3. 在确认窗口中，单击**"设置"**。
   在**监视计划**屏幕上，计划名称旁边会出现**默认**标签。

添加到收藏夹

先决条件

已为您的用户帐户启用双重身份验证。

若要若要将监视计划设为收藏

1. 在**监视计划**屏幕中，单击监视计划的**更多操作**图标。
2. 单击**添加到收藏夹**。
   在**监视计划**屏幕上，计划名称旁边会出现一个星形图标。

监视计划的兼容性问题

在某些情况下，对工作负载应用监视计划可能会导致出现兼容性问题。您可能会发现以下兼容性问题：

- 操作系统不兼容 - 当工作负载的操作系统不受支持时，会出现此问题。
- 代理程序不受支持 - 当工作负载上的保护代理程序版本已过时且不支持监视功能时，会出现此问题。
- 配额不足 - 当租户中的服务配额不足以指派给选定工作负载时，会出现此问题。

如果监视计划应用于多达 150 个单独选定的工作负载，则系统会提示您先解决现有冲突，然后再保存计划。要解决冲突，请消除冲突的根本原因或从计划中删除受影响的工作负载。有关详细信息，请参阅 "解决监视计划的兼容性问题"(第 983 页)。如果在未解决冲突的情况下保存计划，则会为不兼容的工作负载自动禁用该计划，并显示警报。

如果监视计划应用于 150 多个工作负载或设备组，则会先保存该计划，然后检查兼容性。该计划会针对不兼容的工作负载自动禁用，并会显示警报。

解决监视计划的兼容性问题

根据兼容性问题的原因，可以在创建新监视计划的过程中执行不同的操作来解决兼容性问题。

解决兼容性问题

1. 单击**查看问题**。
2. [可选] 要通过从计划中删除工作负载来解决不兼容操作系统的兼容性问题，请执行以下操作：
   a. 在**不兼容操作系统**选项卡上，选择要删除的工作负载。
   b. 单击**从计划中删除工作负载**。
   c. 单击**删除**，然后单击**关闭**。
3. [可选] 要通过在计划中禁用监视器来解决不兼容操作系统的兼容性问题，请执行以下操作：
   a. 在**不兼容操作系统**选项卡上，选择要删除的监视器。
   b. 单击**禁用监视器**。
   c. 单击**禁用**，然后单击**关闭**。
4. [可选] 要通过从计划中删除工作负载来解决不受支持代理程序的兼容性问题，请执行以下操作：
   a. 在**不支持的代理程序**选项卡上，选择要删除的工作负载。
   b. 单击**从计划中删除工作负载**。
   c. 单击**删除**，然后单击**关闭**。
5. [可选] 要通过更新代理程序版本来解决不受支持代理程序的兼容性问题，请单击**转到代理程序列表**。

   注意
   此选项仅适用于客户管理员。

6. [可选] 要通过从计划中删除工作负载来解决配额不足的兼容性问题，请执行以下操作：
   a. 在**配额不足**选项卡上，选择要删除的工作负载。
   b. 单击**从计划中删除工作负载**。
   c. 单击**删除**，然后单击**关闭**。
7. [可选] 要通过增加租户的配额来解决配额不足的兼容性问题，请执行以下操作：
   a. 在**配额不足**选项卡上，单击**转到管理门户**。
   b. 增加客户的服务配额。

   注意
   此选项仅适用于合作伙伴管理员。

重置机器学习模型

当工作负载的模型由于某种原因而变得过时或无效时，可以重置它们。此操作将删除创建的模型和监视器使用基于异常的监视类型为工作负载收集的数据，然后从头开始训练工作负载的机器学习模型。

重置工作负载的机器学习模型

1. 在 保护 中控台中，转到**设备** > **所有设备**。
2. 单击列表中的工作负载，然后单击**详细信息**选项卡。

3. 在**重置机器学习模型**部分中，单击**重置**。
4. 在确认窗口中，再次单击**重置**。

监视警报

监控警报在 保护 中控台上显示，并在监控的工作负载行为异常时通过电子邮件发送。警报会确保在组织的 IT 环境出现任何问题时，利益相关者能够尽快得到通知。

注意
若要通过电子邮件启用监控警报，您必须为相应的警报类型配置至少一个电子邮件通知策略。有关更多信息，请参见"配置电子邮件通知策略"(第 990 页)。

配置监视警报

当将监视器添加到监视计划时，或当编辑监视计划中已可用的监视器时，可以配置监视器的警报设置。

配置监视警报

1. 在**监视器参数**窗口中，转到**生成警报**部分。
2. 在**警报严重性**中，选择与警报优先级相对应的严重性。

选项	描述
严重	这些警报的优先级最高，涉及对工作负载的运行至关重要的问题。尽快解决这些问题。
错误	错误警报不太严重，指示出现了问题或行为不正常。及时解决这些问题，以防止它们引发更严重的问题。
警告	警告警报指示您应该注意某些情况，但它可能尚未引发问题。在解决引发严重警报和错误警报的问题后，请解决这些问题。 这是默认值。
信息	这些警报的优先级最低。“信息”严重性并不指示存在问题。此类警报提供与受监视对象相关操作的信息。

3. 在**警报频率**中，选择满足条件时系统应生成警报的频率。

选项	描述
一次，直到检查通过	系统将生成一次警报，直到检查成功完成。 这是默认值。
连续 X 次失败后	连续 X 次检查失败后，系统将生成警报，其中 X 是一个整数值。

4. 在**警报消息**中，单击铅笔图标，可编辑系统生成警报时将使用的默认警报消息。可以指定包含变量的自定义警报消息。有关可以使用的变量的详细信息，请参阅 "监视警报变量"(第 986 页)。

注意
可以为某些监视器配置多条警报消息。

5. 如果希望系统在受监视指标恢复正常状态且行为再次正常时自动解决警报，请启用**警报自动解决**。默认情况下，该设置处于启用状态。

监视警报变量

可以为不同的监视器配置不同的警报变量。要使用变量，必须将其括在 {{}} 中。

下表提供了有关可用变量的详细信息。

变量	描述	适用于监视器
plan_name	策略的名称	所有监视器
monitor_name	监视计划中子策略的名称	所有监视器
workload_name	工作负载的名称	所有监视器
threshold_value	生成警报的特定监视条件或阈值	所有支持基于阈值的监视的监控器。
threshold_unit	与阈值关联的单位。例如，%、MB 或 mb/s。	所有支持基于阈值的监视的监控器。
time_period	仅当指标值在指定时间段内超出正常水平时，系统才会为检测到的问题生成警报。	所有支持基于阈值的监视的监控器。
time_unit	将与时间段关联的单位(秒/分钟/小时/天)。	所有支持基于阈值的监视的监控器。
anomaly_value	异常值	所有支持基于异常的监视的监控器。
anomaly_unit	将与异常值关联的单位	所有支持基于异常的监视的监控器。
deviation_value	偏差值	所有支持基于异常的监视的监控器。
deviation_unit	将与偏差值关联的单位	所有支持基于异常的监视的监控器。
drive_name	Windows 的驱动器，或 macOS 的分区	磁盘空间
CPU_model	受监视 CPU 的型号	CPU 温度
GPU_model	受监视 GPU 的型号	GPU 温度
hardware_model	受监视组件的型号	硬件更改

变量	描述	适用于监视器
hardware_component	受监视硬件的类型	硬件更改
hardware_model_old	已替换的受监视组件的型号	硬件更改
hardware_model_new	新增的受监视组件的型号	硬件更改
disk_model	磁盘的型号	磁盘传输速率
network_adapter_model	网络适配器的型号	网络使用率
process_name	进程的名称	CPU 使用率(按进程) 内存使用率(按进程) 磁盘传输速率(按进程) 网络使用率(按进程) 进程状态
service_name	服务的名称	Windows 服务状态
software_name	软件应用程序的名称	安装的软件
software_version	软件应用程序的版本	安装的软件
software_version_old	更新前软件应用程序的版本	安装的软件
software_version_new	新的或更新后软件应用程序的版本	安装的软件
number_of_occurrences	事件出现在日志中的次数	Windows 事件日志
event_types	事件的类型	Windows 事件日志
event_source	事件的来源	Windows 事件日志
event_log_name	事件的名称	Windows 事件日志
firewall_software_name	防火墙软件的名称	防火墙状态
antimalware_software_name	防恶意软件软件的名称	防恶意软件状态
user_name	用户的名称	自动运行功能状态
script_name	脚本的名称	自定义

手动响应操作

当您看到警报时，可以选择要对发出警报的事件执行的响应操作。

执行手动响应操作

1. 在 保护 中控台中，转到**警报**。
2. 打开要查看的警报。
3. 单击**响应操作**，然后从下拉列表中选择一个响应操作。

可用于特定警报的响应操作列表取决于警报类型、特定租户的功能可用性以及工作负载操作系统。

下表列出并描述了所有手动响应操作，以供您参考。

手动响应操作	描述	支持的操作系统
浏览磁盘空间使用趋势	打开一个带有**磁盘空间使用情况**图形的窗口，在其中可以执行以下操作： • 浏览磁盘空间使用情况随时间（过去 1 天/7 天/1 个月）变化的情况。 • 浏览选定时长的磁盘空间使用情况的增量，以相对值 (%) 表示。	Windows、macOS
浏览文件大小增长趋势	打开一个带有**文件大小增长**图形的窗口，在其中可以执行以下操作： • 浏览受监视文件和文件夹的总大小随时间（过去 1 天/7 天/1 个月）变化的情况。 • 浏览选定时长的文件总大小的增量，以相对值 (%) 表示。	Windows、macOS
运行脚本	打开一个窗口，在其中可以执行以下操作： 1. 选择要在工作负载上运行的特定脚本。 2. 指定要在其下执行脚本的帐户。 3. 指定运行的最长持续时间。 4. 指定 PowerShell 执行策略。 5. 运行脚本。 要执行此操作，您需要有工作负载的“Advanced Management”包许可证（如果尚未指派）。	Windows、macOS
通过 NEAR 连接	安克诺斯 Connect Client 建立远程连接。	Windows、macOS
通过 RDP 连接	安克诺斯 Connect Client 建立远程连接。	Windows
打开硬件清查	系统会将您重定向到当前工作负载的**硬件清查**	Windows、

手动响应操作	描述	支持的操作系统
	选项卡。	macOS
浏览已加载 CPU 的前 10 个进程	打开一个窗口，其中显示已加载 CPU 并可能导致其过热的前 10 个进程(警报生成时的系统快照)。	Windows、macOS
浏览已加载 GPU 的前 10 个进程	打开一个窗口，其中显示已加载 GPU 并可能导致其过热的前 10 个进程(警报生成时的系统快照)。	Windows、macOS
浏览已加载内存的前 10 个进程	打开一个窗口，其中显示已加载内存的前 10 个进程(警报生成时的系统快照)。	Windows、macOS
浏览已加载磁盘的前 10 个进程	打开一个窗口，其中显示已加载磁盘的前 10 个进程(警报生成时的系统快照)。	Windows、macOS
浏览已加载网络的前 10 个进程	打开一个窗口，其中显示已加载网络接口适配器的前 10 个进程(警报生成时的系统快照)。	Windows、macOS
按进程浏览资源使用情况	打开一个窗口，其中按相关进程显示有关硬件资源使用情况的详细信息：CPU 使用率、内存使用率、磁盘 I/O、网络使用率。	Windows、macOS
重新启动工作负载	打开一个确认窗口。在确认后，重新启动工作负载。	Windows、macOS
启动 Windows 服务	打开一个确认窗口。在确认后，启动 Windows 服务。	Windows
停止 Windows 服务	打开一个确认窗口。在确认后，停止 Windows 服务。	Windows
停止进程	打开一个确认窗口。在确认后，停止警报所指向的进程。	Windows、macOS
启用 Windows Update	打开一个确认窗口。在确认后，启用 Windows Update。	Windows
禁用可移动驱动器上的“自动运行”功能	打开一个确认窗口。在确认后，在工作负载的系统级别上禁用“自动运行”功能。	Windows

重要事项

出于安全原因，需要使用双重身份验证来执行以下手动响应操作：

- 运行脚本
- 通过 NEAR 连接
- 通过 RDP 连接
- 重新启动工作负载
- 启动 Windows 服务
- 停止 Windows 服务
- 停止进程
- 启用 Windows Update
- 禁用可移动驱动器上的“自动运行”功能

查看工作负载的监控警报

在**警报**选项卡上，您可以查看特定工作负载的监控警报，并执行不同的警报操作。

若要查看工作负载的监控警报

1. 在 保护 中控台中，转到**所有设备**。
2. 点击一个工作负载，然后选择**警报**标签。
3. [可选] 在监控警报窗格中，执行以下操作之一：
   - 若要清除警报，请点击**清除**。
   - 若要进行响应操作，请点击**响应操作**，然后点击该操作。
   - 若要联系支持团队，请点击**获取支持**。
4. [可选] 若要清除所有关于工作负载的监控警报，请点击**全部清除**。

查看监视警报的警报日志

可以按时间顺序查看与监视警报相关的所有事件：执行的响应操作（自动或手动）和发送的电子邮件通知。

查看监视警报的审核日志

1. 在 保护 中控台中，转到**警报**。
2. 打开**表视图**。
3. 在警报列表中，单击要查看的监视警报。
4. 单击**详细信息**，然后单击**警报日志**。

配置电子邮件通知策略

电子邮件通知策略会指定哪些用户将从不同的监视器接收电子邮件通知。

从**电子邮件通知**屏幕，您可以对电子邮件通知策略执行以下操作：添加，编辑，启用，禁用和删除。

添加

添加新的电子邮件通知策略

1. 在保护中控台中，转到**设置** > **电子邮件通知**。
2. 点击**添加策略**。
3. 点击**选择收件人**。
4. 在**选择接收者**屏幕中，选择您希望接收电子邮件警报的用户，然后点击**选择**。
5. 在**警报类型**中，选择您希望系统发送电子邮件警报的监视器。
6. 单击**添加**。

编辑

若要编辑电子邮件通知策略

1. 在保护中控台中，转到**设置** > **电子邮件通知**。
2. 点击通知策略的省略号图标，然后点击**编辑**。
3. [可选] 若要更改收件人，请点击**编辑收件人**，在列表中添加或删除用户，然后点击**选择**。
4. [可选] 在**警报类型**中，选择您希望发送给选定收件人的监控警报类型。
5. 单击**保存**。

启用

若要启用电子邮件通知策略

1. 在保护中控台中，转到**设置** > **电子邮件通知**。
2. 在**电子邮件通知**屏幕上，点击电子邮件通知策略的**...**图标。
3. 单击**启用**。

禁用

若要禁用电子邮件通知策略

1. 在保护中控台中，转到**设置** > **电子邮件通知**。
2. 在**电子邮件通知**屏幕上，点击电子邮件通知策略的**...**图标。
3. 单击**禁用**。

删除

删除电子邮件通知策略

1. 在保护中控台中，转到**设置** > **电子邮件通知**。
2. 在**电子邮件通知**屏幕上，点击电子邮件通知策略的**...**图标。
3. 点击**删除**，然后点击**确认**。

查看监控数据

对于每个工作负载，您可以查看已应用监视器的列表、监视器的当前状态，以及图形视图中的历史性能详细信息。您可以使用此信息来分析工作量的状态以及其状态如何随时间变化。

先决条件

- 监视计划已应用于工作负载。
- 工作负载处于联机状态，并有相应监视器的数据。
- 工作负载上安装的相应版本的代理程序支持监视计划。

查看应用于工作负载的监视器和监视器数据

1. 在 保护 中控台中，转到**设备** > **所有设备**。
2. 单击一个工作负载，然后单击**监视**选项卡。

   对于为工作负载启用的每个监视器，**监视**选项卡会显示一个小组件。每个小组件都会显示以下信息。

显示的信息	描述
监视器名称	监视器名称
上次结果	受监视指标的最新值或事件的最新状态
上次检查	监视器上次收集数据的日期和时间
警告	由监控器生成并仍未解决的警报数量。 如果此监视器生成了至少一个未解决的警报，点击该数字将打开**警报**标签页。警报将被过滤，只列出此监视器的警报。

   注意
   在将监视计划应用于工作负载后，这些小组件可在选项卡上显示 15 分钟(或为监视器设置的最低监视频率)。

3. [可选] 要查看有关监视器的更多详细信息，以及为受监视指标收集的历史数据(如果适用)，请在监视器的小组件中，单击省略号图标，然后单击**详细信息**。

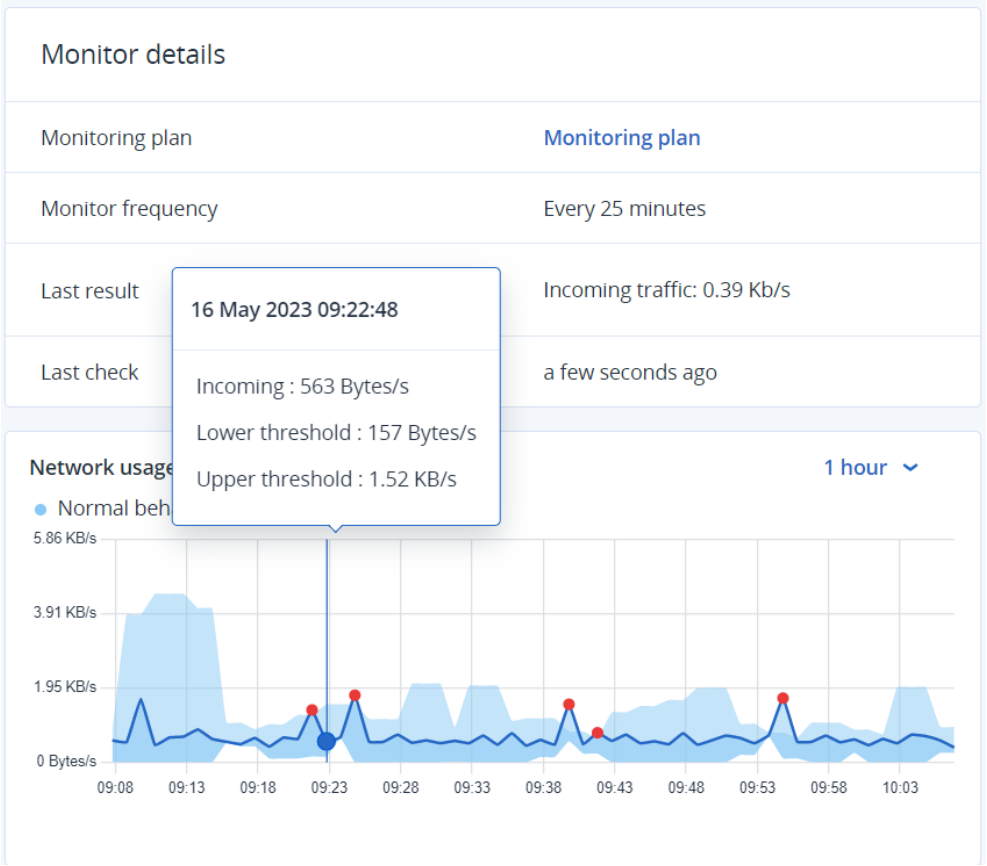
   有关可以在小组件中查看的监视器详细信息的更多信息，请参阅 "监视器小组件"(第 992 页)。

监视器小组件

在监视器小组件中，可以查看有关监视器的以下详细信息。

详细信息	描述
监视	包含监视器的监视计划的名称。监视计划的名称是一个将在视图模式下打开监视计划的链接。

详细信息	描述
计划	
监视频率	监视器从工作负载收集数据的时间间隔
上次结果	受监视指标的最新值或事件的最新状态
上次检查	监视器上次收集数据的日期和时间
上次警报	上次生成警报的日期和时间。仅当至少已为监视器生成一个警报时，才会显示该字段。
历史图表	对于收集时间序列数据的监视器，小组件以图形视图显示所选时段(1 小时、6 小时、12 小时、1 天、1 周或 1 个月)的历史数据。 该图形会显示指标在选定时段内的实际值。如果由于某种原因，代理程序没有将收集到的数据发送到云，则丢失值会显示为虚线，该虚线将数据点与丢失值之前和之后的实际值连接起来。 对于正在使用**基于异常的**监视的监视器，该图形会显示基线区域、显示指标实际值的线以及异常。异常是指超出基线的峰值或值，并会在图形上显示为红点。 如果将鼠标光标悬停在图形上，则可以查看特定时间的实际值和阈值。

详细信息	描述
	 **注意** 图形上的数据会以本地系统的时区显示。这是您访问 保护 中控台的工作负载的浏览器的时区。

其他 Cyber Protection 工具

合规模式

合规模式是专为有更高安全要求的客户端而设计的。此模式对所有备份要求强制加密，仅允许本地设置加密密码。

在合规模式下，在客户租户中创建的所有备份及其单位都会自动使用 AES 算法和 256 位密钥进行加密。用户只能在受保护的设备上设置加密密码，不能在保护计划中设置加密密码。

重要事项
无法禁用合规模式。

限制

- 合规模式仅与 15.0.26390 或更高版本的代理程序兼容。
- 合规模式不适用于运行 Red Hat Enterprise Linux 4.x 或 5.x 及其衍生产品的设备。
- 云服务不能访问加密密码。由于此限制，在合规模式下，某些功能不适用于租户。

不支持的功能

在合规模式下，以下功能不适用于租户：

- 通过 Cyber Protect 中控台恢复
- 通过 Cyber Protect 中控台在文件级别上浏览备份
- 云到云备份
- 网站备份
- 应用程序备份
- 移动设备的备份
- 备份的反恶意软件扫描
- 安全恢复
- 公司白名单的自动创建
- 数据保护地图
- 灾难恢复
- 与不可用功能相关的报告和仪表板

设置加密密码

必须在受保护的设备上本地设置加密密码。不能在保护计划中设置加密密码。若没有密码，创建备份将失败。

警告！
如果您丢失或忘记密码，则无法恢复加密备份。

可以通过以下方式设置加密密码：

1. 在安装保护代理程序期间（适用于 Windows、macOS 和 Linux）。
2. 通过使用命令行（适用于 Windows 和 Linux）。
   这是在虚拟设备上设置加密密码的唯一方法。
   有关如何使用 **Acropsh** 工具设置加密密码的详细信息，请参阅 "加密"（第 391 页）。
3. 在 Cyber Protect Monitor 中（适用于 Windows 和 macOS）。

在 Cyber Protect Monitor 中设置加密密码

1. 以管理员身份登录受保护的设备。
2. 单击通知区域（在 Windows 中）或菜单栏（在 macOS 中）中的 Cyber Protect Monitor 图标。
3. 单击齿轮图标。
4. 单击**加密**。
5. 设置加密密码。
6. 单击**确定**。

更改加密密码

在保护计划创建任何备份之前，可更改加密密码。

不建议您在创建备份后更改加密密码，因为后续备份会失败。要继续保护同一台计算机，必须为其创建新的保护计划。更改加密密码和保护计划将导致创建使用已更改密码加密的新备份。在这些更改之前创建的备份将不受影响。

或者，可以保留已应用的保护计划，仅更改其中的备份文件名。这还会导致创建使用已更改密码加密的新备份。若要了解有关备份文件名的更多信息，请参考 "备份文件名"（第 400 页）。

可以通过以下方式更改加密密码：

1. 在 Cyber Protect Monitor 中（适用于 Windows 和 macOS）。
2. 通过使用命令行（适用于 Windows 和 Linux）。
   有关如何使用 **Acropsh** 工具设置加密密码的详细信息，请参阅 "加密"（第 391 页）。

在合规模式下恢复租户的备份

在合规模式下，无法在 Cyber Protect 中控台中恢复备份。

可使用以下选项：

- 使用可启动媒体恢复整台计算机、磁盘或文件。
- 使用 Windows 文件浏览器，从安装了代理程序的 Windows 计算机的本地备份中提取文件。

不可变存储

不可变存储是一种数据存储类型，可防止文件在一段时间内被更改、修改或删除。它可确保数据保持安全和防篡改，提供了一层额外的保护，可防止未经授权或无意中的修改或勒索软件攻击。

通过使用不可变存储，可以在指定的保留期内访问已删除的备份。可以从这些备份中恢复内容，但不能更改、移动或删除这些备份。在保留期结束后，将永久删除已删除的备份。

不可变存储包含以下备份：

- 手动删除的备份。
- 根据保护计划中**保留时间**部分或清理计划中**保留规则**部分中的设置自动删除的备份。

不可变存储中已删除的备份仍会使用存储空间并收取相应费用。

已删除的租户无需支付任何存储费用，包括不可变存储。

不可变存储模式

对于客户租户，不可变存储在以下模式下可用：

不可变存储在以下模式下可用：

- **监管模式**
  您可以禁用并重新启用不可变存储。您可以更改保留期限或切换到合规性模式。
- **合规模式**

  警告！
  选择合规模式是不可逆的。

  您无法禁用不可变存储。您无法更改保留期限，也无法切换回监管模式。

支持的存储和代理程序

- 仅云存储支持不可变存储。
  - 不可变存储适用于使用 安克诺斯 Cyber Infrastructure 4.7.1 或更高版本的 Acronis 托管和合作伙伴托管云存储。
  - 所有具有 安克诺斯 Cyber Infrastructure Backup 网关的存储均受支持。例如，安克诺斯 Cyber Infrastructure 存储、Amazon S3 和 EC2 存储以及 Microsoft Azure 存储。
  - 不可变存储要求在 安克诺斯 Cyber Infrastructure 中为备份网关服务打开 TCP 端口 40440。在版本 4.7.1 及更高版本中，使用**备份 (ABGW) 公共**流量类型自动打开 TCP 端口 40440。有关流量类型的详细信息，请参阅Acronis Cyber Infrastructure 文档。
- 不可变存储需要版本为 21.12(内部版本 15.0.28532) 或更高版本的保护代理程序。
- 仅支持 TIBX(版本 12) 备份。

启用不可变存储

可以在 Cyber Protect 中控台或管理门户中，配置不可变存储设置。它们均会提供对相同设置的访问。以下过程使用 Cyber Protect 中控台。若要了解如何在管理门户中配置不可变存储设置，请参阅管理员指南中的配置不可变存储。

启用不可变存储

1. 以管理员身份登录到 Cyber Protect 中控台。
2. 转至**设置>系统设置**。
3. 在默认备份选项列表中滚动，然后单击**不可变存储**。
4. 启用**不可变存储**开关。
5. 指定介于 14 到 3650 天之间的保留期。
   默认的保留期为 14 天。较长的保留期会导致存储使用量增加。
6. 选择不可变存储模式，然后根据提示确认您的选择。
   在监管模式下，可以启用或禁用不可变存储，并更改保留期限。可以从监管模式切换到合规模式。

   警告！
   切换到合规模式是不可逆的。选择合规性模式后，将无法禁用不可变存储，也无法更改其模式或保留期。

7. 单击**保存**。
8. 要使现有存档能够支持不可变存储，请在该存档中创建一个新备份。
   要创建新备份，请手动或按预定运行保护计划。

   警告！
   如果在使存档能够支持不可变存储之前删除备份，则将永久删除该备份。

禁用不可变存储

注意
只能在监管模式下禁用不可变存储。

禁用不可变存储

1. 以管理员身份登录到 Cyber Protect 中控台。
2. 在导航菜单中，依次单击**设置** > **系统设置**。
3. 在默认备份选项列表中滚动，然后单击**不可变存储**。
4. 禁用**不可变存储**开关。
5. 单击**禁用**来确认选择。

警告！
禁用不可变存储不会立即生效。在 14 天的宽限期内，不可变存储仍处于活动状态，可以根据其原始保留期访问已删除的备份。在宽限期结束后，将永久删除不可变存储中的所有备份。

访问不可变存储中已删除的备份

在保留期内，可以访问已删除的备份并从中恢复数据。

注意
为了允许访问已删除的备份，应该启用备份存储上的 40440 端口以接收传入的连接。

访问已删除的备份

1. 在**备份存储**选项卡上，选择包含已删除备份的云存储。
2. [仅适用于已删除的存档] 若要查看已删除的存档，请单击**显示已删除**。
3. 选择包含要恢复备份的存档。
4. 单击**显示备份**，然后单击**显示已删除的备份**。
5. 选择要恢复的备份。
6. 继续执行恢复操作，如 "恢复"(第 443 页) 中所述。

地理冗余存储

地理冗余存储通过将数据异步复制到地理上远离主要位置的辅助位置，来确保数据持久性。通过使用地理冗余，即使主要位置不可用，仍可以访问您的数据。

重要事项
复制的数据占用与原始数据相同的存储空间。

启用和禁用地理冗余存储

先决条件

- 仅在合作伙伴管理员在管理门户或通过 API 启用后，才能在 Cyber Protect 中控台中使用地理冗余存储。
- 只有管理员才能启用或禁用 Cyber Protect 中控台中的地理冗余存储。请确保您有管理员权限。

启用地理冗余存储

1. [仅当地理冗余存储已通过 API 启用时] 在顶部的警报“地理冗余可用于您云中的所有数据”中，单击**启用 Geo-redundant Cloud Storage**。
2. 在 Cyber Protect 中控台中，转到**设置** > **系统设置**。
3. 在默认备份选项列表中滚动，然后单击 **Geo-redundant Cloud Storage**。
4. 启用 **Geo-redundant Cloud Storage** 开关。
5. 单击**保存**。
   现在，您的数据即会复制到辅助位置，并将保持可用(即使主要位置出现故障也是如此)。

禁用地理冗余存储

警告！
复制的数据会在禁用地理冗余后一天内删除。

1. 在 Cyber Protect 中控台中，转到**设置** > **系统设置**。
2. 在备份选项列表中滚动，然后单击 **Geo-redundant Cloud Storage**。
3. 禁用 **Geo-redundant Cloud Storage** 开关。
4. 通过键入**禁用**来确认您的选择，然后单击**禁用**。

地理复制状态

地域冗余意味着数据会复制到辅助位置。地理复制状态显示此过程的各个阶段。可能出现以下状态：

- **已同步** - 数据已复制到辅助位置。
- **正在同步** - 数据正在复制到辅助位置。此操作的持续时间取决于数据的大小。
- **挂起** - 数据复制已暂时暂停。
- **已禁用** - 数据复制已禁用。

在 Cyber Protect 中控台中检查复制状态

1. 在 Cyber Protect 中控台中，转到**备份存储**。
2. 选择位置和备份集。
3. 单击**详细信息**，然后检查**地理复制状态**中的状态。

限制

- 当前，复制数据的辅助位置仅在美国、德国和加拿大可用。
- 有关使用地理冗余时灾难恢复服务限制的信息，请参阅灾难恢复文档。

意识度仪表板

如果服务提供商已启用“安全意识培训”服务，则可使用此仪表板。

对于具有以下角色的用户，仪表板可在“客户”级别访问：合作伙伴管理员、客户管理员、保护管理员或网络安全管理员。

仪表板提供组织中安全意识培训进度的概览，并用作导航到 Wizer 中的安全意识培训管理中控台的网关。

运营“安全意识培训”服务

若要管理组织可用的用户和培训内容，请单击意识度 仪表板左上角的 **管理中控台**。将打开 Wizer 管理员中控台。

有关详细说明，请参阅 Wizer 文档。

站点到站点 Open VPN - 附加信息

创建恢复服务器时，请配置其**生产网络中的 IP 地址**及其**测试 IP 地址**。

在执行故障转移(即在云端运行虚拟机)并登录到虚拟机以检查服务器的 IP 地址后，您会看到**生产网络中的 IP 地址**。

在执行测试故障转移时，只能使用**测试 IP 地址**访问测试服务器，该地址仅在恢复服务器的配置中可见。

要从本地站点访问测试服务器，必须使用**测试 IP 地址**。

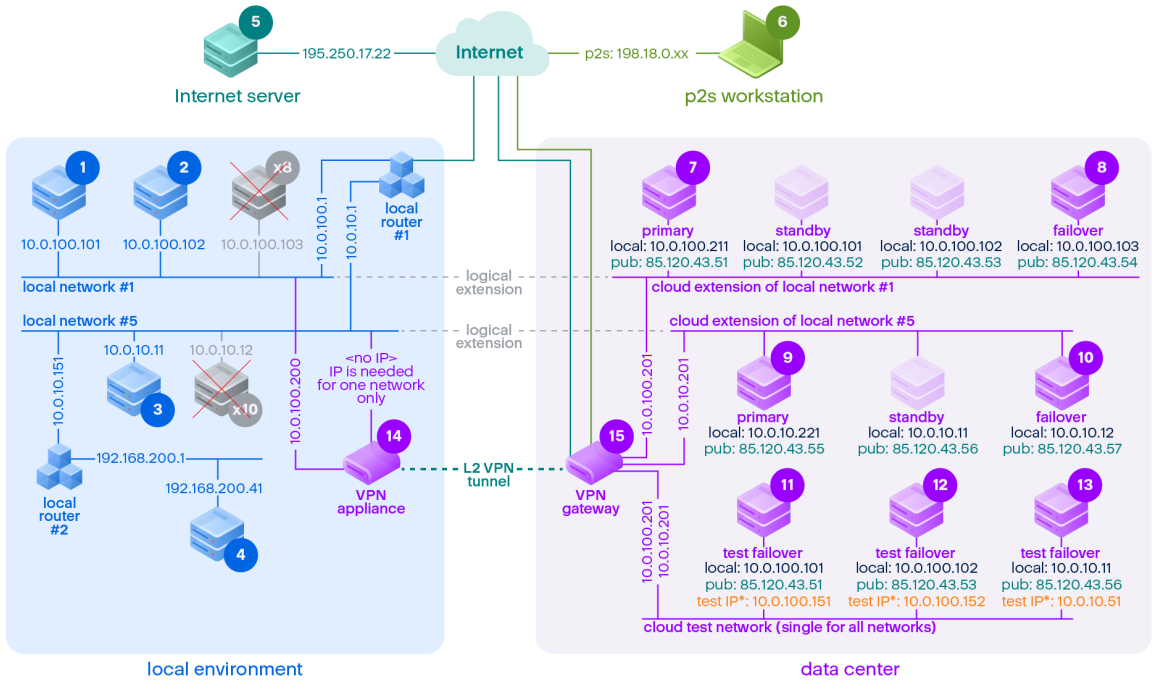
注意

该服务器的网络配置始终会显示**生产网络中的 IP 地址**(因为测试服务器会镜像生产服务器的配置)。出现这种情况是因为测试 IP 地址不属于测试服务器，而是属于 VPN 网关，并使用 NAT 转换为生产 IP 地址。

下图显示了站点到站点 Open VPN 配置的示例。本地环境中的一些服务器使用故障转移恢复到云端(尽管网络基础架构正常)。

1. 客户通过以下方式启用灾难恢复：
   a. 配置 VPN 设备 (14)，并将其连接到专用云 VPN 服务器 (15)
   b. 使用灾难恢复保护一些本地服务器(1、2、3、x8 和 x10)

      本地站点上的一些服务器(如 4)连接到并未连接到 VPN 设备的网络。此类服务器不受灾难恢复保护。
2. 部分服务器(已连接到不同网络)在本地站点中工作：(1、2、3 和 4)
3. 受保护的服务器(1、2 和 3)正在通过测试故障转移(11、12 和 13)进行测试
4. 本地站点中的某些服务器不可用(x8、x10)。执行故障转移后，它们在云端会变为可用(8 和 10)
5. 一些已连接到不同网络的主服务器(7 和 9)在云环境中可用
6. (5)是 Internet 中的服务器，具有公共 IP 地址
7. (6)是使用点到站点 VPN 连接 (p2s) 连接到云的工作站



在此示例中，从**从：**行中的服务器到**至：**列中的服务器，以下连接设置可用（例如，“ping”）。

	至：	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
从：		本地	本地	本地	本地	Internet	p2s	主要	故障转移	主要	故障转移	测试故障转移	测试故障转移	测试故障转移	VPN 设备	VPN 服务器
1	本地		直接	通过本	通过本	通过本地路由器 1 和	否	通过隧道：本地	通过隧道：本地	通过隧道：本地	通过隧道：本地	通过隧道：NAT（VPN 服	通过隧道：NAT（VPN 服	通过本地路由器 1 和隧	直接	否

	至：	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				地路由器 1	地路由器 2	Internet		通过本地路由器 1 和 Internet：公共	通过本地路由器 1 和 Internet：公共	通过本地路由器 1 和 Internet：公共	通过本地路由器 1 和 Internet：公共	务器） 通过本地路由器 1 和 Internet：公共	务器） 通过本地路由器 1 和 Internet：公共	道：NAT（VPN 服务器） 通过本地路由器 1 和 Internet：公共		
2	本地	直接		通过本地路由器 1	通过本地路由器 2	通过本地路由器 1 和 Internet	否	通过隧道：本地 通过本地路由器 1 和 Internet：公共	通过隧道：本地 通过本地路由器 1 和 Internet：公共	通过隧道：本地 通过本地路由器 1 和 Internet：公共	通过隧道：本地 通过本地路由器 1 和 Internet：公共	通过隧道：NAT（VPN 服务器） 通过本地路由器 1 和 Internet：公共	通过隧道：NAT（VPN 服务器） 通过本地路由器 1 和 Internet：公共	通过本地路由器 1 和隧道：NAT（VPN 服务器） 通过本地路由器 1 和 Internet：公共	直接	否
3	本地	通过本地路由器	通过本地路由器		通过本地路由器	通过本地路由器 1 和 Internet	否	通过隧道：本地 通过本地路由器 1 和 Internet：	通过隧道：本地 通过本地路由器 1 和 Internet：	通过隧道：本地 通过本地路由器 1 和 Internet：	通过隧道：本地 通过本地路由器 1 和 Internet：	通过隧道：NAT（VPN 服务器） 通过本地路由器 1	通过隧道：NAT（VPN 服务器） 通过本地路由器 1	通过本地路由器 1 和隧道：NAT（VPN 服务器）	通过本地路由器	否

	至：	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		1	1		2			公共	公共	公共	公共	和 Internet：公共	和 Internet：公共	通过本地路由器 1 和 Internet：公共		
4	本地	通过本地路由器 2 和路由器 1	通过本地路由器 2 和路由器 1	通过本地路由器 2		通过本地路由器 2、路由器 1 和 Internet	否	通过本地路由器 2 和隧道：本地 通过本地路由器 2、本地路由器 1 和 Internet：公共	通过本地路由器 2 和隧道：本地 通过本地路由器 2、本地路由器 1 和 Internet：公共	通过本地路由器 2 和隧道：本地 通过本地路由器 2、本地路由器 1 和 Internet：公共	通过本地路由器 2 和隧道：本地 通过本地路由器 2、本地路由器 1 和 Internet：公共	通过隧道：NAT（VPN 服务器） 通过本地路由器 2、路由器 1 和 Internet：公共	通过隧道：NAT（VPN 服务器） 通过本地路由器 2、路由器 1 和 Internet：公共	通过隧道：NAT（VPN 服务器） 通过本地路由器 2、路由器 1 和 Internet：公共	通过本地路由器 2	否
5	Internet	否	否	否	否		不适用	通过 Internet：公共	通过 Internet：公共	通过 Internet：公共	通过 Internet：公共	通过 Internet：公共	通过 Internet：公共	通过 Internet：公共	否	否
6	p2s	否	否	否	否	通过 Internet		通过 p2s VPN（VPN 服务器）：本地	通过 p2s VPN（VPN 服务器）：本地	通过 p2s VPN（VPN 服务器）：本地	通过 p2s VPN（VPN 服务器）：本地	通过 p2s VPN - NAT（VPN 服务器）	通过 p2s VPN - NAT（VPN 服务器）	通过 p2s VPN - NAT（VPN 服务器）	否	否

	至：	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								通过 Internet：公共	通过 Internet：公共	通过 Internet：公共	通过 Internet：公共	通过 Internet：公共	通过 Internet：公共	通过 Internet：公共		
7	主要	通过隧道	通过隧道	通过隧道和本地路由器 1	通过隧道和本地路由器 1 及 2	通过 Internet（通过 VPN 服务器）	否		直接在云端：本地	通过隧道和本地路由器 1：本地	通过隧道和本地路由器 1：本地	通过 VPN 服务器：NAT	通过 VPN 服务器：NAT	通过隧道和本地路由器 1：NAT	否	仅 DHCP 和 DNS 协议
8	故障转移	通过隧道	通过隧道	通过隧道和本地路由器 1	通过隧道和本地路由器 1	通过 Internet（通过 VPN 服务器）	否	直接在云端：本地		通过隧道和本地路由器 1：本地	通过隧道和本地路由器 1：本地	通过 VPN 服务器：NAT	通过 VPN 服务器：NAT	通过隧道和本地路由器 1：NAT	否	仅 DHCP 和 DNS 协议

	至：	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
					及 2											
9	主要	通过隧道和本地路由器 1	通过隧道和本地路由器 1	通过隧道	通过隧道	通过 Internet (通过 VPN 服务器)	否	通过隧道和本地路由器 1：本地	通过隧道和本地路由器 1：本地		直接在云端：本地	通过隧道和本地路由器 1：NAT	通过隧道和本地路由器 1：NAT	通过 VPN 服务器：NAT	否	仅 DHCP 和 DNS 协议
10	故障转移	通过隧道和本地路由器 1	通过隧道和本地路由器 1	通过隧道	通过隧道	通过 Internet (通过 VPN 服务器)	否	通过隧道和本地路由器 1：本地	通过隧道和本地路由器 1：本地	直接在云端：本地		通过隧道和本地路由器 1：NAT	通过隧道和本地路由器 1：NAT	通过 VPN 服务器：NAT	否	仅 DHCP 和 DNS 协议
11	测试故障转移	否	否	否	否	通过 Internet	否	否	否	否	否		直接在云端：本地	通过 VPN 服务器：	否	仅 DHCP

	至：	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						(通过 VPN 服务器)								本地(路由)		和 DNS 协议
12	测试故障转移	否	否	否	否	通过 Internet (通过 VPN 服务器)	否	否	否	否	否	直接在云端：本地		通过 VPN 服务器：本地(路由)	否	仅 DHCP 和 DNS 协议
13	测试故障转移	否	否	否	否	通过 Internet (通过 VPN 服务器)	否	否	否	否	否	通过 VPN 服务器：本地(路由)	通过 VPN 服务器：本地(路由)		否	仅 DHCP 和 DNS 协议
14	VPN 设备	直接	直接	通过本地路由器 1	通过本地路由器 2	通过 Internet (本地路由器 1)	否	否	否	否	否	否	否	否		否
15	VPN 服务器	否	否	否	否	否	否	否	否	否	否	否	否	否	否	

词汇表

R

Runbook

[灾难恢复] 计划方案，包含自动执行灾难恢复操作的可配置步骤。

U

USB 设备数据库

[设备控制] 设备控制模块维护一个 USB 设备数据库，从中可以将设备添加到设备访问控制的排除列表中。数据库按设备 ID 注册 USB 设备，该 ID 可以在 Cyber Protect 中控台中手动输入或从已知设备中选择。

V

VPN 设备

[灾难恢复] 一种特殊虚拟机，支持通过安全的 VPN 隧道在本地网络和云站点之间建立连接。VPN 设备部署在本地站点上。

VPN 网关（以前称为“VPN 服务器”或“连接网关”）

[灾难恢复] 一种特殊虚拟机，通过安全的 VPN 隧道在本地站点和云站点网络之间提供连接。VPN 网关部署在云站点上。

保

保护代理程序

保护代理程序是要安装在用于数据保护的计算机上的代理程序。

保护计划

保护计划是结合了数据保护模块的计划，其中包括备份、防病毒和反恶意软件保护、URL 过滤、Windows Defender Antivirus、Microsoft Security Essentials、漏洞评估、修补程序管理、数据保护地图和设备控制。

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中所选日创建的第一个备份（单击齿轮图标，然后依次单击备份选项 > 每周备份）。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。

本

本地站点

[灾难恢复] 部署在贵公司本地的本地基础架构。

测

测试 IP 地址

[灾难恢复] 在测试故障转移时所需的 IP 地址，以防止与生产 IP 地址重复。

测试网络

[灾难恢复] 隔离的虚拟网络，用于测试故障转移过程。

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

一种备份格式，初始完整和后续增量备份使用该格式保存到单个 .tibx 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时，单文件备份格式不可用。

点

点到站点 (P2S) 连接

[灾难恢复] 从外部使用端点设备（如计算机或笔记本电脑）与云站点和本地站点进行安全的 VPN 连接。

公

公共 IP 地址

[灾难恢复] 使云服务器可通过 Internet 进行访问所需的 IP 地址。

孤

孤立的备份

孤立的备份是一个不再与保护计划关联的备份。

故

故障恢复

将工作负载从备用服务器（如虚拟机副本或云中运行的恢复服务器）切换回生产服务器。

故障转移

将工作负载从生产服务器切换到备用服务器（如虚拟机副本或云中运行的恢复服务器）。

恢

恢复点目标 (RPO)

[灾难恢复] 因中断而丢失的数据量，以计划中断或灾难事件的时间量形式测量。RPO 阈值定义故障转移的上一个合适恢复点与当前时间之间允许的最大时间间隔。

恢复服务器

[灾难恢复] 原始计算机的 VM 副本，基于存储在云中受保护的服务器备份。恢复服务器用于在发生灾难时切换原始服务器的工作负载。

模

模块

模块是保护计划的一部分，提供特定数据保护功能，例如备份模块、防病毒和反恶意软件保护模块等等。

设

设备控制模块

作为保护计划的一部分，设备控制模块利用每台受保护计算机上的数据丢失保护代理程序的功能子集，来检测和防止通过本地计算机通道对数据进行未经授权的访问和传输。这包括用户访问外围设备和端口、文档打印、剪贴板复制/粘贴操作、媒体格式和弹出操作，以及与本地连接的移动设备的同步。设备控制模块提供

对以下对象的精细化相关控制:受保护计算机上允许用户访问的设备类型和端口,以及用户可以在这些设备上执行的操作。

生

生产网络

[灾难恢复] 内部网络通过 VPN 隧道扩展,从而覆盖本地站点和云站点。本地服务器和云服务器可以在生产网络中相互通信。

数

数据丢失预防(以前称为数据泄漏预防)

集成技术和公司措施系统,旨在检测和预防意外的或有意的泄漏/公司内外未经授权的实体访问机密、受保护或敏感数据,或将此类数据传输给不受信任的环境。

数据丢失预防代理程序

通过应用上下文和内容分析技术的组合,并强制集中管理数据丢失预防策略,数据丢失预防系统的客户端组件保护其主机计算机避免未授权使用、传输和存储机密、受保护或敏感数据。Cyber Protection 提供全功能的数据丢失预防代理程序。但是,受保护计算机上的代理程序功能受限于可用于 Cyber Protection 中的许可的数据丢失预防功能集,并取决于应用于该计算机的保护计算。

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。

物

物理机

由操作系统中安装的代理程序备份的计算机。

虚

虚拟机

由外部代理程序(例如适用于 VMware 的代理程序或适用于 Hyper-V 的代理程序)按虚拟机监控程序级备份的虚拟机。从备份的角度来看,内部附带代理程序的虚拟机视为物理机。

验

验证

检查从备份恢复数据的可能性的操作。文件备份的验证会启动所有文件的恢复(从备份至虚拟目标位置)。对磁盘备份进行验证时,会对保存在备份中的每一个数据块的校验和进行计算。这两个过程都会占用较多资源。虽然验证成功意味着成功恢复的可能性极高,但验证操作并不会检查影响恢复过程的所有因素。

云

云服务器

[灾难恢复] 恢复或主服务器的常规参考资料。

云站点(或 DR 站点)

[灾难恢复] 远程站点,托管在云中并用于运行恢复基础架构,以防发生灾难。

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。

站

站点到站点 (S2S) 连接

[灾难恢复] 通过安全的 VPN 隧道将本地网络扩展到云的连接。

主

主服务器

[灾难恢复]在本地站点(如恢复服务器)上没有链接计算机的虚拟机。主服务器用于保护应用程序或运行各种辅助服务(如 Web 服务器)。

最

最终确定

该操作使从备份运行的临时虚拟机成为永久虚拟机。从根本上讲,这意味着将所有虚拟机磁盘以及在计算机运行期间发生的更改恢复到存储这些更改的数据存储中。

索引

F

G

H

I

L

M

N

O

按

白

保

报

备

本

比

编

变

标

捕

不

步

部

参

操

测

策

查

活

获

基

激

计

加

监

检

建

将

脚

节

解

进

禁

警

静

旧

聚

卷

开

可

密

描

敏

命

默

哪

内

您

排

配

评

其

启

轻

清

取

权

筛

删

上

设

什

生

声

失

实

使

示

事

是

适

收

手

受

我

无

物

系

下

先

显

现

限

压

验

要

移

疑

已

以

易

意

隐

应

战

站

正

支

执

阻

组

最